Study Planner

Review Exercises

Official Cert Guide

Advance your IT career with hands-on learning

CCNP Security Virtual Private Networks

SVPN 300-730

JOSEPH MUNIZ
JAMES RISLER
STEVEN CHIMES

ciscopress.com

CCNP Security Virtual Private Networks SVPN 300-730 Official Cert Guide

Joseph Muniz, Steven Chimes, CCIE No. 35525, James Risler

CCNP Security Virtual Private Networks SVPN 300-730 Official Cert Guide

Joseph Muniz, Steven Chimes, CCIE No. 35525, James Risler

Cisco Press

CCNP Security Virtual Private Networks SVPN 300-730 Official Cert Guide

Joseph Muniz, Steven Chimes, James Risler

Published by:
Cisco Press

`ScoutAutomatedPrintCode`

Library of Congress Control Number: 2021946078

ISBN-13: 978-0-13-666060-6
ISBN-10: 0-13-666060-6

Warning and Disclaimer

This book is designed to provide information about the CCNP Security VPN (SVPN) Implementation 300-730 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.

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.

Special Sales

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact intlcs@pearson.com.

Feedback Information

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

expertise of members from the professional technical community.

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

We greatly appreciate your assistance.

Editor-in-Chief
Mark Taub

Alliances Manager, Cisco Press
Arezou Gol

Director, ITP Product Management
Brett Bartow

Executive Editor
James Manly

Managing Editor
Sandra Schroeder

Development Editor
Ellie Bru

Senior Project Editor
Tonya Simpson

Credit Editor
Kitty Wilson

Technical Editor(s)
Viktor Bobrov, Joseph Mlodzianowksi

Editorial Assistant
Cindy Teeters

Cover Designer
Chuti Prasertsith

Composition

Indexer

Proofreader

About the Author(s)

Joseph Muniz is an architect and security researcher in the Cisco Security Sales and Engineering organization. He is driven by making the world a safer place through education and adversary research. Joseph has extensive experience in designing security solutions and architectures as a trusted advisor for top Fortune 500 corporations and the U.S. government.

Joseph is a researcher and industry thought leader. He speaks regularly at international conferences, writes for technical magazines, and is involved with developing training for various industry certifications. He invented the fictitious character Emily Williams to create awareness around social engineering. Joseph runs The Security Blogger website, a popular resource for security and product implementation. He is the author of and contributor to several publications, including titles ranging from security best practices to exploitation tactics.

When Joseph is not using technology, you can find him on the futbal (soccer) field or raising the next generation of hackers, also known as his children. Follow Joseph at https://www.thesecurityblogger.com and @SecureBlogger.

Steven Chimes, CCIE No. 35525, is a security architect in the Security Sales Engineering organization at Cisco, focused on building cybersecurity solutions for Cisco's largest global customers. He has more than 15 years of experience in the networking and cybersecurity fields, specializing in cross-domain solutions and emerging technologies. He has led the technical design for projects across the IT spectrum, including networking, security, analytics, identity, collaboration, compute, data center, and cloud.

When not building solutions, Steven is either teaching or learning. He is a distinguished speaker at Cisco Live and has spoken at Cisco Live events all over the world. He is also a serial collector of certifications, including CCIE Security, CCNP Enterprise, DevNet Associate, CISSP-ISSAP, GMON, and GCIH, among many others. What Steven finds most fulfilling, though, is

mentoring the next generation of inspired cybersecurity professionals through programs such as Cisco High. Follow Steven @StevenChimes on Twitter.

James Risler is a security training development manager in the Cisco Customer Experience organization. As senior manager of security content engineering at Cisco, he's constantly discovering and exploring the latest trends and issues in security, IT, and business. In his current role, he oversees teams responsible for both security and collaboration course development.

James is passionate about helping organizations understand the impact that security events can have on business and how to mitigate that risk. That's why he works to educate individuals and organizations in a variety of cybersecurity topics, including threat defense, virtual private networks, and firewall configuration, among others. Besides his work at Cisco, James works to help create the next generation of security defenders by holding training sessions and presentations for the University of Tampa Cybersecurity Club.

James is a distinguished speaker at Cisco Live; he holds Certified Information Systems Security Professional (CISSP) and Cisco Certified Internetwork Expert (CCIE) certifications; and he has earned a master's of business administration (MBA) from the University of Tampa. When he is not at work, he is either homebrewing or cooking up a complex meal. Follow James @JimRisler on Twitter.

About the Technical Reviewers

Viktor Bobrov, CCIE No 31489, is a security technical leader on the Customer Experience team at Cisco. He joined Cisco nine years ago and has worked on many large-scale security projects across many industries.

Viktor focuses on Cisco ISE, network segmentation, Cisco ASA, and Cisco AnyConnect technologies. He is also well versed in other security technologies, including Cisco Security Manager (CSM), DMVPN, and GETVPN.

Prior to joining Cisco, Viktor worked at a global advertising company as a global network architect, leading a team of network engineers to manage a network of 1000+ locations.

Aside from Cisco technologies, Viktor is also well versed in Microsoft Active Directory, public key infrastructure (PKI), mobile device management (MDM), and load balancers.

Viktor is a dual CCIE No. 31489 (Enterprise Infrastructure and Security).

Joseph Mlodzianowski is a highly respected member of the cybersecurity community, with more than 25 years in the industry. Joseph spent 8 years working for the Department of Defense and has multiple industry certifications, including CISSP, CCIE, CNE, ACMA, ITIL, and CERT, and he is a member of industry groups such as CyManII, M3aawg, and others.

Joseph is a hacker, instructor, author, and researcher, and he has worked with law enforcement on some of the largest botnet cases, including several industrial control system threats. Joseph is also a founding member of the DEFCON Red Team Village and has run events at some of the largest cybersecurity events in the world, including Black Hat, DEFCON, and RSA Conference. He is currently involved in organizing the Texas Cyber Summit in San Antonio, Texas, and the Grayhat Conference in Orlando, Florida.

Dedications

Joseph Muniz:

I would like to dedicate this book to two people. First, I want to dedicate it to Atticus Muniz, who can't read this book at one and half years old and will likely just use it as a seat or throwing object. Hopefully he will accomplish something great and, while doing so, make time to read this book. Second, I want to dedicate this book to Raylin Muniz, who is 11 going on 20. She continues to impress me with the number of books she consumes each week in between school and other things. Hopefully she also will add this book to her reading list and say she learned something from her dad. That probably won't happen, though.

Steven Chimes:

To my parents, for teaching me that anything is possible

And to my wife, for making everything possible

James Risler:

When you dedicate a book to someone, it must be for a compelling reason. Ann, this book is dedicated to you. Thank you for all you do for me. I cannot thank you enough for your love and support. Love, Jim

Acknowledgments

I'll start by apologizing to James Risler and Steven Chimes for sucking them into writing a book with me. Seriously, though, thanks, guys for putting up with me during the writing process. It's a lot of work but worth the impact we have in the security community.

I also want to thank the technical reviewers, Viktor Bobrov and Joseph Mlodzianowksi, who had to sort through our gibberish rough drafts and help us polish them into what ends up at the bookstore. Thank you, James Manly, Eleanor Bru, and the rest of the Pearson army that takes care of me every time we work on a project such as this one. You always are professional and also make me feel like I'm part of the Pearson family. Thanks for that.

Finally, the most important thank you goes to my friends and family. Anjelica Ruda, thank you for supporting me while I worked on this project during all of those late nights. Thank you, Gary McNiel, for mentoring me as well as giving me the ability to balance work, family, and writing. Finally, thank you everybody who has supported me throughout my career. I truly feel lucky to have met the people in my life who have helped lead me to this moment…publishing this book.

—Joseph Muniz

First, to Joey Muniz and James Risler, thank you for unknowingly agreeing to write a book with me in the middle of a global pandemic; you both are nothing short of amazing. To Joey, a special thank you, first for inviting me to write this book with you, but more importantly for helping guide it through to completion.

To Viktor Bobrov, thank you for always entertaining my challenging AnyConnect questions. I would spend a lot more time stumped in the lab if it were not for you. To both Viktor and Joseph Mlodzianowski, thank you for painstakingly wading through all the pages to find all of our mistakes; the

final book would not be nearly as polished if it were not for your attention to detail. To James Manly, Eleanor Bru, and the rest of the Pearson team, thank you for everything you've done to make this book a success.

To my fellow Cisco colleagues, both past and present, thank you for all you have taught me throughout the years; there is not a day that goes by that I don't learn something new, and I can't imagine a better work family.

Last, but certainly not least, to my friends and family, thank you for all the love and support. To my Mom and Dad especially, thank you for nurturing the spark you saw so many years ago. And to my wife, Asra, words cannot express what your love and encouragement mean to me. I am a better person because of you.

—Steven Chimes

Thank you, Joey, for putting up with me as someone new to this process. You were a godsend. Also, Steven, thank you for all your help on VIRL, I really appreciated the time you took to help me get it up and running. You are both security professionals who set the standard for others to follow.

A special thank you to my family for the support over the years. I am especially thankful to my security team at Cisco. Each of you has been instrumental in helping me over the years: Pat, Paul, Jagdeep, and Bill, know that I really appreciate it. I also want to thank Steven Sowell for his guidance and sticking with me through both the tough times and the good times.

Of course, last but not least, thank you to my friends and family, who have continued to provide love and support. Thank you, Ellie. I think you know I could not have done this without you.

—James Risler

Contents at a Glance

Contents

Reader Services

In addition to the features in each of the core chapters, this book has additional study resources on the companion website, including the following:

Practice exams: The companion website contains an exam engine that enables you to review practice exam questions. Use these to prepare with a sample exam and to pinpoint topics where you need more study.

Interactive exercises and quizzes: The companion website contains interactive hands-on exercises and interactive quizzes so that you can test your knowledge on the spot.

Glossary quizzes: The companion website contains interactive quizzes that enable you to test yourself on every glossary term in the book.

To access this additional content, simply register your product. To start the registration process, go to www.ciscopress.com/register and log in or create an account.* Enter the product ISBN 9780136660606 and click Submit. After the process is complete, you will find any available bonus content under Registered Products.

*Be sure to check the box that you would like to hear from us to receive exclusive discounts on future editions of this product.

Command Syntax Conventions

The conventions used to present command syntax in this book are the same conventions used in the IOS Command Reference. The Command Reference describes these conventions as follows:

- **Boldface** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), boldface indicates commands that are manually input by the user (such as a **show** command).
- *Italic* indicates arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets ([ ]) indicate an optional element.
- Braces ({ }) indicate a required choice.
- Braces within brackets ([{ }]) indicate a required choice within an optional element.

Introduction

Congratulations! If you are reading this Introduction, then you have probably decided to obtain a Cisco certification and want to learn about VPN technology. As of February 24, 2020, in order to obtain a professional-level certification in security from Cisco, a candidate must pass two exams. One required milestone is the 350-701 SCOR core exam. The other exam is a concentration exam, and the Implementing Secure Solutions with Virtual Private Networks SVPN 300-730 exam is one option to meet the concentration exam requirement.

Obtaining a Cisco certification in VPN technology will ensure that you have a solid understanding of how to develop, configure, and support various types of VPN solutions. Securing communication has always been and will continue to be a critical topic for many organizations, and the skills covered in this book are extremely valuable. As more devices are provided network access and the concept of "work from anywhere" increases in popularity, knowledge of VPN technology will continue to be in demand. Protecting the confidentially, integrity, and availability of data is a fundamental requirement for every security program, and VPN technology is a tool commonly used to meet those objectives.

Professional certifications have been an important part of the computing industry for many years and will continue to become more important. Many reasons exist for these certifications, but the most popularly cited reason is credibility. All other factors being equal, a certified employee/consultant/job candidate is considered more valuable than one who is not certified. The SVPN 300-730 exam can be challenging, but this book can serve as a valuable tool for exam preparation to help you become certified in VPN technology. This book can also serve as a resource for those already in the field working with VPN solutions.

Be sure to visit www.cisco.com to find the latest information on CCNP

concentration requirements and to keep up to date on any new concentration exams that are announced.

Goals and Methods

The focus of this book is to teach how to develop and deliver Cisco VPN solutions. By accomplishing the learning objectives in this book, you will prepare yourself for taking the Implementing Secure Solutions with Virtual Private Networks SVPN 300-730 exam as well as deploying VPN technology. The goal of the book is to both help you pass the SVPN 300-730 exam and serve as a go-to resource when you are developing, deploying, and managing VPN technology. This book combines technical concepts with real-world experience, including tips and tricks for troubleshooting VPN deployment problems. Many parts of this book are inspired by our work with customers to deploy VPN technology.

One key methodology used in this book is to help you discover the exam topics that you need to review in more depth, to help you fully understand and remember those details, and to help you prove to yourself that you have retained your knowledge of those topics. Our goal is not to help you pass the SVPN 300-730 simply through memorization. The mixture of technology and lab concepts in this book is meant to help you truly learn and understand the VPN topics needed for both the exam and real-world deployments. This book will help you pass the SVPN 300-730 exam by using the following methods:

- Helping you discover which test topics you have not mastered
- Providing explanations and information to fill in your knowledge gaps
- Supplying exercises and scenarios that enhance your ability to recall and deduce the answers to test questions

Who Should Read This Book?

This book is ideal for anybody interested in learning about VPN concepts and Cisco VPN technology, including those planning to take the SVPN 300-730 exam. However, anyone else who needs a resource for VPN concepts and

Cisco VPN technology will also benefit from this book. We have a handful of objectives for writing this book but the primary focus is to help you pass the exam.

Strategies for Exam Preparation

The strategy you use to study for the SVPN 300-730 exam might be slightly different than strategies used by other readers, depending on the skills, knowledge, and experience you have already obtained. For instance, if you have attended an SVPN 300-730 course, you might take a different approach than someone whose knowledge is based on job experience alone.

Regardless of the strategy you use or the background you have, this book is designed to help you get to the point where you can pass the exam in the least amount of time possible. For instance, there is no need for you to practice or read about encryption concepts if you fully understand them already. However, many people like to make sure that they truly know a topic and thus read over material that they already know. Several book features will help you gain the confidence you need to be convinced that you know some material already and to also help you know what topics you need to study more.

The Companion Website for Online Content Review

All the electronic review elements, as well as other electronic components of the book, exist on this book's companion website. To access the companion website, start by establishing a login at www.ciscopress.com and registering your book. To do so, simply go to www.ciscopress.com/register and enter the ISBN of the print book: 9780136660606. After you have registered your book, go to your account page and click the Registered Products tab. From there, click the Access Bonus Content link to get access to the book's companion website.

Note that if you buy the Premium Edition eBook and Practice Test version of this book from Cisco Press, your book will automatically be registered on

your account page. Simply go to your account page, click the Registered Products tab, and select Access Bonus Content to access the book's companion website.

How to Access the Pearson Test Prep (PTP) App

You have two options for installing and using the Pearson Test Prep application: a web app and a desktop app. To use the Pearson Test Prep application, start by finding the access code that comes with the book. You can find the code in these ways:

- **Print book:** Look in the cardboard sleeve in the back of the book for a piece of paper with your book's unique access code.
- **Premium Edition:** If you purchase the Premium Edition eBook and Practice Test directly from the Cisco Press website, the code will be populated on your account page after purchase. Just log in at www.ciscopress.com, click Account to see details of your account, and click the Digital Purchases tab.
- **Amazon Kindle:** For those who purchase a Kindle edition from Amazon, the access code will be supplied directly by Amazon.
- **Other bookseller eBooks:** Note that if you purchase an eBook version from any other source, the practice test is not included because other vendors to date have not chosen to vend the required unique access code.

Note

Do not lose the access code because it is the only means with which you can access the QA content with the book.

Once you have the access code, to find instructions about both the Pearson Test Prep web app and the desktop app, follow these steps:

Step 1. Open this book's companion website

Step 2. Click the **Practice Exams** button.

Step 3. Follow the instructions listed there for installing the desktop app and for using the web app.

If you want to use the web app only at this point, just navigate to www.pearsontestprep.com, establish a free login if you do not already have one, and register this book's practice tests using the access code you just found. The process should take only a couple of minutes.

Note

Amazon eBook (Kindle) customers: It is easy to miss Amazon's email that lists your Pearson Test Prep access code. Soon after you purchase the Kindle eBook, Amazon should send an email; however, the email uses very generic text and makes no specific mention of PTP or practice exams. To find your code, read every email from Amazon after you purchase the book. Also do the usual checks for ensuring your email arrives, like checking your spam folder.

Note

Other eBook customers: As of the time of publication, only the publisher and Amazon supply Pearson Test Prep access codes when you purchase their eBook editions of this book.

How This Book Is Organized

Although this book could be read cover-to-cover, it is designed to be flexible and allow you to easily move between chapters and sections of chapters to cover just the material that you need to more work with. Chapters 1 through 10 cover SVPN topics that are relevant for the SVPN 300-730 exam. These core chapters cover the following topics:

- **Chapter 1, "Understanding the Implementing Secure Solutions with Virtual Private Networks SVPN 300-730 Exam":** This chapter introduces drivers for getting certified in VPN technology as well as what is involved in getting certified at a professional level for Cisco security.

- **Chapter 2, "Introduction to Virtual Private Networks (VPNs)":** This chapter introduces fundamental VPN concepts, including an overview of the topics that covered in that book and a look at the Cisco technologies that offer VPN capabilities.

- **Chapter 3, "Site-to-Site VPNs":** This chapter takes a close look at site-to-site VPN technology and concepts you need to know to pass the SVPN 300-730 exam. This chapter also lays the groundwork for Chapters 4 through 6.

- **Chapter 4, "Group Encrypted Transport VPN (GETVPN)":** This chapter takes a closer look at a specific site-to-site VPN topic: GETVPN. This chapter covers everything from designing to managing GETVPN using Cisco technology.

- **Chapter 5, "Dynamic Multipoint Virtual Private Network (DMVPN)":** This chapter takes a deep dive into DMVPN. You need to master the deployment, management, and troubleshooting concepts covered in the chapter because they are heavily featured in the SVPN 300-730 exam.

- **Chapter 6, "FlexVPN Configuration and Troubleshooting":** This chapter covers various FlexVPN learning objectives outlined in the SVPN 300-730 exam blueprint as well as tips and tricks used in real-world FlexVPN deployments.

- **Chapter 7, "Remote Access VPNs":** This chapter examines remote access VPN technology. You will learn fundamental remote access VPN concepts, including which Cisco technologies support remote access VPNs. This chapter lays the groundwork for Chapters 7 through 10.

- **Chapter 8, "Clientless Remote Access SSLVPNs on the ASA":** This chapter focuses on clientless remote accesss VPN concepts specific to the Cisco ASA. Clientless VPNs continue to grow in popularity, and you

need to understand them for the SVPN 300-730 exam.

- **Chapter 9, "AnyConnect VPNs on the ASA and IOS":** This chapter examines client-based remote access VPNs. The client you need to know for the SVPN 300-730 exam is Cisco AnyConnect, which is one of the VPN technologies deployed most widely in organziations around the world. This chapter covers how to deliver remote access VPNs using Cisco AnyConnect from both an appliance and IOS.

- **Chapter 10, "Troubleshooting Remote Access VPNs":** This chapter provides a wrap-up of the remote access VPN topics, with a focus on troubleshooting.

- **Chapter 11, "Final Preparation":** The final chapter covers how to prepare for the SVPN exam and resources you can use as a next step after reading this book.

The questions for each certification exam are a closely guarded secret. However, Cisco has published an exam blueprint that lists the topics you must know to successfully complete the exam. The blueprint for the SVPN 300-730 exam lists the following topics and the percentage of the exam that is dedicated to each of them:

15%	1.0 Site-to-site Virtual Private Networks on Routers and Firewalls 1.1 Describe GETVPN 1.2 Describe uses of DMVPN 1.3 Describe uses of FlexVPN
20%	2.0 Remote access VPNs 2.1 Implement AnyConnect IKEv2 VPNs on ASA and routers 2.2 Implement AnyConnect SSLVPN on ASA 2.3 Implement Clientless SSLVPN on ASA 2.4 Implement Flex VPN on routers
35%	3.0 Troubleshooting using ASDM and CLI 3.1 Troubleshoot IPsec 3.2 Troubleshoot DMVPN 3.3 Troubleshoot FlexVPN 3.4 Troubleshoot AnyConnect IKEv2 on ASA and routers 3.5 Troubleshoot SSL VPN and Clientless SSLVPN on ASA
30%	4.0 Secure Communications Architectures 4.1 Describe functional components of GETVPN, FlexVPN, DMVPN, and IPsec for site-to-site VPN solutions 4.2 Describe functional components of FlexVPN, IPsec, and Clientless SSL for remote access VPN solutions 4.3 Recognize VPN technology based on configuration output for site-to-site VPN solutions 4.4 Recognize VPN technology based on configuration output for remote access VPN solutions 4.5 Describe split tunneling requirements for remote access VPN solutions 4.6 Design site-to-site VPN solutions 4.6.a VPN technology considerations based on functional requirements 4.6.b High availability considerations 4.7 Design remote access VPN solutions 4.7.a VPN technology considerations based on functional requirements 4.7.b High availability considerations 4.7.c Clientless SSL browser and client considerations and requirements 4.8 Describe Elliptic Curve Cryptography (ECC) algorithms

You should be proficient with these topics for the exam as well as for designing and implementing Cisco VPN technology in the real world.

Each version of the exam can have topics that emphasize different functions or features, and some topics can be rather broad and generalized. The goal of this book is to provide the most comprehensive coverage to ensure that you are well prepared for the exam. Although some chapters might not address specific exam topics, they provide a foundation that is necessary for a clear understanding of important topics. Your short-term goal might be to pass this exam, but your long-term goal should be to become a qualified CCNP security engineer with an understanding of VPN technology.

It is 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 book should not be your only reference when preparing for the certification exam. You can find a wealth of information at Cisco.com that covers each topic in great detail. If you think you need more detailed information on a specific topic, read the Cisco documentation that focuses on that topic.

Note that as VPN technologies continue to evolve, Cisco reserves the right to change the SVPN 300-730 exam topics without notice. Check Cisco.com to verify the actual list of topics to ensure that you are prepared before taking the exam. You can view the current exam topics on any current Cisco certification exam by visiting the Cisco.com website, choosing Menu, choosing Training & Events, and selecting from the Certifications list. Note also that, if needed, Cisco Press might post additional preparatory content on the web page associated with this book, at http://www.ciscopress.com/title/9780136660606. It’s a good idea to check the website a couple of weeks before taking your exam to be sure that you have up-to-date content.

Part I: Virtual Private Networks (VPN)

Chapter 1. Understanding the Implementing Secure Solutions with Virtual Private Networks SVPN 300-730 Exam

This chapter covers the following subjects:

- **Why Learn VPN Technology:** This section explains why VPN technology is important for many organizations and their users.
- **The Cisco Certification Program:** This section provides an overview of the Cisco certification process and discusses how the exams are set up and administered.
- **SVPN 300-730 Exam:** This section covers what the SVPN exam is and its place in the Cisco certification program.

"The only impossible journey is the one you never begin."

—Tony Robbins

You are about to start a journey learning about virtual private networks. Why is this topic relevant, and what has motivated you to pick up this book? Are you purely interested in passing the Implementing Secure Solutions with Virtual Private Networks (SVPN 300-730) exam to eventually obtain the Cisco Certified Network Professional (CCNP) certification for security? Or do you have a specific need for learning about this topic? Do you work for one of the many organizations that need to accommodate teleworking in general or because of the COVID-19 pandemic? The COVID-19 pandemic opened the eyes of many C-level executives regarding their organizations' capabilities to enable their workforces to work from home.

If you are here just for the purpose of passing the SVPN 300-730 exam, we hope to convince you that the topic of VPNs is very relevant, regardless of who you work for or your outlook on cybersecurity. If you desire to better understand VPN technology or need to develop a strategy for supporting remote access for your organization, you have acquired the right resource.

This chapter looks at why you might want to learn about VPN technology, the Cisco certification program, and the SVPN 300-730 exam.

Why Learn VPN Technology

You might be wondering why VPN technology is important to your organization or for personal use. Maybe you are interested in passing the SVPN 300-730 exam, and reading this book is part of your study plan, but you really don't understand why so much hype surrounds leveraging VPN technology. This section helps clear up confusion about the importance of VPN technology.

Most people today use at least one mobile device, with links to many facets of their lives. Think about all the social media applications, banking applications, email, and communication resources on such a device. To maintain these and other resources on a mobile device, the device must constantly communicate on different networks as the device owner moves around the world. Without network connectivity, most of the applications on a mobile device have no value. Essentially, a mobile device's value depends on having connectivity to the Internet, whether via cellular or Wi-Fi. Through that connectivity, sensitive information is constantly exchanged. Imagine what could happen if the wrong person were able to access that data! An attacker with access to a compromised mobile device could cause havoc in the victim's social circles and financial situation.

How easy is it to compromise a mobile device? Instead of attacking a device, can an attacker just attack how data is exchanged between the device and the Internet? In this book, we'll talk about both of these issues. This chapter begins by taking a look at one tool that attackers love to use to abuse mobile device communication: the Wi-Fi Pineapple by Hak5 (see Figure 1-1). Pen testers also like to use this tool to simulate what could happen if an attacker abused a vulnerability within a targeted system. Let's look at how an attacker could use the Wi-Fi Pineapple to accomplish this goal.

Figure 1-1 Wi-Fi Pineapple by Hak5

The Wi-Fi Pineapple leverages a few exploits targeting mobile endpoints that are looking to connect to their trusted home networks. Most mobile devices store frequently used network SSIDs, such as home or corporate network SSIDs, so when the user is within proximity of those environments, the mobile device automatically establishes connectivity. This convenience opens up a mobile device to an exploit known as Karma. To take advantage of this exploit, a tool like the Wi-Fi Pineapple will listen for mobile devices sending probes for their trusted SSIDs and reply back as one of those SSIDs. For example, if your home network is called WuTangLAN, your mobile device may periodically send a probe to see if the SSID WuTangLAN is available in the area. If your mobile device detects that WuTangLAN is available in the area, it will automatically switch over to that network, based on assumed trust that it is an SSID you commonly use to access the Internet. If a Wi-Fi

Pineapple is in the area, it will hear that probe and reply back as a fake WuTangLAN SSID to establish a connection between the victim device (your mobile phone) and the Internet. This is a man-in-the-middle attack (see Figure 1-2.)

Figure 1-2 Wi-Fi Pineapple Karma Attack

To make things worse, the Wi-Fi Pineapple includes an exploit known as SSL Strip that filters out encrypted versions of websites but permits unencrypted versions of websites. When a victim has unknowingly connected to a Wi-Fi Pineapple and then uses the mobile device to connect to a trusted website, only the unencrypted version of the website is permitted. This allows the Wi-Fi Pineapple to snoop on the traffic and capture sensitive data such as passwords. Figure 1-3 shows the Karma log picking up a few devices from unwitting users (with MAC addresses and SSID changed to protect the users).

Note

Learn more about the Wi-Fi Pineapple at https://shop.hak5.org/products/wifi-pineapple.

Figure 1-3 Karma Log Within Wi-Fi Pineapple

As you can see in this example, the threat to mobile devices is real. Keep in mind the Wi-Fi Pineapple is just one of many tools available that could be used to compromise a mobile device.

How can you prevent a device such as a Wi-Fi Pineapple from exploiting your mobile devices? By using a VPN. A VPN encrypts traffic between your mobile device and your remote VPN concentrator so that a device such as a Wi-Fi Pineapple that wants to snoop won't be able to intercept any traffic. Even if a Wi-Fi Pineapple between your device and the VPN concentrator were able to perpetrate a man-in-the-middle attack, confidentiality and integrity would still be maintained because an attacker can't view or modify the encrypted data between your device and the remote VPN concentrator. Using a VPN can prevent any form of man-in-the-middle attack where an attacker device attempts to snoop on communication between devices (for example, when checking email at a local coffee shop or at a hotel). Best practice for all mobile workers is to encrypt their traffic using a VPN.

A common challenge is provisioning sensitive resources to remote sites or users in a secure manner. Say that you work at company located in the United Kingdom. You recently acquired some new technology and need experts from the manufacturer of the new technology, which is located in Australia, to remotely access a system at your UK headquarters for troubleshooting purposes. How can you securely control who and what can access your internal UK resources from Australia? Using a VPN is once again a possible answer. Not only can encryption be established between the remote Australian user and your internal services but various controls can be put into place, such as limiting accessibility to certain resources using portals and other controls that are covered in this book.

Without security controls, exposing access for a trusted user could lead to malicious parties discovering the open connection and also accessing the inside network. In addition, if security controls are not put in place, a trusted user might be able to access other systems outside of what they are supposed to connect to. Access can be necessary, but it must be controlled to avoid overexposing internal resources.

Figure 1-4 shows a tool called Masscan that can quickly scan targets for open ports. Malicious parties use tools like Masscan to scan targets to see if

companies have left services exposed to the public. Where services are exposed in this way, an attacker can exploit, pivot, escalate privileges, and accomplish various goals, ranging from taking down or modifying internal systems to stealing data.

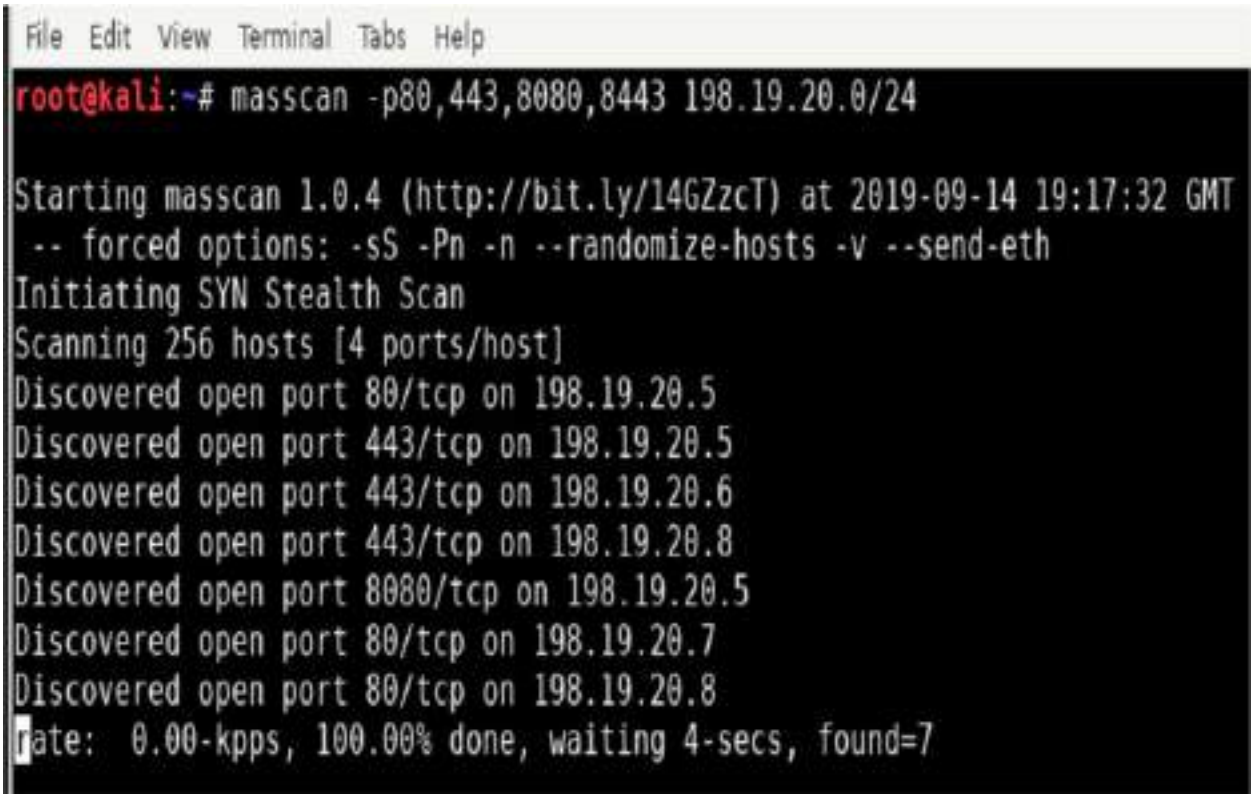


Figure 1-4 Masscan Running Against a Target

When an organization grows or merges with another organization that has locations elsewhere around the world, new connectivity challenges arise. For example, the different organizations' systems might need to be accessed within company networks and also available across multiple locations with different IP address ranges. Say that one company is located in Germany, and another is located in the United States. Network services are provided by local Internet service providers, which means data must cross between various public networks—which are untrusted and risky—as data travels between the German and U.S. offices. A site-to-site VPN solution can permit a user to travel between these offices and access the resources in the two offices without requiring changes to the network configuration on the user's system. The user's laptop can access the same services at both locations

thanks to an encrypted tunnel built between the offices to permit communication. Later chapters in this book provide various examples of connecting locations together using different site-to-site VPN concepts.

These are just a few of the many use cases that can be solved by using VPN technology. VPNs have been around for a while, and there are many versions of VPN technology used on today's networks. The COVID-19 pandemic has increased the demand for learning about VPN technology because many organizations have needed to accommodate a remote workforce. In many organizations, existing VPN architectures were not equipped to meet the needs of an entire workforce. Organizations also faced challenges with the quality of the remote work experience, including performance of mission-critical applications, as well as security concerns. It is important to understand that VPN technologies differ in the level of protection they provide, as well as in their performance, configuration, upkeep, and expansion options. Later chapters of this book cover the approaches that are currently accepted in the industry as well as those that have been deemed obsolete. This book will help you design a VPN architecture that can not only accommodate your current remote access requirements but also enable growth to meet future demand.

The Cisco Certification Program

The Cisco certification program is an industry-respected source that validates candidates' skills in specific technology categories. The Cisco Certification Network Professional (CCNP) Security program focuses on various skills related to security solutions at a professional level. Cisco offers many other security certifications that touch on different products and concepts, but its flagship program for Cisco-based security tools consists of the CCNA (associate), CCNP (professional), and CCIE (expert) certifications.

In 2019, Cisco announced major changes to the Cisco certification program, including replacing the CCNP program with a new set of exam requirements. The previous CCNP Security program required candidates to pass the following four exams:

- Implementing Cisco Secure Access Solutions 300-208 (SISAS 300-208)

- Implementing Cisco Edge Network Security Solutions 300-206 (SENSS 300-206)
- Implementing Cisco Secure Mobility Solutions 300-209 (SIMOS 300-209)
- Implementing Cisco Threat Control Solutions 300-210 (SITCS 300-210)

For the old CCNP Security program, the last date a candidate could become CCNP certified following the old approach was February 23, 2020. Today, only the newer CCNP exams are available, including the SVPN 300-730 exam, which is the focus of this book.

Note

You can learn more about the older CCNP program at https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/professional/ccnp-security.html#~stickynav=1.

The new CCNP Security program launched February 24, 2020. To obtain a CCNP Security certification under the new program, a candidate must pass two exams: a core exam and a concentration exam. The required core exam is Implementing and Operating Cisco Security Core Technologies 350-701 (SCOR 350-701). This exam tests a broad range of topics, including the following categories:

- Security Concepts
- Network Security
- Securing the Cloud
- Content Security
- Endpoint Protection and Detection
- Secure Network Access, Visibility, and Enforcement

Note

Learn more about the 350-701 SCOR exam at https://learningnetwork.cisco.com/community/certifications/ccnp-security/scor/exam-topics.

The CCNP Security concentration exams are designed to go deeply into specific topics. The following list shows all of the concentration exam options at the time of this publication:

Note

Remember that you need to pass only one concentration exam, so if you pass the SVPN 300-730 exam, you don't have to take on any of these other exams to achieve the CCNP Security certification. You would just need to pass the SVPN 300-730 and SCOR 350-701 exams.

- Security Networks with Cisco Firepower Next Generation Firewall (SSNGFW) and Security Networks with Cisco Firepower Next-Generation IPS (SSFIPS) 300-710 (SNCF 300-710)
- Implementing and Configuring Cisco Identity Services Engine 300-715 (SISE 300-715)
- Securing Email with Cisco Email Security Appliance 300-720 (SESA 300-720)
- Securing the Web with Cisco Security Appliance 300-725 (SWSA 300-725)
- Implementing Secure Solutions with Virtual Private Networks 300-730 (SVPN 300-730)
- Implementing Automation for Cisco Security Solutions 300-730 (SAUTO 300-735)

If you have already started working toward the CCNP Security certification following the old program, you can use a migration tool that allows some items to be credited toward the new program (see https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/professional/ccnp-security-migration-tool.html). In particular, if you passed any of the old CCNP Security certification exams before February 23, 2020, they will migrate to a certain specialist certification and count as your concentration exam requirement for the CCNP Security certification. Unless you passed all four old CCNP security program exams before February 23, 2020, however, you are required to pass the SCOR 350-701 exam before you can obtain a CCNP Security certification.

The SVPN 300-730 Exam

You might have purchased this book with the goal of preparing for the SVPN 300-730 exam. This section sets you up for success by reviewing what you should expect to see on the SVPN 300-730 exam as well as how this book can help you prepare for it. We can't give you the exact test questions that will appear on the exam because that would be a violation of the Cisco certification program. If your expectation is to pass the exam by simply memorizing questions and a few tables, you probably will not be successful using this or any other authorized resource unless you already know the exam topics and are just looking for a quick refresher. However, this book provides everything you need to study to pass the exam. Plus, it includes other real-world concepts and technologies to round out your education on VPNs.

The first task in preparing for the SVPN 300-730 exam is to understand what it is and the topics that are covered. The SVPN 300-730 exam is a 90-minute exam that tests your knowledge related to implementing secure remote communications with VPN solutions, including communications, architectures, and troubleshooting. Table 1-1 lists the topics covered in version 1.1 of the SVPN 300-730 exam.

Table 1-1 SVPN 300-730 Exam Topics

Percentage of Exam	Topic
15%	1.0 Site-to-site Virtual Private Networks on Routers and Firewalls 1.1 Describe GETVPN 1.2 Implement DMVPN 1.3 Implement FlexVPN
20%	2.0 Remote access VPNs 2.1 Implement AnyConnect IKEv2 VPNs on ASA and routers 2.2 Implement AnyConnect SSLVPN on ASA 2.3 Implement Clientless SSLVPN on ASA 2.4 Implement FlexVPN on routers
35%	3.0 Troubleshooting using ASDM and CLI 3.1 Troubleshoot IPsec 3.2 Troubleshoot DMVPN 3.3 Troubleshoot FlexVPN 3.4 Troubleshoot AnyConnect IKEv2 on ASA and routers 3.5 Troubleshoot SSLVPN Clientless SSLVPN on ASA
30%	4.0 Secure Communications Architectures 4.1 Describe functional components of GETVPN, FlexVPN, DMVPN, and IPsec for site-to-site VPN solutions 4.2 Describe functional components of FlexVPN, IPsec, and Clientless SSL for remote access VPN solutions 4.3 Recognize VPN technology based on configuration output for site-to-site VPN solutions 4.4 Recognize VPN technology based on configuration output for remote access VPN solutions 4.5 Describe split tunneling requirements for remote access VPN solutions 4.6 Design site-to-site VPN solutions 4.6.a VPN technology considerations based on functional requirements 4.6.b High availability considerations 2019 Cisco Systems, Inc. This document is Cisco Public. 4.7 Design remote access VPN solutions 4.7.a VPN technology considerations based on functional requirements 4.7.b High availability considerations 4.7.c Clientless SSL browser and client considerations and requirements 4.8 Describe Elliptic Curve Cryptography (ECC) algorithms

Note

Topics can change, so make sure to validate the SVPN 300-730 learning objectives at https://learningnetwork.cisco.com/community/certifications/ccnp-security/svpn/exam-topics

Cisco exams are administered by authorized exam providers, either at a test center or online. For exams at a test center, you must physically go to a testing center to take a Cisco certification exam. The specifics of the testing center may vary, but typically, you should expect to be seated at a computer and provided a note pad. You can use the note pad to take notes, but you will not be allowed to take the note pad with you after you complete the exam. You will not have any resources available other that what you know about the topic. You will not be allowed to bring in any study materials or tools such as a cell phone that could be used to look up answers; you will be monitored during the entire testing process to ensure that you do not violate this policy. You must use the computer that is provided to choose the correct answers within the provided time.

As an alternative to taking the exam at a test center, it is now possible to take many exams online. The exam will still be proctored and monitored by the authorized exam provider, but instead of traveling to a test center to take the exam, you can do it from the comfort of your home or office. If you select this option, be sure to familiarize yourself with the requirements and rules, as you will be responsible for setting up a testing space that meets the exam provider's requirements.

Cisco exams include various types of questions. According to the latest Cisco certification exam tutorial, you will not be allowed to go back to any question that you have completed. This means that when you see a question, you need to make sure you are entering the best answer because you can’t mark a question and return to it later.

One question type you will see on the exam is a multiple-choice single-

answer question (see Figure 1-5). This format provides a question and allows only one answer. You must select the best answer and click Next. You can change your answer as many times as you want until you click Next. Once you select Next, however, your answer is recorded, and you are provided the next question. As you work through the exam, you do not get any indication of whether your answers are correct. The test engine simply moves you to the next question and shows how much time you have remaining to take the exam.

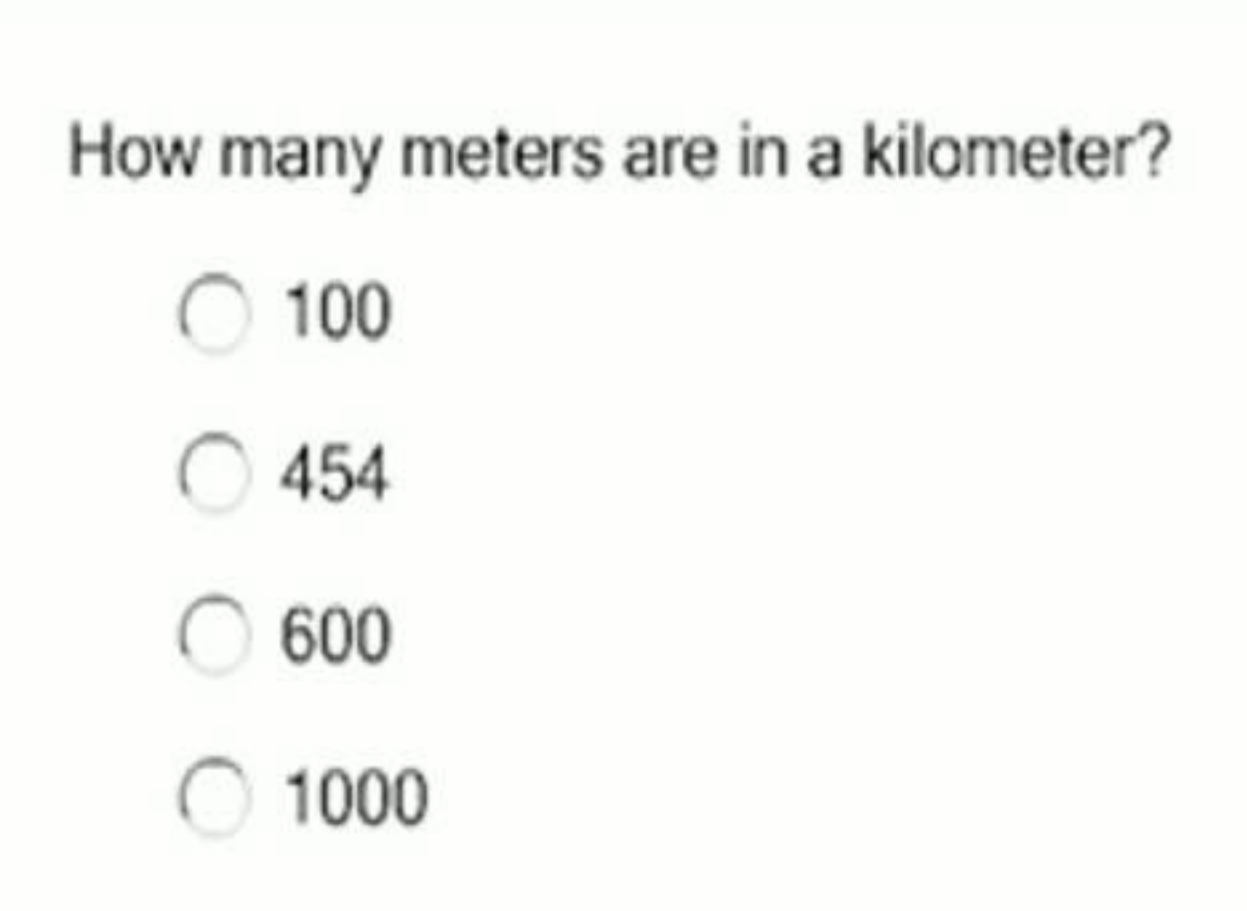


Figure 1-5 Sample Multiple-Choice Single-Answer Question

Another possible question is a multiple-choice, multiple-answer question. For this question type, you are told how many answers you must choose in order to get the question correct. You can choose any answers and make as many changes as you want until you click the Next button. Once you select Next, your answers are submitted, and you move to the next question.

A third possible question type is a drag-and-drop question. This question format requires you to drag possible answers into open boxes. For example, in Figure 1-6, you can see that not all of the possible choices are required to answer the question because there are seven possible answers and only six answer slots. Sometimes drag-and-drop questions permit you to use the same answer twice; other times you can only drag one answer to one slot. Sometimes some of the yellow boxes do not need to be filled. Sometimes you need to use the same answer in different boxes. Make sure to read the directions for such a question and properly answer based on what it asks you to do. Remember that you can change your answers as many times as you want until you click Next to submit your answers.

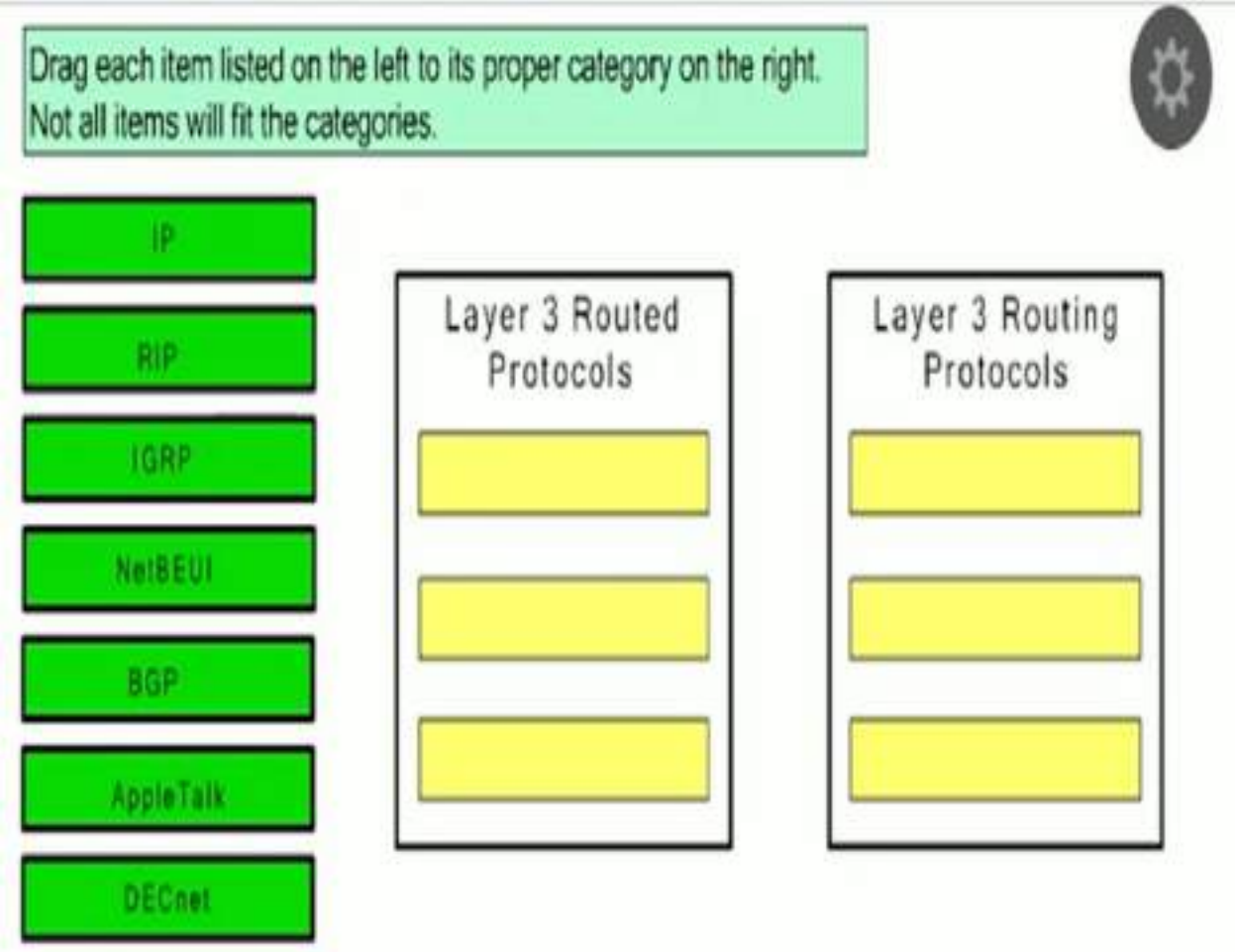


Figure 1-6 Sample Drag-and-Drop Question

When answering drag-and-drop questions, it is often helpful to use the process of elimination. First, select every answer you know is correct; this

reduces the number of answers you are not sure about and helps you increase your chances of selecting the correct answer.

Another important tactic is to be sure to choose an answer even if you don't know for sure that it's correct. On a Cisco exam, you gain points by answering correctly. You don't gain points by leaving a question blank, and you also don't lose points if you answer incorrectly; in either case, you simply don't earn any points. Therefore, there is no harm in guessing, and you might just get lucky.

Another question category you may encounter is a fill-in-the-blank question. Such a question displays a question and empty boxes, which you are expected to fill with the proper responses. You need to click a box before you are able to type in your answer. Make sure you don't miss any empty boxes before proceeding to the next question. In most situations, it doesn't matter if you type your answers with uppercase or lowercase letters; however, command-line and other case-sensitive answers do require that you correctly use uppercase and lowercase. A question's directions specify whether case is a concern. As with the other question types, when you fill in all the blanks, click Next, and you are taken to the next questions. Once you click Next, you are not allowed to go back to the question.

You might see a few testlet questions on your exam. Such questions are based on specific scenarios. For a testlet question, you see the scenario at the top part of the screen and one or more questions at the bottom of the screen. You can scroll to move through the scenario if the entire scenario doesn't fit on the screen. The right side of the question section indicates how many questions are involved with the testlet. By clicking a question number, you can view that question. Testlet questions may be multiple-choice single-answer or multiple-choice multiple-answer. You can change your answers to the individual questions as many times as you want until you submit your answers for the entire testlet. You can also answer a testlet's questions in any order, but it's important to make sure you answer all questions before proceeding to submit your answers. Once you click Next, you are taken to the next question. Figure 1-7 shows an example of a testlet question with a popup asking if you would like to proceed. You would want to click Next only if you have answered all questions and are ready to finalize your testlet answers

and move on to the next question.

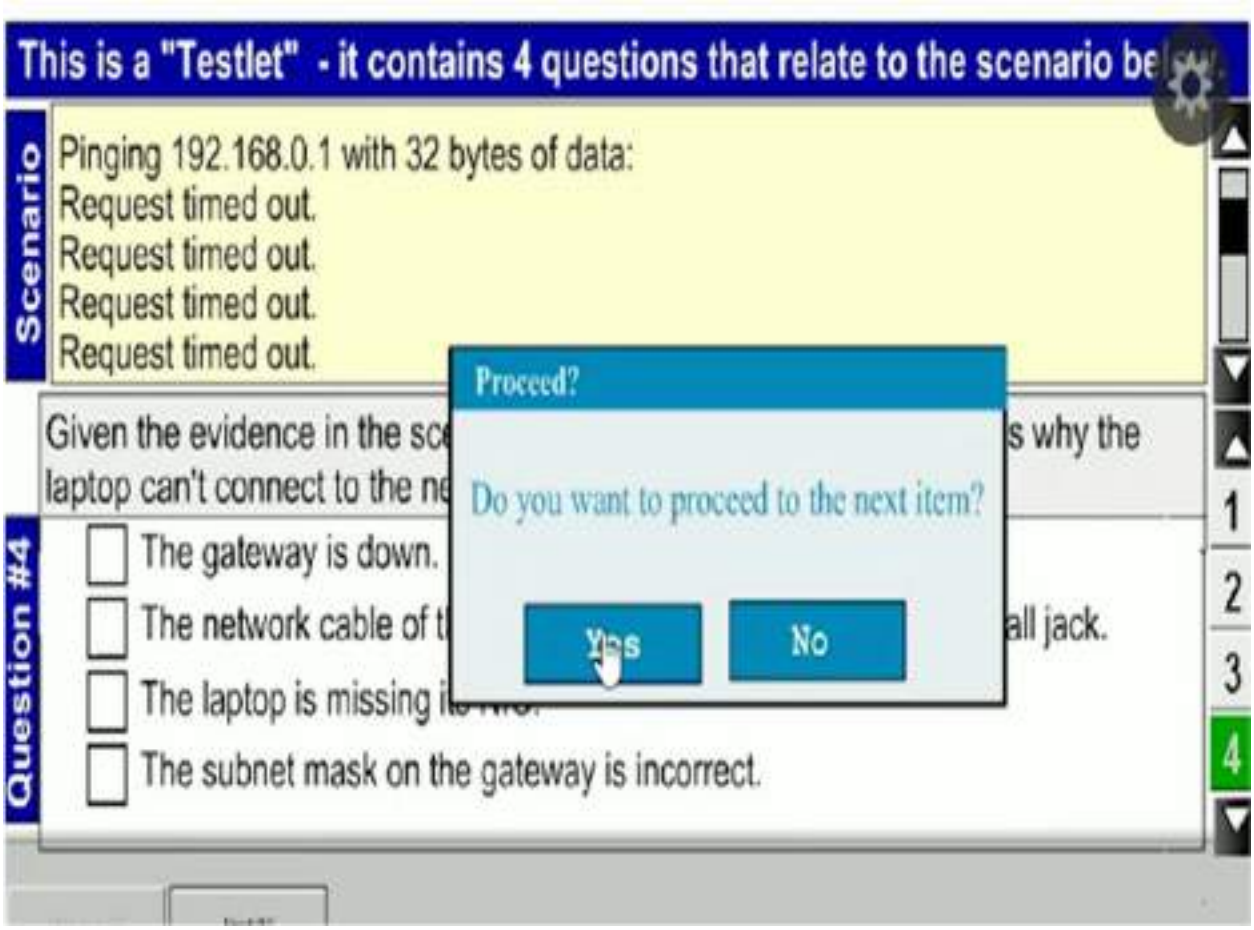


Figure 1-7 Sample Testlet Question

One final question type you may encounter is a simulation-based (or simulet) question (see Figure 1-8). Such a question provides you a network diagram with equipment you might be able to click to access the command line or a management graphical user interface (GUI). For such a question, commands that are needed to complete the required tasks are available. With a simulet question, you see a problem statement at the top of the window, and you need to perform what is being asked, based on the directions for accessing equipment that is displayed on the left. For example, if you see a serial cable connected to a router, you might need to click it to access the serial interface of the router. When you access any device, you have access to privileged mode. In simulet questions, you will likely only be tested on specific steps rather than having to perform a lot of configuration.

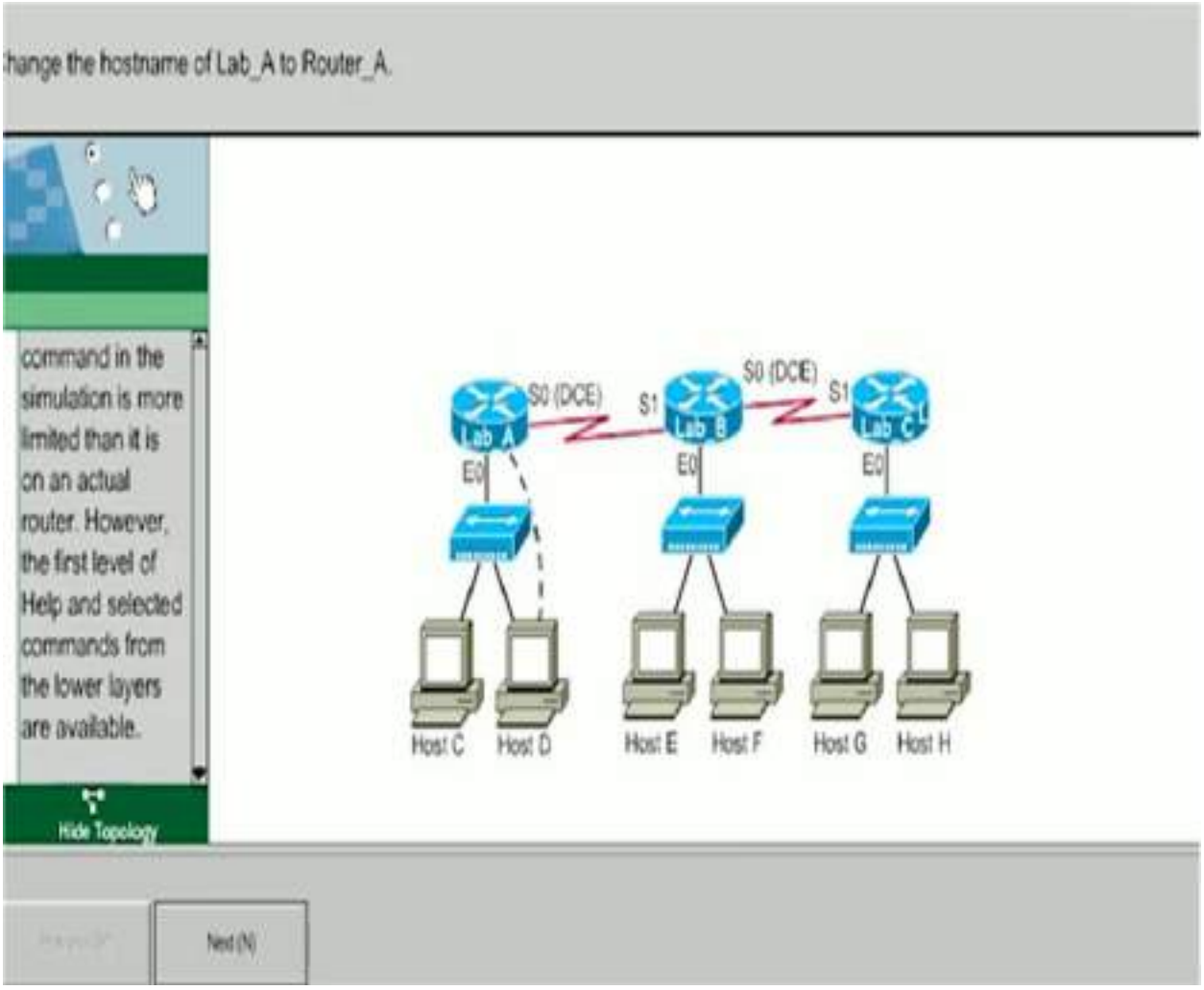


Figure 1-8 Sample Simulet Question

You should expect to see one or more simulet questions asking you to configure different types of VPN scenarios, but the majority of the questions will be other formats. Remember that you have only 90 minutes to take this exam, so you need to ensure that no single question consumes too much of your exam time.

Exam Preparation

People use different tactics to learn concepts. Some people read about topics, while others spend time using visual learning resources such as hands-on time with equipment. This book attempts to accommodate different learning styles by providing an overview of a concept, screenshots of associated

technologies regarding the hands-on steps that are needed to perform a task, and various types of cheat sheets to help you learn and remember key points. The layout of this book follows the learning requirement for the SVPN 300-730 exam and discusses additional topics we feel are relevant to real-world environments using VPN technology.

Summary

As you have seen in this chapter, it is important to understand VPN technologies today. VPN technologies protect users' privacy, prevent man-in-the-middle attacks, and enable remote workers to securely access their organizations' networks. VPNs are also crucial in many organizations' disaster planning efforts.

This chapter also describes Cisco certification and the SVPN 300-730 exam in particular. This book helps prepare you for this exam by providing questions, memory tables, and other tools that help you cement your knowledge of the SVPN 300-730 exam topics. This book also covers many topics that might not be covered on the exam but that are relevant based on our experience and trends in the industry. However, Cisco exams do change, and we recommend treating all topics covered in this book as important to mastering VPN technology.

The next chapter provides a high-level overview of VPN technology.

Chapter 2. Introduction to Virtual Private Networks (VPN)

This chapter covers the following subjects:

- **VPN Offerings:** This section provides an overview of various remote access and site-to-site VPN options.
- **VPN Technology Components:** This section provides a review of essential components that make up a VPN solution.
- **VPN Protocols:** This section introduces protocols commonly used with a VPN architecture.
- **Cisco VPN Portfolio:** This section looks at protocols and technology related to Cisco's VPN portfolio.
- **Cisco Security Appliance Management:** This section reviews options for managing Cisco VPN technology.
- **VPN Logging:** This section introduces logging options for Cisco VPN technology.

"Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say

—Edward Snowden

This chapter covers the following exam objectives:

- 1.0 Site-to-site Virtual Private Networks on Routers and Firewalls
  - 1.1 Describe GETVPN
  - 1.2 Describe DMVPN
  - 1.3 Describe FlexVPN

- 4.0 Secure Communications Architectures
  - 4.1 Describe functional components of GETVPN, FlexVPN, DMVPN, and IPsec for site-to-site VPN solutions
  - 4.2 Describe functional components of FlexVPN, IPsec, and Clientless SLL for remote access VPN solutions
  - 4.6 Design site-to-site VPN solutions
    - 4.6.a VPN technology considerations based on functional requirements
  - 4.7 Design remote access VPN solutions
    - 4.7.a VPN technology considerations based on functional requirements
    - 4.7.b High availability considerations

Virtual private networks (VPNs) require three key ingredients to function in a secure manner: confidentiality, integrity, and availability (also known as the CIA triad). Failing to enforce the CIA triad can lead to unwanted exposure and loss of data. Enforcing the CIA triad on your data could keep your social media accounts from being compromised, prevent your bank accounts from being liquidated by unauthorized parties, and ensure that company classified or personal data is not leaked to dark markets. VPN technologies can assist in ensuring CIA and preventing data catastrophes.

Learning beyond the SVPN concepts:

- General VPN Overview Concepts
- VPN Portfolio – Cisco Firepower and Cisco Meraki concepts

“Do I Know This Already?” Quiz

The “Do I Know This Already?” quiz enables you to assess whether you should read this entire chapter thoroughly or jump to the “Exam Preparation Tasks” section. If you are in doubt about your answers to these questions or your own assessment of your knowledge of the topics, read the entire chapter.

Table 2-1 lists the major headings in this chapter and their corresponding "Do I Know This Already?" quiz questions. You can find the answers in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes."

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

Foundation Topics Section	Questions
VPN Offerings	2
VPN Technology Components	1
VPN Protocols	3, 5, 9
Cisco VPN Portfolio	4, 8, 10
Cisco Security Appliance Management	6
VPN Logging	7

1. Which of the following is *not* a deployment model for a site-to-site VPN architecture?

a. Full mesh

b. Hub-and-spoke

c. Mesh-to-spoke

d. Spoke-to-spoke

2. What can a Cisco Integrated Services Router device offer?

a. Site-to-site VPN capabilities

b. Remote access capabilities

c. Both site-to-site and remote access capabilities

d. Cisco routers do not provide VPN services.

3. Which of the following is *not* a VPN protocol?

a. VAM

b. IKEv2

c. L2TP

d. SSTP

e. PPTP

4. Which of the following is *not* a Cisco VPN option?

a. FlexVPN

b. IKEv2 VPN

c. DMVPN

d. SSLVPN

e. GETVPN

5. Which of the following are tunnel-less VPN options? (Choose two.)

a. DMVPN

b. EasyVPN

c. IPsec VPN

d. GRE-based VPN

6. Which of the following is *not* an option for managing a Cisco security device?

a. Cisco SecureX

b. Cisco Security Manager (CSM)

c. Cisco Adaptive Security Device Manager (ASDM)

d. Cisco Defense Orchestrator

7. What is the purpose of DART?

a. Diagnostics and reporting

b. Data and resilience

c. Detection and response

d. Data and return

8. Which of the following options support a remote access client? (Choose two.)

a. DMVPN

b. SSLVPN

c. GETVPN

d. FlexVPN

e. Static IPsec

9. Which protocol is L2TP always paired with?

a. PPTP

b. IPsec

c. SSL

d. IKE

10. Which of the following are reasons to use SSL for a VPN? (Choose two.)

a. Many host-based security capabilities are needed.

b. There is no need for high-end security.

c. It runs over HTTPs ports.

d. It uses a web browser.

Foundation Topics

VPN Offerings

A *virtual private network (VPN)* is two or more remote devices that transmit data to each other securely over an unsecured network, such as the Internet. VPNs leverage tunnels to encapsulate data packets, most commonly within IP packets for transmission over IP-based networks. Encryption is used to ensure data privacy, and authentication is enforced to protect the integrity and confidentiality of the data. This means an employee using a laptop, smartphone, or IoT device can connect through a VPN to the corporate network from anywhere in the world and maintain data privacy. In addition, virtual tunnels can be set up between different offices to allow data to be shared over the untrusted Internet.

VPN Technologies vs. Services

Many flavors of VPN technology are available for organizations to choose from. Our first method for categorizing all available VPN technologies is grouping offerings into VPN technologies and VPN services. The following is how each of these VPN groups can be defined:

- **VPN technologies:** A VPN technology is a tool that provides encryption between endpoints. VPN technology is the primary focus of this book.
- **VPN services:** A VPN service is a package that includes one or more VPN services, where you do not own the technology providing the service. An example of a VPN service is a website management service that includes a VPN encryption option for transferring data between a host and the server hosting the website. For example, the user interface could be a web front end hiding the VPN and web transfer technology. A user can simply drag files into a web page, and within minutes, their data appears in a management portal and is transferred to storage space within the cloud. The user is not responsible for configuring or managing the backend VPN technology. Managing the VPN technology is the responsibility of the service provider. VPN services is not the focus of

this book.

Some VPN service providers enable you to choose the type of VPN that is used. In other cases, the service provider handles any technology selection, setup, and maintenance. Figure 2-1 shows an advertisement for TunnelBear, which is an example of a VPN service provider. A TunnelBear customer does not have to maintain hardware or deal with complicated VPN configuration. TunnelBear provides the VPN service and is responsible for all backend requirements.

Figure 2-1 An Advertisement for the TunnelBear VPN Service

This book focuses on VPN technologies that you configure and maintain. The Secure Solutions with Virtual Private Networks exam (SVPN 300-730 exam) covers VPN technologies and requires you to understand how to design and configure these technologies.

This brings us to the next level of grouping we use in this book to further define the types of available VPN technologies to organizations. There are two main categories:

- *Remote access VPNs*: Remote users or devices use these VPNs to connect to a network.
- *Site-to-site VPNs*: These VPNs provide connections between one or more networks.

Chapters 3 through 6 focus on site-to-site VPN technology, and Chapters 7 through 10 focus on remote access VPN. You will find that many concepts covered apply to both types of VPN technology, and we narrow down such repetitive data once a topic is covered. We also include technology that falls within these categories but is not part of the SVPN exam based on what is used in organizations around the world. The focus of this book is to pass the SVPN exam; however, we also want to provide real-world VPN concepts that extend beyond the exam to help you be a well-rounded VPN professional. We identify when material is not on the current version of the SVPN exam, but know that the SVPN learning objectives can change.

Remote Access VPNs

A remote access VPN provides access to devices outside of a trusted network. For example, remote users leveraging specific endpoint devices such as laptops, tablets, and smartphones and requiring access to the inside corporate network would use a remote access VPN. Essentially, a remote access VPN enables a computer to connect to a secured network from an untrusted network. For example, an employee using a coffee shop's unsecured network can use a remote access VPN to transfer information between her laptop and her company's internal network.

Remote Access VPN Use Cases

There are dozens of use cases for remote access VPNs. One very common use case for a remote access VPN is allowing external users to access resources that are available only in a secured environment. Say that a traveling salesperson needs to update confidential sales records that are accessible only when an employee is connected to the internal network. A remote access VPN can allow that salesperson to perform work and can limit the person's access to only his business needs. This book covers many of the options for building remote access VPNs. Figure 2-2 shows a basic design of a remote access VPN architecture.

Figure 2-2 Generic Remote Access VPN

Another use case for a remote access VPN is allowing a user to browse the Internet while maintaining privacy, with all traffic leaving the host encrypted through a VPN tunnel. Imagine that our traveling salesperson goes to a coffee shop and uses the coffee shop network to connect to his company's internal network to modify the secret business records. Even if a device such as a Wi-Fi Pineapple (refer to Chapter 1, "Implementing Secure Solutions with Virtual Private Networks SVPN 300-730 Exam") were able to perform a man-in-the-middle attack and capture the traffic between the traveling salesperson and the corporate network, all that traffic would be encrypted, keeping the salesperson's session secured.

A remote access VPN can also be used in other scenarios, such as to bypass

local security controls. For example, countries like China strictly filter certain types of websites, such as Facebook. A user in China who attempts to access Facebook will be blocked by filtering technology deployed by the Chinese government. That user could use a remote access VPN to bypass the Chinese filtering and access a system outside the Chinese network and connect to Facebook. For example, a traveling salesperson could go to China and use a VPN to connect to his U.S.-based organization. He would be able to access Facebook through the VPN tunnel.

Note

We do not recommend or encourage any behavior that could be considered illegal, including bypassing local security solutions by using a VPN.

You will be expected to know some specific remote access VPN topics to pass the SVPN 300-730 exam. For example, you need to understand client-based VPNs using Cisco AnyConnect with both IKEv2 and Secure Sockets Layer (SSL), clientless VPNs, and FlexVPN. You need to understand how to configure these technologies by using certain Cisco tools, such as the Cisco Adaptive Security Appliance (ASA) configured through the Cisco Adaptive Secure Device Manager (ASDM). This book covers these topics and more.

Site-to-Site VPNs

A site-to-site VPN connects different locations over untrusted networks. The goal is typically to give multiple users or devices at one location access to resources at another location. For example, imagine an organization that has several offices and needs to share data between each location while maintaining security.

Hub-and-Spoke Design

There are three basic designs for a site-to-site VPN. The first design is a hub-and-spoke design, in which one location, such as the main headquarters, acts as the hub and connects to multiple branch offices, which are the spokes. For

this VPN design, a separate VPN tunnel is established between the hub and each individual remote office. Spoke offices can communicate with other spoke offices only if traffic travels through the headquarters hub location. Figure 2-3 shows a basic example of a hub-and-spoke VPN.

Figure 2-3 Generic Hub-and-Spoke VPN

Spoke-to-Spoke Design

Another site-to-site VPN design option is a spoke-to-spoke VPN architecture, in which two devices communicate directly with each other. Either site can initiate a connection, as long as connectivity can be established between the locations. Figure 2-4 shows the hub-and-spoke design from Figure 2-3 with spoke-to-spoke connections added between the branch offices as well as the remote office. Essentially, Figure 2-4 shows a hybrid of a hub-and-spoke architecture for communication with HQ and a spoke-to-spoke architecture used between the smaller locations.

Figure 2-4 Hub-and-Spoke VPN with Spoke-to-Spoke Connections

Full Mesh Design

Another site-to-site VPN architecture is a full mesh. In a *full mesh* architecture, every VPN device in the network communicates with every other VPN device by using a unique VPN tunnel. This means every VPN device has a direct peer relationship with all other VPN devices. This enables smooth communication because a bottleneck can't form at a single VPN gateway; it also reduces overhead because a gateway does not have to handle all the encryption and decryption. The full mesh approach is ideal when multiple peers need to communicate with each other and resources are available to support this approach. A full mesh is the most reliable type of VPN and includes the most redundancy.

Hybrid Design

In the example shown in Figure 2-4, all locations except one have a VPN connection established between the remote location and a branch office. Figure 2-5 shows that missing connection added, so every location has a VPN tunnel to every other location. As you can see, this is the most ideal architecture from a redundancy viewpoint; however, it might not be possible due to the cost and upkeep required to maintain this type of VPN architecture. As discussed later in this chapter, technologies such as DMVPN, FlexVPN, and GETVPN can simplify the deployment of full mesh connectivity.

Figure 2-5 Generic Full Mesh VPN

As you have seen in the previous examples, site-to-site VPN architectures can be combined to form hybrid designs. In a partial mesh architecture, some devices use the full mesh approach, and other devices use a hub-and-spoke or a spoke-to-spoke design. A partial mesh does not provide the same level of redundancy as a full mesh but can be less expensive to implement. An organization may use a partial mesh approach when it has deployed a full mesh between branch locations and wants to add a less important network such as a small office.

Tiered Hub-and-Spoke Design

Another hybrid site-to-site architecture is a tiered hub-and-spoke architecture, which connects different hub-and-spoke networks together. In this design, traffic is permitted from the spoke or hub groups to their most immediate hub, depending on how VPN connections are established. An example could be two different organization networks that need to connect to a single headquarters due to a recent acquisition. The headquarters would represent the first tier of this design, and the main branch offices would be the second tier. The branch offices could also be connected with each other; however, networks that are spokes off each branch office could be designed in a hub-and-spoke architecture, and those spokes would be the third tier. Figure 2-6

shows an example of this approach.

Figure 2-6 Hybrid Site-to-Site VPN Design

The SVPN 300-730 exam requires you to know about some specific site-to-site VPN topics. For example, you need to understand and know how to deploy and troubleshoot GETVPN, DMVPN, and FlexVPN, which can be configured over a hub-and-spoke or spoke-to-spoke network and can leverage IPv4 or IPv6. This book covers these and other site-to-site VPN topics you need to know for the exam.

The best way to choose a VPN architecture is to validate the requirements of the VPN being considered, such as required equipment, the cost of the solution, supported protocols, the expected version of software that will be needed for the project to be successful, and, most importantly, the desired outcome.

VPN Technology Components

The type of VPN you plan to use may depend on the available physical or virtual technology. VPN components can include the system providing the VPN service and, sometimes, software such as a client that is used to establish a VPN connection when a remote access VPN is being used. With a

clientless remote access design, a client is not required for the remote access VPN.

Hardware VPN Support

When it comes to hardware supporting VPN capabilities, routers commonly support site-to-site VPN capabilities, and security-focused tools tend to support remote access VPN capabilities. Customers often desire unified products—that is, multifunctional tools—and hybrid technology is becoming popular to provide everything from security and remote access VPN capabilities to networking and site-to-site VPN capabilities, all on the same appliance. Hybrid technology offering both remote access and site-to-site VPN capabilities is most commonly used in small business solutions. Larger enterprise technology tends to provide either routing and site-to-site VPN capabilities or security defense capabilities along with remote access VPN options. We look at these technology trends in more detail shortly.

The SVPN 300-730 exam focuses on technologies you need to know. The general concepts involved in setting up, troubleshooting, and maintaining a VPN are vendor agnostic. As long as you understand the technology, the protocols used, and how things are supposed to work, you should be able to build a VPN on most vendor or open-source platforms. The following sections look at different categories of technology that can offer VPN capabilities, beginning with routers. You will not be required to know the models of Cisco technology being used in the SVPN exam; however, you will be required to know how to work with such technology.

Routers

By definition, a router is a network device that forwards data packets between computer networks. Over time, routers have become a lot more capable, offering various features ranging from voice to security capabilities. In regard to security capabilities expected from a router, supporting site-to-site VPN functionality is always at the top of the list. It is common for routers to send traffic across untrusted networks, prompting concerns about loss of confidently and integrity of any data that is sent. To address data compromise concerns, a site-to-site VPN encrypts traffic between routers.

Router VPN Use Cases

Routers can be used for remote access VPN services, but they are more commonly used with site-to-site VPNs. Routers used in homes and small offices more commonly offer remote access capabilities than do routers used for larger enterprises and service providers. A smaller location with limited space for equipment and a relatively small budget is likely to want a single solution that provides a range of network and security needs. A smaller router may be used to connect back to the enterprise using a site-to-site connection while also enabling users who are away from their home office to connect back to the home router; in such a case, the router may also send remote access traffic to the larger enterprise through a site-to-site VPN connection. Such solutions work in smaller environments but can't scale to larger networks. Therefore, a larger office may use enterprise routers for site-to-site VPN services and leverage separate security appliances or other dedicated solutions for remote access VPN services. In general, the remote access VPN capabilities on security appliances are more feature rich than on routers.

For the SVPN 300-730 exam, you need to know how to work with a few Cisco router models. Cisco IOS and IOS XE software includes both IP Security (IPsec) and Transport Layer Security (TLS) encryption technologies within the following routing platforms that you should be familiar with for the exam:

- Cisco ISR (Integrated Services Router) for branch offices
- Cisco ASR (Aggregation Services Router) 1000 Series for data centers and other headend locations
- Cisco CSR (Cloud Services Router) 1000V Series

Note

The specifics of how to configure a VPN vary for different Cisco technologies. For the SVPN 300-730 exam, you do not need to memorize the management GUI layout for each Cisco product. You do need to know how to configure, maintain, and troubleshoot VPN technology, and the same

concepts apply across multiple Cisco technologies. We highly recommend focusing on what and why each step is being performed when configuring a VPN rather than on where steps are located within a specific Cisco product management GUI for the SVPN 300-730 exam.

Router VPN Capabilities

Our focus in this book is on the VPN capabilities of routers. Most Cisco routers support Group Encrypted Transport VPN (GETVPN), Dynamic Multipoint VPN (DMVPN), GRE-based VPN (also known as Point-to-Point VPN), and standards-based IPsec VPN for site-to-site VPNs. Some models support both IPsec and SSLVPN for remote access, and others do not. SSL support depends on the version of code and licenses being used.

Cisco ISR Series routers come in many shapes and sizes and are the go-to option for branch offices. As their name indicates, these routers offer many services, including WAN connectivity, software-defined networking (SD-WAN), NetFlow export, security monitoring, and Wi-Fi access. While smaller options such as Cisco ISR routers offer remote access VPN capabilities, larger branch option routers such as the ASR 1000 Series do not. The ASR 1000 targets the data center and large enterprise market and does not offer remote access VPN capabilities. The performance of a router depends on the model, platform, and the services enabled.

The following list provides a quick summary of Cisco routers that offer VPN capabilities:

Note

Learn more about Cisco branch routers at https://www.cisco.com/c/en/us/products/routers/branch-routers/index.html.

- **Cisco ISR 4000 Series:** This series of routers is designed for large enterprise branch offices. They do not support SSLVPN.

- **Cisco ISR 1000 Series:** This series of routers targets small to medium-size businesses. They can support SSLVPN for remote access if the right license is enabled.

- **Cisco ISR 900 Series:** These routers are designed for small and home offices. They can support SSLVPN for remote access if the right license is enabled.

- **Cisco ISR 800 Series:** The 800 series targets small to medium size businesses looking for routing, voice, video, security, application performance, wireless and cloud connection all in one solution. These routers can support SSLVPN for remote access if the right license is enabled.

- **Cisco 5000 Enterprise Network Compute System Series:** This series of router is designed to be a hybrid platform including a traditional router sand server with small infrastructure footprint. They do not support SSLVPN.

- **ASR 1000 Series:** These routers are designed to sit at the edge of a data center or large office connecting to a WAN; they can also be used as service provider points of presence (POPs). This series can provide SD-WAN with encryption and traffic management at 2.5 to 200 Gbps. For remote VPN support, IKEv2 can be used; SSL-based remote access is not supported.

- **Cisco CSR Series:** The Cisco CSR is a virtual-form-factor router that delivers WAN gateway and network services functions in virtual and cloud environments. Features offered include routing, firewall, Network Address Translation (NAT), QoS, application visibility, failover, WAN optimization, and VPN capabilities. The CSR Series supports both SSL and IKEv2 for remote access VPNs.

Note

The SVPN 300-730 exam will not test you on the physical components of a Cisco router.

Security Appliances

A security appliance can be dedicated to a specific capability (for example, a firewall) or offer multiple capabilities (for example, a firewall and VPN in one solution). The combination of capabilities in a security appliance has led to many industry terms, such as *unified threat management (UTM)* and *next-generation (NG)*. We address the history of the term *next generation* shortly, but first we step back and look at the Cisco history of offering VPN technology in security appliances.

History of Cisco VPN Technology

Cisco first offered VPN capabilities in appliances around the year 2000, when Cisco acquired Altiga Networks. This acquisition led to the Cisco VPN 5000 and Cisco VPN 3000 Series. The 5000 Series appliances were eliminated in 2002, however, and the VPN 3000 became the industry standard for remote access VPN requirements. The VPN 3000 Series was so successful that it led to the creation of the industry-recognized SSLVPN category, which any competitor would have to support if they wanted to have a chance at winning remote access VPN business. Around 2005, Cisco found that many customers that were looking for remote access VPN capabilities where also interested in acquiring firewall appliances. In response to customer demand, Cisco released the Cisco ASA (Adaptative Security Appliance) Series, which provided a hybrid solution including Cisco PIX firewall and VPN 3000 features. When the ASA product line had been on the market for some time, Cisco announced end of sale for all PIX and VPN 3000 products.

Note

The SVPN 300-730 exam does not cover the VPN 3000 product line as it is no longer sold.

Over time, Cisco has increased its focus on security through acquisitions of companies like Sourcefire and Meraki, and these acquisitions have impacted the VPN offerings in Cisco security products. At the time of this publication, the Cisco security-focused product lines that provide VPN capabilities are the ASA Series, Meraki security appliances, and Cisco Secure Firewall offerings. For the SVPN 300-730 exam, you need to understand how to configure various VPN features using either a Cisco router or Cisco ASA, even though options such as Cisco Secure Firewall can run similar VPN configurations. This book provides examples of both ASA and Cisco Secure Firewall and Meraki options to prepare you for both the exam and real-world environments.

Note

The Cisco Secure Firewall can provide various VPN capabilities, depending on the model and software used. We highly recommend monitoring changes in the SVPN 300-730 exam for additional learning requirements targeting the Cisco Secure Firewall appliances.

Note

On the SVPN 300-730 exam, you should expect the remote access VPN questions to be related to the Cisco ASA technology, because routers are not commonly used for remote access VPNs except in smaller environment.

VPN Clients

Another component of some remote access VPN deployments is the client installed on the endpoint, which can be used for IPsec or SSL/TLS. For

example, a remote access IPsec VPN consists of a VPN client and a VPN headend device, commonly called the VPN gateway. The VPN client resides on the user's workstation or mobile device and initiates the VPN tunnel to the remote network via the VPN gateway waiting to accept connections. When a VPN client initiates a connection to the VPN gateway device, negotiation starts with authenticating the user and the user's device. As an example of this negotiation, IPsec uses Internet Key Exchange (IKE) followed by IKE Extended Authentication (Xauth) to perform the negotiation process. For IPsec, after the negotiation completes, a profile is pushed to the client, and a security association is created to complete the connection. For SSL connections, a TLS or DTLS tunnel is established to complete the connection.

The process for an IPsec VPN depends on the protocols used and how the VPN technology is set up. Because SSL/TLS VPNs can be reached by public computers, it can be complicated to keep endpoints protected with these clients. Vendors like Cisco offer various controls to combat this challenge, including integration with network access control (NAC) technology to ensure that devices are safe before permitting VPN connections. In addition, there are remote access VPN options that do not use VPN clients; these options are commonly referred to as clientless. This book covers setup, maintenance, and troubleshooting for both client-oriented and clientless remote access VPN architectures.

Cisco AnyConnect

The Cisco flagship multiple-purpose security client is known as Cisco AnyConnect Secure Mobility Client. This client can be installed on desktop or mobile devices and provides features such as web security, malware defense, phishing protection, command and control blocking, 802.1x supplicant services, and VPN capabilities. AnyConnect was created to be used as a VPN client, but its capabilities have grown, and AnyConnect's deployment base as a multifunctional security endpoint has expanded.

End users can an obtain AnyConnect a number of ways. They can download the AnyConnect software from a web or file server or obtain it from an enterprise software management system. AnyConnect can also be pushed

down from a Cisco ASA appliance, Secure Firewall appliance, or Cisco ISE server. For example, when a workstation attempts to connect to the corporate network, Cisco ISE can be configured with a posture check, which will push AnyConnect to any workstation that does not have AnyConnect installed. Another example would be a workstation connecting to the Cisco ASA appliance over the Internet, with the ASA redirecting users to download AnyConnect as part of establishing a remote access VPN. Figure 2-7 shows an example of a Cisco ASA pushing down the option to download the AnyConnect client.

Figure 2-7 Cisco ASA Offering AnyConnect to an Endpoint

AnyConnect Capabilities

The Cisco AnyConnect core client is included with the default AnyConnect package. Additional modules are also included with the default package, but extra licenses and configuration may be required to enable certain features.

Also, configuration settings such as client profiles can also be included with the AnyConnect software and downloaded as a single package. Alternatively, client profiles can be added as part of the update process after the AnyConnect client is installed and a connection with the VPN gateway is established. We cover specific AnyConnect configuration steps in Chapter 8 and troubleshooting steps in Chapter 10.

Other VPN Clients

A variety of open-source VPN options that are available on the market include VPN gateways and clients. Most modern browsers also include native VPN clients. One example of an open-source VPN option is Openswan, which is an IPsec VPN option for Linux. tcpcrypt is another example that is supported on both Windows and macOS. Cisco equipment supports OpenConnect, which is not officially associated with Cisco. For the SVPN 300-730 exam, you only need to be familiar with the Cisco AnyConnect client.

VPN Protocols

Regardless of whether you use a Cisco or non-Cisco option for your VPN deployment, you need to choose which VPN protocol to leverage. Some hardware and VPN designs have limited options for protocol support, and others give you different options that will impact the performance and level of security obtained from the VPN setup.

There are five different protocol options you can use when choosing how to encrypt traffic with a VPN. It is important to choose a VPN that supports the right protocol for your business needs because the protocol used determines the level of security provided by the VPN. The VPN protocol may also rely on certain ports, which can limit its usability on certain networks that block such ports. Some VPN protocols can leverage port 443, which is used for normal encrypted Internet traffic and allows a VPN to hide within other encrypted traffic to bypass censorship and other filtering enabled on a network security tool such as a firewall. Each protocol’s encryption strength is based on many factors; the more resistant a protocol is to cracking, the lower your risk of data exposure.

Note

We do not condone using a VPN to bypass security when it is illegal or unethical to do so.

A number of popular protocols are available in most commercial VPN solutions. The following sections discuss PPTP, SSTP, SSL/TLS, OpenVPN, L2TP/IPsec, and IKEv2.

Point-to-Point Tunneling Protocol (PPTP)

Point-to-Point Tunneling Protocol (PPTP), which dates back to the late 1990s, was the first VPN protocol widely available to the public. It uses Microsoft Point-to-Point Encryption (MPPE) along with MS-CHAP for authentication. Because PPTP has been around for so many years, many solutions have PPTP built in to their platforms. PPTP is simple to set up and enables a wide range of device support because it doesn't require any additional software. In some situations, such as with legacy platforms, PPTP is the only available protocol. For example, PPTP may be the only protocol option with an older piece of factory equipment. PPTP is very fast compared to other protocol options.

PPTP Pitfalls

If security is crucial, PPTP is not the best protocol choice. Security experts, including Microsoft, have deemed PPTP obsolete due to its vulnerability to various attacks. If you are using PPTP, anybody from a nation-state to a general hacker can snoop on your connections. Two tools available for Kali Linux, thc-pptp-bruter and asleap, can be used to brute-force attack endpoints that use PPTP. Figure 2-8 shows an example of launching a wordlist-based brute-force attack by using thc-pptp-bruter within Kali Linux.

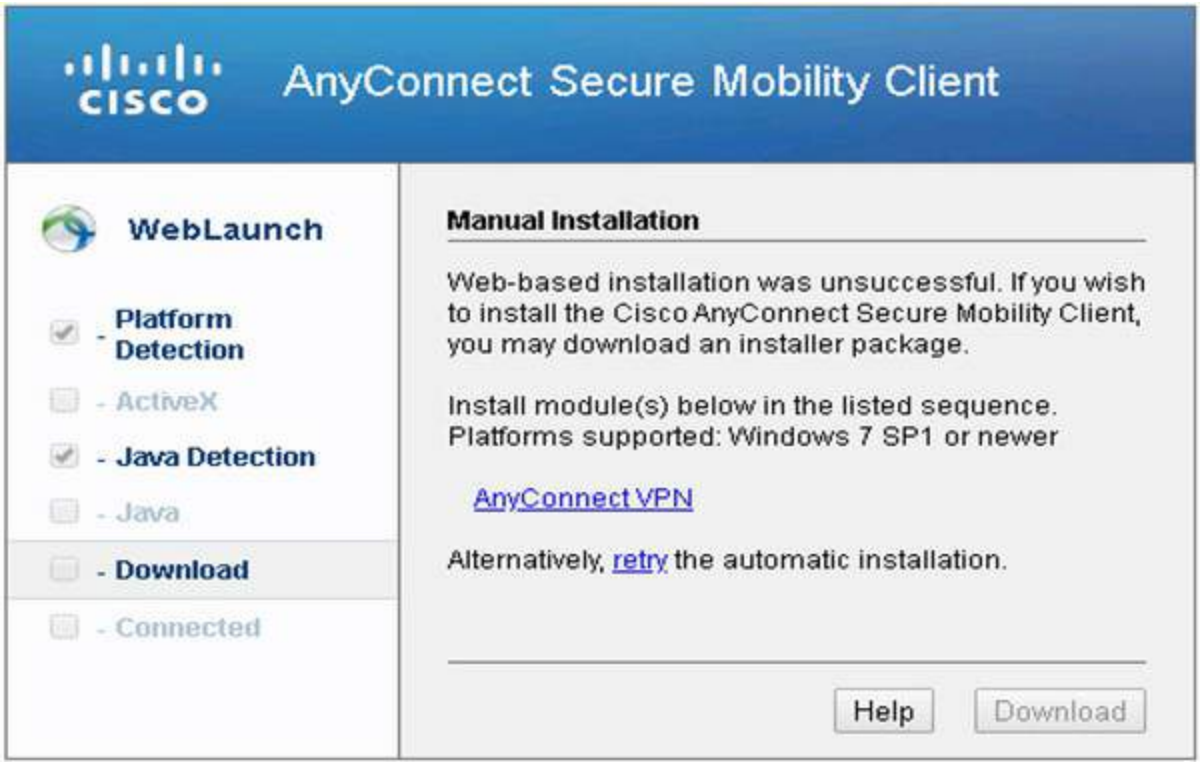


Figure 2-8 Brute-Force Attack Using thc-pptp-bruter

PPTP requires port 1721 and Generic Routing Encapsulation (GRE) protocol, both of which can be blocked by security platforms such as firewalls, so the use of PPTP is limited. PPTP may be fast on a reliable connection. However, with a connection that experiences packet loss, PPTP may generate a massive number of TCP retransmit attempts, dramatically slowing down the experience. In short, PPTP is not recommended.

Secure Socket Tunneling Protocol (SSTP)

Microsoft has provided a new and improved version of PPTP known as *Secure Socket Tunneling Protocol (SSTP)*, which was first available in Windows Vista SP1 in 2008. SSTP uses *Secure Sockets Layer (SSL)* 3.0, which is much better than PPTP and fully integrated into Windows. SSTP is predominantly a Windows-based VPN protocol but has also been used on other operating systems from time to time. SSTP overcomes the dependencies on port 1721 by using TCP port 443, so local security tools are not likely to prevent it. One issue with SSTP is that it relies on SSL 3.0,

which has been deprecated by the Internet Engineering Task Force (ITF) due to its vulnerability to POODLE attacks. Unless Microsoft changes SSTP so it does not rely on SSL 3.0, SSTP is not recommended.

Note

Learn more about a POODLE attack on SSL 3.0 at https://www.us-cert.gov/ncas/alerts/TA14-290A.

SSL/TLS

These protocols leverage web browsers or client applications to provide secure remote access VPN capabilities. For the purposes of SSLVPNs, SSL has been replaced by its successor, Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS). Modern SSLVPNs rely on the TLS protocol to encrypt and authenticate data. One major advantage to SSLVPNs is their capability to use TCP 443 for the transmission of data. Because TCP 443 is commonly allowed by networks, users are more likely to be successful connecting with an SSLVPN client over TCP 443 than with a VPN client using IPsec. This is one of the major reasons, along with many other reasons that will be covered later in this book, that SSLVPNs are the primary method for connecting to Cisco ASA firewalls. You can expect to see a large number of SSLVPN questions on the SVPN 300-730 exam.

IPsec with IKE

Internet Key Exchange (IKE) is a deprecated protocol used to set up security associations in the IPsec protocol suite. IKE uses pre-shared or X.509 certificates for authentication and leverages Diffie-Hellman key exchange to set up a shared session secret from which cryptographic keys are created. Diffie-Hellman groups such as 1, 2, 5, 22, 23, and 24 are also considered deprecated algorithms.

IKEv1 was deprecated for a number of reasons. Due to their age, systems

supporting IKEv1 are much more likely to contain implementation vulnerabilities that will never be patched. Second, due to vulnerabilities in IKEv1, systems supporting IKEv1 can be used for packet amplification attacks. Finally, IKEv1 systems are likely to have been configure for the weak Diffie-Hellman Groups 2 and 5 and are likely not capable of supporting modern algorithms to secure data communications, such as AES-GCM. No new improvements have been made to IKEv1 in more than a decade since the industry has pointed all IKE deployments to use Version 2. Nonetheless, the protocol is still widely deployed, so you need to understand it.

IPsec with IKEv2

Internet Key Exchange Version 2 (IKEv2) was developed through a partnership between Microsoft and Cisco, with the goal of developing a secure and flexible tunneling protocol option. By itself, IKEv2 is just a negotiation protocol. However, it can be paired with IPsec encryption to provide security capabilities for VPN connections. IKEv2 is popular because it is available in any Windows platform from Windows 7 on, as well as in mobile platforms such as Apple iOS and Blackberry. In addition, open-source versions of IKEv2 are supported by platforms like Linux and Android.

One huge benefit of IKEv2 is its stability. It supports Mobility and Multihoming Protocol (MOBIKE), which makes quick reconnections possible when switching between different connections. This is ideal for people who travel often and for mobile devices. IKEv2 is a reliable alternative to OpenVPN due to its dependability and availability in many Windows and mobile platforms. We recommend using IKEv2 if it is available, and you need to understand this protocol for the SVPN 300-730 exam.

Easy VPN

Easy VPN (EzVPN) is an IPsec VPN option supported on older Cisco routers and security appliances that uses the Unity client protocol, which allows many IPsec VPN parameters to be defined at an IPsec gateway, which can also be the EzVPN server. EzVPN simplifies VPN deployments by having

security polices defined at the headend (that is, the EzVPN server) and pushed to remote VPN devices. This practice ensures that clients have up-to-date policies in place before establishing VPN connections. EzVPN simplifies VPN deployment for remote offices and mobile employees. Newer Cisco routers such as the ISR 1000 Series do not support EzVPN; only the ASA 5505 supports EzVPN. IKEv2 is preferred over EzVPN for new deployments.

L2TP

Layer 2 Tunneling Protocol (L2TP) was released at around the same time as PPTP. Like PPTP, L2TP is widely available and can run on most major platforms. L2TP is a tunneling protocol that doesn't provide any encryption. It is almost always paired with IPsec for encryption, so when you hear somebody mention L2TP or IPsec for a VPN, it is likely a combination of L2TP and IPsec. L2TP also uses AES ciphers; 3DES ciphers are no longer recommended as a collision attack has proven them obsolete.

Note

This article from threatpost provides details on a collision attack against 3DES: https://threatpost.com/new-collision-attacks-against-3des-blowfish-allow-for-cookie-decryption/120087/.

L2TP has similar limitations to PPTP in that it requires certain ports—such as UDP 500 and UDP 4500—to be open. If a security tool such as a firewall filters these ports, L2TP will not work. Over time, L2TP has fallen out of favor due to rumors that well-funded security agencies can exploit the protocol. So while there is no proof that L2TP has been compromised, many people avoid it for this reason. L2TP may be an option for casual use; however, there are better options, such as OpenVPN and IKEv2.

VPN Protocol Comparison

After reviewing the VPN protocols, you should come to the following conclusions:

- Avoid using PPTP and SSTP whenever possible.
- SSL/TLS is a good option for reliable connectivity. Most AnyConnect deployments today use SSLVPN.
- EzVPN is an option for ensuring that the latest updates are pushed to remote systems and providing simplicity in deploying a VPN to remote devices and offices; however, it is being phased out, and IKEv2 is a better option.
- IKEv2 is a strong option for VPNs; however, in some cases, IKEv1 may be the only supported option.
- L2TP can work if it is properly set up, but it is not recommended if IKEv2 or SSL/TLS is available.

We look more closely at each of these protocols as we review the configurations of various VPN options. Know that some VPN options offer only one protocol, whereas others offer multiple protocol options. We recommend not using a VPN option that supports only one protocol unless that protocol is OpenVPN or IKEv2.

Cisco VPN Portfolio

The SVPN 300-730 exam focuses on VPN options supported in Cisco solutions. For the exam, you need to know VPN options such as DMVPN, GETVPN, FlexVPN, and SSLVPN. The following sections quickly review each of these options. You will learn a lot more about each of these topics later in this book.

DMVPN

Dynamic Multipoint VPN (DMVPN) is a Cisco IOS software solution for building scalable IPsec VPNs (that is, router-based site-to-site VPNs).

DMVPN uses multipoint Generic Routing Encapsulation (mGRE) for overlay and IKEv1 or IKEv2 for authentication and key exchange. DMVPN is supported on both IPv4 and IPv6 (that is, it can be dual-stacked) and allows hub-to-spoke as well as on-demand spoke-to-spoke communication. DMVPN enables a branch to communicate with other branches over a public WAN or the Internet but doesn't require a permanent VPN connection between sites.

DMVPN Use Cases

One popular use case for DMVPN is for deploying voice and/or video across different networks over a DMVPN connection. Another common use case is for connecting many branch offices over a public network such as the Internet or a private network using MPLS. DMVPN is known for its zero-touch configuration, which translates to reduced complexity in deploying and supporting site-to-site requirements. Another common use case for DMVPN is to provide resiliency for applications based on DMVPN by incorporating routing with standards-based IPsec technology. We dive into DMVPN in detail in Chapter 5.

Group Encrypted Transport VPN (GETVPN)

Group Encrypted Transport VPN (GETVPN) is a tunnel-less VPN solution that provides highly secure communication between systems that are grouped together in a network. GETVPN addresses some of the limitations of DMVPN. For example, DMVPN supports direct spoke-to-spoke traffic, but when a spoke wants to send traffic to another spoke, it first must create a new IPsec security association, which can take time and cause delays. GETVPN solves the scalability issue by using a single IPsec security association for all routers in a group rather than using individual security associations. GETVPN also supports multicast traffic natively, without using GRE, whereas other options have to use GRE for encapsulation. GETVPN is ideal for private networks like MPLS VPNs. We look more closely at GETVPN in Chapter 4. In addition, Chapter 3 covers more details about security associations.

FlexVPN

Unlike DMVPN and GETVPN, *FlexVPN* is an IPsec-based VPN technology used on Cisco IOS devices that can support different site-to-site or remote access VPN options. FlexVPN is based on IKEv2 for origin authentication and key exchange; unlike DMVPN, FlexVPN does not support IKEv1. FlexVPN uses a centralized policy management infrastructure with the RADIUS framework. FlexVPN supports both IPv4 and IPv6 for transport and overlay protocols, and these concepts are likely to be on the SVPN exam. FlexVPN is newer than DMVPN, and we look more closely at FlexVPN in Chapter 6.

SSLVPN

SSLVPN is a remote access encryption solution that uses Transport Layer Security (TLS) to protect data communication between a software client (such as AnyConnect) and a corporate network. SSL/TLS functions are ubiquitous in modern web browsers. This means that, unlike with IPsec (which is a client-based VPN technology), SSL can provide remote access VPN capabilities without having a client installed (that is, it is a clientless VPN solution) or can use a combination of client and web services to provide VPN capabilities. SSLVPNs are commonly called web VPNs, based on the use of the client's web browser.

SSLVPN Use Cases

There are popular use cases for SSLVPNs. One huge advantage of using SSL is its ease of use for end users. Client-based VPN options such as IPsec are likely to have different implementation and configuration requirements, whereas SSL just requires a modern web browser but could also use a client such as AnyConnect. Because SSL runs over the standard HTTPs port, it isn't blocked by security tools such as firewalls. Variations of SSLVPNs can overcome some security risks. For example, it is possible to validate that a system being permitted an SSLVPN connection is authorized for that connection and allowing only authorized devices while denying authorized users attempting to connect to an SSLVPN with a personal computer. This book covers different SSL architectures and SSL features available in Cisco products. It also compares SSL client VPNs with SSL clientless VPNs to help you decide when to use either approach when considering SSL as a VPN

approach.

Site-to-Site VPN Comparison

Table 2-2 compares a number of different site-to-site VPN options. This table summarizes the benefits of each option, when it makes sense to use each VPN option, which systems support each VPN option, how well the options can scale, management options, and topology options. The table also addresses routing options, QoS options, multicast support, non-IP protocol support, private IP address support, and high availability options. You should know these data points for the SVPN 300-730 exam.

Table 2-2 Comparison of Site-to-Site VPN Options

	GETVPN	DMVPN	GRE-Based VPN	Easy VPN	Standard IPsec VPN
		Tunnel-less VPN		Tunnel-Based VPN	
Benefits	• Simplifies encryption integration on IP and Multiprotocol Label Switching (MPLS) WANs • Simplifies encryption management through use of "group keying" instead of point-to-point key pairs • Enables scalable and manageable any-to-any connectivity between sites • Supports QoS, multicasting, and routing	• Simplifies encryption of configuration and management for point-to-point GRE tunnels • Supports QoS, multicasting, and routing	• Enable transport of multicasting and routing traffic across an IPsec VPN • Support non-IP protocols • Supports QoS	• Simplifies IPsec and remote site device management through dynamic configuration policy push • Supports QoS	• Provides encryption between sites • Supports QoS
When to Use	• Use when adding encryption to MPLS or IP WANs while preserving any-to-any connectivity and networking features • Use with other scalable, full-time meshing for IPsec VPNS • Use to enable participation of smaller routers in meshed networks • Use to simplify encryption key management while supporting routing, QoS, and multicasting	• Use to simplify configuration for hub-and-spoke VPNs and support routing, QoS, and multicasting • Use to provide low-scale, on-demand meshing	• Use when routing must be supported across a VPN • Use for the same functions as hub-and-spoke DMVPN but with a more detailed configuration	• Use to simplify a VPN overall • Use when configuration and management are the primary goal and only limited networking features are required • Use to provide a simple, unified configuration framework for a mix of Cisco VPN products	• Use when multivendor interoperability is required
Interoperability	Cisco routers only	Cisco routers only	Cisco routers only	Cisco ASA 5500 Series, Cisco VPN 3000 Series, and Cisco PIX firewall	Multivendor
Scale	Thousands	Thousands with hub-and-spoke; hundreds with partially meshed spoke-to-spoke connections	Thousands	Thousands	Thousands
Provisioning and Management	CLI and Cisco Security Manager	Cisco Security Manager and Cisco Router and Security Device Manager	Cisco Security Manager and Cisco Router and Security Device Manager	Configuration automatically pushed to remote sites from headend; headend policies defined in Cisco Security Manager or Cisco Router and Security Device Manager	Cisco Security Manager and Cisco Router and Security Device Manager
Topology	Hub-and-spoke; any-to-any	Hub-and-spoke; on-demand spoke-to-spoke partial mesh; spoke-to-spoke connections automatically terminated when no traffic present	Hub-and-spoke; small-scale meshing as manageability allows	Hub-and-spoke	Hub-and-spoke; small-scale meshing as manageability allows
Routing	Supported; Cisco GETVPN any-to-any connectivity capability can also be used to provide secure routing across an entire router backbone	Supported	Supported	Not Supported	Not Supported
QoS	Supported	Supported	Supported	Supported but QoS policy is not dynamically pushed to remote sites	Supported
Multicast	Natively supported across MPLS and private IP networks, tunneled across Internet-based WANs	Tunneled	Tunneled	Not supported	Not supported
Non-IP Protocols	Not supported	Not supported	Supported	Not supported	Not supported
Private IP Addressing	Requires use of GRE or DMVPN with Cisco GETVPN to support private addresses across public Internet backbones	Supported	Supported	Supported	Supported
High Availability	Routing	Routing	Routing	Stateless failover	Stateless failover

Network Design	DMVPN (mGRE)	GETVPN (tunnel-less)	SSLVPN (TLS)	FlexVPN (DVTI, IKEv2)	EasyVPN (dynamic Crypto Map/DVTI, IKEv1)	Static IPsec (Crypto Map, SVTI, IPsec/GRE)
Remote access (software client)						
Hub-and-spoke only (hardware client)						
Hub-and-spoke with spoke-and-spoke						

Table 2-3 compares some of the other VPN topics covered in this chapter, including remote access VPN options. We recommend being familiar with these topics before moving on to other chapters in this book.

Table 2-3 Comparing VPN Options

Network Design	DMVPN (mGRE)	GETVPN (tunnel-less)	SSLVPN (TLS)	FlexVPN (DVTI, IKEv2)	EasyVPN (dynamic Crypto Map/DVTI, IKEv1)	Static IPsec (Crypto Map, SVTI, IPsec/GRE)
Remote access (software client)	N/A	N/A	Supported	Supported	Not supported	N/A
Hub-and-spoke only (hardware client)	Supported	N/A	N/A	Supported	Not supported	Not supported
Hub-and-spoke with spoke-and-spoke	Dynamic mesh supported	Any to any (full-mesh) supported	N/A	Not supported	N/A	Not supported

Network Design	DMVPN (mGRE)	GETVPN (tunnel-less)	SSLVPN (TLS)	FlexVPN (DVTI, IKEv2)	EasyVPN (dynamic Crypto Map/DVTI, IKEv1)	Static IPsec (Crypto Map, SVTI, IPsec/GRE)
Remote access (software client)	N/A	N/A	Supported	Supported	Not supported	N/A
Hub-and-spoke only (hardware client)	Supported	N/A	N/A	Supported	Not supported	Not supported
Hub-and-spoke with spoke-and-spoke	Dynamic mesh supported	Any to any (full-mesh) supported	N/A	Not supported	N/A	Not supported

Cisco ASA Licensing

The Cisco ASA product line has been on the market since 2005. Over the years, there have been changes to the hardware and license structures, which impact what type and how many site-to-site VPN sessions can be supported. Cisco ASA appliances offer different variations of licenses, including permanent and time-based licenses. A permanent license, which applies only to the appliance on which the license is installed, never expires. Such a license typically applies a permanent activation key, and an ASA can have only one key installed at any given time. If new desired features are needed for a permanent license, a new activation key needs to be created for those

features.

You can see the current activation key by using the command **show** *activation-key*, which provides information like the following:

```
Running Permanent Activation Key: 0x00000000 0x00000000
0x00000000
0x00000000 0x00000000
```

Time-Based License

The time-based license functions shown in this example are valid for only a specific time. You can install one or more time-based activation keys, but only one key can apply to one feature. This means you can install multiple time-based keys as long as each key applies to a different feature. When a time-based key is within 30 days of expiration, the ASA generates daily system log messages alerting you of the situation. If a license expires, certain features may be deactivated or features may be reduced. A license's expiration log looks like this:

```
%ASA-4-444005: Timebased license key 0x8c9911ff 0x715d6ce9
0x590258cb


0xc74c922b 0x17fc9a will expire in 29 days.
```

Note

With Cisco ASA Version 8.3(1) and later, time-based key expiration does not depend on the configured system time and date. The license countdown automatically occurs based on the actual uptime of the ASA. This is ideal if an ASA isn't used for a period of time because it means you won't lose license time if the ASA is not being used.

Licensing Options

The number of licenses required for an ASA deployment depends on the type

of license being used. Cisco ASA appliances used to use a Base, Security Plus, and Premium option format but licensing has been simplified into two tiers. The first tier is AnyConnect Plus, which includes basic VPN services such as device and per-application VPN, trusted network detection, basic device context collection, and Federal Information Processing Standards (FIPS) compliance. The second tier is AnyConnect Apex Licensing, which includes everything in Plus as well as more advanced services such as endpoint posture checks, network visibility, next-generation VPN encryption, and clientless remote access VPN. Table 2-4 highlights a comparison between AnyConnect Plus and Apex licensing. We cover licensing in more detail in Chapter 8.

Table 2-4 AnyConnect Plus and Apex License Feature Comparison

Plus License	Apex License
Device or system VPN (including Cisco phone VPN)	All Plus features plus the other features in this column
Third-party IPsec IKEv2 remote access VPN clients (non-AnyConnect client)	Network Visibility Module (new in 4.2)
Per-application VPN	Unified endpoint compliance and remediation (posture) (Identity Services Engine Apex is required and licensed separately)
Cloud Web Security and Web Security Appliance	Suite B or next-generation encryption (including third-party IPsec IKEv2 remote VPN clients)
Cisco Umbrella Roaming (Umbrella Roaming services are licensed separately)	Clientless (browser-based) VPN connectivity
Network Access Manager	ASA multicontext-mode remote access
Cisco AMP for Endpoints Enabler (AMP for Endpoints is licensed separately)	SAML authentication (new in 4.4 and requires ASA 9.7.1 or later)

Managing Licensing

Note

Learn more about ASA and Secure Firewall licensing at

https://www.cisco.com/c/en/us/td/docs/security/asa/roadmap/licenseroadmap.html.

One final ASA license concept to cover is how licenses are managed. The traditional method for applying licenses is by obtaining license keys from Cisco or authorized resellers and applying those keys to the associated ASA by using the command line or a GUI management platform. The license file that you obtain is called a product authorization key (PAK) license. Cisco also offers smart software licensing for certain models, such as the ASAv, ASA on Secure Firewall, and Secure Firewall appliances; this type of licensing enables you to manage a pool of licenses centrally. Smart licensing does not require a PAK, which also means licenses are not bound to an ASA serial number. Smart licensing simplifies the processes of deploying and retiring ASAs without requiring management of each unit's license key.

Note

Learn more about Cisco smart licensing at https://www.cisco.com/c/en/us/products/software/smart-accounts/software-licensing.html.

Cisco Secure Firewall Series for Site-to-Site VPNs

In addition to the ASA Series, two other Cisco security product lines offer site-to-site VPN capabilities: the Cisco Secure Firewall Series and Meraki. As with the ASA Series, there are different Secure Firewall series hardware models that offer different amounts of VPN session support as you increase in appliance size. Licensing for the Cisco Secure Firewall Series is similar to licensing for the ASA Series in that there is the classic approach of installing a PAK file or using Cisco smart licensing. The good news for site-to-site VPN support on a Cisco Secure Firewall solution is that the Cisco Secure Firewall Series does not require additional licenses; basic Cisco Secure Firewall licensing provides support for site-to-site VPN capabilities.

Cisco Secure Firewall Limitations

There are limitations to the VPN features offered on a Cisco Secure Firewall Series solution for a site-to-site VPN. The following options were available as of the time of this publication:

- Both IPsec IKEv1 and IKEv2 are supported.
- Certificates and automatic or manual pre-shared keys for authentication are supported.
- IPv4 and IPv6 are supported.
- Static and dynamic interfaces are supported.
- The VPN alerts when the tunnel goes down.
- Point-to-point (PTP), hub-and-spoke, and full mesh deployments are available.
- Network objects with a range option are not supported in a VPN.
- Cisco Secure Firewall VPNs are only backed up using the Cisco Secure Firewall Management Center backup options.
- There is not a per-tunnel or per-device edit option for Cisco Secure Firewall VPNs; only the whole topology can be edited at the time of publication.
- Cisco Secure Firewall VPNs are not supported in a clustered environment at the time of this publication.
- VPN tunnel status is not updated in real time but at an interval of 5 minutes in the Cisco Secure Firewall Management Center at the time of this publication.
- Transparent mode is not supported. Only tunnel mode is supported.

The Cisco Secure Firewall Series product line is continuously being updated. We highly recommend that you validate the current data sheet associated with the Cisco Secure Firewall model you are considering for your site-to-site

VPN project to ensure that all required features and licenses are obtained. We talk more about Cisco Secure Firewall in Chapter 7. Know that Cisco Secure Firewall is not part of the current version of the SVPN learning objectives, but that could change with a future version of the exam.

Cisco Meraki Licensing

The last security appliance option in the Cisco catalog that supports site-to-site VPNs is the Cisco Meraki Series. In particular, VPN capabilities are available in Cisco Meraki MX Series devices. A popular Cisco Meraki VPN feature is site-to-site VPN tunnel creation using a single mouse click. Meraki focuses on simplifying deployment and management by leveraging an appliance-to-cloud-management architecture. Essentially, all Meraki appliances must be licensed and managed using the Meraki cloud management center. This simplified architecture can allow for capabilities such as single-click enablement of a site-to-site VPN. With this approach, it is possible to generate an automatic mesh site-to-site VPN solution.

Cisco Meraki VPN Options

With a site-to-site VPN in a Meraki MX-Z device, you can provide the following with one click:

- Advertise the local subnets that are participating in the VPN.
- Advertise the WAN IP addresses on Internet 1 and Internet 2 ports.
- Download the global VPN route table from the dashboard. This occurs automatically, based on each MX's advertised WAN IP/local subnet in the VPN network.
- Download the pre-shared key for establishing the VPN tunnel and traffic encryption.

The Meraki MX series offers three configuration options for setting up a VPN automatically:

- **Off:** The specified MX-Z will not participate in the site-to-site VPN.

- **Hub (or Mesh):** The MX-Z device will establish VPN tunnels to all remote Meraki VPN peers that are also configured in this mode.
- **Spoke:** The MX-Z will establish direct tunnels only to the specified remote MX-Z devices.

The Meraki MX series offers the following additional options:

- Two tunneling options: split tunnel and full tunnel
- Automatic and manual (port forwarding) NAT
- Limited VPN subnet translation
- OSPF route advertisement
- Three IPsec policies: Default, Amazon VPC, or Microsoft Azure Instance
- Phase 1 and 2 encryption support for AES-128, AES-192, AES-256, and 3DES
- Authentication with MD5 or SHA-1

Like other Cisco security solutions, the Meraki Series product line is continuously being updated. We highly recommend that you validate the current data sheet associated with the Meraki model you are considering for your site-to-site VPN project to ensure that all required features and licenses are obtained. We look more at the Cisco Meraki VPN capabilities in Chapter 7. Cisco Meraki is not part of the current SVPN learning objectives, but that could change with a future version of the exam.

Cisco Security Appliance Management

Our next topic to review is how Cisco security devices are managed. Smaller organizations will use a local management option, meaning they will log in to each security appliance and perform individual configurations. As organizations grow, the need for a centralized manager comes into play. Larger organizations need a way to standardize configurations by enforcing templates for how they want their technology to function as well as

consolidate events and logs, so the security operation center and network operations teams are able to keep up with the workload.

Cisco Security Management Options

There are a few options for managing Cisco security devices:

- **Cisco Security Manager (CSM):** Provides centralized management for Cisco ASA appliances, Cisco 4200 and 4500 Series sensors, and the AnyConnect Secure Mobility Client. CSM is an older option for those that leverage specific Cisco security technologies.

- *Cisco Secure Firewall Management Center (FMC)*: FMC provides centralized management of Cisco Firepower Next Generation Firewall (NGFW), Cisco Firepower Next Generation IPS (NGIPS), and Cisco AMP (Advanced Malware Protection) for networks as well as threat correlation for network sensors and AMP for Endpoints.

- *Cisco Secure Firewall Device Manager (FDM)*: FDM can manage multiple 1000 Series and 2100 Series devices and select 5500-x Series devices running the Cisco Secure Firewall (FTD) software image. Each FTD image is managed individually through FDM.

- *Cisco Adaptive Security Device Manager (ASDM)*: ASDM is one of the management options for Cisco ASA appliances. It can also manage the Cisco AnyConnect Secure Mobility Client. ASDM is a free GUI used to configure, monitor, and troubleshoot Cisco firewall appliances and service modules; it targets small deployments because it can manage only one firewall at a time. ASDM includes setup wizards to help simplify firewall and VPN configuration tasks, offers real-time log viewing for troubleshooting and checking on the health of services, as well as other troubleshooting tools, such as debugging, packet tracking, and packet capturing tools, as well as the ability to do software upgrades.

- *Cisco Defense Orchestrator (CDO)*: CDO offers cloud-based

management of Cisco security devices ranging from the ASA Series to other firewall and network devices. The demand for cloud management continues to increase. CDO is expected to eventually enable management of all Cisco Secure Firewall and ASA options in the near future.

- **Meraki cloud management:** All Cisco Meraki solutions are managed from a cloud-based GUI that provides centralized visibility and control without any additional costs. Meraki's approach to management offers many values, including licensing and configuring devices before they are connected to a network for the first time; automation of monitoring and alerting; quick feature updates; support for large, dispersed networks; and one of the simplest approaches to providing networking and security services on the market. The demand for cloud management continues to increase, and Meraki's entire platform is built around its cloud management strategy.

Chapter 3, "Site-to-Site VPNs," walks through the configuration of a site-to-site VPN using local command-line options as well as Cisco ASDM. You will need to understand both options for the SVPN 300-730 exam as well as to deploy a site-to-site VPN in real life. Some of the steps shown in Chapter 3 can be simplified using other Cisco management options, including setup wizards. In Chapter 3 you will see how to build VPNs both with and without setup wizards so you can get a feel for different approaches to configuring site-to-site VPNs.

VPN Logging

Logging can be extremely useful for troubleshooting and monitoring what occurs during a VPN session. Imagine the impact to a business that suddenly can't access resources. If a site-to-site connection between a major branch goes offline, think of the number of employees who would complain that "the network is down" and blame the team responsible for the network. This scenario is a common nightmare for network administrators and one you want to avoid by using best practices for redundancy and failover within VPN solutions. Every architecture can go down and, in the end, logging is what enables you to view what is going on. In situations that impact a large group of people, such as a branch office going down, every minute matters,

and having the right logs can make the difference between quickly remediating the issue and having a failure in VPN turn into a major incident.

Logging Collection Points

Logging can occur in different parts of a VPN solution. The VPN gateway provides information about users accessing the remote access VPN, details on the VPN session (from how it is established to how it is terminated), and data on how a site-to-site VPN is performing, members of the VPN group, and many other details, depending on the technology and type of VPN being used. Most Cisco devices use syslog service for logs; however, solutions such as Cisco Secure Firewall Management Center use eStreamer. A logging service in a Cisco device accepts messages and stores them in files, prints them on the screen, or sends them externally, depending on the device configuration. Logs can be collected by a centralized logging system to be analyzed or exported to a data repository for data archiving purposes. Many government organizations have data archiving requirements such as storing remote access VPN logs for three to five years.

ASA Logging

The Cisco ASA Series comes with logging controls to help reduce some of the clutter and allow administrators to zero in on events that matter. Logging types can be enabled or disabled based on severity levels. For example, any notification logs could be ignored, while more severe events impacting the performance of a VPN could be exported to a centralized logging system or sent directly to the administration team. Log messages can be sent via an SNMP management station, sent to specific email addresses, viewed within an ASA management tool such as ASDM, or seen via Telnet and SSH sessions. Log buffer settings can be configured to specify what logs are stored locally on the Cisco solution and indicate when logs are either deleted or exported to an external source. Figure 2-9 shows an example of using the ASDM Real-Time Log Viewer to monitor AnyConnect remote access VPN logs. This example shows many of the logs that are generated just from a single user connecting to a network from a remote location. As you can imagine, filtering capabilities are essential to any logging system. Having

logs is good, but if you can’t read them, the value of logging quickly diminishes as the log data becomes unmanageable.

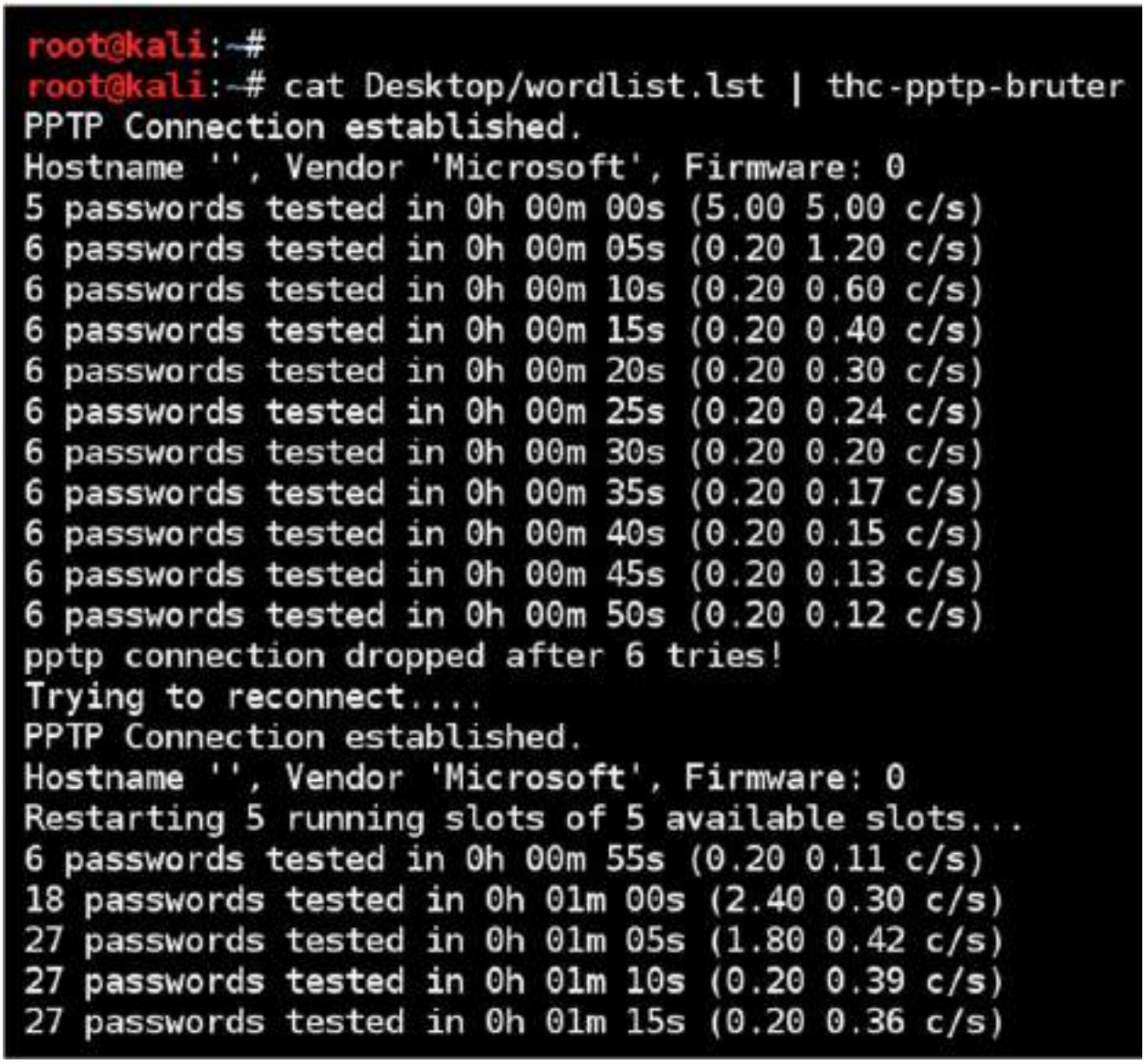


Figure 2-9 Real-Time Log Viewer Example

When it comes to pulling log data from a VPN gateway, it is common to have system-level and security logs delivered to a centralized logging solution. Centralizing log collection makes it possible to view all logs in one spot as well as aggregate event details to better troubleshoot a situation that impacts one or more devices.

SIEM

Most customers we meet with use a security information and event management (SIEM) tool as a centralized log collection solution. The biggest values from using a SIEM tool include simplifying the process of searching through huge amounts of log data, correlating multiple events from different logs into one single entry, and developing reports that cover the state of security and performance for the entire organization. Some SIEM tools are better at mining log data and doing security information management, and others are more threat focused, leaning toward security event management.

Figure 2-10 shows an example of Splunk viewing Cisco ASA AnyConnect data associated with a remote access VPN deployment. Splunk, which can digest huge amounts of log data, allows an administrator to search data in much the same way it is possible to search the Internet using a web browser. In the example shown in Figure 2-10, searching on the term “VPN” and the field “Cisco_ASA_user” filters out all log data outside any event associated with a Cisco AnyConnect VPN log.

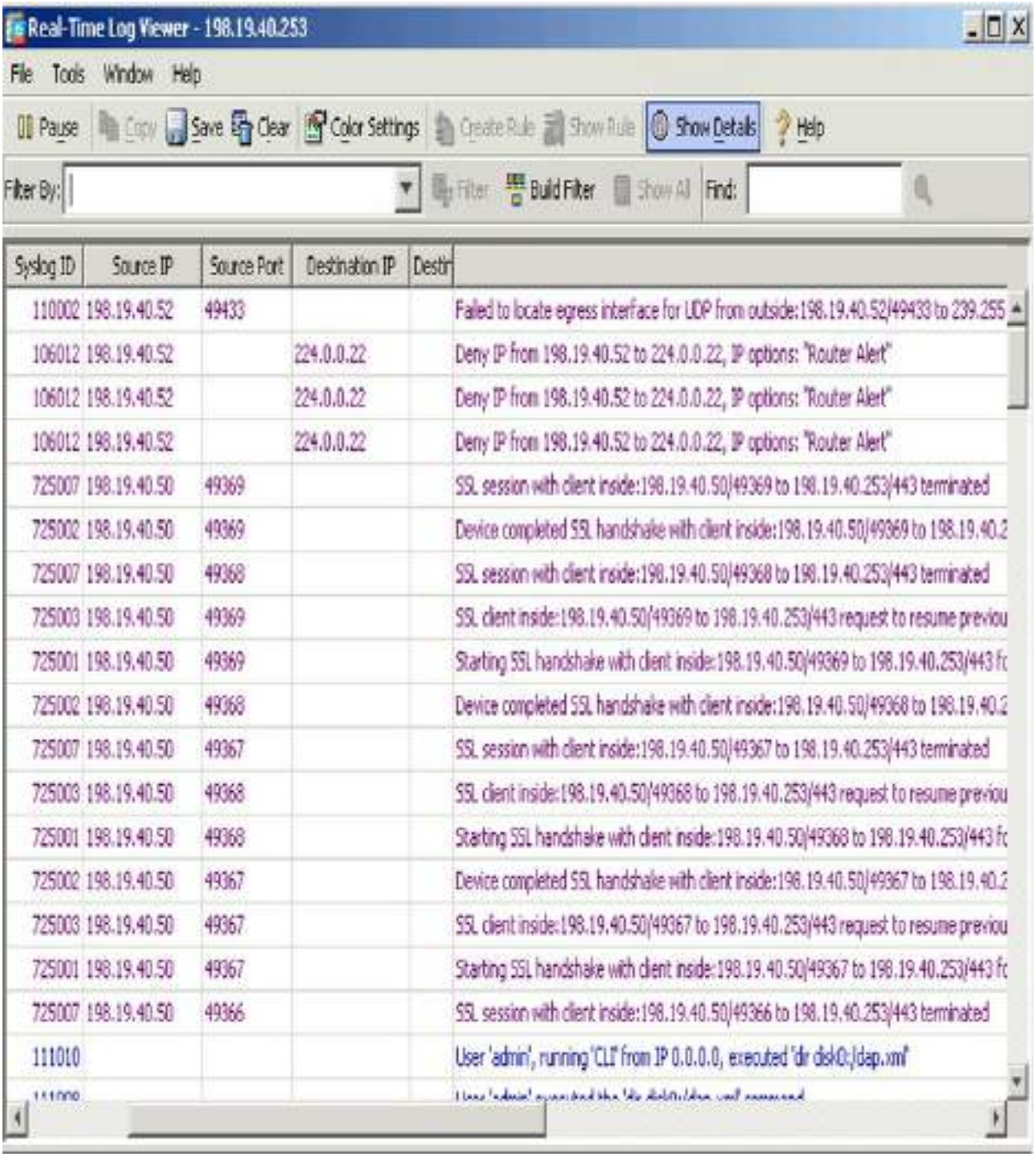


Figure 2-10 Splunk Managing Cisco AnyConnect Logs

VPN Client Logging

Another source for log data is the VPN client (if one is being used). Most VPNs create log files on the client systems, and these files contain details

regarding the entire VPN session, from connection to termination. For example, OpenVPN can be found at C:\Program Files (x86)\OpenVPN Technologies\OpenVPN Client\etc\log\openvpn_(unique_name).log on a Windows system. This file can contain details regarding the entire life cycle of OpenVPN usage unless the user or administrator purges the records or the system runs out of storage space.

Cisco AnyConnect generates verbose events that are logged by the host system and that can be exported or read directly from a client device. Details include information about communication between the client and VPN gateway, as long as the client's records have not been purged. Figure 2-11 shows an example of viewing such log details with Cisco AnyConnect after a VPN connection is established. You can view details related to the VPN and information about each step the VPN takes during its life cycle, as well as other useful log details. You can also choose to export the data to a text file, which is a much simpler way to view the log details.

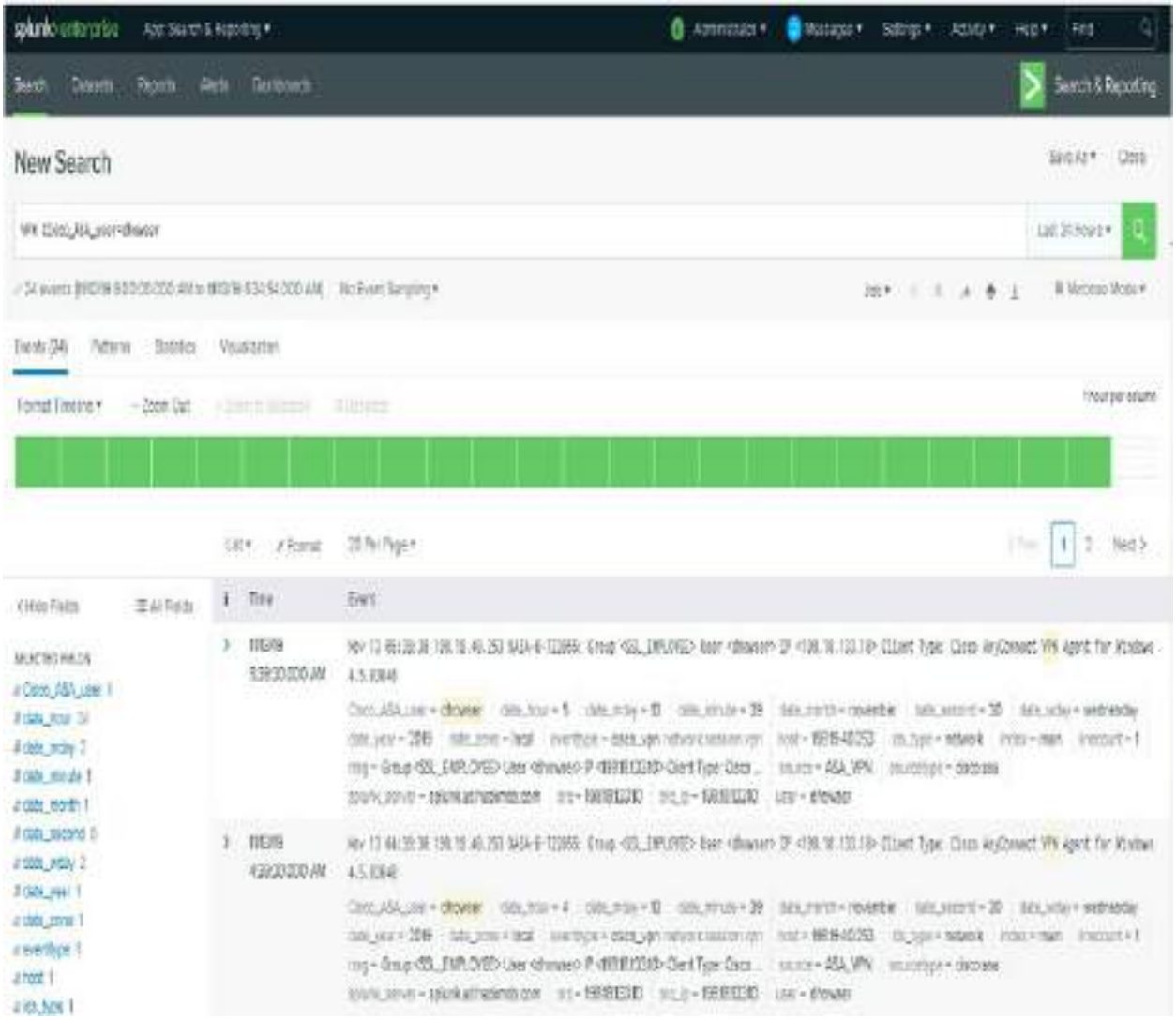


Figure 2-11 Cisco AnyConnect Message Details

DART

Another approach to analyzing Cisco AnyConnect files and connections is by using the Diagnostic and Reporting Tool (DART). DART is a wizard that bundles all client logs and configuration and diagnostic information for analyzing and troubleshooting the AnyConnect client connection. When the wizard completes, results are exported to a single .zip file that can be shared with an administrator. Figure 2-12 shows an example of the DART wizard. In later chapters, you will find more details regarding collecting and viewing Cisco AnyConnect logs using tools like DART.

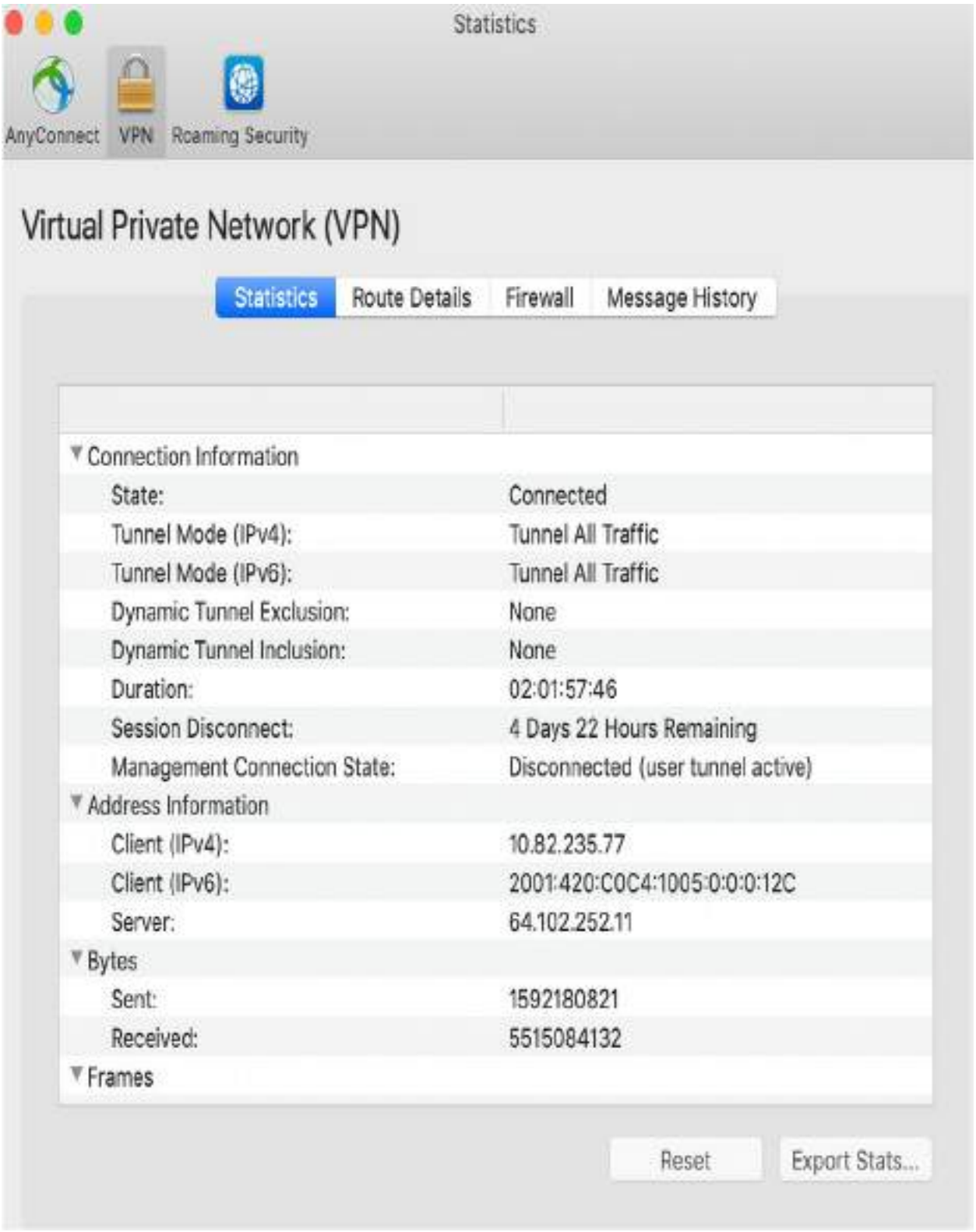


Figure 2-12 The Cisco AnyConnect DART Wizard

Logging Challenges

Sometimes logging is seen as a bad thing. Unwanted logging—that is, collecting and viewing information about a VPN connection and all associated user data without the involved parties knowing or approving—can be a violation of privacy. Imagine how employees would feel if they were told their organization is collecting information about whom they speak with. Some employees might find this offensive, and it could even be illegal in certain countries. It is highly recommended that you be open about what data you are collecting with your VPN solutions as well as any other network policies that must be followed upon establishing a remote access VPN session, as well as any other network services you plan to offer. Cisco AnyConnect has banner features that can be used for these alerting purposes.

Regarding site-to-site VPN logging awareness, we recommend having a formal policy for any internal network usage; this policy should state what is considered non-approved behavior as well as how logging is enabled to monitor for such behavior. An acceptable use policy (AUP) is a digital document that users accept upon accessing a network. Figure 2-13 shows an example of a Cisco AnyConnect banner that acts as an AUP, which the user must accept before the VPN connection is established. We highly recommend having a legal professional validate your AUP to provide the maximum legal protection possible and be compliant with local laws.

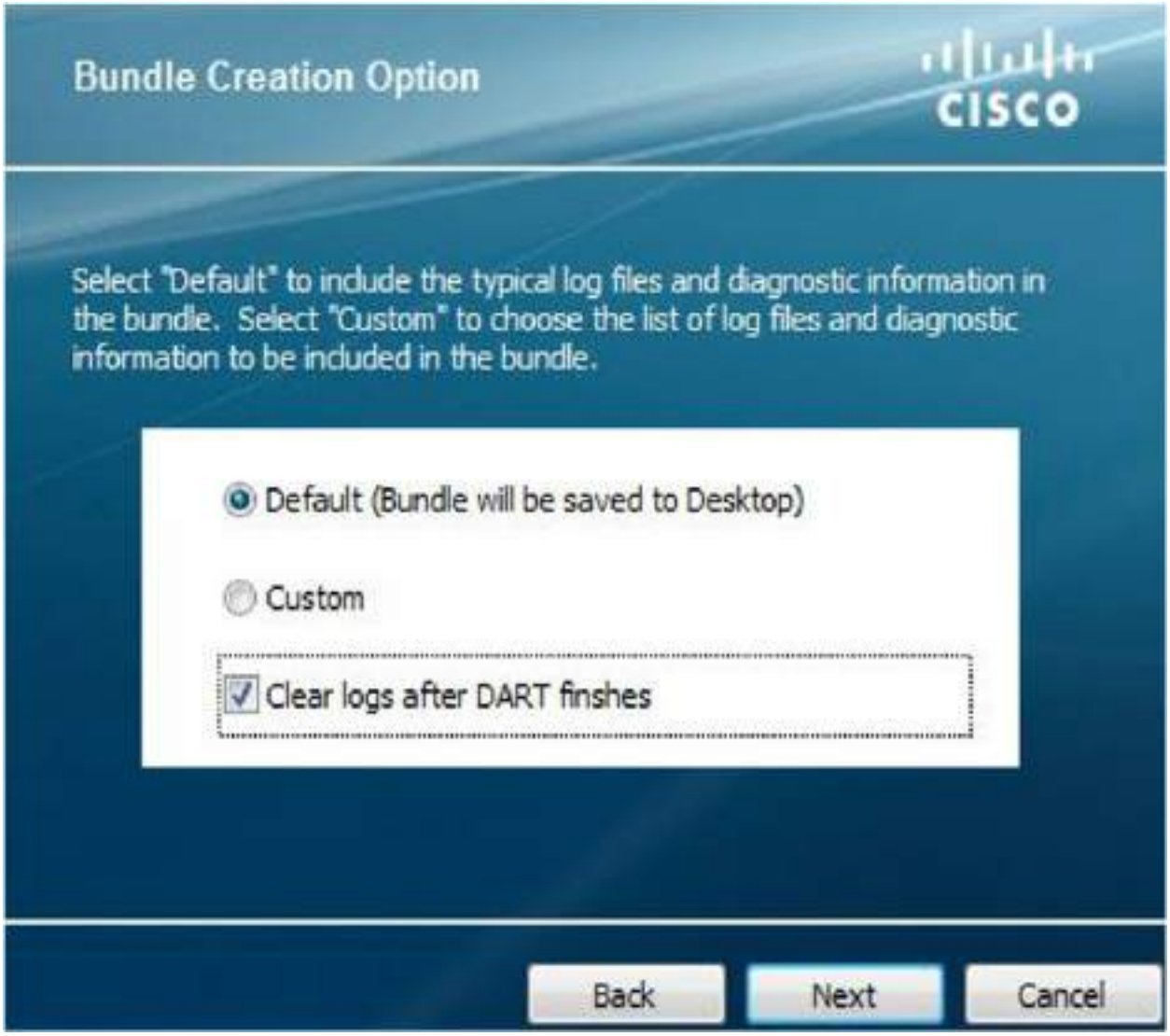


Figure 2-13 Cisco AnyConnect Banner/AUP

Logging concerns can also come into play when levering a VPN service provider. Many people seek a VPN for privacy reasons, so it should make sense that customers might be upset if they do not get the privacy they are seeking when they use a VPN service. Providers that stress a no-logging policy tend to be hosted from exotic locations such as Panama (NordVPN), the British Virgin Islands (ExpressVPN), and Romania (CyberGhost). There haven't been any documented privacy violations from VPN service providers that are based in countries like the United States, but this doesn't mean you shouldn't be concerned. We recommend doing research and asking a service provider if privacy is something you should be concerned about when using its VPN service. Some VPN service providers are transparent about logging.

For example, TunnelBear publishes what it stores (see Figure 2-14), so customers know where they stand regarding logging.

Figure 2-14 TunnelBear Data Collection and Use Policy

Summary

This chapter provides a high-level overview of VPN technology to prepare you to dive deeper into VPN concepts. This chapter looks at various VPN technology categories, including site-to-site VPNs and remote access VPNs. It looks at VPN hardware, software protocols, and logging possibilities, with a focus on technologies offered by Cisco.

At this point, you should have a broad understanding of what VPN options are available in today's market, including the VPN capabilities that Cisco offers. The following chapters continue to focus on Cisco VPN technology concepts that are specific to the SVPN 300-730 exam, and they also discuss third-party and open-source concepts that are relevant to real-world architectures.

Chapters 3 through 6 focus on site-to-site VPN concepts, and Chapters 7 through 10 dive into remote access VPN concepts. Chapters 3 and 7 serve as a general review of the technology category while the chapters that follow dive deep into specific VPN topics you need to know for the SVPN exam. Make sure to first master the concepts in the introduction chapters before moving to the deeper focused chapters.

Now we are ready to take on the first major VPN technology category, which is a closer look at site-to-site VPN technology.

References

Anand, Adity (July 14, 2018). SSL Strip & How Awesome It Is! Retrieved from https://medium.com/bugbountywriteup/ssl-strip-how-awesome-it-is-a0eb79e28bcc

Document ID 1458444803226729 (March 13, 2015). Cisco Easy VPN Q&A. Retrieved from https://www.cisco.com/c/en/us/products/collateral/security/ios-easy-vpn/eprod_qas0900aecd805358e0.html

Document ID 1456177868598773 (February 22, 2016). Cisco IOS SSL VPN: Router-Based Remote Access for Employees and Partners Data Sheet. Retrieved from https://www.cisco.com/c/en/us/products/collateral/security/ios-sslvpn/product_data_sheet0900aecd80405e25.html

@merakisimon (March 20, 2016). VPN Made Easy for All. Retrieved from https://meraki.cisco.com/blog/2016/03/vpn-made-easy-for-all/

Mimoso, Michael (August 29, 2016). New Collision Attacks Against 3DES,

Blowfish Allow for Cookie Decryption. Retrieved from https://threatpost.com/new-collision-attacks-against-3des-blowfish-allow-for-cookie-decryption/120087/

Exam Preparation Tasks

As mentioned in the section “How to Use This Book” in the Introduction, you have a couple of choices for exam preparation: the exercises here, Chapter 11, “Final Preparation,” and the exam simulation questions in the Pearson Test Prep practice test software.

Review All Key Topics

Review the most important topics in the chapter, noted with the key topics icon in the outer margin of the page. Table 2-5 lists these key topics and the page number on which each is found.

Table 2-5 Key Topics for Chapter 2

Key Topic Element	Description	Page Number
Figure 2-3	Generic Hub-and-Spoke VPN	
Figure 2-4	Hub-and-Spoke VPN with Spoke-to-Spoke Connections	
Figure 2-5	Generic Full Mesh VPN	
Figure 2-6	Hybrid Site-to-Site VPN Design	
Table 2-2	Comparison of Site-to-Site VPN Options	
Section	Cisco ASA Licensing	
List	Cisco Security Appliance management options	

Complete Tables and Lists from Memory

Print a copy of Appendix C, "Memory Tables" (found on the companion website), 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 companion website), 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:

- remote access VPN
- site-to-site VPN
- full mesh
- Point-to-Point Tunneling Protocol (PPTP)
- Secure Socket Tunneling Protocol (SSTP)
- Secure Sockets Layer (SSL)
- Datagram Transport Layer Security (DTLS)
- Internet Key Exchange (IKE)
- Internet Key Exchange Version 2 (IKEv2)
- Easy VPN (EzVPN)
- Layer 2 Tunneling Protocol (L2TP)
- Dynamic Multipoint VPN (DMVPN)
- Group Encrypted Transport VPN (GETVPN)
- FlexVPN
- Cisco Secure Firewall Management Center (FMC)
- Cisco Secure Firewall Device Manager (FDM)
- Cisco Adaptive Security Device Manager (ASDM)
- Cisco Defense Orchestrator (CDO)

Part II: Site-to-Site VPN

Chapter 3. Site-to-Site VPNs

This chapter covers the following subjects:

- **Site-to-Site VPN Architecture:** This section describes how to develop a plan to build a site-to-site VPN architecture.
- **Site-to-Site Components:** This section provides a short review of the key components needed for a site-to-site VPN.
- **VPN Tunnel Concepts:** This section provides an overview of foundational VPN tunnel concepts.
- **Router Configuration with IKEv1:** This section describes how to develop a plan for and configure a basic IKEv1-based site-to-site VPN.
- **Router Configuration with IKEv2:** This section describes how to develop a plan for and configure a basic IKEv2-based site-to-site VPN.
- **Appliance Configuration:** This section describes how to develop a plan for and configure site-to-site VPNs for different Cisco security appliance options.
- **High Availability:** This section provides a review of the high availability options with Cisco site-to-site VPN technology.

“Invisible threads are the strongest ties.”

—Friedrich Nietzsche

This chapter covers the following exam objectives:

- 1.0 Site-to-site Virtual Private Networks on Routers and Firewalls
  - 1.1 Describe GETVPN
  - 1.2 Describe DMVPN
  - 1.3 Describe FlexVPN

- 4.0 Secure Communications Architectures
  - 4.1 Describe functional components of GETVPN, FlexVPN, DMVPN, and IPsec for site-to-site VPN solutions
  - 4.3 Recognize VPN technology based on configuration output for site-to-site VPN solutions
  - 4.6 Design site-to-site VPN solutions
    - 4.6.a VPN technology considerations based on functional requirements
  - 4.7 Design remote access VPN solutions
    - 4.7.a VPN technology considerations based on functional requirements
    - 4.7.b High availability considerations

Companies that are successful are likely to grow in size. Growth can occur by hiring more people, partnering with other businesses, or merging or acquiring another organization. As growth occurs, there is likely to be a point where resources need to be shared between different parts of the organization over untrusted mediums like the Internet. This is where site-to-site VPN technology can come to the rescue.

Site-to-site VPN technology can provide a lot of functionality and financial value. The most obvious value is allowing one or more trusted locations to communicate across an untrusted medium. However, connecting one or more resources over an untrusted medium isn't as simple as providing full access to anything for anybody. Opening up that level of access could lead to unauthorized data access. Different levels of access need to be granted based on business requirements and security policies. A properly designed and implemented site-to-site VPN architecture balances ease of accessing resources and granting access to only what is required. A best practice for data access control is to provide access to only what is needed; this is called "least privilege access."

Conceptionally, least privilege access sounds simple, but in practice, it can be extremely complex. As an example, a site-to-site VPN might need to support users with multiple job roles, accessing resources from different locations and

from multiple different device types. We teach you not only how to connect different locations using site-to-site VPN technology but also look at how to choose and enforce the right security controls within the access you provide. Such skills are required to properly deliver site-to-site VPN services and to pass the SVPN 300-730 exam.

This chapter explores site-to-site VPN technology. The goal is to address various site-to-site architectures and features so you can adjust your design to meet both your business and security needs. You will find that there are many options available in modern VPN technology, including different levels of encryption, hardware, and software, as well as various levels of effort required to set up, maintain, and troubleshoot different site-to-site VPN options. We cover all of this over the next few chapters to prepare you for real-world deployments as well as the SVPN 300-730 exam.

Learning beyond the SVPN concepts:

- Site-to-site VPN Architecture and Design Considerations
- Appliance Configuration – Cisco Secure Firewall and Cisco Meraki

"Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz enables you to assess whether you should read this entire chapter thoroughly or jump to the "Exam Preparation Tasks" section. If you are in doubt about your answers to these questions or your own assessment of your knowledge of the topics, read the entire chapter. Table 3-1 lists the major headings in this chapter and their corresponding "Do I Know This Already?" quiz questions. You can find the answers in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes."

Table 3-1 "Do I Know This Already?" Foundation Topics Section-to-Question Mapping

Foundation Topics Section	Questions
Site-to-Site VPN Architecture	9
Site-to-Site Components	1, 6, 8
Router Configuration with IKEv1	3, 5, 10
Router Configuration with IKEv2	4, 7
Appliance Configuration	2
High Availability	10

1. Which of the following mechanisms are found within IPsec? (Choose two.)

a. SHA

b. AH

c. ESP

d. TTL

2. What is the command-line command on an ASA running Version 8.4 or greater to create a IKEv1 policy?

a. crypto ikev1 policy 1

b. crypto isakmp policy 1

c. crypto pki ikev1

d. ikev1 crypto 1

3. Which of the following occurs during phase 2 of the IKE key exchange?

a. IKE policy negotiation

b. IPsec SA exchange

c. Authentication

d. Diffie-Hellman (temporal keys)

4. Which of the following is a characteristic of IKEv2?

a. Public key encryption is used for authentication.

b. Both peers must use the same authentication.

c. NAT is supported by default

d. Multi-hosting is not supported.

e. None of these options are correct.

5. Which of the following are possible authentication methods for IKE? (Choose all that apply.)

a. RSA signature method

b. RSA encrypted nonces method

c. Pre-shared keys

d. Public and private key

6. Which of the following are the primary components of a VPN tunnel? (Choose three.)

a. A transport protocol

b. An initiation protocol

c. A carrier protocol

d. A passenger protocol acting as the protocol that is being encapsulated.

7. True or false: With IKEv2, both peers use the same authentication.

a. True

b. False

8. What is the purpose of digital certificates? (Choose two.)

a. Authenticating websites, people, and devices

b. Holding identity credentials

c. Authorizing systems

d. Validating authorized systems

9. Which of the following is the least important question to ask when planning a site-to-site VPN project?

a. How much is the up-front technology?

b. Does an industry analyst show this technology as best of breed?

c. Who can you call for support, and what does support cost?

d. Is the technology being used close to end of sale/end of support?

10. Which of the following is not a site-to-site VPN high availability option?

a. Hot standby

b. Cold standby

c. Active/standby

d. Active/active

Foundation Topics

We kick off this part of the book with a focus on site-to-site VPN concepts, which is the first of two VPN technology categories you need to know for the SVPN exam. This chapter serves as a primer for Chapters 4 through 6 and covers the foundational concepts behind site-to-site VPN technology. The remaining part of the book focuses on remote access VPN.

Why care about site-to-site VPN technology? Besides knowing it is a requirement for the SVPN exam, you should care about this topic based on

how widely used it is within all types of organizations around the world. The Internet is a dangerous place, and security needs to be applied between locations looking to share data. Many common threats such as data loss, breach of data confidentiality, and modification of data can be avoided by implementing a strong site-to-site VPN architecture.

Different flavors of site-to-site VPN technologies are available when using Cisco security appliances. The SVPN exam specifically calls out requirements for knowing how to identify, deploy, and troubleshoot GETVPN, DMVPN, and FlexVPN. The next three chapters focus specifically on these topics. Before moving to those chapters though, make sure you master the foundational concepts covered in this chapter.

Site-to-Site VPN Architecture

As mentioned in Chapter 2, "Introduction to Virtual Private Networks (VPNs)," a site-to-site VPN is a VPN that connects different locations over untrusted networks. Chapter 2 provides a handful of site-to-site design examples, including hub-and-spoke, spoke-to-spoke, full mesh, and hybrid VPNs. Which approach is right for your organization? What technologies and configurations are involved with a site-to-site VPN? This chapter begins to answer these questions.

Site-to-Site Design Considerations

The first place to start when deciding which approach to use for a site-to-site VPN project is to review the project at a high level. This is where we start when we consult with customers. Many times, particular design elements or available equipment quickly narrows down the possible options for the project. It is important to consider the following when collecting high-level information about a potential project:

- What is the budget?
- What technology is available for the VPN project?
- What is your expected future growth?

- What is the current traffic on the network?
- How many sites are part of the design?
- What are your high availability and network resilience requirements?
- What existing skill sets and technology familiarity do you have in your organization?
- What are your in-house versus external management expectations for the solution?
- What compliance requirements do you need to keep in mind?

When we consult with customers on choosing the right site-to-site VPN for a project, the answers to these questions lead us to the options that could work, based on the customer's design needs. The available budget will impact factors such as how much redundancy and which features are within reason. The available technology is extremely important because many customers already have tools that can be used in a VPN, such as their existing routers or firewalls, but they need to configure the equipment or purchase additional licensing. Compliance and technical requirements obviously narrow down the design, and we find that such requirements may be adjusted based on the technology and budget available. Existing skill sets and technology familiarity will also influence the design; for example, if the organization has always used Cisco equipment, they will likely want to continue to use Cisco equipment. Most engineers would rather work with technology they are familiar with than learn a whole new vendor's way of configuring and managing technology.

Scoping a Project

When scoping a site-to-site VPN project, it is very important to consider the full life cycle of the project. Sometimes vendors and service providers offer free hardware, software, or services up front but force the use of additional hardware, software, or services after their technology is initially implemented as a way to make a sale. In such cases, the full deployment of a solution might end up actually costing more than other options and provide fewer

features and less support. To avoid such a pitfall, consider the following aspects of the life cycle of your VPN project:

- How much does the upfront technology cost?
- What additional technology will be needed during the life cycle of the project?
- What services are required to install the entire solution properly?
- Are any additional services left out of the scope (for example, deploying software to each endpoint, upgrading existing systems, technology training)?
- Is the technology close to end of sale/end of support?
- Who can you call for support? Is there a cost for that?
- How reputable are the technology and the company?

It is ideal to use this list when planning any request for technology and services.

Once you have scoped out the high-level design of a VPN project, the next step is to fill in the details to make it all work, starting with choosing the components to use.

Site-to-Site Components

A variety of technology components are involved with a site-to-site VPN. You will find that some elements are required for a site-to-site VPN regardless of the approach used, while others depend on the approach and vendor of choice. An important factor in deciding which VPN technology to use is available technology; it is a good idea to leverage existing investments whenever possible.

Routers vs. Security Appliances

An important aspect to consider is the hardware or software that will provide the VPN service. From a high level, we can simply break this down into two categories: routers and security appliances.

Chapter 2 summarizes the different VPN types and the Cisco technologies that support VPNs. Cisco routers (or IOS-based VPNs) have options such as GETVPN, DMVPN, GRE-based VPN, and FlexVPN. None of these options, however, are supported on a Cisco security appliance such as the Cisco ASA. This means if routers are being used for a site-to-site VPN, you are likely going to have more design options than if you use security appliances. You also need to validate the models of hardware used and confirm the versions of code being used; different models of hardware support different numbers of VPN sessions, and different versions of code support different VPN options. Cisco routers that support site-to-site VPNs typically run IOS or IOS XE. This includes CSR Series and ASR 1000 Series routers.

Note

Most Cisco routers do not require additional licenses to support a basic IPsec site-to-site VPN. You should validate your project's scope using the data sheet for the Cisco router to confirm any licensing requirements before proceeding with a project.

Cisco Security Appliances for Site-to-Site VPNs

Cisco security appliances also offer site-to-site VPN functionality. The hardware limitations and license options for such an appliance determine whether and how many VPN sessions are supported. The hardware limitations can be found by looking at the model's data sheet. Keep in mind that certain licensing may be required to be installed before a VPN can be configured. The following Cisco security appliances support site-to-site VPN functionality:

- Cisco Adaptive Security Appliance (ASA) Series

- Cisco Secure Firewall Series
- Cisco Meraki MX Series

Note

For the SVPN 300-730 exam, you are likely to only be tested on the command line and GUI for the Cisco ASA Series.

IPsec

An important consideration with VPN technology is how data is protected by the VPN. *IP Security (IPsec)* is a popular option to use when choosing how a VPN will function. Basically, IPsec is a framework of related protocols used to secure communication at the network layer. The IPsec framework is made up of open standards developed by the Internet Engineering Task Force (IETF) that are designed to offer data confidentiality, data integrity, and data authentication between participating peers. IPsec accomplishes these goals by providing authentication, encryption of IP network packets, key exchange, and key management.

Authentication Header

IPsec originally defined two options for imposing security on IP packets. The first mechanism, *Authentication Header (AH)*, is a protocol defined in RFC 4302 that specifies a method for digitally signing IP packets. Signing packets is accomplished by hashing the IP header and data payload. Using this hash, a new AH header is built, and it is then prepended to the packet. Think of this new header as a digital validation that the data has not been changed. A hash (for example, MD5 or SHA) is a generated number that can be reproduced to validate the source; a different value is generated if any change occurs in what is being hashed. Even a change in a single bit will generate a new hash, indicating that a change has been made. This newly created packet is transmitted via normal routing means until it reaches the destination IPsec peer, where the AH header is removed, validated and the original payload is

sent on its destination. AH also includes replay protection, using a Sequence Number field within the AH header. This replay protection excludes fields that are expected to change, such as the Time-to-Live (TTL) field.

Note

Authentication Header (AH) is used to digitally sign data to ensure that it hasn't been modified (providing data integrity, data origin authentication, and replay protection). This means AH provides a mechanism for authentication; the actual data inside the packet is not encrypted. AH isn't used much in today's networks.

Encapsulating Security Payload

The second original IPsec mechanism is the *Encapsulating Security Payload (ESP)* protocol, defined in RFC 4303, which is used to encrypt data and ensure the integrity of data packets. ESP uses the same algorithms as AH; however, it provides coverage differently from AH. ESP is added after the standard IP header, and it is important to point out that this means it contains the standard IP header. This is important because it allows easy routing of traffic with standard IP devices. It also makes IPsec backward compatible with IP routers and devices that were not designed to function with IPsec. ESP operates at the network layer and can be viewed as containing several parts. Security Parameter Index and Sequence Number are only authenticated but not encrypted. The remaining four parts—Payload Data, Padding, Pad Length, and Next Header—are all encrypted during transmission. ESP supports multiple encryption protocols which you can choose to enable or opt out of.

Note

ESP provides encryption (data confidentiality) and authentication (data integrity, data origin authentication, and replay protection). ESP can be used only for encryption, only for authentication, or for both.

Comparing AH and ESP

It is important to understand the difference between ESP and AH and why this difference exists. AH authenticates an entire IP packet, including the outer packet. ESP authenticates only the IP datagram portion of the IP packet. If you do not want to expose any part of the outer packet for security reasons, you might want to use AH; if you want ease of routing, you might consider ESP the best option. With either AH or ESP, you need to choose the algorithm used to encode authentication data in the AH or ESP headers.

Note

Expect the SVPN 300-730 exam to challenge your understanding of the differences between ESP and AH.

Figure 3-1 shows an example of AH and ESP when used in transport mode and tunnel mode. We cover transport and tunnel mode concepts later in this chapter.

Figure 3-1 AH and ESP in Transport Mode and Tunnel Mode

ISAKMP

To support IPsec, the Internet Key Exchange (IKE) protocol (RFC 7296) was added to specify which services are to be incorporated in packets, which cryptographic algorithms will be used to provide those services, and a mechanism for sharing keys used with those cryptographic algorithms. Internet Security Association and Key Management Protocol (ISAKMP) is now also specified as part of the IKE protocol suite. ISAKMP defines how security associations (SAs) are set up and used to define direct connections between two hosts that are using IPsec. A security association includes all relevant attributes of the connection, including the cryptographic algorithm used, the IPsec mode, the encryption key, and other parameters related to the transmission of data over the VPN connection. ISAKMP traffic functions on UDP port 500.

Many other protocols and algorithms use or are used by IPsec, including encryption and digital signature algorithms, which you can learn more about by reviewing RFC 6071. Keep in mind that if you are looking to permit IPsec traffic, you will likely need to permit UDP port 500 for ISAKMP, IP protocol 50 for ESP, and IP protocol 51 for AH traffic. Also know that IPsec could be configured without using IKE; however, IKE enhances IPsec by providing additional features, flexibility, and simplification of configuration for the IPsec standards, including keepalives. GRE keepalives are essential for network resilience because the heartbeat must be maintained to avoid unwanted failover. We cover failover concepts later in this chapter.

Note

Make sure to understand the components of IPsec, including which ports and protocols are used as well as their role in VPN technologies.

IKE Security Association

We stated that IKE handles the negotiation of the SA, which, simply put, is the process of establishing security attributes between two network entities

trying to build the site-to-site VPN. This explains how VPN peers exchange certain information, including information on protecting negotiation, establishing a shared secret over an insecure medium, and authenticating each peer.

Figure 3-2 provides a visual of this process to help you understand IKE. Phase 1 is the IKE negotiation. Phase 2 is the SA exchange. Finally, if everything works, data is sent.

Figure 3-2 IKE Data Flow Diagram

IKE Version 1 and 2

There are currently two versions of IKE: Version 1 (IKEv1) and Version 2 (IKEv2). IKEv1 (released in 1998 and described in RFC 2409) is the older version and is still used today; however, it has been declared obsolete by the IETF. Cisco and Microsoft worked together to develop IKEv2, which was released in 2005 and described in RFC 4306. IKEv2 is a low-latency alternative to IKEv1 with the data format ISAKMP.

The biggest difference between IKEv1 and IKEv2 is that IKEv2 is much simpler and more reliable than IKEv1 because fewer messages are exchanged during the establishment of the VPN, additional security capabilities are

available, and there is support for mobile devices. IKEv2 supports mobile devices with its resilience to network changes. Table 3-2 compares IKEv1 and IKEv2.

Note

Make sure you understand the fundamentals of IKEv1 and IKEv2 for the SVPN 300-730 exam.

Table 3-2 Comparison of IKEv1 and IKEv2

Parameter	IKEv1	IKEv2
		One
Exchange messages	Nine for main mode; six for aggressive mode	
Authentication methods		
Authentication	Both peers use the same authentication	Each peer can use different authentication (for example, one using PSK and the other using RSA-Sig)
Number of combinations of a source IP range, a destination IP range, a source port, and a destination port allowed per IPsec SA	One	Multiple (IPv4 and IPv6 addresses can be configured for the same child SA)
Multi-hosting	Not supported	
Rekeying	Not defined	Defined
NAT traversal and dead peer detection	Can be defined as an extension	Supported by default
Remote access VPN	Not defined but supported by vender-specific implementations such as Mode config and Xauth	Supported by default; options including the following:
Multi-homing, mobile clients, and DoS protection	Not supported	Supported, as described in RFC 4555 (DoS protection includes anti-replay function, cookies for mitigating flooding attacks, and vulnerabilities found with IKEv1)

Parameter	IKEv1	IKEv2
Number of exchange modes	Two: main and aggressive	One
Exchange messages	Nine for main mode; six for aggressive mode	Four
Authentication methods	• Pre-shared key (PSK) • Digital signature (RSA-Sig) • Public key encryption • Revised mode of public key encryption	• Pre-shared key (PSK) • Digital signature (RSA-Sig)
Authentication	Both peers use the same authentication	Each peer can use different authentication (for example, one using PSK and the other using RSA-Sig)
Number of combinations of a source IP range, a destination IP range, a source port, and a destination port allowed per IPsec SA	One	Multiple (IPv4 and IPv6 addresses can be configured for the same child SA)
Multi-hosting	Not supported	Supported using multiple IDs on a single IP address and port pair
Rekeying	Not defined	Defined
NAT traversal and dead peer detection	Can be defined as an extension	Supported by default
Remote access VPN	Not defined but supported by vender-specific implementations such as Mode config and Xauth	Supported by default; options including the following: • Extensible Authentication Protocol (EAP) • User authentication over EAP associated with IKE authentication • Configuration payload (CP)
Multi-homing, mobile clients, and DoS protection	Not supported	Supported, as described in RFC 4555 (DoS protection includes anti-replay function, cookies for mitigating flooding attacks, and vulnerabilities found with IKEv1)

Parameter	IKEv1	IKEv2
Number of exchange modes	Two: main and aggressive	One
Exchange messages	Nine for main mode; six for aggressive mode	Four
Authentication methods	• Pre-shared key (PSK) • Digital signature (RSA-Sig) • Public key encryption • Revised mode of public key encryption	• Pre-shared key (PSK) • Digital signature (RSA-Sig)
Authentication	Both peers use the same authentication	Each peer can use different authentication (for example, one using PSK and the other using RSA-Sig)
Number of combinations of a source IP range, a destination IP range, a source port, and a destination port allowed per IPsec SA	One	Multiple (IPv4 and IPv6 addresses can be configured for the same child SA)
Multi-hosting	Not supported	Supported using multiple IDs on a single IP address and port pair
Rekeying	Not defined	Defined
NAT traversal and dead peer detection	Can be defined as an extension	Supported by default
Remote access VPN	Not defined but supported by vender-specific implementations such as Mode config and Xauth	Supported by default; options including the following: • Extensible Authentication Protocol (EAP) • User authentication over EAP associated with IKE authentication • Configuration payload (CP)
Multi-homing, mobile clients, and DoS protection	Not supported	Supported, as described in RFC 4555 (DoS protection includes anti-replay function, cookies for mitigating flooding attacks, and vulnerabilities found with IKEv1)

Key IKE Concepts

Make sure you know the following general IKE concepts for the SVPN 300-730 exam:

- IKE is based on the following underlying security protocols: ISAKMP, SKEME, and OAKLEY.
- IKEv2 supports AES, 3DES, Camellia, ChaCha20, and PFS+. (It also supports MOBIKE for network changes.)
- IKEv2 offers support for remote access by default, thanks to the use of EAP authentication.
- IKEv2 consumes less bandwidth than IKEv1.
- IKEv2 is resistant to network changes and is ideal for mobile devices, thanks to MOBIKE support.
- IKEv2 has built-in NAT traversal, unlike IKEv1, which must be explicitly configured.
- IKEv2 supports more algorithms than IKEv1.
- IKEv2 is more resistant to DoS attacks than IKEv1 because IKEv2 first determines whether the requestor actually exists.
- IKEv2 only uses UDP port 500, which can be blocked by a firewall or network tool.

Note

Avoid using weak pre-shared keys when using IKE. IKE is used to establish the shared secret for an IPsec connection. Both IKEv1 and IKEv2 could be vulnerable to Bleichenbacher's Oracle treat if weak pre-shared keys are used.

Learn more about this potential vulnerability at https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-felsch.pdf. Security patches that address this threat are related to vulnerability CVE-2018-0131.

IKE Authentication

In Table 3-2, you can see that different authentication options can be used as you configure IKE. Those options impact the additional steps you need to perform in order to properly configure an IKE policy on a Cisco device. IKEv1 has four different options, and IKEv2 has two. The following are all the different authentication methods and the expected additional configuration required in an IKE policy:

- **RSA signature method (rsa-sig):** If you use RSA signatures as the authentication method in your IKE policy, you will likely configure all peers to obtain certificates from a *certificate authority (CA)*, which are covered shortly. The certificates are used by each peer to securely exchange public keys. Both peers show valid certificates and automatically exchange public keys as part of any IKE negotiation using RSA signatures.

- **RSA encrypted nonces method (rsa-encr):** If the RSA encrypted nonces method is used in your IKE policy, you need to make sure each peer has the other peer's public keys. To be clear, rsa-encr does not use certificates like RSA signatures. Instead, a public/private key exchange process is used. A hybrid approach could also be used; in such a case, the initial connection would use RSA signatures to share keys, and then all future exchanges could use the RSA encrypted nonces method. This hybrid approach would require both the RSA signature and RSA encrypted nonces policies to be configure, and the RSA signature policy would have a lower priority. Any failure in rsa-encr would fall back to the rsa-sig policy. Remember that if the rsa-sig policy is also being used, you

need to have a CA configured.

- **Pre-shared keys (pre-share):** If pre-shared keys are used, you need pre-shared keys to be shared between peers. You learn more about this in the IKE configuration examples later in this chapter.
- **Digital certificates:** If you used digital certificates as the authentication method in an IKE policy, a CA must be set up to issue digital certificates. This approach simplifies authentication because you only need to enroll each peer with the CA rather than manually configure each peer to exchange keys, as in the RSA approach. If you have a larger network, it is highly recommended that you use the digital certificate approach. Cisco devices treat RSA signatures and digital certificates similarly in terms of configuration.

Note

There are differences between a digital signature (rsa-sig) and a digital certificate. A digital signature is used to verify that a document, message, or transaction is authentic—that is, the message was actually generated by the sender and not modified by a third party. Think of this as not only signing the document but proving that the message being sent is accurate, validating that the message hasn’t been tampered with, and providing nonrepudiation, meaning the sender can’t deny having sent the message.

A digital certificate is similar to an identification card such as a passport or driver’s license. Digital certificates are issued by a recognized authority and are used to validate the identity of the user or device presenting the certificate. You should expect to see SVPN 300-730 questions that challenge your understanding of these two concepts.

Later in this chapter you will see how to configure a few site-to-site VPN design examples. If you look back at Table 3-2, you will notice that IKEv2 only offers digital certificates and RSA-sig for authentication, and IKEv1 offers all four authentication methods.

VPN Tunnel Concepts

Part of creating a VPN is establishing an encrypted connection between two or more networks. Encrypting a connection means using a tunnel to encapsulate packets inside a transport protocol. Tunneling has three primary components:

- **Passenger protocol:** This protocol is the protocol that is encapsulated. Examples of passenger protocols include IP, AppleTalk, Banyan VINES, Connectionless Network Service, DECnet, and Internetwork Packet Exchange (IPX).
- **Carrier protocol:** This is a protocol such as a Generic Routing Encapsulation (GRE) protocol or IPsec.
- **Transport protocol:** This protocol is used to carry the encapsulated protocol. Typically, the transport protocol is IP.

Figure 3-3 illustrates the components involved in tunneling.

Figure 3-3 Tunneling Components Diagram

IPsec can be used for tunneling with or without the GRE protocol. IPsec can be used to protect one or more data flows between a pair of hosts, between

Cisco routers supporting IPsec, or between a Cisco router supporting IPsec and a host. We will look at how this works in site-to-site VPN configuration example using Cisco routers later in this chapter.

IPsec Tunnel Mode

IPsec can be configured in either tunnel mode or transport mode (see Figure 3-4). With IPsec tunnel mode, the entire original IP datagram is encrypted and becomes the payload in a new IP packet. Using IPsec tunnel mode allows a network device, such as a router, to perform encryption on behalf of hosts. Essentially, the network device becomes an IPsec proxy to other devices. The source router encrypts packets and forwards them along the IPsec tunnel. The destination router decrypts the original IP datagram and forwards it to the destination system. The security value of using IPsec tunnel mode is defending against traffic analysis attacks. This type of attack occurs when an attacker views VPN packets to determine the source, destination, and purpose of the traffic. IPsec tunnel mode prevents this type of attack by allowing an attacker to determine only the tunnel endpoints and not the true source or destination of the packets passing through the tunnel, even if they are the same as the tunnel endpoints.

IPsec Transport Mode

IPsec transport mode only has the IP payload encrypted, and the original IP header is left intact. The advantage of using IPsec transport mode is that the payload is encapsulated, and the original IP header is used. Devices connected to a public network can see the final source and destination of the packet if traffic is viewed because the original header is included. The benefit of allowing this visibility is that special processing may occur by intermediate network devices, based on the information in the IP header. The entire header is not exposed; the Layer 4 header is encrypted, which limits what can be examined via the packet header. The disadvantage of this approach is that part of the IP header is exposed, and this exposure could lead to an attacker performing some limited traffic analysis attacks.

Figure 3-4 IPsec Tunnel Modes

Certificate Authorities

In site-to-site VPN configurations, a certificate authority (CA) is responsible for issuing digital certificates. Digital certificates are verifiable small data files that contain identity credentials to help websites, people, and devices represent their authentic online identities. Think of a digital certificate as a passport that a CA must validate. Without a CA, something else would be needed to validate a digital certificate to ensure it represents a trusted source. This means a CA plays a critical role in how the Internet functions because there is a great need to validate everything online to ensure that trust is maintained between parties.

Let's look at an example of the role of a CA. Your browser has likely at some point warned you that you are attempting to visit a website that is not using a certificate from a trusted CA (see Figure 3-5). What the browser is saying in such a case is that the CA is not installed as a trusted authority, so there may be risks in visiting that website. This may or may not be bad; it could be that the site is using a self-signed certificate, which is not trusted, or it could mean that an attacker is attempting a man-in-the-middle attack. Another possibility is that the source may be validated, but the CA used to validate the source

might not be installed. Keep in mind that if you proceed when your browser gives you a CA warning, you could be exposing yourself to a threat, such as a snooping attack from an unwanted party, commonly called a man-in-the-middle attack.

Figure 3-5 Certificate Warning Example

Later in this chapter, you will see how a CA can be used during the authentication process in a site-to-site VPN. Certificates are very popular, especially for larger deployments as well as those leveraging IKEv2.

Crypto Map Concepts

When building site-to-site VPNs, you need to configure crypto map policies. A *crypto map* in a VPN configuration serves two purposes. First, it needs to select data flows that need security processing. Second, it needs to define the policy for flows that are selected for security processing and the crypto peer toward which that traffic needs to flow. Crypto maps are applied to interfaces. The crypto map concept was first introduced with dedicated crypto concepts but later was expanded for IPsec. We will look more closely at configuring crypto maps when we cover building an IOS-based site-to-site VPN configuration, later in this chapter.

GETVPN/DMVPN/FlexVPN

When creating a site-to-site VPN, you need to consider your deployment approach. Cisco solutions can use a few site-to-site VPN frameworks, as discussed in the next few chapters. Let's first look at GETVPN.

GETVPN

One approach we cover here is Group Encrypted Transport VPN (GETVPN), which eliminates the need for point-to-point tunnels and their associated overlay routing by instead using trusted groups. All group members in GETVPN share a common security association, also known as a *group SA*. The group SA enables group members to decrypt traffic that was encrypted by any other group member. In a GETVPN setup, there isn't a need to negotiate point-to-point IPsec tunnels between members of a group; this means GETVPN is a tunnel-less option.

Benefits of GETVPN include the following:

- It provides native routing without requiring a tunnel overlay.
- Large-scale any-to-any IP connectivity is possible using a group IPsec security architecture.
- It is ideal for quality of service (QoS)—because it preserves the IP source and destination addresses—and multicast—because it integrates with multicast without replication issues.
- It is transport agnostic.
- It leverages an underlying IP VPN routing infrastructure without the need for an overlay routing control plane.

DMVPN

Another framework option is Dynamic Multipoint VPN (DMVPN). DMVPN is ideal when you need to support distributed applications such as voice and video. DMVPN can be deployed with capabilities such as QoS, IP Multicast,

split tunneling, and routing-based failover. Larger networks use DMVPN for its ability to maintain performance for business-critical applications. Many organizations also use DMVPN to integrate services such as voice and video.

The following is a quick summery of the benefits of using DMVPN:

- The Multipoint GRE (mGRE) tunnel interface allows a single GRE interface to support multiple IPsec tunnels, reducing the size and complexity of the configuration.
- Dynamic discovery of IPsec tunnel endpoints and crypto profiles eliminates the need to configure static crypto maps defining every pair of IPsec peers, further simplifying the configuration.
- Routing protocols are used to exchange network information between the hub and spokes.
- It enables spokes to be deployed with dynamically assigned public IP addresses (behind an ISP's router).

FlexVPN

A third option is FlexVPN, which is the Cisco version of the IKEv2 standard offering for both site-to-site and remote access VPNs. FlexVPN can be used with tunnel interfaces and can also support legacy VPN implementations using crypto maps. Think of FlexVPN as a way to combine multiple frameworks (crypto maps, EzVPN, and DMVPN) into a single comprehensible set and bind it all together into a more simplified and flexible approach to deploying VPNs. With FlexVPN, configurations typically begin with the **crypto ikev2** command and also include smart defaults that help administrators use best practices when configuring a VPN.

The following list summarizes the benefits of FlexVPN:

- It can run along all existing IPsec VPNs.
- It can use GRE, allowing almost anything to run over it.
- IPsec secures the payload and supports both IPv4 and IPv6.

- Virtual interfaces allow per-spoke features such as firewalls, QoS, and ACLs.
- Multiple functionalities are embedded within one framework.

In the next few chapters, you will learn more about each of these approaches, when they would be ideal for a VPN deployment, and how to configure and troubleshoot each of them. Make sure you understand the fundamental components involved with each approach, such as what type of encryption and security associations are used.

Note

The SVPN 300-730 exam includes questions that validate your understanding of what technologies are used by each Cisco site-to-site VPN approach—that is, the components of a VPN. It might ask questions about relationships to IPsec, IKE, security associations, ESP, and AH. However, the exam will not test your knowledge of the details of Cisco hardware/models.

Now that we have covered the basic hardware, software, and protocols associated with site-to-site VPN architectures, we are ready to put these concepts into action. First, we will review how to configure a site-to-site VPN using Cisco routers. After that, we will look at how a site-to-site VPN can be configured on a Cisco security appliance like the ASA and Meraki Series.

Router Configuration with IKEv1

For the site-to-site VPN examples in this section, we focus on using Cisco routers (that is, IOS-based site-to-site VPN configurations). The first example uses Cisco ISR Series devices. The SVPN 300-730 exam is not likely to test you on the differences between the Cisco hardware models. You should, however, be able to configure a site-to-site VPN on any of these Cisco offerings because the core configuration steps are the same.

The first example shows how to set up a GRE with an IPsec tunnel. However, you could also set up this VPN by using only IPsec for the tunnel. In this first example, you will use IKEv1. Figure 3-6 shows a visual example of the desired configuration with the IP addresses used for this example.

Figure 3-6 Site-to-Site VPN Lab Diagram

The following lists the different parts required to plan and configure an IKEv1 site-to-site VPN for a Cisco router:

- Plan the VPN
- Configure the tunnel
- Configure Network Address Translation
- Configure encryption and IPsec
- Configure QoS

The following sections examine the details of these parts.

Planning the VPN

Earlier in this chapter, we listed some questions you should consider when planning how to deploy the best site-to-site VPN for your project. For this example, when you examine the answers to those questions, you find that the

customer wants to leverage existing equipment because its current Cisco ASR 1000 Series routers are capable of supporting site-to-site VPN capabilities. Because the customer already owns the Cisco routers, it can be assumed that the people who will support this solution are familiar with Cisco and how IOS configuration works. This is a point in favor of continuing to use this equipment rather than acquiring an appliance option or another vendor router.

The next step is to make sure interfaces are available and determine what IP addresses will be used. For this setup, the headquarters gateway and remote office will connect over Ethernet interface 1/0 using the 172.24.2.0/24 network. Both locations have different inside networks, but there may be an overlap of internal IP addresses being used, which means NAT has to be used. NAT allows clients at each location to maintain their existing IP address but communicate over the VPN and access systems at each of the other location.

For this scenario, you will be accessing the headquarters router called Router_HQ1 and the remote office router called Router_Remote2. You will build the site-to-site VPN between these locations. You can start the configuration by setting up the tunnel between the headquarters and the remote office.

Configuring the Tunnel

Once you have planned how the VPN scenario will look and validated that the proper hardware and licensing exists, you are ready to set up the tunnel. You learned earlier in this chapter that tunneling encapsulates data packets inside a transport protocol using a virtual interface. However, you shouldn’t think of a tunnel as having a specific protocol. The tunnel is more of a passageway for a point-to-point encapsulation scheme. Because you are using a spoke-to-spoke configuration—that is, one spoke is the HQ and the other is the remote site—for this example, you are required to configure a separate tunnel for each link. Tunnel mode options include GRE, IPsec, and IPsec over GRE.

Why Use GRE with IPsec?

When it comes to deciding which tunneling option is right for your deployment, network redundancy (also known as network resilience) is an important factor to consider. GRE can be used with IPsec to pass routing updates between sites on an IPsec VPN. Without GRE, common routing protocols that rely on broadcast and multicast will not work over the IPsec tunnel. IPsec with GRE works by encapsulating a plaintext packet, and then IPsec (in either transport mode or tunnel mode) encrypts the packets. Essentially, GRE over IPsec allows the use of dynamic routing updates, and static IP security does not. Some protocols, such as BGP, can work without IPsec over GRE; however, IGRP, EIGRP, and RIP can't pass updates without IPsec over GRE. OSPF's default configuration also requires IPsec over GRE, but OSPF can be configured to function without GRE. Allowing for multicast routing updates used in protocols such as OSPF and EIGRP using IPsec over GRE permits the delineation of primary and secondary routers. If the primary is loss, route updates can be provided for failover to the secondary, thus achieving network resiliency. The same concept can apply using an IPsec over GRE site-to-site VPN connection between two VPN routers.

Let's review how GRE and IPsec tunnel options work.

Configuring a GRE Tunnel

GRE tunnels are capable of handling transportation of multiprotocol and IP Multicast traffic between two locations that have only IP unicast connectivity. To configure a GRE tunnel for a site-to-site VPN using Cisco routers, you must configure the tunnel interface as well as a source and destination on both routers. This is done in global configuration mode. Follow these steps:

Step 1. Specify a tunnel interface number and configure the tunnel interface:

```
Router_HQ1(config)# interface tunnel 0
Router1(config-if)# ip address 192.168.3.3 255.255.255.0
```

Step 2. Specify the tunnel interface source address:

```
Router_HQ1(config-if)# tunnel source 192.168.2.4
255.255.255.0
```

Step 3. Specify the tunnel interface destination address:

```
Router_HQ1(config-if)# tunnel destination 192.168.2.5
```

Step 4. Optionally, configure GRE as the tunnel mode:

```
Router_HQ1(config-if)# tunnel mode gre ip
```

Note

You can also select IPsec as an option by using this command:

```
Router1(config-if)# tunnel mode ipsec ipv4
```

Step 5. Bring up the tunnel interface:

```
Router_HQ1(config)# interface tunnel 0
Router_HQ1(config-if)# no shutdown
%LINK-3-UPDOWN: Interface Tunnel0, changed state to up
```

Step 6. Configure traffic from the remote router by adding a **route** statement:

```
Router_HQ1(config-if)# exit
Router_HQ1(config)# ip route 10.1.4.0 255.255.255.0
tunnel 0
```

Step 7. Verify the tunnel, source, and destination and use a ping to test the connectivity, as shown in Example 3-1.

Example 3-1 Verifying the Tunnel, Source, and Destination and Pinging to Test Connectivity

```
Router_HQ1# show interfaces tunnel 1
Tunnel1 is up, line protocol is up
Hardware is Tunnel
MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation TUNNEL, loopback not set
Keepalive not set
Tunnel source 1101:1::1, destination 1501:1::1
Tunnel protocol/transport IPSEC/IPV6
Tunnel TTL 255
Tunnel transmit bandwidth 8000 (kbps)
```

```
Tunnel receive bandwidth 8000 (kbps)
Tunnel protection via IPSec (profile “tunpro”)
Last input 00:08:23, output 00:04:28, output hang never
Last clearing of “show interface” counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output
drops: 3
Queueing strategy: fifo
Output queue: 0/0 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
39 packets input, 22734 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
57 packets output, 30130 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 output buffer failures, 0 output buffers swapped out

Router_HQ1(config)# ping 192.168.3.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.6, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
4/5/8 ms
```

You can configure IPsec with or without a GRE tunnel. Earlier in this chapter, you saw that IPsec has options for tunnel mode and transport mode. Basically, IPsec tunnel mode means the entire original IP datagram is encrypted and becomes the payload in a new IP packet; IPsec transport mode preserves the original source and addresses. The decision of which approach to use depends on concerns related to exposing the IP header to potential man-in-the-middle-attacks and whether support for special processing is required.

Configuring Network Address Translation

Our next focus is Network Address Translation (NAT), which we will break down into two parts. One part focuses on site-to-site networks avoiding address collision, and other focuses on inside to outside, and vice versa, address conversion. The first focus of NAT is designed for IP address conservation and limits the number of unique IP addresses assigned to

systems on the network. Internal networks can use unregistered IP addresses (in ranges such as 192.168.0.0/16, 172.16.0.0/12, and 10.0.0.0/8) and connect them to the Internet. NAT essentially functions as a router connecting the private and public IP addresses by translating internal network addresses into legal addresses before the packets are forwarded on. NAT can be configured on a border router between the inside and outside, or public, domains; however, keep in mind that the goal is not to have NAT traffic within the tunnel. The goal is to use NAT with traffic between locations so there isn't an overlap in IP addresses when one resource at the remote site connects to a resource within the HQ network. NAT is designed to protect against this.

Note

IKEv1 does not have built-in NAT traversal but IKEv2 does. However, Cisco routers support NAT traversal with IKEv1 even though it is not part of the specification.

The second NAT objective is to configure static translation with the goal of translating internal local IP addresses into globally unique IP addresses before sending packets to an outside network. This must be done if traffic is going to pass across a public network during site-to-site communication. Static translation uses a one-to-one mapping between the internal local address and an inside global address. This approach is useful when a host on the inside must be accessible by a fixed address from the outside.

Note

Dynamic NAT could also be used. It provides an address from a pool of addresses rather than checking for a one-to-one static mapping.

There are four addresses to consider with NAT:

- **Inside local address:** The IP address assigned to a host on the inside network. This is typically not a legitimate IP address and might be from an unregistered range.
- **Inside global address:** A legitimate IP address representing one or more inside local IP addresses to the outside public network.
- **Outside local address:** The IP address assigned to an outside host as it appears to the inside network. This may or may not be a legitimate address as it was allocated from address space that is routable on the inside network.
- **Outside global address:** The IP address assigned to a host on the outside network by the host owner. This means the address was allocated by the host owner rather than the inside network.

The NAT process can work by first having an inside host open a connection to an outside host. The border router checks the NAT table upon receiving the first packet from the inside host. If the router has a static translation, the router replaces the inside address with the IP address configured as its static translation address. If dynamic translation is being used, the inside address is translated into an address pulled from a dynamic address pool of publicly routable IP addresses, and an entry is added to the router's NAT translation table. Future communication is translated by the border router, using the NAT translation table prepopulated by the static IP address assignment or dynamically populated as dynamic addresses are assigned to devices that do not have static translation assigned within the NAT translation table.

NAT Example

Next, let's look at how to configure static NAT for our site-to-site VPN example. This is using the first NAT objective covered, because this chapter's focus is for a site-to-site VPN connection. Remember that you need to bridge together two different networks that could be using the same inside IP address ranges. To address this concern, you can add NAT. Follow these steps:

Step 1. Create a static NAT translation:

```
Router_HQ1(config)# ip nat inside source static 10.1.6.5
10.2.2.2
```

Step 2. Specify the inside interface:

```
Router_HQ1config)# interface fastethernet 0/1
```

Step 3. Specify the interface as being an inside network:

```
Router_HQ1(config-if)# ip nat inside
```

Step 4. Specify the outside interface:

```
Router_HQ1(config-if)# interface serial 2/0
```

Step 5. Specify the interface facing the Internet:

```
Router_HQ1(config-if)# ip nat outside
```

Step 6. Verify the configuration, as shown in Example 3-2.

Example 3-2 Verifying the Configuration

```
Router_HQ1# show ip nat translations verbose
Pro Inside global      Inside local       Outside local
Outside
global
--- 10.2.2.2           10.1.6.5            ---                  -
--
    create 00:10:28, use 00:10:28, flags:
static

Router_HQ1# show running-config

interface FastEthernet0/1
 ip address 10.1.6.5 255.255.255.0
 no ip directed-broadcast
 ip nat inside

interface serial2/0
 ip address 172.16.2.2 255.255.255.0
 ip nat outside

ip nat inside source static 10.1.6.5 10.2.2.2
```

These steps assume that you are using the minimal required interfaces for NAT. You could configure multiple inside and outside interfaces, and this

would be expected for multiple locations. You can also set up network redundancy.

Configuring Encryption and IPsec

As mentioned earlier in this chapter, IPsec is a framework that provides data confidentiality, data integrity, and data authentication between participating peers. As also mentioned earlier in this chapter, IPsec uses IKE to handle negotiation of protocols and algorithms as well as generate the encryption and authentication keys to be used by IPsec. As you saw earlier, certificate authorities can be used to validate trust between peers. Now it's time to apply all of these ingredients to a router-based site-to-site configuration as part of establishing encryption and trust between peers. Make sure you understand how these ingredients apply for the SVPN 300-730 exam!

For this configuration example, you will use IKEv1 but will see what differences you would see if IKEv2 were used. First, you need to create IKE policies. IKE is enabled by default on Cisco routers—globally for all interfaces. IKE can also be enabled on individual interfaces for Cisco ASA appliances. You must create IKE policies for the different combinations of security algorithms. Remember that an IKE policy defines a combination of security parameters that is used during IKE negotiation. Once the two peers agree on which encryption and authentication algorithms are to be used, IKE authenticates the peers to each other. You can configure multiple IKE policies or use the default policy, which has the lowest priority and default parameter values.

IKE Policy Example

Note

An IKE policy configured with a higher priority (that is, a low number) triggers before the default policy unless you adjust the default policy's priority.

Follow these steps to create a custom IKE policy—but remember that you could just use the default IKE policy instead on modern Cisco routers:

Step 1. Enter config-isakmp mode and create a policy name:

```
Router_HQ1(config)# crypto isakmp policy 1
```

Step 2. Specify the encryption algorithm (ideally AES):

```
Router_HQ1(config-isakmp)# encryption aes
```

Step 3. Specify the hash algorithm (MD5 or SHA):

```
Router_HQ1(config-isakmp)# hash sha
```

Step 4. Name the authentication method:

```
Router_HQ1(config-isakmp)# authentication pre-share
```

Here you use pre-shared keys, but you could use RSA encrypted nonces (rsa-encr) or RSA signatures (rsa-sig) instead.

Note

The authentication method used impacts additional steps after your policy is created. Remember that this example uses IKEv1.

Step 5. Name the Diffie-Hellman group identifier, where group 5 is 1536 bits and group 2 is 1024 bits:

```
Router_HQ1(config-isakmp)# group 5
```

Step 6. Specify the security association's lifetime, in seconds:

```
Router_HQ1(config-isakmp)# lifetime 86400
```

86400 represents 1 day.

Step 7. Exit back to the global configuration mode:

```
Router_HQ1(config-isakmp)# exit
```

Step 8. Optionally, specify the time interval for IKE keepalive packets (where the default is 10 seconds) as well as the retry interval (in this

case, 3 seconds):

```
Router_HQ1(config)# crypto isakmp keepalive 15 3
```

Authentication Options

Remember that the authentication you selected for your IKE policy determines which additional steps must be taken to complete the configuration. Each authentication option requires different additional configuration steps. The following is a quick summary of the authentication options you could use:

- **RSA signature method (rsa-sig):** If you use RSA signatures as the authentication method in your IKE policy, you must configure all peers to obtain certificates from a CA.
- **RSA encrypted nonces method (rsa-encr):** If the RSA encrypted nonces method is used in your IKE policy, you need to make sure each peer has the other peer's public keys because certificates are not being used.
- **Pre-shared keys (pre-share):** If pre-shared keys are used, you need pre-shared keys.

Pre-shared Key Example

For this example, you will use pre-shared keys because that is what is used in the previous IKE configuration. The steps to create pre-shared keys are as follows:

Step 1. Specify the ISAKMP identity, which can be the address or hostname the router will use when communicating with remote routers during the IKE negotiations:

```
Router_HQ1(config)# crypto isakmp identity address
```

Step 2. Specify the shared key the router will use with remote routers. For this example, the key is test123, and remote address is 192.168.2.5:

```
Router_HQ1(config)# crypto isakmp key test123 address
192.168.2.5
```

Step 3. At the remote router (router2), specify the ISAKMP identity, which can be the address or hostname the router will use when communicating with remote routers during the IKE negotiations:

```
Router_Remote2(config)# crypto isakmp identity address
```

Step 4. At the remote router (router2), specify the shared key the router will use with remote routers. For this example, the key is test123, and remote router is 192.168.2.4:

```
Router_Remote2(config)# crypto isakmp key test123 address
192.168.2.4
```

Note

This must be the same key that the other router used.

Digital Certificate Example

You might also have decided to use digital certificates as the authentication method, which is very popular for mid-sized to larger deployments. Next, you will see how that would be configured on a Cisco IOS router. In this case, you can assume that you will use the IOS default ISAKMP policy, which uses DES, SHA, and RSA signatures. You can also assume the default Diffie-Hellman group 1 and a day lifetime (that is, 86,400 seconds), based on how you configured the previous steps in the sample site-to-site VPN configuration on a Cisco IOS router.

Follow these steps to configure the headend of the VPN:

Note

Each router peer must be enrolled with a CA.

Step 1. Log in to the router headend, access config mode, and declare a CA by using the domain name of the CA (in this case, VPN_CA):

```
Router_HQ1(config)# crypto pki trustpoint VPN_CA
```

Step 2. Specify the URL of the SCEP server in place of *url*:

```
Router_HQ1(ca-trustpoint)# enrollment url url
```

Step 3. Optionally, specify RA (registration authority) mode if your CA system includes an RA:

```
Router_HQ1(ca-trustpoint)# enrollment mode ra
```

Cisco routers automatically determine the mode, but you can manually specify it.

Step 4. Specify the location of the LDAP server if your CA provides an RA and supports LDAP, replacing *url* with the URL:

```
Router_HQ1(ca-trustpoint)# query url url
```

Step 5. Optionally, specify that other peer certificates can still be accepted by your router, even if the appropriate certificate revocation list (CRL) is not accessible to your router:

```
Router_HQ1(ca-trustpoint)# revocation-check crl none
```

Step 6. Optionally, specify how many times the router will continue to send unsuccessful certificate requests before ending attempts (where *number* is the number of attempts):

```
Router_HQ1(ca-trustpoint)# enrollment retry count number
```

Step 7. Exit ca-identity configuration mode:

```
Router_HQ1(ca-identity)# exit
```

Step 8. Verify your policy:

```
Router_HQ1(config-isakmp)#show crypto isakmp policy
Protection suite priority 1
encryption algorithm:    DES - Data Encryption Standard
(56 bit keys)
hash algorithm:    Secure Hash Standard
```

```
authentication method:    Pre-Shared Key
Diffie-Hellman group:    #1 (768 bit)
lifetime:    86400 seconds, no volume limit
```

Configuring a Crypto Map

One final encryption step to cover is configuring crypto maps. You learned earlier in this chapter that a crypto map defines the policy for flows that are selected to be processed as well as the crypto peer toward which traffic will be sent.

Crypto maps can be static or dynamic. If you use static crypto maps, you define the specific peers and the policies each one is going to use. This is fine for smaller networks, but it can be a challenge as you scale to a larger site-to-site VPN design. Dynamic crypto maps use a shared policy, which means multiple peers can use the same policy characteristics. An example could be multiple remote offices using DHCP as part of their policy. Think of using dynamic crypto maps as a way to simplify configuration from the headend because you don't have to statically map each peer's individual policy.

Note

Another option that could be used is a virtual tunnel interface (VTI). There are some key differences between crypto maps and VTIs:

- Crypto maps require an ACL, and VTIs do not.
- Running routing protocols over the VPN can be more challenging with crypto maps than with VTIs because VTIs can participate in the routing process.
- Crypto maps can be more difficult to configure.

We cover dynamic virtual tunnel interfaces and virtual tunnel interfaces in Chapter 4, "Group Encrypted Transport VPN (GETVPN)."

Crypto Map Example

In the following configuration example, you will create a crypto map entry that uses IKE to establish the security association. You need to go back to the headquarters router and follow these steps:

Step 1. Create the crypto map and specify a location address. For this case, you can use local-address serial 2/0 and call it cryptomap01:

```
Router_HQ1(config)# crypto map cryptomap01
local-address serial 2/0
```

This step is required only if you have previously used the loopback command or if you are using GRE tunnels.

Step 2. Enter the crypto map configuration mode and specify a sequence number for the crypto map you created in step 1 (which is cryptomap01):

```
Router_HQ1(config)# crypto map cryptomap01 2 ipsec-isakmp
```

In this case, you configure the crypto map to use IKE to establish the security associations. You should be in the crypto map config mode.

Step 3. Create an extended access list to specify which traffic will be protected by IPsec and which traffic will not be protected by IPsec:

```
Router_HQ1(config-crypto-map)# match address 111
```

Step 4. Specify the remote IPsec peer (in this case, the remote router) by hostname or IP address:

```
Router_HQ1(config-crypto-map)# set peer 172.23.2.7
```

Step 5. Create a transform set, which is a combination of individual IPsec transforms designed to enact a specific security policy for traffic, and call it Transform1:

```
Router_HQ1(config)# crypto ipsec transform-set Transform1
esp-aes esp-sha-hmac
```

Step 6. Indicate which transform sets are allowed for this crypto map entry, and then type **exit**:

```
Router_HQ1(config-crypto-map)# set transform-set
Transform1
Router_HQ1(config-crypto-map)# exit
```

You can list multiple transform sets in order of priority, with the highest priority set first. In this case, you use Transform1 as your only set.

Step 7. Verify the crypto map, as shown in Example 3-3.

Example 3-3 Verifying the Crypto Map

```
Router_HQ1# show interfaces tunnel 1
Crypto Map: "s4second" idb: Serial2/0 local address: 172.16.2.2
Crypto Map "s4second" 2 ipsec-isakmp
        Peer = 172.23.2.7
        Extended IP access list 111
            access-list 111 permit ip
                source: addr = 10.2.2.2/255.255.255.0
                dest:   addr = 10.1.5.3/255.255.255.0S
        Current peer: 172.23.2.7
        Security-association lifetime: 4608000 kilobytes/3600
seconds
        PFS (Y/N): N
        Transform sets={proposal4,}
```

Applying Crypto Maps

Now that the crypto map is created, you need to apply it to an interface. You need to do this for each interface IPsec traffic will flow through. Think of this as the crypto map interface telling the router to have any traffic that will travel through that interface to be applied against the crypto map. The crypto map will tell the router which policy to use during the connection or security association negotiation.

Follow these steps to apply the crypto map to the serial 2/0 interface of the headquarters router:

Step 1. Specify the physical interface to apply the crypto map against (in this case, serial 2/0) and enter configuration mode:

```
Router_HQ1(config)# interface serial 2/0
```

Step 2. Apply the crypto map you created:

```
Router_HQ1(config-if)# crypto map cryptomap01
```

Step 3. Exit back to global configuration mode:

```
Router_HQ1(config-if)# exit
```

Step 4. Go to privileged EXEC mode and clear the existing IPsec security associations so any changes are used immediately:

```
Router_HQ1# clear crypto sa
```

Step 5. As shown in Example 3-4, verify that the crypto map is applied to the interface by using the command **show crypto map interface** against the specific interface you applied the crypto map against.

Example 3-4 Verifying That the Crypto Map Is Applied to the Interface

```
Router_HQ1# show crypto map interface serial 2/0
Crypto Map “s4second” 2 ipsec-isakmp
        Peer = 172.23.2.7
        Extended IP access list 111
            access-list 111 permit ip host 10.2.2.2 host
10.1.5.3
        Current peer:172.23.2.7
        Security association lifetime:4608000 kilobytes/1000
seconds
        PFS (Y/N):N
        Transform sets={ proposal4, }
```

Configuring QoS

At this point, your site-to-site VPN is configured, but you want to make sure the performance over the VPN is acceptable to users; that is, you could configure QoS against higher-priory traffic to improve the VPN service. Think of QoS as a method of creating better and more predictable service. You can use QoS to improve loss characteristics, avoid or deal with network congestion, shape traffic, and enforce traffic priorities. QoS is out of scope for this chapter and the SVPN exam, but know it is an additional option once the VPN is up.

Note

QoS can provide value, but it can also cause problems if not used properly.

For example, if you prioritize traffic for one application, you may be degrading service for another. Make sure to plan traffic priorities before deploying a QoS strategy.

Router Configuration with IKEv2

Earlier in this chapter, you learned about the differences between IKEv1 and IKEv2. Essentially, IKE is an encryption protocol that handles request and response actions. IKE ensures that traffic is secure by establishing and handling the SA attribute within an authentication suite, which is usually IPsec.

Primary Router Configuration Example

You need to know both IKEv1 and IKEv2 for the SVPN 300-730 exam, and you will see both options deployed over real networks. Therefore, this section walks through a VPN configuration using IKEv2 with IPsec.

Note

IKE concepts are foundational for future chapters that leverage both IKEv1 and IKEv2.

Defining the IKEv2 Keyring

To begin router configuration with IKEv2, you need to configure the IKEv2 *keyring*, which consists of pre-shared keys associated with an IKEv2 profile. These pre-shared keys perform authentication. An IKEv2 keyring is a repository of symmetric and asymmetric pre-shared keys and is independent of the IKEv1 keyring.

The IKEv2 keyring is associated with an IKEv2 profile, which you will configure in a later step. The IKEv2 keyring gets its virtual routing and

forwarding (VRF) context from the associated IKEv2 profile. Follow these steps to configure the IKEv2 keyring:

Step 1. Define the new keyring:

```
Router_HQ1(config)# crypto ikev2 keyring KR1
```

Step 2. Specify the peer name:

```
Router_HQ1(config-ikev2-keyring)# peer PeerRemote
```

Step 3. Specify the IP address of the peer router:

```
Router_HQ1(config-ikev2-keyring)# address 192.168.2.5
```

Step 4. Specify the pre-shared key that will be used between peers:

```
Router_HQ1(config-ikev2-keyring)# pre-shared-key
Secret_Key
```

Defining the IKEv2 Proposal

Next, you need to define the IKEv2 proposal, which consists of transforms. Much as with IKEv1, with IKEv2 transforms are used in the negotiation of IKE SAs. Follow these steps to define the IKEv2 proposal:

Step 1. Define the name for the proposal for the remote router:

```
Router_HQ1(config)# crypto ikev2 proposal PRO-Remote
```

Step 2. Specify the encryption type, integrity type, and group:

```
Router_HQ1(config-ikev2-proposal)# encryption aes-cbc-256
Router_HQ1(config-ikev2-proposal)# integrity sha512
Router_HQ1(config-ikev2-proposal)# group 24
```

Defining IKEv2 Policies

Next, you need to build an IKEv2 policy, which contains IKEv2 proposals. Proposals are used to negotiate the encryption algorithm, integrity algorithm, PRF algorithms, and Diffie-Hellman group. Follow these steps:

Step 1. Define the name for the policy:

```
Router_Remote2(config)# crypto ikev2 policy POL-Remote
```

Step 2. In the policy configuration state, name the proposal created in step 1:

```
Router_Remote2(config-ikev2-policy)# proposal PRO-Remote
```

Defining a Crypto ACL for IPsec Secured Traffic

A crypto ACL is not like a normal ACL; it isn't used to permit or deny traffic as normal ACLs do. Instead, a crypto ACL permit state is used to identify the traffic that is to be secured using IPsec. You use a crypto ACL **deny** statement to identify the traffic that you do not want to secure. Essentially, you use a crypto ACL to define which traffic will and will not be encrypted. Follow these steps:

Step 1. Define the extended ACL, which you can call HQ-Remote-CACL:

```
Router_HQ1(config)# ip access-list extended HQ-Remote-
CACL
```

Step 2. Define the traffic that will be permitted meaning (that is, the traffic that will be encrypted, which in this case is 192.168.2.0 class C traffic):

```
Router_HQ1 config-ext-nacl# permit ip 192.168.2.0
0.255.255.255
```

Defining a Transform Set

As with IKEv1, you use a transform set to define how the data traffic will flow between IPsec peers. You define the transform set in one step:

Step 1. Define the transform set with parameters:

```
Router_HQ1(config)# crypto ipsec transform-set TS_Remote
esp-aes esp-sha512-hmac
```

Defining an IKEv2 Profile

Creating an IKEv2 profiles is similar to the process of building an IKEv1 ISAKMP profile. You define the keyring, remote IP address, and local and remote authentication:

Step 1. Define the name of the IKEv2 profile:

```
Router_HQ1(config)# crypto ikev2 profile Remote-Profile
```

Step 2. Specify the IP address of router2:

```
Router_HQ1(config-ikev2-profile)# match identity remote
address 192.168.2.5 255.255.255.2555
```

Step 3. Define the local authentication, remote authentication, and keyring:

```
Router_HQ1(config-ikev2-profile)# authentication local
pre-share
Router_HQ1(config-ikev2-profile)# authentication remote
pre-share
Router_HQ1(config-ikev2-profile)# keyring local KR1
```

Defining Crypto Maps

You need to create crypto maps to connect together all pieces of the IPsec configuration. You do this by using a crypto map, which can contain one or more entries. In this case, you need to include the crypto ACL, transform set, remote peer, and other information, such as the security lifetime for the data connection in this VPN:

Step 1. Specify the name for the crypto map (in this case, CMAP-Remote2):

```
Router_HQ1(config)# crypto map CMAP-Remote2 10 ipsec-
isakp
```

Step 2. In the crypto map configuration state, set the IP address for the remote peer:

```
Router_HQ1(config-crypto-map)# set peer 192.168.2.4
```

Step 3. Define the other items you built in previous steps, including the group, transform set, and profile, and specify the lifetime of the data connection:

```
Router_HQ1(config-crypto-map)# set pfs group24
Router_HQ1(config-crypto-map)# set security-association
lifetime seconds 3600
Router_HQ1(config-crypto-map)# set transform-set
TS_Remote
Router_HQ1(config-crypto-map)# set ikev2-profile Remote-
Profile
```

```
Router_HQ1(config-crypto-map)# match address HQ-Remote-
CACL
```

Activating Crypto Maps

Finally, you apply the crypto maps to interfaces that will send traffic through the VPN. For this example, assume that the HQ1 router will use interface gi0/0:

```
Router_HQ1(config)# interface gi0/0
Router_HQ1(config-if)# crypto map CMAP-Remote2
```

Repeating Similar Steps for the Other Router

You need to repeat on the Remote2 router steps similar to those you just took. Slight changes are needed to point toward the HQ1 router. Here is a summary of the configuration steps:

Step 1. Define the keyring on Router2:

```
Router_Remote2(config)# crypto ikev2 keyring KR1
```

Step 2. Name the other peer (in this case, PeerHQ1):

```
Router_Remote2(config-ikev2-keyring)# peer PeerHQ1
```

Step 3. Specify the IP address of the peer router (in this case, the HQ router):

```
Router_Remote2(config-ikev2-keyring)# address 192.168.2.4
```

Step 4. Specify the pre-shared key you created on HQ1:

```
Router_Remote2(config-ikev2-keyring)# pre-shared-key
Secret_Key
```

Step 5. Define the name for the proposal for the remote router:

```
Router_Remote2(config)# crypto ikev2 proposal PRO-HQ1
```

Step 6. In the proposal configuration state, specify the encryption type, integrity type, and group:

```
Router_Remote2(config-ikev2-proposal)# encryption aes-
cbc-256
```

```
Router_Remote2(config-ikev2-proposal)# integrity sha512
Router_Remote2(config-ikev2-proposal)# group 24
```

Step 7. Define the name for the policy:

```
Router_Remote2(config)# crypto ikev2 policy POL-HQ1
```

Step 8. In the policy configuration state, name the proposal created in step 7:

```
Router_Remote2(config-ikev2-policy)# proposal PRO-HQ1
```

Step 9. Define the extended ACL:

```
Router_Remote2(config)# ip access-list extended Remote-
HQ-CACL
```

Step 10. Define the traffic that will be permitted (that is, the traffic that will be encrypted):

```
Router_Remote2(config-ext-nacl)# permit ip 192.168.3.0
0.255.255.255
```

Step 11. Name the transform set and provide parameters:

```
Router_Remote2(config)# crypto ipsec transform-set TS_HQ1
esp-aes esp-sha512-hmac
```

Step 12. Define the name of the IKEv2 profile:

```
Router_Remote2(config)# crypto ikev2 profile HQ1-Profile
```

Step 13. Set the IP address of the HQ1 router:

```
Router_Remote2(config-ikev2-profile)# match identity
remote address 192.168.2.4 255.255.255.2555
```

Step 14. Define the local authentication, remote authentication, and keyring:

```
Router_Remote2(config-ikev2-profile)# authentication
local pre-share
Router_Remote2(config-ikev2-profile)# authentication
remote pre-share
Router_Remote2(config-ikev2-profile)# keyring local KR2
```

Step 15. Name the crypto map (in this case, CMAP-HQ1):

```
Router_HQ1(config)# crypto map CMAP-HQ1 10 ipsec-isakp
```

Step 16. Set the IP address for the remote HQ1 peer:

```
Router_HQ1(config-crypto-map)# set peer 192.168.2.5
```

Step 17. Define the parameters you created in the previous steps:

```
Router_HQ1(config-crypto-map)# set pfs group24.
Router_HQ1(config-crypto-map)# set security-association
lifetime seconds 3600
Router_HQ1(config-crypto-map)# set transform-set TS_HQ1
Router_HQ1(config-crypto-map)# set ikev2-profile PRO-HQ1
Router_HQ1(config-crypto-map)# match address Remote-HQ-
CAL
```

Step 18. Apply the crypto map to an interface:

```
Router_HQ1(config)# interface gi0/0
Router_HQ1(config-if)# crypto map CMAP-HQ1
```

Note

The detailed router configuration examples provided in this chapter should give you an understanding how an IOS-based site-to-site VPN can be built. We will look more at IOS-based VPN configuration of routers in upcoming chapters. The following section shows how to perform a similar configuration using a few different Cisco security appliance options.

Appliance Configuration

Configuring a site-to-site VPN for a Cisco security appliance is a different process from configuring a site-to-site VPN for a router, although the architecture and design concepts are similar. You can access and modify the configuration of a Cisco appliance such as an ASA firewall by using a few approaches. You could access the command-line interface (CLI) and perform the steps required to set up a site-to-site VPN. Another option is to use a graphical user interface (GUI) option such as Cisco Adaptive Security Device Manager (ASDM), Cisco Security Manager (CSM), or Cisco Defense Orchestrator (CDO).

For the first Cisco appliance example, you will build a site-to-site VPN on a Cisco ASA. You will use IKEv1 IPsec for a site-to-site tunnel between a Cisco 5515-X Series ASA running software Version 9.2.x and a Cisco 5515-

X Series ASA running Version 8.2.x. As a reminder, UDP point 500 needs to be available for ISAKMP, IP protocol 50 for ESP, and protocol 51 for AH. UDP 4500 also needs to be opened for the IPsec data plane when NAT traversal is needed. Figure 3-7 shows this lab setup. You will use both ASDM and CLI for the following configuration examples.

Note

ASA Version 8.4 and later provide support for both IKEv1 and IKEv2.

Figure 3-7 ASA Site-to-Site Configuration

ASDM Example

This section shows you how to build a site-to-site VPN by using a GUI like ASDM to configure a Cisco ASA. You can access Cisco ASDM by going to the management IP address of the ASA in a web browser and following the prompts to install ASDM. In this example, as shown in Figure 3-8, the management interface is 198.19.40.253.

Note

You must set up access for ASDM, or you won't be able to access the GUI.

This should be part of your initial setup of the ASA solution, along with other steps, including setting a username and password.

Figure 3-8 Cisco ASDM Launcher

When you are able to access ASDM, you can simplify the site-to-site deployment by using the Site-to-Site VPN wizard, as shown in these steps:

Step 1. Find the Site-to-Site VPN wizard by going to **Wizards** > **VPN Wizards** > **Site-to-Site VPN Wizard** (see Figure 3-9).

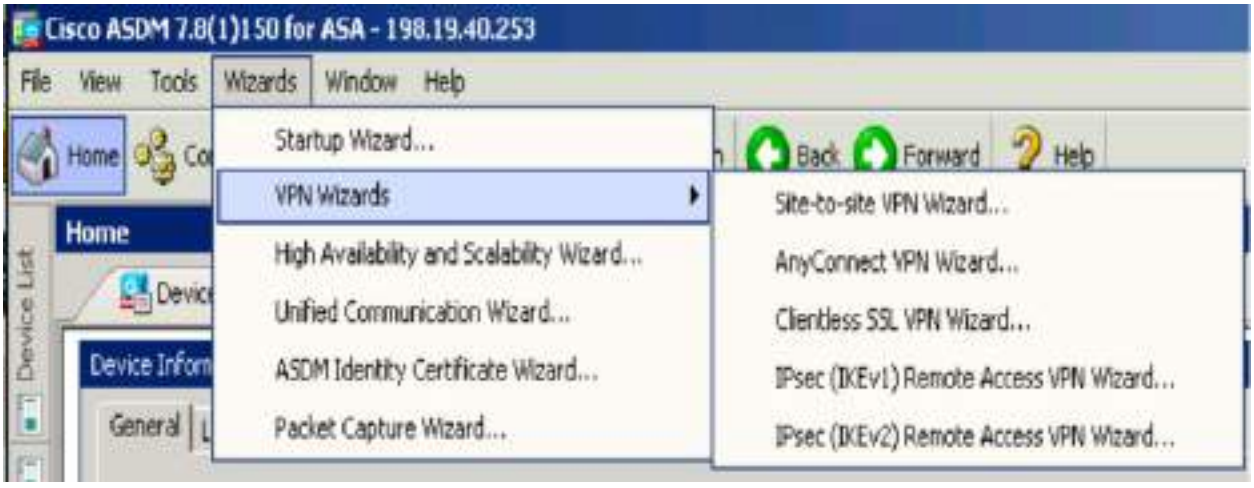


Figure 3-9 Accessing the Site-to-Site VPN Wizard in ASDM

Step 2. On the wizard home page, which includes a visual diagram and a video of how site-to-site VPNs can be configured, click the **Next** button (see Figure 3-10).

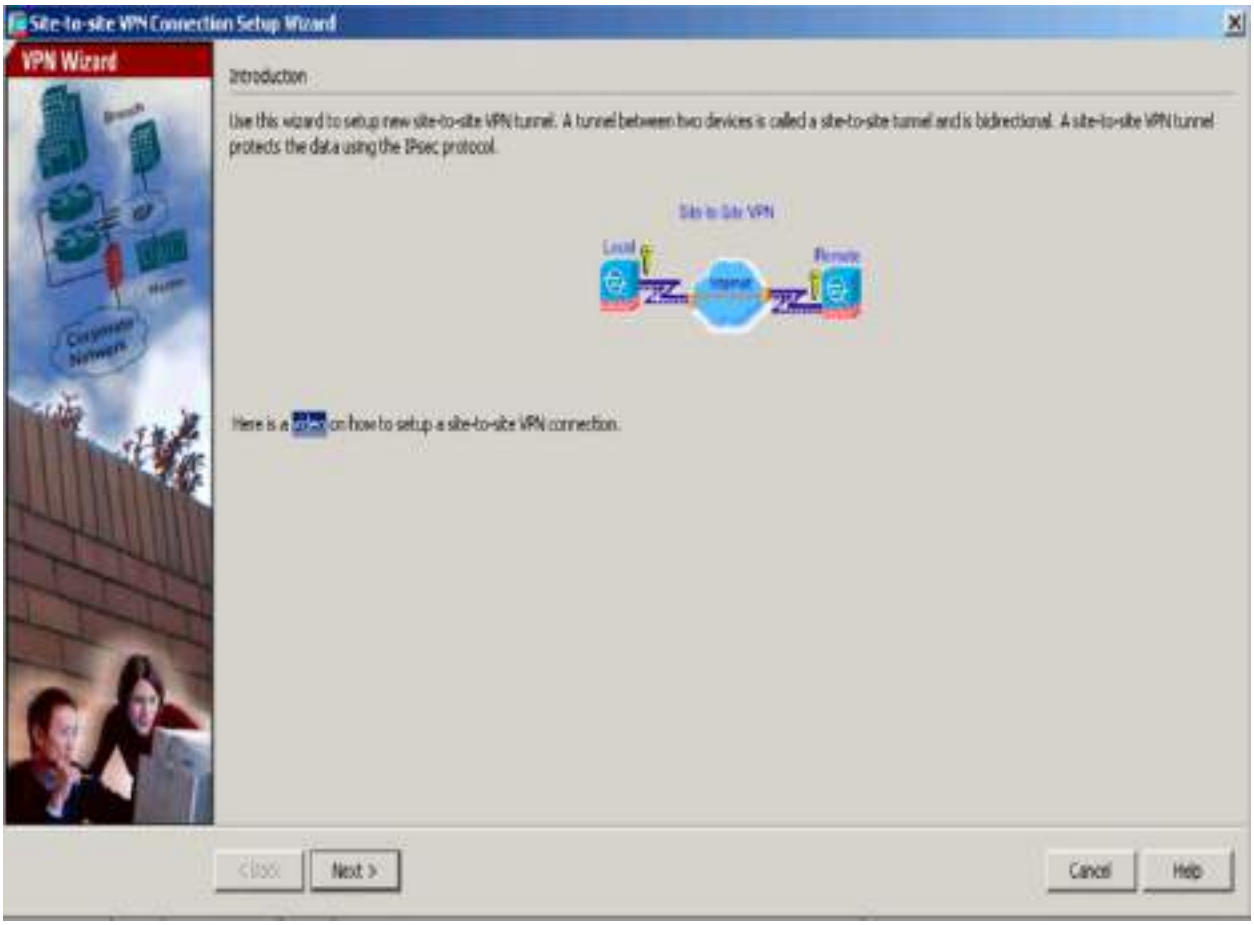


Figure 3-10 ASDM Site-to-Site VPN Wizard Introduction Page

Step 3. When you are asked to configure the peer IP address for the site-to-site VPN, use **192.168.1.1** on the remote ASA, which you will call ASA SITE-B, and specify that the VPN access interface is the **outside** interface (see Figure 3-11). Click the **Next** button.

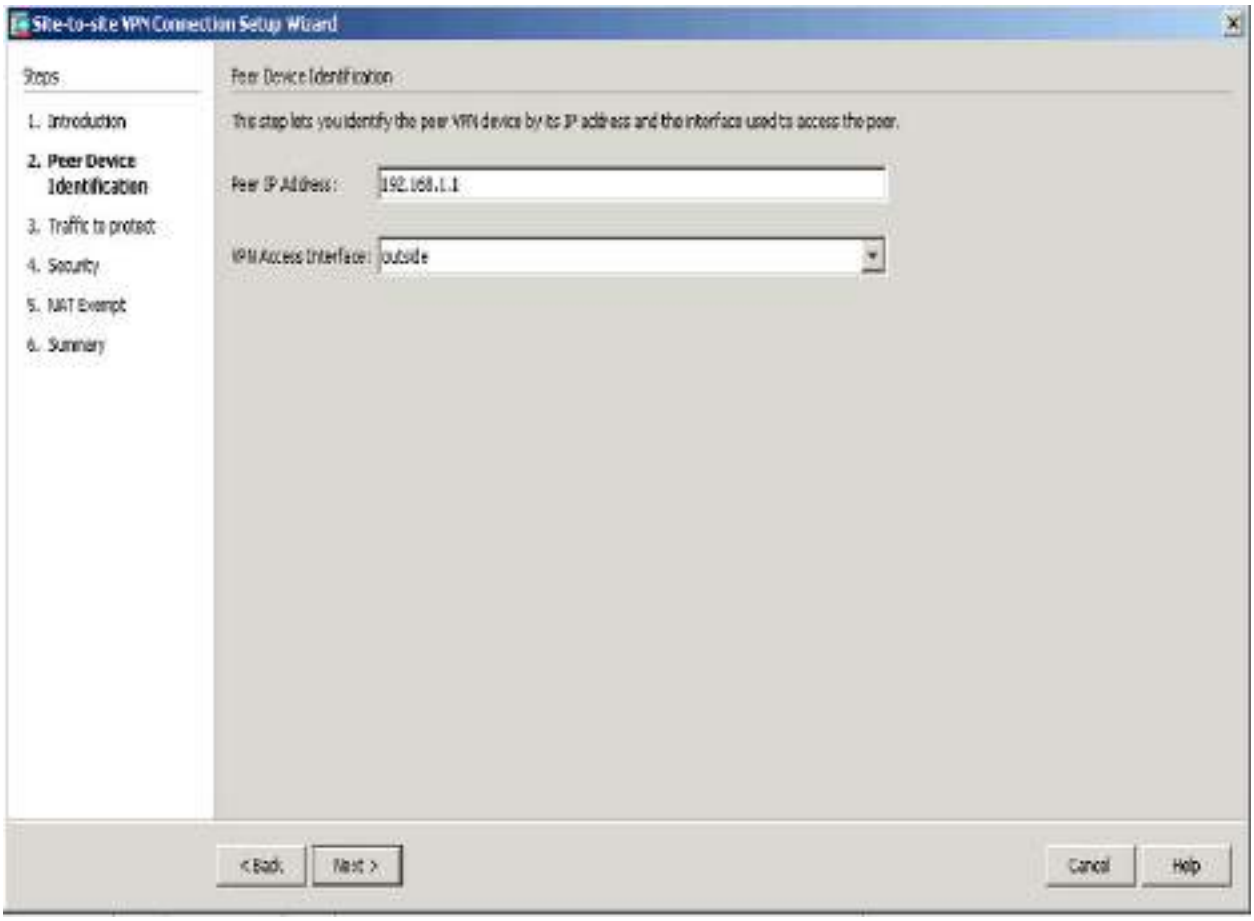


Figure 3-11 ASDM Site-to-Site VPN Wizard Peer Device Setup Page

Step 4. Define the local and remote networks, which represent the traffic source and destination: **10.2.2.0/24** for the local network and **10.1.1.0/24** for the remote network (see Figure 3-12). Click **Next**.

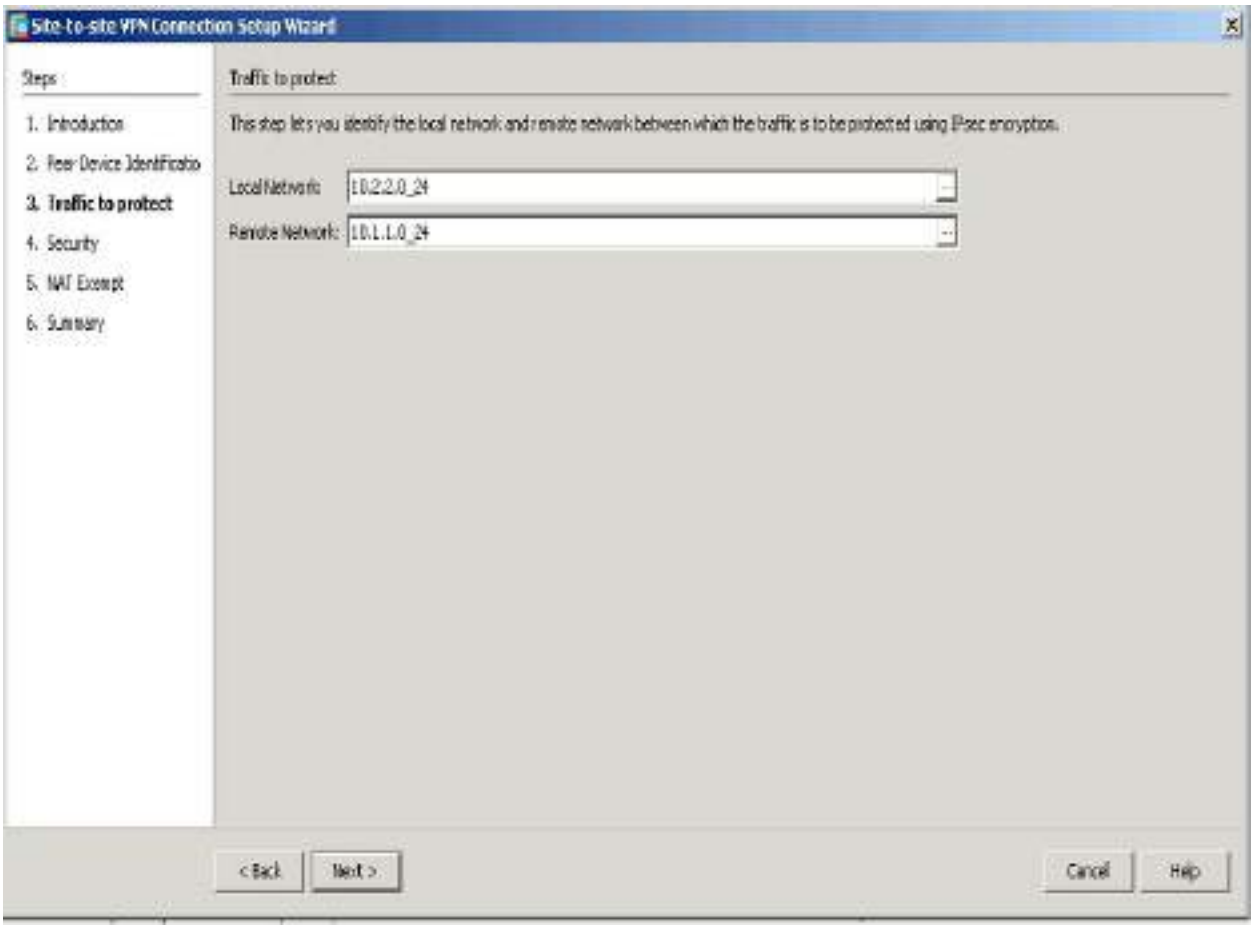


Figure 3-12 ASDM Site-to-Site VPN Wizard Connection Setup Page

Step 5. On the Security page, configure a pre-shared key (see Figure 3-13). This process is similar to the process you used to configure the site-to-site VPN on the Cisco routers. This key must be the same on both ASAs. Click **Next**.

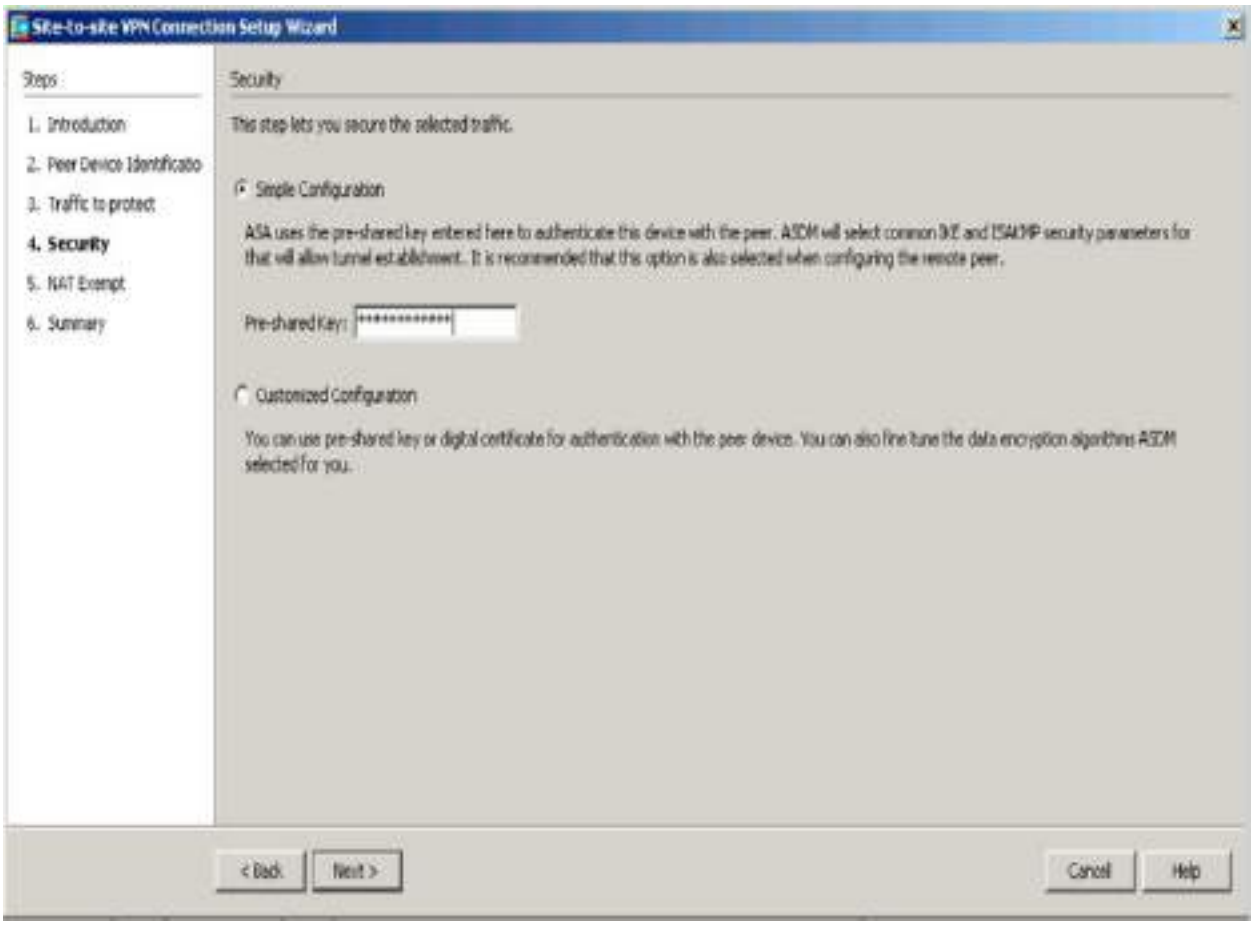


Figure 3-13 ASDM Site-to-Site VPN Wizard Peer Device Setup Page

Step 6. On the next screen, where you build the NAT rule for this VPN setup, choose whether any network such as the ASA side host/network should be exempt from the NAT rule (see Figure 3-14). This is important to ensure that NAT is performed properly. Click **Next**.

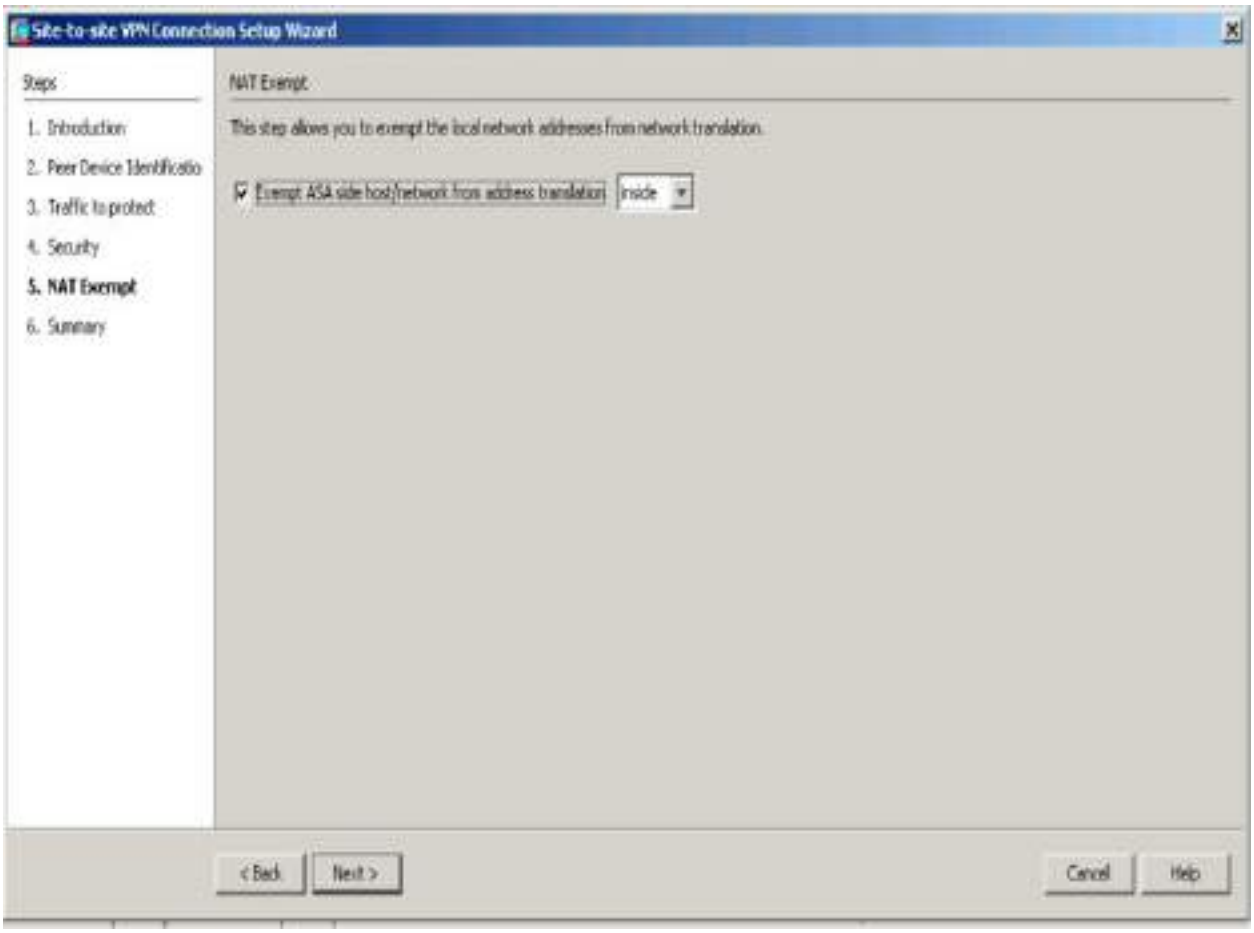


Figure 3-14 ASDM Site-to-Site VPN Wizard NAT Example Page

Step 7. On the final page of the wizard, read the summary of the configuration that will be pushed to the ASA (see Figure 3-15). This is a good place to review the associated command-line code with your configuration to ensure that you understand what command-line entries are being created by the ASA Site-to-Site VPN wizard. Click **Finish** to complete the wizard.

Note

For the SVPN 300-730 exam, we highly recommend that you make sure you understand the associated command-line entries that are created by the Site-to-Site VPN wizard. The wizard shows you all of the command-line code it is about to deploy, and you should study that output!

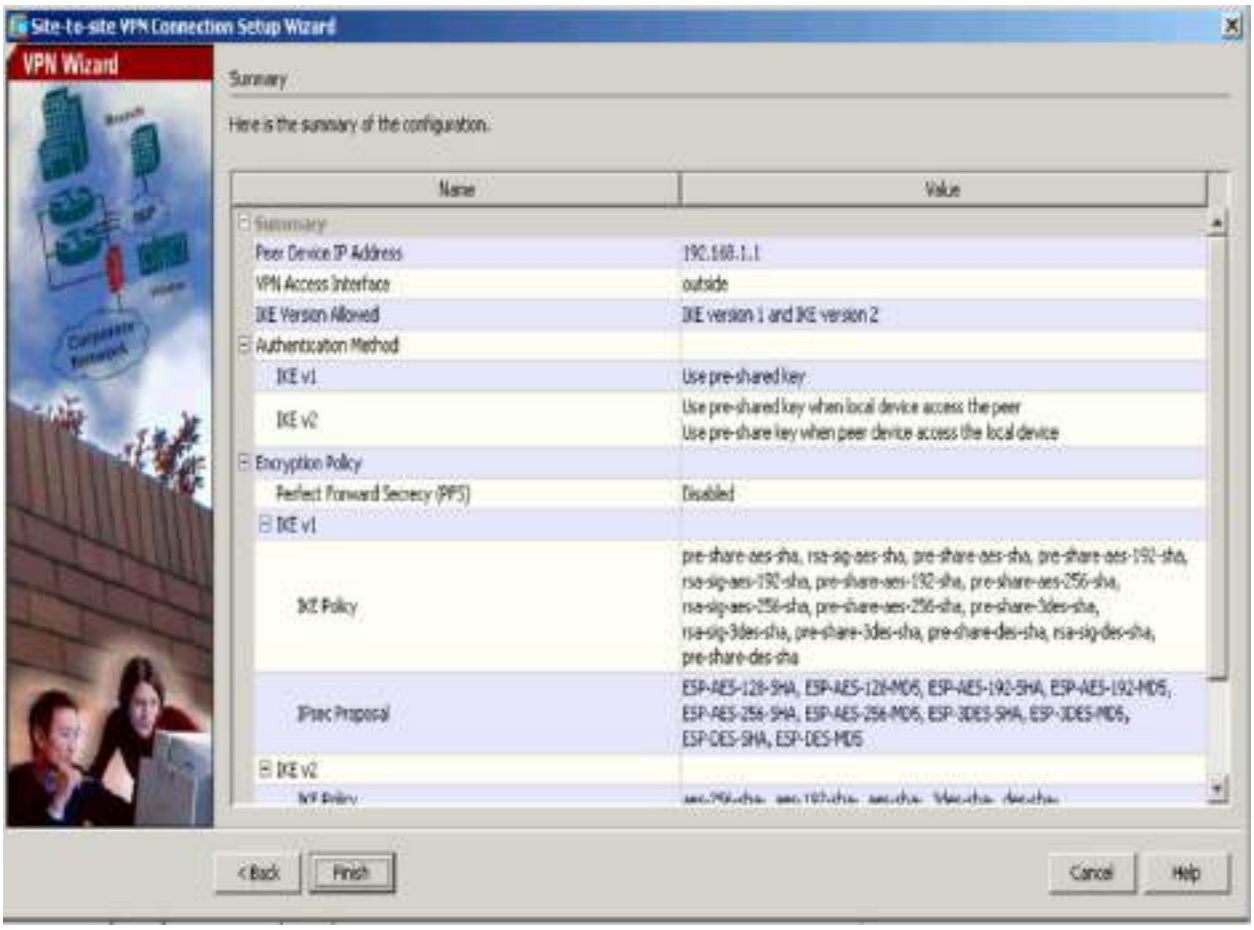


Figure 3-15 ASDM Site-to-Site VPN Wizard Summary Page

Step 8. Verify that the site-to-site VPN is built by going to **Monitoring** > **VPN**. You should be able to see the peer IP address, the protocol used to build the tunnel, the encryption algorithm, the time when the tunnel came up, the up-time of the tunnel, and the number of packets that have been passed through the tunnel. You will learn more about monitoring and troubleshooting VPNs on the ASA in Chapter 10.

Note

Click the Refresh button to update the information shown on the VPN page.

ASA Command-Line Example

In the example in this section, you will build on the same site-to-site VPN you have begun to create, but this time you will do so by using the ASA CLI. You have already built the ASA configuration on the HQ site, and now you need to build the ASA configuration at the remote site. In this example, you will build the connection back to the headquarters. This means you will build an IKEv1 IPsec site-to-site VPN on an ASA running Version 8.4 or later software. The final result will be similar to the CLI output displayed on the configuration summary page of the ASDM Site-to-Site VPN wizard.

You begin the CLI configuration by configuring IKEv1, and then you configure IPsec. Follow these steps:

Step 1. Enable IKEv1 on the outside interface:

```
Crypto ikev1 enable outside
```

Step 2. Create an IKEv1 policy that defines the methods to be used for hashing, authentication, Diffie-Hellman group, lifetime, and encryption:

```
crypto ikev1 policy 1
!The 1 in the above command refers to the Policy suite
priority(1 highest, 65535 lowest)
  authentication pre-share
  encryption aes
  hash sha
  group 2
  lifetime 86400
```

Step 3. Under the IPsec attributes, create a tunnel group and configure the peer IP address as well as the tunnel pre-shared key:

```
tunnel-group 192.168.1.1 type ipsec-l2l
tunnel-group 192.168.1.1 ipsec-attributes
 ikev1 pre-shared-key cisco
 ! Note the IKEv1 keyword at the beginning of the pre-
shared-key command.
```

Step 4. Create an access list that defines the traffic to be encrypted and sent through the tunnel. There can be one or more entries, depending on how many subnets will be involved with the site-to-site VPN. For this example, the traffic that will be using the VPN will be coming

from the source 10.2.2.0 subnet and going to the 10.1.1.0 network. Since you are using Version 8.4 or later, you need to build network objects for these subnets and permit this traffic by using an access list:

```
object network 10.2.2.0_24
 subnet 10.2.2.0 255.255.255.0
object network 10.1.1.0_24
 subnet 10.1.1.0 255.255.255.0

access-list 100 extended permit ip object 10.2.2.0_24
object 10.1.1.0_24
```

Note

In ASA Version 8.4 and later, object groups serve as containers for networks, subnets, host IP addresses, or multiple objects. For the SVPN 300-730 exam, make sure you understand how object groups work. You can find a general overview of ASA objects in the latest ASA documentation.

Step 5. Configure the transform set, which must use the keyword IKEv1 and which must also be created on the other ASA:

```
crypto ipsec ikev1 transform-set myset esp-aes esp-sha-
hmac
```

Step 6. Configure a crypto map and apply it to the outside interface. The crypto map should include the peer IP addresses, the access list that contains the VPN traffic, the transform set, and an optional Perfect Forward Secrecy setting used to create a new pair of Diffie-Hellman keys that are used to protect associated data:

```
crypto map outside_map 20 match address 100
crypto map outside_map 20 set peer 192.168.1.1
crypto map outside_map 20 set ikev1 transform-set myset
crypto map outside_map 20 set pfs
crypto map outside_map interface outside
```

Step 7. Create a NAT rule and ensure that the VPN traffic is not subjected to any other NAT rule (see Example 3-5).

Example 3-5 Creating a NAT Rule for Sourcing Traffic

```
nat (inside,outside) 1 source static 10.2.2.0_24 10.2.2.0_24
destination static
 10.1.1.0_24 10.1.1.0_24 no-proxy-arp route-lookup

object-group  network to a dynamic range of IP addresses within
the
10.1.1.0/24 subnet. Remember that dynamic NAT means a IP
address comes
from a pool of addresses. 10.x.x.x_SOURCE
 network-object  10.4.4.0 255.255.255.0
 network-object  10.2.2.0 255.255.255.0

object network 10.x.x.x_DESTINATION
 network-object  10.3.3.0 255.255.255.0
 network-object  10.1.1.0 255.255.255.0

nat (inside,outside) 1 source static 10.x.x.x_SOURCE
10.x.x.x_SOURCE destination
 static 10.x.x.x_DESTINATION  10.x.x.x_DESTINATION no-proxy-arp
route-lookup
```

Note

When you plan to use multiple subnets, you must create object groups with all source and destination subnets. Those object groups must be used in the NAT rule.

Step 8. Create an internal group policy to define specific settings that will apply to the tunnel, including VPN attributes, such as LT2P using IPsec, SSL VPN client, Web VPN, and the VPN idle timeout:

```
group-policy SITE_A internal
vpn-tunnel-protocol ikev1
vpn-idle-timeout none
```

The vpn-idle-timeout attribute allows the tunnel to stay idle without any traffic. You can define the idle time by using minutes or state none, as you did in the example to keep the tunnel up regardless of whether traffic is seen.

Step 9. Set the default group policy under the tunnel group:

```
tunnel-group 192.168.1.1 general-attributes
 default-group-policy SITE_A
```

This means the default settings that you did not define in the group policy will be pulled from a global default policy.

Step 10. To verify that the site-to-site VPN is working, verify that the Phase 1 configuration is active on each side by checking the status of the security association of the ASA 5515:

```
show crypto ikev1 sa

Active SA: 1
   Rekey SA: 0 (A tunnel will report 1
Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 192.168.1.1
    Type    : L2L             Role    :
initiator
    Rekey   : no              State   :
MM_ACTIVE
```

Step 11. Verify Phase 1 on the ASA 5510:

```
show crypto isakmp sa

Active SA: 1
   Rekey SA: 0 (A tunnel will report 1
Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 172.16.1.1
    Type    : L2L             Role    :
initiator
    Rekey   : no            State   :
MM_ACTIVE
```

Step 12. Verify phase 2 on the ASA 5515 by using the same command (see

Example 3-6).

Example 3-6 Verifying Phase 2 on an ASA 5515 by Using **show crypto ipsec sa**

```
show crypto ipsec sa

interface: FastEthernet0
   Crypto map tag: outside_map, local addr. 192.168.1.1
  local ident (addr/mask/prot/port):
(10.1.1.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port):
(10.2.2.0/255.255.255.0/0/0)
  current_peer: 172.16.1.1
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 20, #pkts encrypt: 20, #pkts digest 20
   #pkts decaps: 20, #pkts decrypt: 20, #pkts verify 20
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0,
   #pkts decompress failed: 0, #send errors 0, #recv errors 0
    local crypto endpt.: 192.168.1.1, remote crypto endpt.:
172.16.1.1
    path mtu 1500, media mtu 1500
    current outbound spi: 3D3
    inbound esp sas:
     spi: 0x136A010F(325714191)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       slot: 0, conn id: 3442, flow_id: 1443, crypto map:
outside_map
       sa timing: remaining key lifetime (k/sec): (4608000/52)
       IV size: 8 bytes
       replay detection support: Y
    inbound ah sas:
    inbound pcp sas:

    inbound pcp sas:
    outbound esp sas:
     spi: 0x3D3(979)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       slot: 0, conn id: 3443, flow_id: 1444, crypto map:
outside_map
       sa timing: remaining key lifetime (k/sec): (4608000/52)
       IV size: 8 bytes
       replay detection support: Y
    outbound ah sas:
```

```
    outbound pcp sas

  #pkts encaps: 20, #pkts encrypt: 20, #pkts digest 20
  #pkts decaps: 20, #pkts decrypt: 20, #pkts verify 20
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0,
  #pkts decompress failed: 0, #send errors 0, #recv errors 0
   local crypto endpt.: 172.16.1.1, remote crypto endpt.:
172.16.1.1
   path mtu 1500, media mtu 1500
   current outbound spi: 3D3
   inbound esp sas:
    spi: 0x136A010F(325714191)
      transform: esp-aes esp-sha-hmac ,
      in use settings ={Tunnel, }
      slot: 0, conn id: 3442, flow_id: 1443, crypto map:
outside_map
      sa timing: remaining key lifetime (k/sec):
(4608000/52)      IV size: 8 bytes
      replay detection support: Y
   inbound ah sas:
   inbound pcp sas:
   inbound pcp sas:
   outbound esp sas:
    spi: 0x3D3(979)
      transform: esp-aes esp-sha-hmac ,
      in use settings ={Tunnel, }
      slot: 0, conn id: 3443, flow_id: 1444, crypto map:
outside_map
      sa timing: remaining key lifetime (k/sec): (4608000/52)
      IV size: 8 bytes
      replay detection support: Y
   outbound ah sas:
   outbound pcp sas

   Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA
during rekey)
Total IKE SA: 1

1   IKE Peer: 172.16.1.1
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE
```

Note

You can debug the site-to-site configuration by using the following command for Phase 1:

```
debug crypto ikev1 255
```

Use the following command for Phase 2:

```
debug crypto ipsec 255
```

We cover troubleshooting in more detail in Chapter 6.

Cisco Secure Firewall Example

This section walks through another Cisco appliance configuration—this one for a basic site-to-site VPN on Cisco Secure Firewall. This section assumes that you have two or more Cisco Secure Firewall systems configured and are building a site-to-site VPN.

Note

The SVPN 300-730 exam currently does not include Cisco Secure Firewall configuration as part of the learning objectives. However, we cover it because Cisco Secure Firewall is a widely deployed option and a popular upgrade option from a Cisco ASA investment.

To build a site-to-site VPN using Cisco Secure Firewall, follow these steps:

Step 1. Log in to your Cisco Secure Firewall solution (see Figure 3-16).

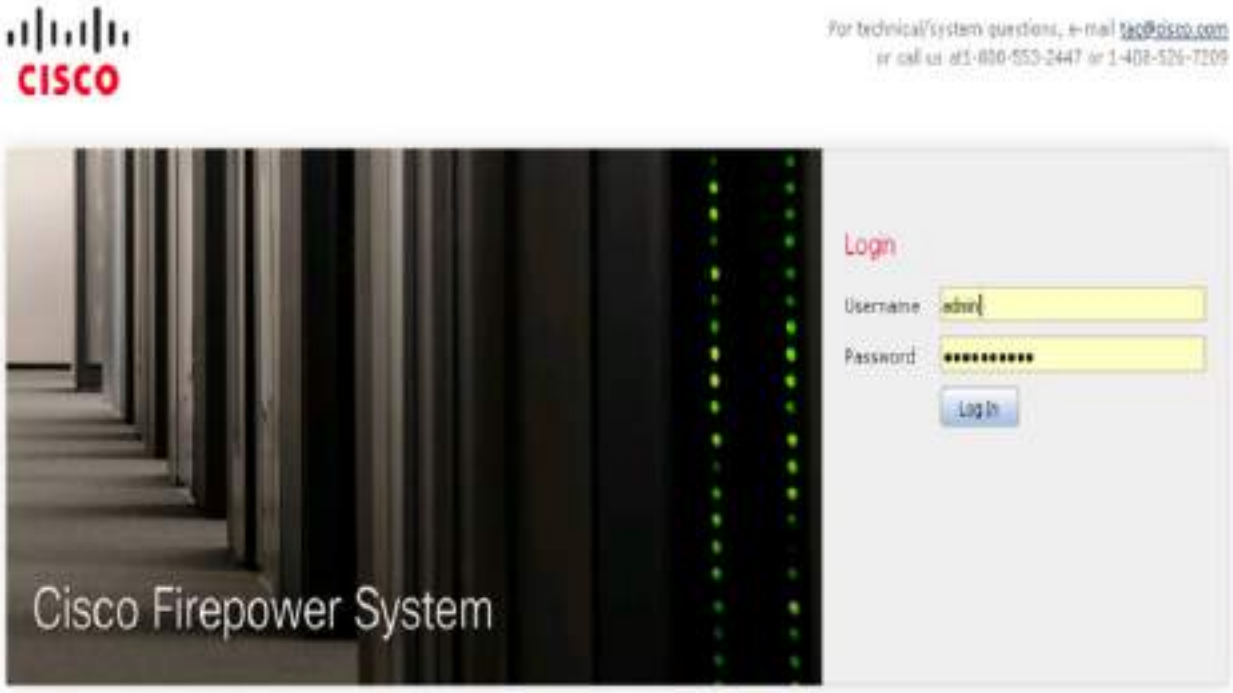


Figure 3-16 Cisco Secure Firewall Login Screen

Step 2. To access the site-to-site VPN capabilities, go to **Devices** > **VPN** > **Site to Site** (see Figure 3-17). If you haven't yet built a site-to-site VPN on the Cisco Secure Firewall solution, the next screen shows that you have nothing configured.

Figure 3-17 Accessing Site to Site in Cisco Secure Firewall

Step 3. Click the **Add VPN** button on the right side of the screen to add a new VPN and select **Firepower Threat Defense Device** (see Figure

3-18).

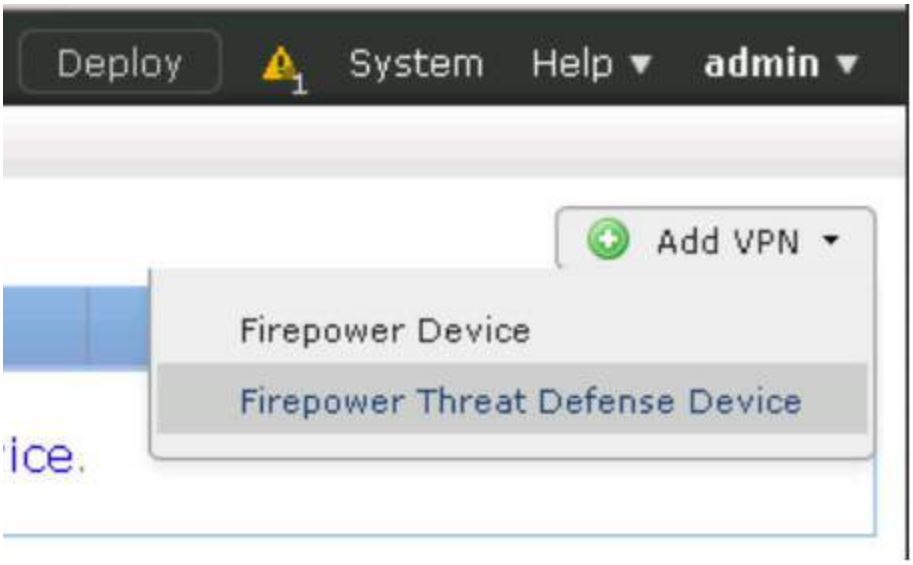


Figure 3-18 Selecting Firepower Threat Defense for a VPN Configuration Example

Step 4. In the main site-to-site VPN page, give your new VPN a name. It is recommended to include FTD in the name because that is the device type you are configuring. Next to Network Topology, choose **Point to Point** (see Figure 3-19).

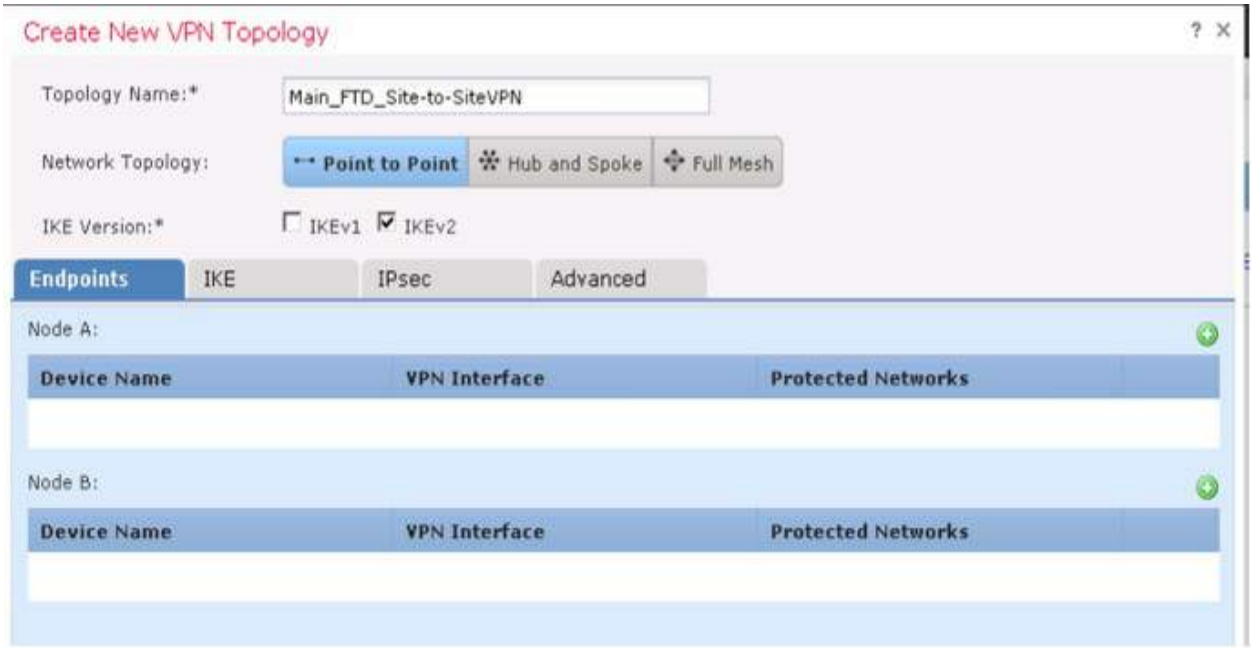


Figure 3-19 Configuring a New Site-to-Site VPN with Cisco Secure Firewall

Step 5. Click the green plus sign icon to add devices or nodes and choose which device to add, which interface will be part of the VPN, what IP address to use, the connection type, and associated certificate networks that will be protected by the VPN (see Figure 3-20). Click **OK**. Repeat this step for each Cisco Secure Firewall solution included in the site-to-site VPN setup.

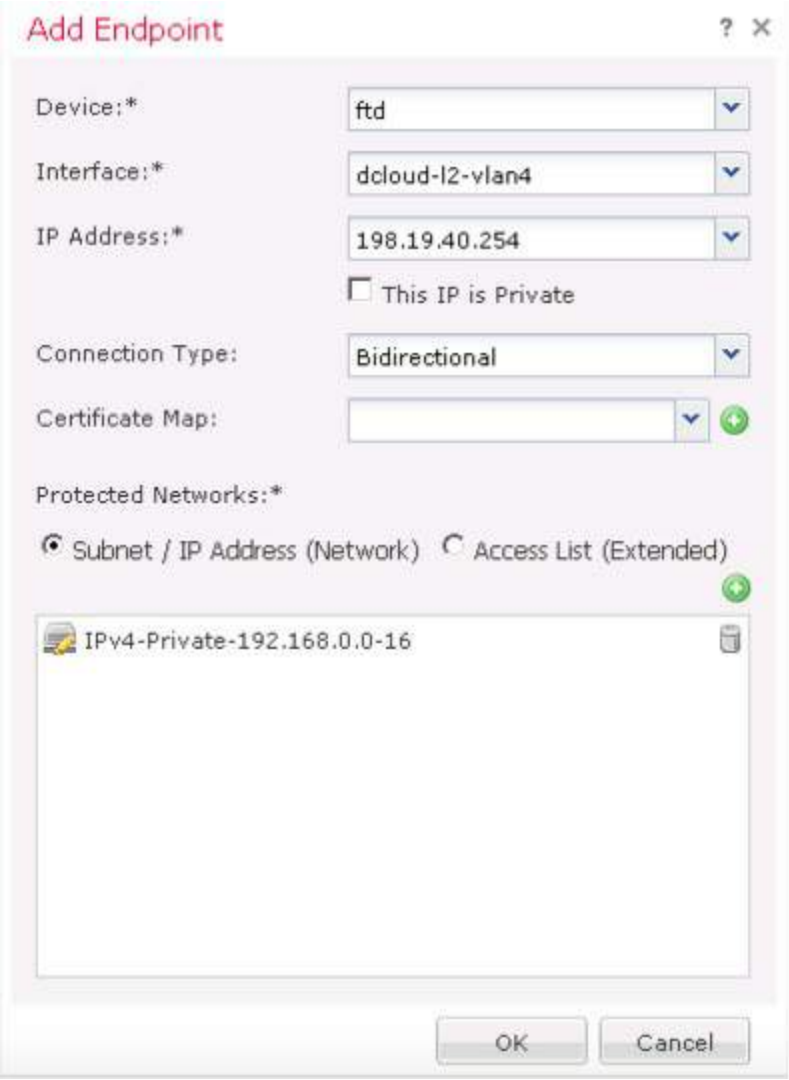


Figure 3-20 Choosing Nodes to Participate in the VPN

Step 6. On the next tab, select configuration options for IKEv2, as shown in Figure 3-21.

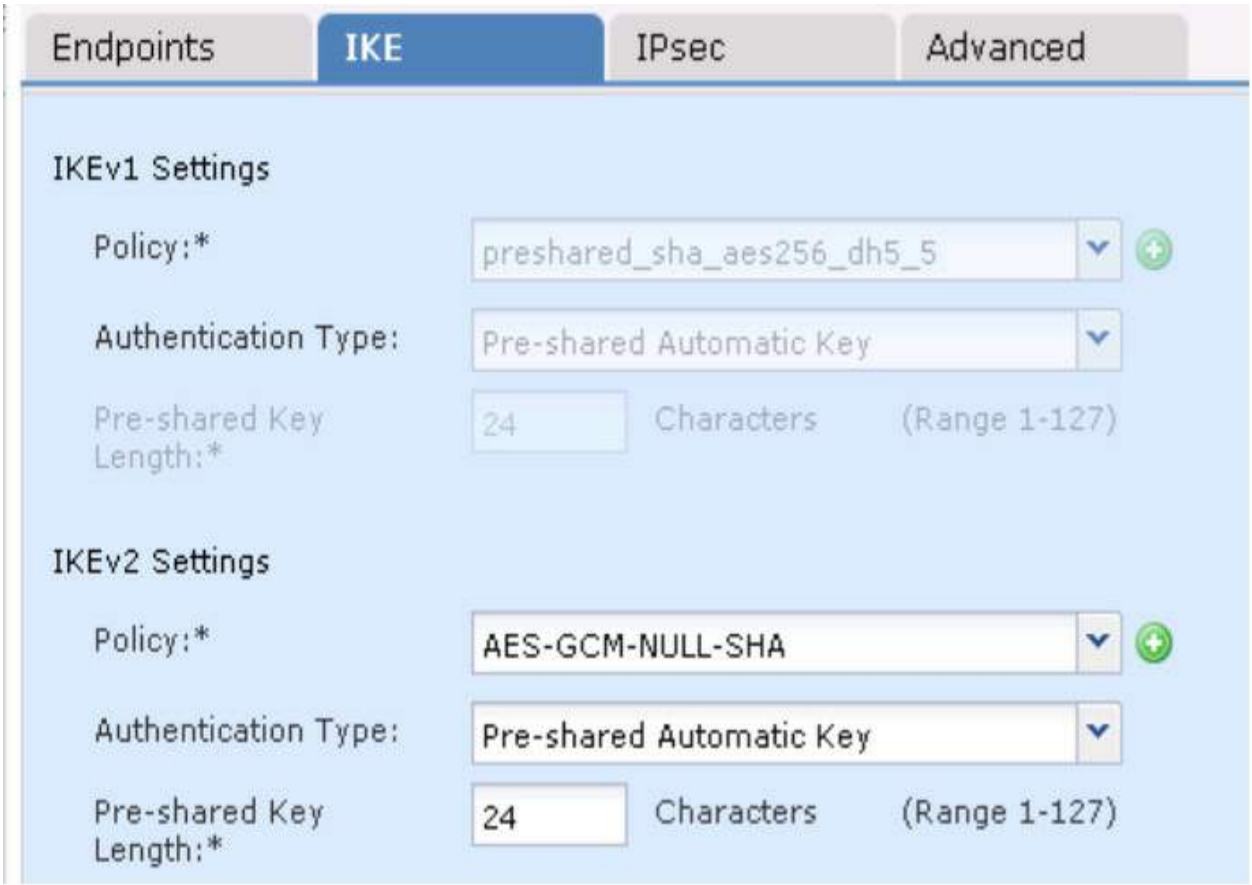


Figure 3-21 IKEv1 and IKEv2 Configuration Options for Cisco Secure Firewall

Step 7. If you are using IPsec, select the IPsec tab and choose whether you are using tunnel or transport mode as well as the other settings shown in Figure 3-22.

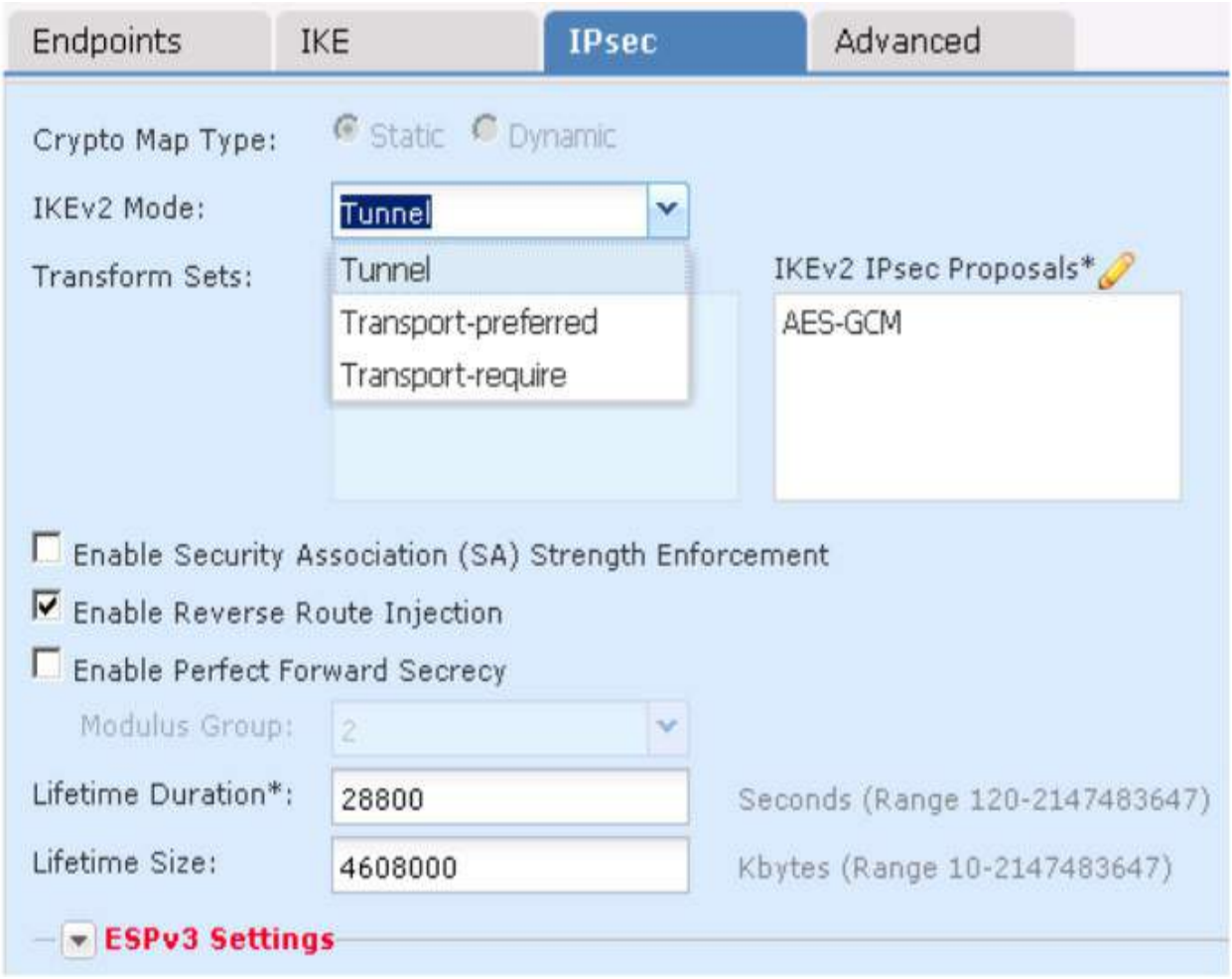


Figure 3-22 IPsec Configuration Options for Cisco Secure Firewall

Step 8. On the Advanced tab, select advanced settings for IKE, IPsec, and the VPN tunnel, as shown in Figure 3-23. You can see that there are various options for setting up keepalives when traffic is not seen across the VPN, peer validation, IKEv2 security associations, IPsec fragmentation prior to encryption, and various certificate map settings. (You saw similar configuration options with the Cisco ASA site-to-site VPN setup earlier in this chapter.)

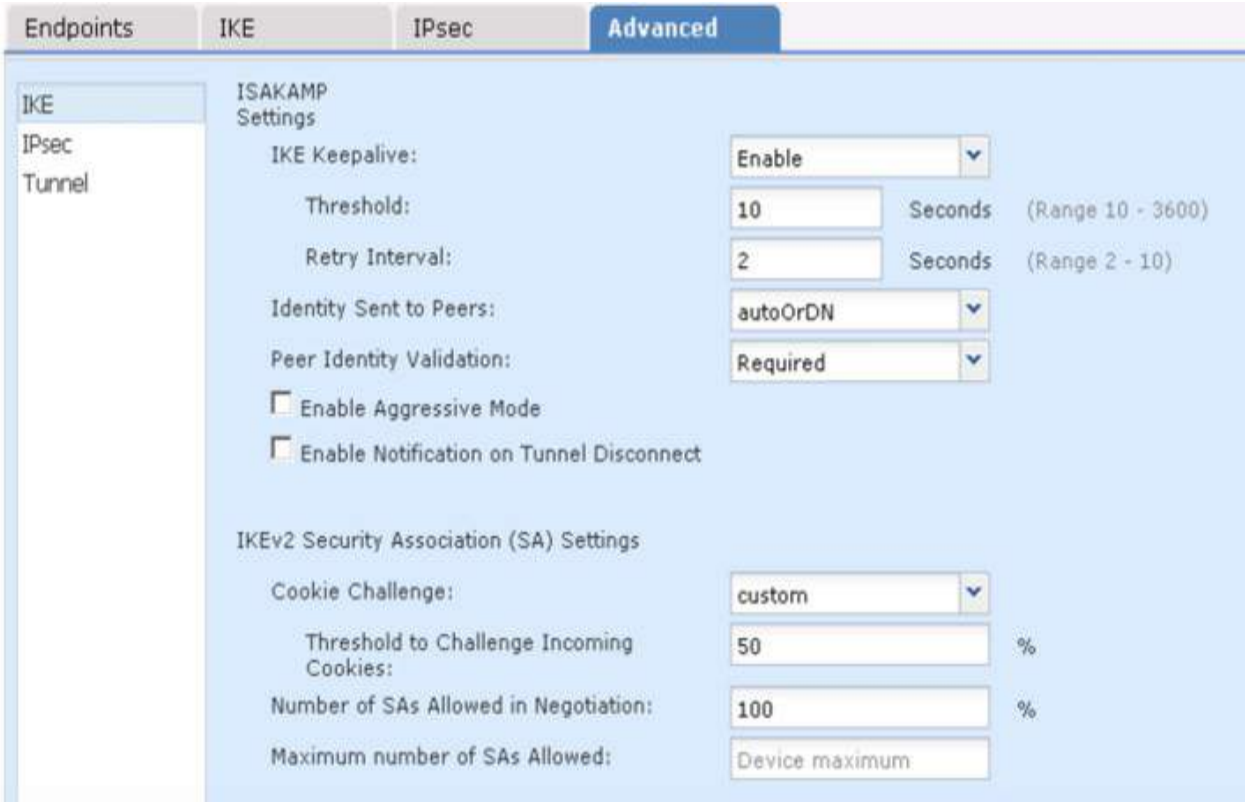


Figure 3-23 Advanced VPN Configuration Options for Cisco Secure Firewall

When your options are selected, click **Save** and deploy the changes to all the associated Cisco Secure Firewall appliances. You can monitor the VPN by using system messages, VPN health events, system logs, or the CLI.

Note

You should notice a lot of similarity between using Cisco routers, Cisco Secure Firewall, and Cisco ASA technologies to set up site-to-site VPNs. Make sure you understand the fundamental concepts of creating site-to-site VPNs within each platform as you prepare for the SVPN 300-730 exam. You need to understand each step as well as the order of the steps and why each step is being used. You also need to be able to compare each step to alternative options. For example, the exam might ask you how IKEv2 could be used as an alternative to IKEv1 or whether either version of IKE is

supported. We will go much deeper into all of these concepts over the next few chapters, as we cover the different Cisco site-to-site deployment options.

Cisco Meraki Example

One last example that is a bit different from the site-to-site VPN configurations we have covered thus far in the chapter is setting up a site-to-site VPN on a Cisco Meraki solution.

Note

The SVPN 300-730 exam currently does not include Cisco Meraki configuration as part of the learning objectives; however, we cover it because Cisco Meraki is a widely deployed option and secure access service edge (SASE), becoming an industry standard.

In Chapter 2, we touched on the Meraki one-touch site-to-site VPN. Now it's time to see it in action. This section assumes that you have purchased and deployed two or more Meraki MX appliances and have the proper license to run a site-to-site VPN.

To access any configuration options for Cisco Meraki, you need to access the cloud-based management dashboard at https://dashboard.meraki.com. This is how you access your personal cloud Meraki manager for all Meraki products. When you access the Meraki main dashboard, you see the different product options as well as options to view aspects of your entire organization, as seen by Cisco Meraki. This is your centralized window into your entire Meraki deployment.

Follow these steps to set up a Meraki site-to-site VPN:

Step 1. Find the site-to-site VPN options by going to **Security & SD-WAN** > **Configure** > **Site-to-site VPN** (see Figure 3-24).

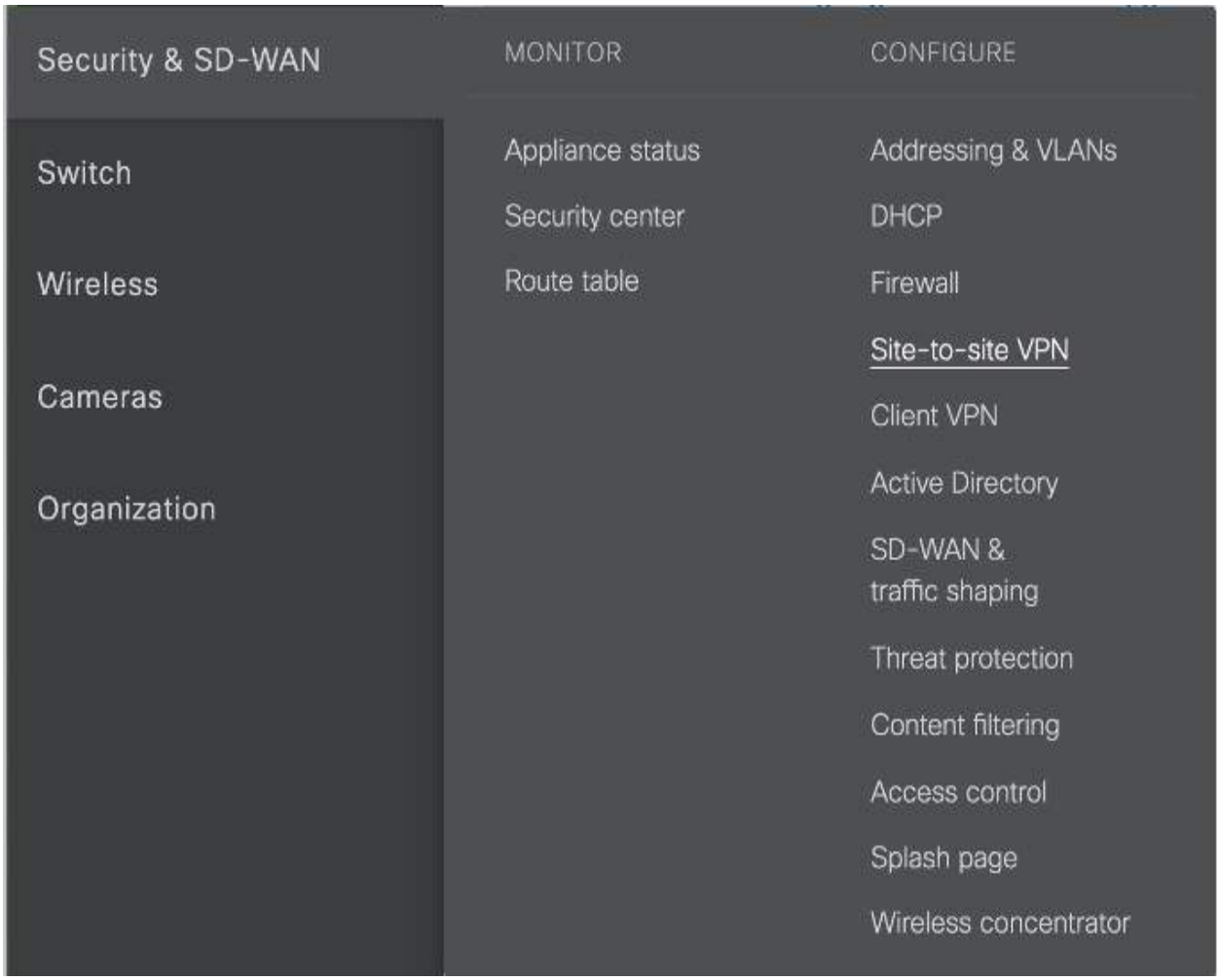


Figure 3-24 Accessing the Cisco Meraki Site-to-Site VPN Configuration

Step 2. On the next screen, where you see the site-to-site VPN options, select the **Site-to-Site VPN** option and either **Hub** (representing a full mesh) or **Spoke** (representing a hub and spoke) to add the current Meraki MX to the VPN configuration. By default, Off is selected to remove the currently selected MX from any site-to-site configuration (see Figure 3-25). When you select Hub or Spoke, new configuration options appear below the high-level VPN options page.

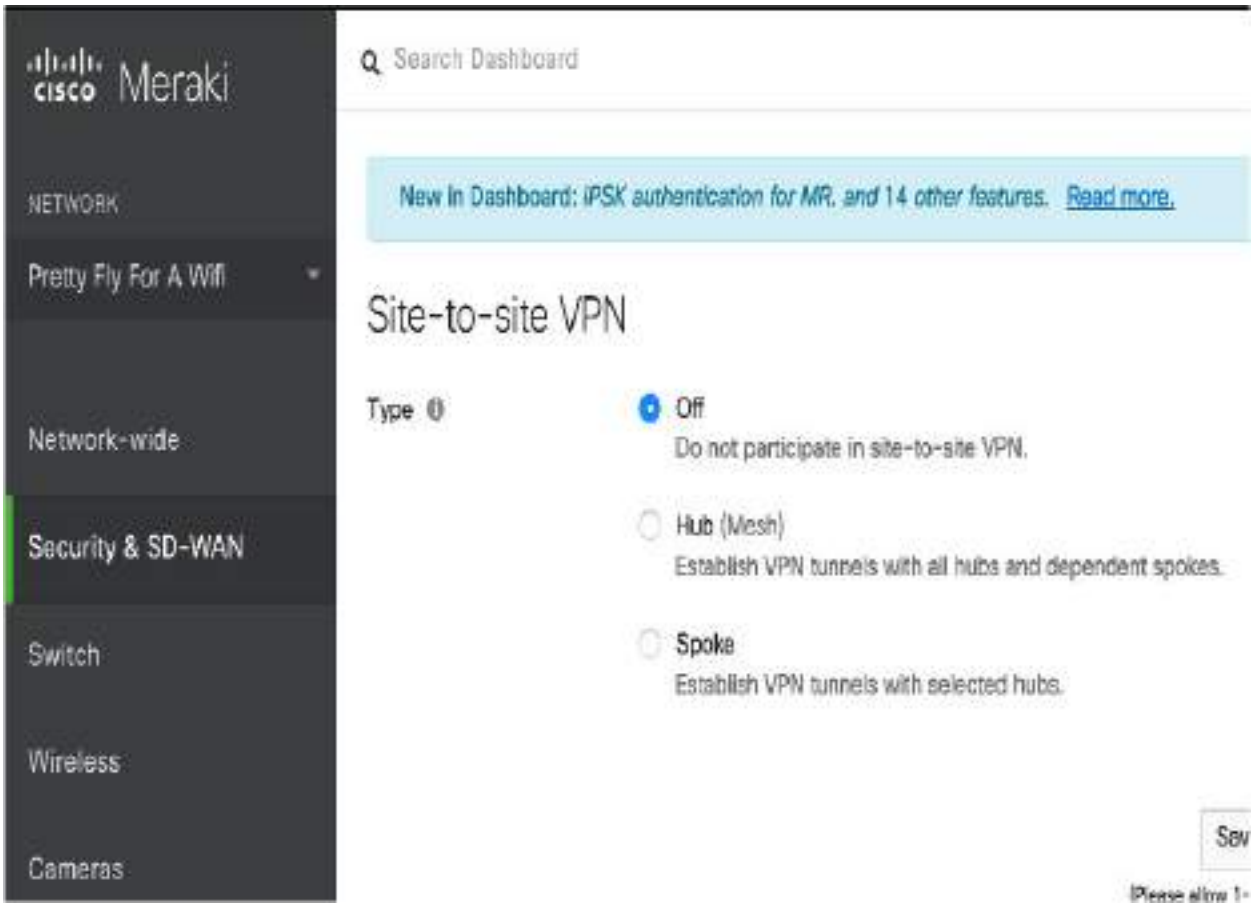


Figure 3-25 Cisco Meraki Site-to-Site VPN Enablement Page

If this is the first MX you are setting up for the site-to-site VPN, you see a warning similar to the one shown in Figure 3-26, stating that no other hubs are in the VPN. Below that message will be the VPN setting options.

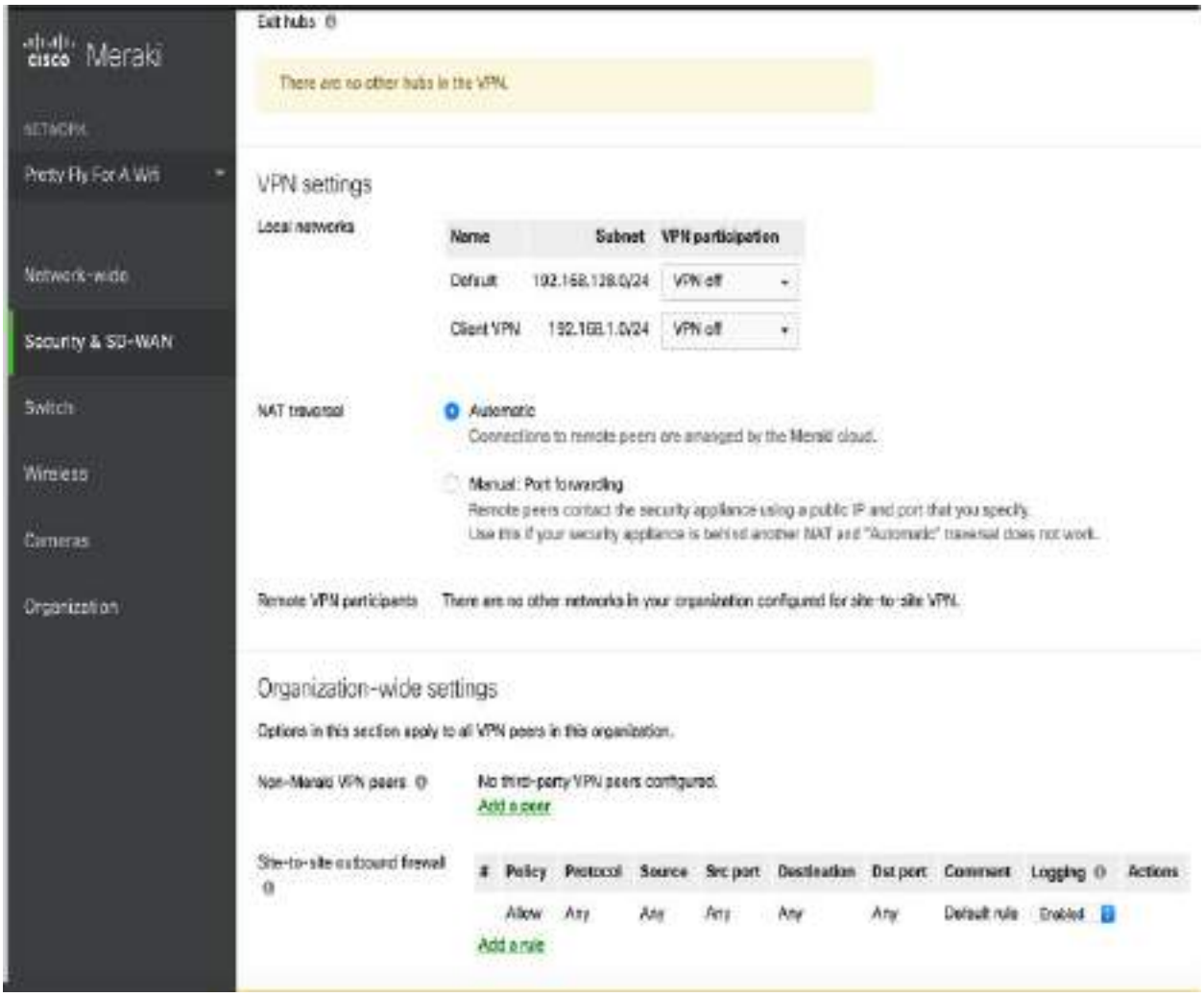


Figure 3-26 Cisco Meraki Site-to-Site VPN Configuration Page

Step 3. Scroll past the warning message to the configuration settings. You have the option to choose whether the local networks and client VPN networks are to be part of the site-to-site VPN configuration. By default, they are both not included. You can set NAT to Automatic or use the Manual Port Forwarding option. If you have a remote VPN set up, you are permitted to include those participants within your site-to-site VPN, and check boxes are available to add them to your site-to-site VPN configuration.

Step 4. In the Organization-wide Settings section, select other MX systems as well as the firewall rules you want to open for site-to-site VPN outbound traffic. Click **Save**.

Step 5. Repeat steps 1–4 to build a site-to-site VPN between two or more MX appliances.

As you can see, setting up a site-to-site VPN with Meraki devices is relatively easy. All the options you need are on a single page in the Cisco Meraki management GUI.

High Availability

One final site-to-site VPN concept we need to cover is high availability. Your VPNs will likely support mission-critical traffic, and redundancy and resilience are likely important to your site-to-site VPN design.

An organization is likely to have high-availability requirements to ensure that its network doesn't go down when there is a failure on one or more site-to-site VPN nodes. You can take several approaches to adding high availability to your site-to-site VPN architecture. One approach is purchasing redundant equipment and configure a method for the secondary system to take over when the primary system is no longer available. Another approach is to acquire backup equipment but not have it set up. A third method is to change how traffic is routed when a primary system goes down. By using one or more of these approaches, you can avoid a broken VPN situation. Best practice is to consider implementing a combination of these approaches to increase your network's resilience against interrupted site-to-site VPN service.

High Availability Options

Let's look at each of the possible approaches to implementing high availability with a site-to-site VPN architecture:

- **Active/active:** This high-availability design involves splitting traffic between two nodes so that both VPN-providing technologies are being

actively used. If one system goes down, the other system takes on the load for both systems, acting as the solo primary VPN technology (up to its capacity). This approach provides a few benefits, including offering high availability while also leveraging both VPN solutions for maximum return on investment. The disadvantages of this approach are sizing both appliances to be able to handle the load for all traffic, maintaining traffic that is split between two appliances, and the likely increased costs as both VPN-providing technologies are expected to be used, requiring the full cost for both appliances. Cost for this option depends on the vendor, technology, and licenses used.

- **Active/standby:** With this approach, one VPN appliance acts as the active primary VPN-providing technology, and there is a second technology that is not used unless the primary system becomes unavailable. For automated failover, there is a heartbeat setup between the primary and standby systems, where the standby system periodically validates that the primary system is active. If the heartbeat is interrupted between the primary and secondary systems, a failover occurs, causing the secondary system to become the primary VPN provider. Failover can occur automatically or manually, depending on the technology and licenses being used. It is common for this approach to cost less than an active/active design because one system is not expected to be used unless a failover occurs. The actual costs of the failover solution depends on the technology and licenses used.

- **Cold standby:** With this approach, a second VPN solution is ready to be used in a failover configuration but is not set up. If the primary system goes down, manual effort is required to transfer the VPN to the failover system.

- **Routed standby:** This approach creates redundancy by using a networking approach rather than dedicating hardware. All systems that access the primary VPN know how to access it, based on its available IP address and routing that permits traffic to that VPN source. A routed failover changes the routing and/or IP address of the primary system and routes traffic somewhere else until the primary system goes down. It’s possible that a routed standby is essentially how a failover occurs between two active/active or active/standby VPN appliances or traffic

could just be permitted to certain sources while the primary system is down. The details of this approach depend on the vendor used and how the network is configured.

Consider the following factors as you plan for high availability in a site-to-site VPN:

- Available hardware/software
- Cost of the complete support
- Required licenses
- Location of redundant systems
- Required training and support
- Available bandwidth to support redundant links
- Compliance and backup requirements
- Desired level of redundancy and resilience to VPN outages

High Availability Considerations

The best approach for your organization depends on a few factors. If you plan to use an active/active or active/standby design, you need to ensure that the equipment is sized properly. An active/active approach is likely to have larger hardware and higher costs than an active/standby approach. If you plan to automate the failover between the VPN solutions, you need to make sure the proper level of bandwidth is available to support the heartbeat between the VPN technologies. Keep in mind that any lag that disrupts the connection between the VPN systems causes unwanted failover to occur.

When considering which Cisco security appliances to use, you need to think about the different requirements that must be met in order for different high-availability capabilities to be supported. Here is a summary of considerations for Cisco security appliances configured for high availability:

- Must use the same model.
- Must have same number and types of interfaces. (For the Cisco Secure Firewall 9300 chassis, all interfaces must be preconfigured in FXOS identically before high availability is enabled.)
- Must have the same modules installed, if any are used.
- Must have the same RAM installed.

There are also software and configuration requirements to consider regarding Cisco security appliances providing high availability. Here is a summary of those requirements:

- Must be in the same context mode (single or multiple).
- If configured for single mode, must be in the same firewall mode (routed or transparent).
- Must have the same major (first number) and minor (second number) software version on both appliances. The only exception is that different versions can be used during the upgrade process while maintaining failover.
- Both appliances must use the same AnyConnect images.
- For the Cisco Secure Firewall 9300 Series, appliances must have the same flow offload mode (enabled or disabled).

Note

For the SVPN 300-730 exam, you need to know the expectations for what is required on Cisco ASA appliances for high availability to work. This includes expected communication between the systems as well as the hardware and configuration items that must match between both systems.

When using Cisco technology to perform high availability, specific traffic is passed between the systems. If one system needs to monitor whether the

other system is alive, hello messages (also known as keepalives) need to be continuously passed. The current state of the units—either active or standby—is also beaconed back and forth to ensure that both systems know their current role. MAC address and link status messages are passed back and forth to ensure that the systems are communicating with the proper peers. Finally, configuration replication and synchronization occur to ensure that the backup system has the latest configuration if it is required to become the primary unit.

High Availability Costs

You will find there are different costs for different high-availability options as you meet with different vendors. Some vendors charge less for active/standby than active-active since the backup system is used only when a failover occurs. As mentioned in Chapter 2, Cisco offers flexible licensing that does not count usage against a license unless the capability is being used. An example for site-to-site VPN design would be to acquire a 90-day license for the standby appliance and a full license for the primary system. The assumption would be that the standby system would never be used unless the primary system went down, and 90 days would be enough time to troubleshoot and reestablish connectivity to the primary. Also, keep in mind that both ASAs need to have the same license type for this to work.

If you are looking to save costs, a cold standby option might be the best choice. You can find different variations of a cold standby based on the readiness of the backup system. For the most basic cold standby, you can purchase redundant hardware and store it at another location. This approach would require labor to unbox and stand up the system in the event that the primary VPN-providing technology goes down. Industry experts recommend having a cold standby system unboxed, racked, and ready to be used, with a base configuration installed. It is also recommended to set up a system that periodically pulls the latest configuration from the primary solution and stores it in a location from which you can download in the event that the primary system goes down. This would allow the cold standby system to upload a recent configuration as it takes over the primary system role.

High Availability Technology Considerations

Another consideration is requirements for the technology being used. We already pointed out the importance of bandwidth between systems using an automated failover approach. Some systems may also require dedicated interfaces for the heartbeat. For example, the Cisco ASA uses an unused data interface for the failover link. This means a normal networking interface can't also act as the heartbeat, which could be a showstopper if your design includes currently running equipment that may not have the available processing power, bandwidth, or interfaces to support the site-to-site failover design.

Another example of limitations for failover is options within a Cisco router. On a Cisco router, only the stateless form of IPsec failover is supported. The stateless failover in routers uses protocols such as Hot Standby Router Protocol (HSRP) to provide primary-to-secondary cutover and also allows the active and standby VPN gateways to share a common virtual IP address. You need to make sure the routers involved with the site-to-site VPN are capable of supporting your architecture requirements.

Bidirectional Forwarding Detection

One important IOS failover concept is Bidirectional Forwarding Detection (BFD). Cisco routers can use a BFD protocol to provide fast-forwarding path failure detection for all media types, encapsulations, topologies, and routing protocols. Such a protocol allows administrators to detect forwarding path failures much more quickly than is possible with traditional protocol hello mechanisms.

IOS Failover Example

Because you will likely want to set up failover on an IOS-based site-to-site VPN, let's examine how these failover settings look on a Cisco router. To configure BFD on a Cisco router, follow these steps:

Step 1. Create a BFD single-hop template:

```
Router(config)# bfd-template single-hop bfdtemplate1
```

Step 2. Configure the transmit and receive intervals between BFD packets and the number of BFD control packets that must not be seen before BFD finds that the peer is no longer available:

```
Router(bfd-config)# interval min-tx 120 min-rx 100
multiplier 3
```

Step 3. Enter the interface intended for failover and provide either an IPv4 or IPv6 address:

```
Device(config)# interface FastEthernet 4/0
Device(config)# interface gigabitethernet
0/0/0
Device(config-if)# ip address 10.201.201.1
255.255.255.0
Device(config-if)# ipv6 address
2001:db8:1:1::1/32
```

Step 4. Enable the BFD template:

```
Router(config)# bfd template bfdtemplate1. bfd template
template name
```

One final failover concept you need to consider is how a configuration can be exported from a Cisco IOS or security appliance–based site-to-site VPN. Enabling such an export provides an additional redundancy plan that is activated when both primary and backup systems go down. In addition, the backed-up configuration can be used for a cold standby option, and it can also be used to validate whether unwanted changes or corruption has occurred in your active VPN architecture. You can export configuration manually on almost all Cisco technologies, and many security appliances and routers offer the ability to specify automatic exportation of configuration on a regular basis.

Summary

This chapter explores the steps involved in developing and configuring site-to-site VPNs. It starts by looking at planning for a future site-to-site VPN project. It also covers many key concepts and components used when

building site-to-site VPNs. In addition, this chapter walks through the configuration required to build a site-to-site VPN between Cisco IOS routers. It also looks at building site-to-site VPNs between Cisco security appliances, including Cisco ASA appliances, Cisco Secure Firewall, and Cisco Meraki. Finally, this chapter covers high-availability concepts as they apply to site-to-site VPN architectures.

Now that you have a basic understanding of how site-to-site VPN technology works, it's time to look more closely at the different VPN frameworks Cisco offers to support site-to-site capabilities. First up is a closer look at GETVPN.

References

Aditya, Venkata, and Rahul Govindan (April 13, 2018). Configure IKEv1 IPsec Site-to-Site Tunnels with the ASDM or CLI on the ASA. Retrieved from https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/119141-configure-asa-00.html

Anand, Adity (July 14, 2018). SSL Strip & How Awesome It Is! Retrieved from https://medium.com/bugbountywriteup/ssl-strip-how-awesome-it-is-a0eb79e28bcc

Cisco Secure Firewall Appliances Next-Generation Firewall Datasheet. Retrieved from https://www.cisco.com/c/en/us/products/collateral/security/firepower-ngfw/datasheet-c78-742480.html

Cisco IOS VPN Configuration Guides. Retrieved from https://www.cisco.com/c/en/us/td/docs/security/vpn_modules/6342/vpn_cg.html

Crypto Maps. Retrieved from https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21/IPSec/21_IPSec-Reference/b_21_IPSec_chapter_0110.pdf

Firepower Management Center Configuration Guide, Version 6.2. Retrieved from https://www.cisco.com/c/en/us/td/docs/security/firepo

wer/620/configuration/guide/fpmc-config-guide-v62/firepower_threat_defense_site_to_site_vpns.html

Latosiewicz, Marcin (August 29, 2017). Crypto Map Based IPsec VPN Fundamentals—Negotiation and Configuration. Retrieved from https://community.cisco.com/t5/security-documents/crypto-map-based-ipsec-vpn-fundamentals-negotiation-and/ta-p/3153502

Mocan, Tim (February 20, 2019). What Is IKEv2? Retrieved from https://www.cactusvpn.com/beginners-guide-to-vpn/what-is-ikev2/

Site-to-Site VPN Settings. Retrieved from https://documentation.meraki.com/MX/Site-to-site_VPN/Site-to-site_VPN_Settings

Snyder, Joel (March 21, 2011). Cisco Has Long History with VPNs. Retrieved from https://www.networkworld.com/article/2200809/cisco-has-long-history-with-vpns.html

What Are Certificate Authorities & Trust Hierarchies? Retrieved from https://www.globalsign.com/en/ssl-information-center/what-are-certification-authorities-trust-hierarchies/

Exam Preparation Tasks

As mentioned in the section “How to Use This Book” in the Introduction, you have a couple of choices for exam preparation: the exercises here, Chapter 11, “Final Preparation,” and the exam simulation questions in the Pearson Test Prep software online.

Review All Key Topics

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

Table 3-3 Key Topics for Chapter 3

Key Topic Element	Description	Page Number
Figure 3-1	AH and ESP in Transport Mode and Tunnel Mode	
Figure 3-2	IKE Data Flow Diagram	
Table 3-2	Comparison of IKEv1 and IKEv2	
List	IKE concepts	
List	Authentication methods used in an IKE policy	
Figure 3-3	Tunneling Components Diagram	
Figure 3-4	IPsec Tunnel Modes	
List	Addresses to consider with NAT	
List	Authentication options used with IKE	
List	Options for high availability for a site-to-site VPN deployment	

Complete Tables and Lists from Memory

Print a copy of Appendix C, "Memory Tables" (found on the companion website), 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 companion website), 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:

IP Security (IPsec)
Authentication Header (AH)
Encapsulating Security Payload (ESP)
certificate authority (CA)
crypto map

Chapter 4. Group Encrypted Transport VPN (GETVPN)

This chapter covers the following subjects:

- **GETVPN Overview:** This section provides an overview of how GETVPN uses a single security association to encrypt traffic between group members.
- **GETVPN Components:** This section examines the building blocks of GETVPN and how they work together to create a unique solution for either MPLS or a private IP network.
- **GETVPN Implementation and Configuration:** This section steps through the components of a GETVPN configuration. Examples demonstrate how the GETVPN building blocks work on a key server and on a group member.

"Passwords are like underwear: you don't let people see it, you should change it very often, and you shouldn't share it with strangers."

—Chris Pirillo

This chapter covers the following exam objectives:

- 1.0 Site-to-site Virtual Private Networks on Routers and Firewalls
  - 1.1 Describe GETVPN
- 4.0 Secure Communications Architectures
  - 4.1 Describe functional components of GETVPN, FlexVPN, DMVPN, and IPsec for site-to-site VPN solutions
  - 4.3 Recognize VPN technology based on configuration output for site-to-site VPN solutions
  - 4.6 Design site-to-site VPN solutions

Group Encrypted Transport VPN, more commonly referred to as GETVPN, provides a solution for tunnel-less, any-to-any and confidential branch communications. GETVPN leverages the concept of a trusted group to eliminate point-to-point tunnels and their associated overlay routing. GETVPN uses the concept of group members, where group members share a common security association, commonly referred to as an SA. Using this approach, GETVPN enables group members to encrypt and decrypt traffic with any other group member using the same SA. This eliminates the need to negotiate point-to-point IPsec tunnels between members of the group and associated overhead.

The Implementing Secure Solutions with Virtual Private Networks (SVPN) 300-730 exam expects you to be able to describe the functional components of GETVPN, recognize GETVPN technology, and identify troubleshooting problems within a GETVPN deployment. After reviewing this chapter, you will be able to accomplish the following:

- Describe GETVPN
- Identify functional components of GETVPN solutions
- GETVPN Configuration and Implementation
- GETVPN Status Commands

Learning beyond the SVPN concepts

- GETVPN Fundamental Concepts
- GETVPN Design Considerations

“Do I Know This Already?” Quiz

The “Do I Know This Already?” quiz enables you to assess whether you should read the entire chapter. If you miss no more than one of these self-assessment questions, you might want to move ahead to the “Exam Preparation Tasks” section of the chapter. Table 4-1 lists the major headings in this chapter and the “Do I Know This Already?” quiz questions related to

the material in each of those sections to help you assess your knowledge of these specific areas. The answers to the "Do I Know This Already?" quiz appear in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes."

Table 4-1 "Do I Know This Already?" Foundation Topics Section-to-Question Mapping

Foundation Topics Section	Questions
GETVPN Overview	1–3
GETVPN Components	4–7
GETVPN Implementation and Configuration	8–10

1. What are the key benefits of GETVPN over traditional VPN solutions for enterprise organizations? (Choose two.)

a. It enables instant IP communication, thanks to IPsec.

b. An overlay routing protocol is required.

c. Any-to-any IP communication is possible.

d. It is a tunnel-based solution.

2. Why is GETVPN not used over a public network such as the Internet? (Choose two.)

a. Unchanged IP header

b. IP header encryption

c. RFC 1918 IP address requirement

d. Lack of support for NAT

3. Which protocol in GETVPN is responsible for securing the control plane

communications?

a. IPsec

b. GDOI

c. KEK

d. ISAKMP

4. What are the primary components of GETVPN? (Choose three.)

a. GDOI protocol

b. IKEv2 protocol

c. Key server

d. Group member

5. Which GETVPN component is responsible for sending out encryption keys?

a. GDOI protocol

b. IKEv2 protocol

c. Key server

d. Group member

6. In the GDOI protocol, which of the following is responsible for sending out the new key to group members?

a. TEK

b. ISAKMP

c. IPsec

d. KEK

7. For which component would it be vital to have a redundant solution?

a. GDOI

b. KEK

c. Key server

d. Group member

8. Which component would require an RSA private key?

a. Group member

b. Key server

c. None

d. Both

9. In a GETVPN solution, which component is responsible for establishing the IPsec encryption policy?

a. Group member

b. Key server

c. GDOI

d. All of the above

10. On a group member router, where is the group identity specified?

a. IKE policy

b. GDOI group

c. Transform set

d. Crypto map

Foundation Topics

VPN technology has been adapted to fit a wide set of solutions, and *Group Encrypted Transport VPN (GETVPN)* is a perfect example of a unique environment that dictated an unusual set of requirements on an existing technology. Organizations typically use GETVPN to encrypt traffic across private network solutions such as *Multiprotocol Label Switching (MPLS)* networks. Typically, a service providers MPLS network carries traffic from numerous other enterprise organizations, and GETVPN ensures

confidentiality across that network. Before we get into the specifics of GETVPN, we need to look at why this particular VPN implementation was developed.

Today, enterprise customers require instantaneous branch-to-branch and branch-to-main office communication for a wide variety of applications, such as voice over IP, video, and other delay-sensitive applications. Because some of these applications, such as video, involve high-bandwidth traffic, the traditional hub-and-spoke solutions do not suffice for branch-to-branch communications. MPLS was designed to address the enterprise need for both high speed and bandwidth capacity.

MPLS Security Challenges

MPLS provides the services that enterprises need while meeting and exceeding application bandwidth and speed requirements. However, there is a security challenge related to data confidentiality and integrity. If service providers are intermixing your enterprise traffic across the same platforms as other organizations, what assurances do you have that your traffic is secure? GETVPN was created to ensure that organizations could meet government regulations such as the Health Insurance Portability and Accountability Act (HIPPA), Gramm-Leach-Bliley Act (GLBA), and Payment Card Industry Data Security Standard (PCI-DSS). Even if your traffic is on a private IP network run and managed by the service provider, you still should consider your organization’s security needs to ensure that your network maintains government-mandated encryption.

Figure 4-1 illustrates a service provider MPLS network with two organizations using that infrastructure for communication. The dotted line indicates the VPN encryption used by each company. Company A and Company B will not see each other’s traffic, especially if they are using a GETVPN solution. Even in the event of a service provider configuration error, GETVPN will provide confidentiality.

Figure 4-1 GETVPN MPLS Service Provider View

Technically, it is possible to run solutions such as a site-to-site VPN or a Dynamic Multipoint VPN (DMVPN) solution over an MPLS network, but such solutions introduce limitations. For example, both site-to-site VPN and DMVPN solutions introduce administrative overhead in the form of configuration complexity as well as resource overhead due to the large number of security associations. The larger the MPLS network grows, the more impactful these limitations become. As another example, site-to-site VPN solutions suffer from multicast replication issues. These can be solved with DMVPN; however, this requires overlaying a secondary routing domain into the infrastructure to ensure that the spoke endpoints can locate each other.

Figure 4-2 provides an example of an MPLS solution for a four-site organization with private IP addresses used on the inside and also by the service provider. We do not get into the specifics of MPLS tagging in this chapter, but it is safe to say that one of the advantages of the service provider MPLS solution is that the IP address routing, configuration, and infrastructure management can be shifted to a service provider. There are numerous other benefits, such as not needing to use Network Address Translation (NAT). To the company, the MPLS network is just a private IP transport being managed by another organization.

Figure 4-2 GETVPN Corporate Solution

GETVPN Overview

GETVPN has a unique way of solving the challenge that other VPN solutions face in managing a large number of *security associations (SAs)*. In typical site-to-site VPN solutions, each VPN tunnel adds one or more SAs. The more VPN tunnels, the more SAs that are created. In comparison, GETVPN uses a single SA for all the group members. Using a single SA eliminates hub-and-spoke solutions and partial mesh configurations. However, just because you have a single SA does not mean your security posture is weakened, because there are security enhancements that address these concerns. As shown in Figure 4-3, the GETVPN protocol *Group Domain of Interpretation (GDOI)* establishes the SA between the group members—in this case, Site A, Site B, and Site C. With a single SA, traffic from Site B can flow to Site C or Site A without delay and with encryption.

Figure 4-3 GETVPN Security Association Trust Groups and Tunneless VPN

GETVPN also introduces the concept of a trusted group. Each VPN router in a trusted group trusts the other routers in the group and can send traffic between itself and any member of the group. Because all group members share a common SA, this results in two distinct important advantages for GETVPN:

- Any group member can decrypt traffic that was encrypted by any other group member.
- Tunnel negotiation is not required because GETVPN is a non-tunnel-based solution.

GDOI Protocol

How does GETVPN achieve encryption without VPN tunnels between the locations? The answer lies in the use of the GDOI protocol. RFC 6407, which describes GDOI, states that “GDOI provides group key management to support secure group communications.” While other VPN solutions discussed in this book use Internet Key Exchange (IKE) to negotiate SAs; GETVPN uses GDOI to manage the group SA with the IPsec protocol stack used to encrypt the payload between the communicating devices.

In a traditional IPsec solution with ESP, the sender encrypts the entire IP payload and then wraps another new IP datagram around it in order to deliver it to the decrypting device. With GETVPN, the router encrypts the payload and then transmits the IP datagram with the original source and destination IP addresses. Because there is no outer wrapper on the IP datagram, a tunnel between the devices is not necessary; GETVPN is therefore referred to as a tunnel-less solution. Figure 4-4 compares an IP header for a traditional IPsec site-to-site VPN and an IP header for GETVPN.

Figure 4-4 GETVPN IP Packet Comparison

Figure 4-5 shows an IP packet traveling from host 10.2.2.10 to 10.3.3.50. The new IP header added is a copy of the original header generated by the host. The group member receiving the encrypted payload has the key to decrypt the IP packet before forwarding on to its final destination.

Figure 4-5 GETVPN Packet

Because GETVPN does not create VPN tunnels between sites and the original IP datagrams are left intact, this solution creates a unique challenge. Basically, GETVPN does not work in NAT environments. Therefore, this type of solution is rarely used across public networks, such as the Internet. GETVPN is ideally suited for either an MPLS network or a private IP network. Private IP network implementations can be found in large enterprises and government entities.

GETVPN Benefit Summary

Some of the general benefits from using GETVPN are as follows:

- Multicast infrastructure solutions do not require an overlay solution to replicate multicast traffic between multiple sites (see Chapter 5, "Dynamic Multipoint Virtual Private Network (DMVPN)").
- No overlay routing protocol is required.
- GETVPN supports large-scale deployments and instant any-to-any IP communication with IPsec.
- Because the original IP source and destination are preserved, GETVPN integrates well with end-to-end QoS solutions. In addition, you have more intermediate control over your IP payloads, so optimal and efficient routing for both unicast and multicast traffic can be achieved.
- GETVPN supports both IKEv1 and IKEv2.

GETVPN Components

Before you can dive into GETVPN configuration, you first must understand how the various components of GETVPN work together so that device-to-device communication is secured. This section covers the role of the key

server and the group member. It also discusses how devices communicate and encrypt payloads. Finally, this section addresses why group members communicate with key servers and what information they exchange.

Figure 4-6 provides an overview of the components involved in a GETVPN. This figure shows only one key server and three group members. We use this example throughout the chapter to help you form a conceptual understanding and for a detailed configuration example. First, let's review how the key server works within GETVPN.

Figure 4-6 GETVPN Components

GETVPN Key Server

GETVPN has three primary components: the key server, the group member, and the GDOI protocol. Throughout the rest of this section, we look at each of these topics, as well as how IPsec functions in a GETVPN solution.

The key server is the most critical device in a GETVPN solution. The following are minimal components that should be configured on a key server:

- IKE policy

- RSA key for rekeying
- IPsec policies
- Traffic classification

The key server is responsible for registering the group members and sending out encryption keys. In addition, the key server is responsible for the rekeying process that occurs periodically. A key server cannot be a group member, and you need only one key server. The key server uses the GDOI protocol to communicate with the group members. Upon initialization, a group member registers with the key server by using either use a pre-shared key or certification (PKI). Once a group member is authorized, it retrieves the policy configuration and the two keys used for communication with other group members. Key servers are responsible for maintaining the SA policy, authenticating group members, and providing session keys for encrypting/decrypting traffic. When a group member tries to register with the key server, the key server checks a the group ID and IKE credentials.

Policy configuration for group members occurs in the key server. This policy configuration includes the crypto ACL, encryption protocols, rekeying timers, and security association information. Besides the policy information, the key server provided two keys to group members: the *key encryption key (KEK)* and the *traffic encryption key (TEK)*. The KEK protects control plane communications, such as the rekeying process, and the TEK is responsible for payload encryption between group members. TEK supports the IPsec SA that all group members use to encrypt and decrypt payloads.

GETVPN Group Member

A group member requires minimal configuration because both the policy and SA information are retrieved from the key server. During registration, the group member provides the group ID to get the policy and keys. A group member is a VPN router that is a member of a GDOI group and can encrypt traffic being sent to any other group member since they all use the same IPsec SA. A fault tolerance concern would be having a single key server. It is possible to configure multiple key servers—up to eight of them for each

group. A group member registers to one of the key servers, and the key server then replicates that information to the primary key server. The primary key server is responsible for maintaining the database of all registered group members and for the rekeying synchronization process.

GETVPN GDOI Protocol

The GDOI protocol, which is specified in IETF standard RFC 6407, is used as the communication mechanism between key servers and group members in a VPN. It is protected by ISAKMP Phase 1, which is the same method used in other IPsec site-to-site tunnels. Phase 1 IKE protects the Phase 2 exchange in which the members pull down the SA from the key server. The KEK is used when the key server pushes out a new key to group members. The key server can use multicast to push out the keys or notify them of the rekeying. The multicast feature enables GETVPN to scale and support a large number of group members. The key server sends out the rekeying information prior to the SA expiration time in order to ensure that the group members have the new key. Later in this chapter, you will see the unicast method of rekeying selected in a configuration example.

GETVPN Security Controls

GETVPN has some unique security controls that are different from what you see in site-to-site VPNs, DMVPN, or FlexVPN. As mentioned earlier, the KEK is responsible for control plane protection between the group members and the key server. How do you secure the data plane communication if all group members use the same SA and key? The TEK is responsible for the data plane security through encryption of the communication payloads between the group members.

Three security controls are unique to GETVPN:

- Rekeying

- Time-Based Anti-Replay (TBAR)
- IP-Delivery Delay Detection Protocol (IP-D3P)

Rekeying

Rekeying, which is configured in the key server, is a policy that is pushed out to the group members and facilitated by the KEK. Before the existing key expires, a new key is generated, and then the group members are notified to transition to the new key. This is the base security control to prevent an attacker from learning the SA key, which changes at a configured frequency.

TBAR

Traditional IPsec solutions do not share a common SA, and because GETVPN has a group SA, you need a mechanism to prevent anti-replay. This is achieved through *Time-Based Anti-Replay (TBAR)*, which is a pseudo-time clock established for the group and managed by the key server. The key server keeps the pseudo-time synchronized via rekeying updates. When a packet arrives, the group member compares the pseudo-timestamp referenced in the packet with the synchronized time, and if the packet arrived too late, the group member drops the packet.

IP-D3P

IP-Delivery Delay Detection Protocol (IP-D3P) is designed to address IP delivery delay attacks. In this type of attack, which is similar to a replay attack, a packet that is not fresh (that is, not recently generated) is sent to a host or router. The IP-D3P datagram includes a header and an IP payload plus a timestamp that the receiver can use to compare to the local time. If the timestamp of the packet is outside the accepted window, the packet is not accepted. This setting, like the other security settings, is set at the key server and is part of the GDOI configuration parameters. This feature must be enabled.

Note

IP-D3P is an interoperability feature, which means that the Cisco IOS software and GDOI versions must be the same.

Now that we have covered the components and general concepts behind GETVPN, you are ready to start planning out what your GETVPN architecture could look like. This brings us to the design considerations you should be thinking about when developing a GETVPN solution.

GETVPN Design Considerations

Before you jump into configuring a GETVPN network, it is critical that you first establish a goal for the solution. Essentially, you need to determine what business problems you are aiming to solve. You will find that this recommendation will carry forward with any deployment you choose to use and a best practice that will be in future chapters.

This section considers common GETVPN design challenges and issues you need to think about as you develop your GETVPN architecture. You need to think about what value and limitations hardware will have. You need to think about whether GETVPN is the best option or whether another deployment option is better. You need to think about what your current investments are and whether they could be leveraged versus having to acquire new technology. All of this can impact how the design will look, including considerations for post deployment hurdles such as managing the solution and user/administration training.

GETVPN Fault Tolerance Considerations

One additional design consideration that will be echoed in future chapters is considerations for high availability/fault tolerance. These terms are used interchangeably throughout this book because both have the same end goals, and both terms are often used. The SVPN exam will likely have only a small number of questions involving fault tolerance, so coverage in this book is limited; however, real-world deployments will surely include some form of fault tolerance if budget allows. *Budget* is the key factor because we find that

is the most common limitation for why a real-world deployment would not include fault tolerance.

Chapter 3 includes a section on high availability/fault tolerance. Those fundamental concepts apply to any form of VPN. To summarize, options can include active or passive configurations to share load or push load to another system if it's a primary system. Options can include redundant hardware that is powered on and ready or powered off and available to fire up if an event occurs. Options can purely be configuration-based, meaning if a fault is found, the deployment will reroute traffic another way to accommodate the loss of system or connection. The focus for every chapter moving forward in regard to fault tolerance is specific to the chapter's focus. Moving forward, know that the general fault tolerance/high availability concepts covered in Chapter 3 apply to any deployment and must be part of your deployment considerations.

Key GETVPN Considerations

It is a good idea to create a design on paper first and then share it with your peers to validate and assess the design. We repeat this approach in future chapters of this book because this best practice applies to GETVPN as well as to any VPN topic covered.

The following are some of the many factors that should be documented and discussed before an implementation:

- IOS requirements
- Platform capabilities (and upgrade options)
- IP address scheme: IPv4, IPv6, or both
- Tunnel addresses
- External (public) addresses
- GETVPN key server and group members
- Routing requirements

- Authentication method: RSA signature, PKI, or pre-shared key
- Encryption scheme
- Deployment strategy
- Application requirements

GETVPN Implementation and Configuration

This next section covers the basics of configuring a GETVPN solution and how to configure both a key server and a group member. This section does not cover IKEv2 configuration for GETVPN because that protocol is discussed in detail in Chapter 6, "FlexVPN Configuration and Troubleshooting." Furthermore, the configuration examples in this section do not include an MPLS network; for the sake of simplicity, they include a private IP network.

Figure 4-7 shows the building blocks needed for a key server and a group member. As you can see, there are basically three distinct configuration blocks: ISAKMP configuration, IPsec configuration, and GDOI group creation. In the following configuration example, you will see these building block pieces laid out.

Figure 4-7 GETVPN Basic Requirements

The GETVPN IP network consists of three group member routers and one

key server. Each router provides VPN interconnection to the other routers, thus creating a VPN core IP network. As you can see in Figure 4-8, this example has an internal IP block at each of the three locations 10.1.0.0/16, 10.2.0.0/16, and 10.3.0.0/16, and the outside IP addresses are mandated by the private IP network. In this example, the routers are using a 172.16.x.0 address block for the outside, or private, network interface. The GETVPN identifier is the group member number, which in this case is 5. The key server defines both the GDOI information and the SA used by the group member routers. Figure 4-8 shows the topology and IP addresses used for the following key server and group member configuration examples.

Figure 4-8 GETVPN Topology

Configuring a Key Server

You set up the key server by building out the IKE policy that the key server will use and that the group members will need. The group members will have identical IKE policies. Next, the key server sets the IPsec transform policy, which will be downloaded by the group member. Finally, the GDOI protocol information needs to be established. This is where the SA information for the routers that are part of the GDOI network is defined and where the rekeying parameters are established by the key server. Figure 4-9 shows the pieces necessary for key server configuration.

Figure 4-9 GETVPN Key Server Configuration Requirements

IKE Phase 1 Policy

Example 4-1 shows the base IKE phase 1 policy configuration. With GETVPN, authentication is handled either through pre-shared key (PSK) or public key infrastructure (PKI). For simplicity, this example uses PSK for authentication.

Example 4-1 The GETVPN Key Server IKE Phase 1 Policy

```
KS1(config)# crypto isakmp policy 1
KS1(config-isakmp)# encryption aes 128
KS1(config-isakmp)# hash sha256
KS1(config-isakmp)# group 14
KS1(config-isakmp)# lifetime 3600
KS1(config-isakmp)# authentication pre-share
```

Key Server PSK Authentication

Because the configuration in Example 4-1 calls for PSK authentication, the commands in Example 4-2 are required for each group member to have a key specified on the key server.

Example 4-2 The GETVPN Key Server PSK Authentication

```
KS1(config)# crypto isakmp key cisco address 172.16.10.2
KS1(config)# crypto isakmp key cisco address 172.16.20.2
KS1(config)# crypto isakmp key cisco address 172.16.30.2
```

IKE Phase 2 Policy

Example 4-3 establishes the IPsec transform used between all the group members and the lifetime before the security associate expires and must be reauthenticated. In Figure 4-7, this is the IPsec information that each group member uses to secure the traffic between sites during communication.

Example 4-3 The GETVPN Key Server IKE Phase 2 Policy

```
KS1(config)# crypto ipsec transform-set Group5-Transform esp-
aes esp-sha-hmac
KS1(cfg-crypto-trans)# crypto ipsec profile Profile1
KS1(ipsec-profile)# set security-association lifetime seconds
7200
KS1(ipsec-profile)# set transform-set Group5-Transform
```

Key Server RSA Key

The configuration in Example 4-4 ensures that the key server has a certificate for signing rekeying messages for the group members. This component of the configuration is critical because the key server must be able to encrypt the TEK and KEK used by the group members.

Example 4-4 The Key Server RSA Key

```
KS1(config)# crypto key generate rsa general-keys label GETKEYS
mod 2048 export
```

Key Server GDOI

Example 4-5 shows how to configure the GDOI group number and identity used by the routers in the SA.

Example 4-5 The Key Server GDOI

```
KS1(config)# crypto gdoi group Group5
KS1(config-gkm-group)# identity number 555
KS1(config-gkm-group)# server local
```

Unicast Rekeying Parameters

Example 4-6 shows a continuation of the GDOI group configuration and defines the rekeying method that group members must use. In this example, the key server establishes the rekeying method, which is unicast (as opposed to multicast). In addition, this example specifies the RSA certificate that will be used for the encryption.

Example 4-6 Key Server Unicast Rekeying Parameters

```
KS1(gkm-local-server)# rekey transport unicast
KS1(gkm-local-server)# rekey lifetime seconds 86400
KS1(gkm-local-server)# rekey retransmit 10 number 2
KS1(gkm-local-server)# rekey authentication mypubkey rsa
GETKEYS
KS1(gkm-local-server)# address ipv4  172.16.5.5
```

Example 4-7 is a continuation of the GDOI configuration parameters, as you can see from the router prompt (**gkm-local-server**). This prompt indicates that you are configuring GDOI key server parameters on the local server. This is where you configure the access list used by the group members to determine what is encrypted between sites—in this case, basically all 10.0.0.0 through 10.3.0.0 traffic.

Example 4-7 Key Server Unicast Rekeying Parameters

```
KS1(gkm-local-server)# sa ipsec 1
KS1(gkm-sa-ipsec)# profile Profile1
KS1(gkm-sa-ipsec)# match address ipv4  101
KS1(gkm-sa-ipsec)# replay counter window-size 5
```

Key Server Policy Access List

Example 4-8 configures the access list required for the solution in Figure 4-6. The key server must inform the group members what IP packets will need to be encrypted between the sites. A routing solution is still required between the sites.

Example 4-8 Key Server Policy Access List Download

```
KS1(config)# access-list 101 permit ip 10.0.0.0 0.3.255.255
10.0.0.0 0.3.255.255
```

Configuring Group Members

The configuration of group members is much simpler than the configuration of the key server. Notice in Figure 4-10 that the first two building blocks are identical to the key server configuration. The GDOI parameters are taken from the key server distribution, but you must specify the key server you need to synchronize with, and you might have a secondary key server for redundancy. Finally, unlike in the key server configuration, the group members need to establish and attach the IPsec policy to the router's outside interface.

Figure 4-10 GETVPN Group Member Configuration Requirements

Group Member IKE Phase 1 Policy

Example 4-9 shows the base IKE Phase 1 policy configuration used by both the key server and all the group member routers. Notice that pre-shared key authentication is defined, as it was on the key server.

Example 4-9 GETVPN Key Server IKE Phase 1 Policy

```
GM1(config)# crypto isakmp policy 1
GM1(config-isakmp)# encryption aes 128
GM1(config-isakmp)# hash sha256
GM1(config-isakmp)# group 14
GM1(config-isakmp)# lifetime 3600
GM1(config-isakmp)# authentication pre-share
```

Group Member PSK Authentication

Example 4-10 shows the pre-shared authentication information required by the key server to protect Phase 1 negotiation. In this example, you must specify not only the other group members but the key server because in order to share the GDOI policy, you must make sure to share it securely. The security for this is provided by ISAKMP.

Example 4-10 GETVPN Key Server PSK Authentication

```
GM1(config)# crypto isakmp key cisco address 172.16.5.5
GM1(config)# crypto isakmp key cisco address 172.16.20.2
GM1(config)# crypto isakmp key cisco address 172.16.30.2
```

Group Member GDOI Information

Example 4-11 shows the GDOI group member information required. The group identity and key server IP address are specified in this part of the configuration.

Example 4-11 Group Member GDOI Information

```
GM1(config)# crypto gdoi group Group5
GM1(config-gkm-group)# identity number 555
GM1(config-gkm-group)# server address ipv4 172.16.5.5
```

Crypto Maps

Example 4-12 shows the creation of a crypto map for the GDOI protocol and specification of the group member number that you will attempt to use to register with the key server.

Example 4-12 Establishing a Crypto Map

```
GM1(config)# crypto map GVPN-Map 10 gdoi
GM1(config-crypto-map)# set group Group5
```

Finally, Example 4-13 shows how to apply the crypto map to the group member routers' outside interface.

Example 4-13 Applying a Crypto Map to an Interface

```
GM1(config)# interface GigabitEthernet0/2
GM1(config-if)# ip address 172.16.10.2 255.255.255.0
GM1(config-if)# crypto map GVPN-Map
```

That covers all the steps regarding delivering a generic GETVPN deployment. Make sure you understand each step involved so you can recognize GETVPN configuration exam questions and be able to speak about the components as well as what purpose they serve. Next, let's look at how to validate the status of your new or existing GETVPN deployment.

GETVPN Status Commands

The final topic to cover is how to validate whether things are working within your GETVPN deployment. You can do this using different **show** commands, and you will want to know what the output looks like for each command before taking the SVPN exam. This will help answer questions testing you on recognizing a GETVPN as well as troubleshooting potential problems. Figure 4-11 shows the output of the key server status and parameters. The identity Group 5 is listed, and the IP-D3P security feature is disabled.

```
KS1#sh crypto gdoi ks
Total group members registered to this box: 0

Key Server Information For Group Group5:
    Group Name                  : Group5
    Re-auth on new CRL          : Disabled
    Group Identity              : 555
    Group Type                  : GDOI (ISAKMP)
    Group Members               : 0
    Rekey Acknowledgement Cfg: Cisco
    IPSec SA Direction          : Both
    IP D3P Window               : Disabled
    CKM status                  : Disabled
    ACL Configured:
        access-list 101
```

Figure 4-11 show crypto gdoi ks Output

Figure 4-12 shows the output on the key server group information and parameters. This would be particularly useful if the key server were supporting multiple group identities. This configuration can be used on the group member as well as on the key server. The command lists more detail about GDOI, such as the rekeying status, which could be useful for troubleshooting. In addition, the output shows whether this solution is configured for IPv4 (as in this case) or IPv6.

```
KS1#sh crypto gdoi group Group5
    Group Name                  : Group5 (Unicast)
    Re-auth on new CRL          : Disabled
    Group Identity              : 555
    Group Type                  : GDOI (ISAKMP)
    Crypto Path                 : ipv4
    Key Management Path         : ipv4
    Group Members               : 0
    IPSec SA Direction          : Both
    IP D3P Window               : Disabled
    CKM status                  : Disabled
    Group Rekey Lifetime        : 86400 secs
    Rekey Retransmit Period     : 10 secs
    Rekey Retransmit Attempts: 2

      IPSec SA Number           : 1
      IPSec SA Rekey Lifetime: 7200 secs
      Profile Name              : Profile1
      Replay method             : Count Based
      Replay Window Size        : 512
      Tagging method            : Disabled
      ACL Configured            : access-list 101

     Group Server list          : Local
```

Figure 4-12 show crypto gdoi group group5 Output

Figure 4-13 shows a list of the group members that have registered. In this example, you see only two registrations, but there were actually three members. The display output has been shortened because the third group member registration did not add additional value.

```
KS1#sh crypto gdoi ks members

Group Member Information :

Number of rekeys sent for group Group5 : 1
Number of retransmits during the last rekey for group Group5 : 2
Duration of the last rekey for group Group5 : 21092 msec

Group Member ID    : 172.16.10.2         GM Version: 1.0.17
 Group ID          : 555
 Group Name        : Group5
 Group Type        : GDOI (ISAKMP)
 GM State          : Registered
 Key Server ID     : 172.16.5.5
 Rekeys sent       : 1
 Rekeys retries    : 0
 Rekey Acks Rcvd   : 1
 Rekey Acks missed : 0

 Sent seq num : 0       0       0       1
Rcvd seq num :  0       0       0       1

Group Member ID    : 172.16.20.2         GM Version: 1.0.17
 Group ID          : 555

Group Member Information :

 Group Name        : Group5
 Group Type        : GDOI (ISAKMP)
 GM State          : Registered
 Key Server ID     : 172.16.5.5
 Rekeys sent       : 0
 Rekeys retries    : 0
 Rekey Acks Rcvd   : 0
 Rekey Acks missed : 0
```

Figure 4-13 show crypto gdoi ks members Output

Figure 4-14 demonstrates the concept of KEK versus TEK. The output shows that KEK uses the RSA signature key name GETKEYS. With TEK policy, the transform for payload encapsulation is identified, and the access list is used to decide which packets are encapsulated and which are not.

```
KS1#sho crypto gdoi ks policy
Key Server Policy:
For group Group5 (handle: 2147483650) server 172.16.5.5 (handle: 2147483650):

  # of teks : 1  Seq num : 0
  KEK POLICY (transport type : Unicast)
    spi : 0x5520E1CB5E18EB46DA39127B75D5C1B6
    management alg     : disabled    encrypt alg       : 3DES
    crypto iv length   : 8           key size          : 24
    orig life(sec)     : 86400       remaining life(sec): 85060
    time to rekey (sec): 84835
    sig hash algorithm : enabled     sig key length    : 294
    sig size           : 256
    sig key name       : GETKEYS
    acknowledgement    : Cisco

  TEK POLICY (encaps : ENCAPS_TUNNEL)
    spi                : 0x7309A230
    access-list        : 101
    CKM rekey epoch    : N/A (disabled)
    transform          : esp-aes esp-sha-hmac
    alg key size       : 16            sig key size          : 20
    orig life(sec)     : 7200          remaining life(sec)   : 5861
    tek life(sec)      : 7200          elapsed time(sec)     : 1339
    override life (sec): 0             antireplay window size: 512
    time to rekey (sec): 5115
```

Figure 4-14 show crypto gdoi ks policy Output

Group Member Show Commands

The following figures illustrate the use of key **show** commands from a group member's perspective. In Figure 4-15, the output from the group member console shows some key information. First, it shows the start of the group member registration process to Group5 and the key server IP address 172.16.5.5. Next, it shows that the GDOI process is started, and Group5 is using unicast rekeying rather than multicast. Furthermore, you can see the KEK and TEK updated on the group member. Finally, the output shows the successful installation of the group member policy onto this particular member of Group5 SA.

```
*Aug  4 16:11:37.089: %CRYPTO-5-GM_REGSTER: Start registration to KS 172.16.5.5 for group Group5 using address 172.16.30
.2
*Aug  4 16:11:37.089: %CRYPTO-6-GDOI_ON_OFF: GDOI is ONend
R3#
*Aug  4 16:11:37.389: %GDOI-5-GM_REKEY_TRANS_2_UNI: Group Group5 transitioned to Unicast Rekey.
*Aug  4 16:11:37.389: %GDOI-5-SA_KEK_UPDATED: SA KEK was updated
*Aug  4 16:11:37.389: %GDOI-5-SA_TEK_UPDATED: SA TEK was updated
*Aug  4 16:11:37.393: %GDOI-5-GM_REGS_COMPL: Registration to KS 172.16.5.5 complete for group Group5 using address 172.1
6.30.2
*Aug  4 16:11:37.393: %GDOI-5-GM_INSTALL_POLICIES_SUCCESS: SUCCESS: Installation of Reg/Rekey policies from KS 172.16.5.
5 for group Group5 & gm identity  172.16.30.2
```

Figure 4-15 Group Member Console Output

Figure 4-16 shows the output of the **show crypto isakmp sa** command and clearly demonstrates that GETVPN is different from other VPN solutions. You can see that the client state is GDOI_IDLE rather than QM_IDLE.

```
HQ#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
172.16.5.5      172.16.10.2     GDOI_IDLE         9001 ACTIVE
```

Figure 4-16 show crypto isakmp sa Output

In Figure 4-17, the output from the **show crypto gdoi detail** command provides validation of the group information (Group5), the group type, and the crypto path. Notice that the ACL has not been received because this group member is still registering (see Figure 4-18).

```
HQ#sh crypto gdoi detail
GROUP INFORMATION

    Group Name                  : Group5
    Group Identity              : 555
    Group Type                  : GDOI (ISAKMP)
    Crypto Path                 : ipv4
    Key Management Path         : ipv4
    Rekeys received             : 0
    IPSec SA Direction          : Both

     Group Server list          : 172.16.5.5

Group Member Information For Group Group5:
    IPSec SA Direction          : Both
    ACL Received From KS        :
```

Figure 4-17 show crypto gdoi detail Output, Part 1

Figure 4-18 shows further output from **show crypto gdoi detail**. You can see the port on which GDOI communicates (848) as well as the IP address this member is using to register and the IP address of the key server. You can also see the rekeying cipher and rekeying hash. Each part of this output is a key to how GETVPN functions between the key server and group members and between group members.

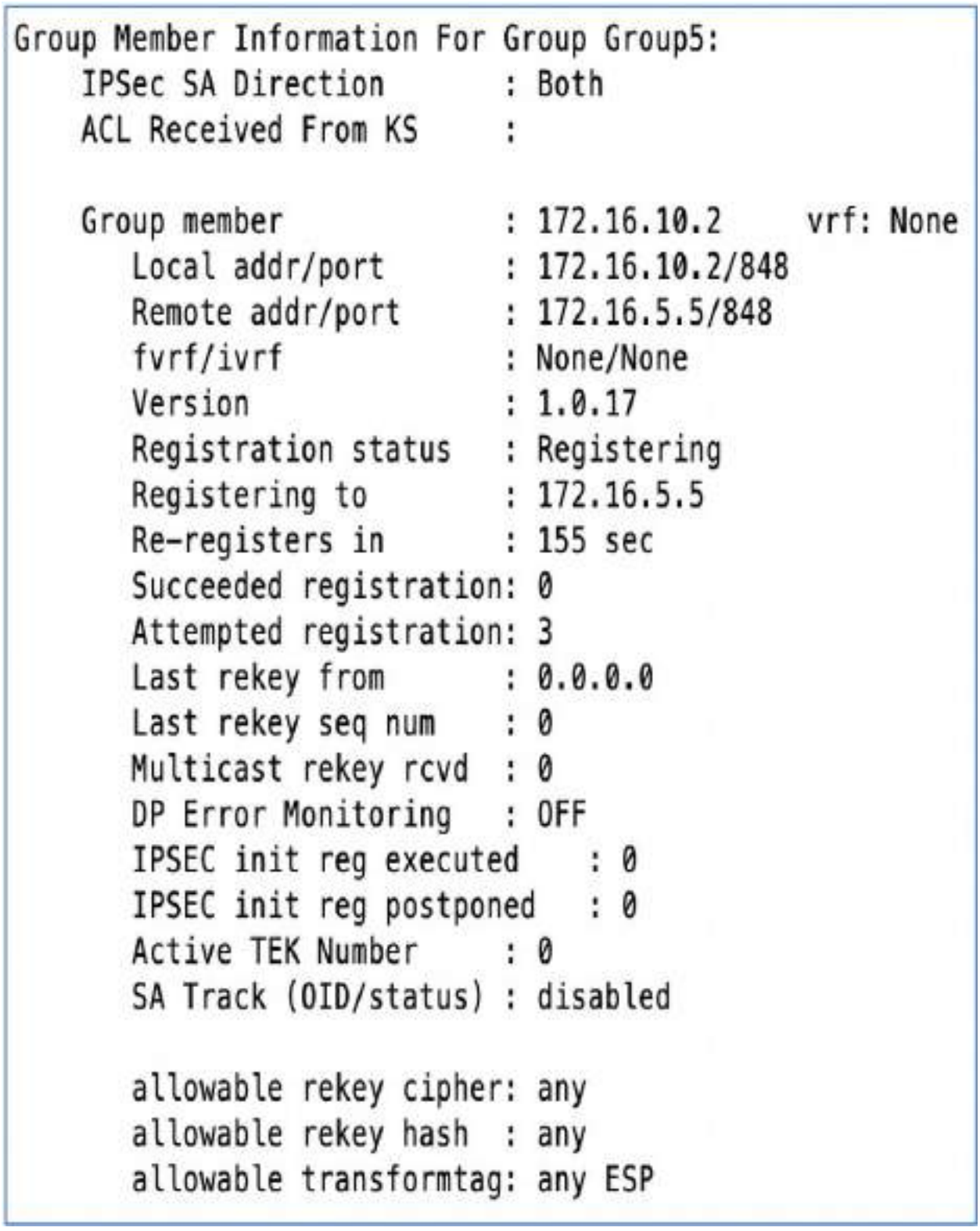


Figure 4-18 show crypto gdoi detail Output, Part 2

Figure 4-19 shows a subset of the output from the command **show crypto gdoi**. It focuses on the two keys used by the key server: the KEK used to secure communication between the key server and group members and the TEK used to secure traffic between group members.

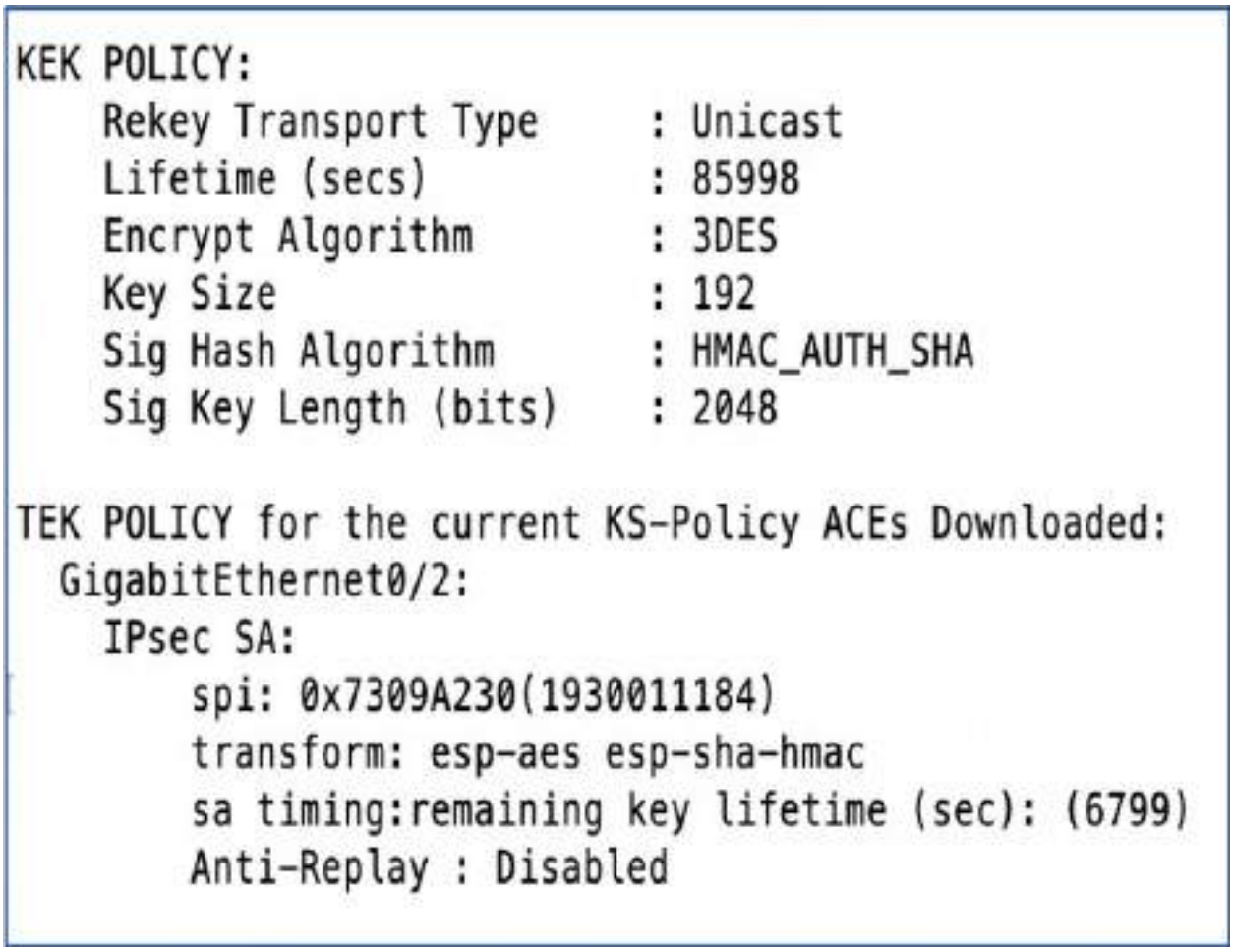


Figure 4-19 show crypto gdoi Output Subset

Figure 4-20 shows the output of the **show crypto gdoi gm acl** command. The interesting thing about this output is the ACL that was configured on the key server and downloaded by the group members; it shows what traffic will be encrypted between group members.

```
R2#show crypto gdoi gm acl
Group Name: Group5
 ACL Downloaded From KS 172.16.5.5:
   access-list   permit ip 10.0.0.0 0.3.255.255 10.0.0.0 0.3.255.255
 ACL Configured Locally:
 ACL of default bypass policy for group-key management traffic:
   GigabitEthernet0/2: deny udp host 172.16.20.2 eq 848 any eq 848
```

Figure 4-20 show crypto gdoi gm acl Output

GETVPN Status Commands Summary

Table 4-2 consolidates the key commands covered in this last section. The commands are organized in a list divided by running the command from either key server or group member. We highly recommend leveraging these commands during any deployment, and know their outputs and purposes for the SVPN exam.

Table 4-2 GETVPN Status Commands

Focus Point	Command
Key Server Show Commands	show crypto gdoi ks show crypto gdoi group group5 show crypto gdoi ks members show crypto gdoi ks policy
Group Member Show Commands	show crypto isakmp sa show crypto gdoi show crypto gdoi detail show crypto gdoi gm acl

That wraps up the steps in designing, configuring, and validating a GETVPN deployment. This last section focused on status validation, and many of these same commands can also be used for troubleshooting. In the next chapter, we focus on troubleshooting concepts, which will be similar for troubleshooting all forms of site-to-site VPN deployments.

Summary

This chapter introduced the Group Transport Encryption VPN (GETVPN) technology and its extensive benefits for enterprise environments using an MPLS or private network. This chapter covered a number of topics included on the SVPN 300-730 exam, such as GETVPN components and how GETVPN works. To give you a better understanding of how GETVPN works and the role of each of the components, this chapter provided a step-by-step configuration example. In addition, this chapter showed the basic components as organized building blocks that demonstrate the functions the configurations reviewed aim to achieve. This chapter also provided command output to link together the configuration building blocks and a successful solution.

Next up is a focus on DMVPN technology, followed by FlexVPN. GETVPN,

DMVPN, and FlexVPN, making up the key site-to-site VPN topics you need to know for the SVPN exam.

References

GETVPN Deployment Guide. Retrieved from https://www.cisco.com/c/en/us/products/collateral/security/group-encrypted-transport-vpn/deployment_guide_c07_554713.html

Group Encrypted Transport VPN Configuration Guide. Retrieved from https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_getvpn/configuration/xe-3s/sec-get-vpn-xe-3s-book.pdf

Troubleshooting Common GETVPN Issues. Retrieved from https://www.cisco.com/c/en/us/support/docs/security/group-encrypted-transport-vpn/116958-troubleshoot-getvpn-00.html#anc14

Exam Preparation Tasks

As mentioned in the section "How to Use This Book" in the Introduction, you have a couple of choices for exam preparation: the exercises here, Chapter 11, "Final Preparation," and the exam simulation questions in the Pearson Test Prep software online.

Review All Key Topics

Review the most important topics in the chapter, noted with the key topics icon in the outer margin of the page. Table 4-3 lists these key topics and the page number on which each is found.

Table 4-3 Key Topics for Chapter 4

Key Topic Element	Description	Page Number
Section	GDOI Protocol	
List	GETVPN Benefits Summary	
List	Components of a key server	
List	Three unique security controls unique to GETVPN	
Example 4-1	The GETVPN Key Server IKE Phase 1 Policy	
Example 4-3	The GETVPN Key Server IKE Phase 2 Policy	
Example 4-9	GETVPN Key Server IKE Phase 1 example	
Example 4-10	GETVPN Key Server PSK Authentication	
Example 4-12	Establishing a Crypto Map	
Table 4-2	GETVPN Status Commands	

Complete Tables and Lists from Memory

There are no memory tables in this chapter.

Define Key Terms

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

Group Encrypted Transport VPN (GETVPN)
Multiprotocol Label Switching (MPLS)
security association (SA)
Group Domain of Interpretation (GDOI)
key encryption key (KEK)
traffic encryption key (TEK)
Time-Based Anti-Replay (TBAR)
IP-Delivery Delay Detection Protocol (IP-D3P).

Chapter 5. Dynamic Multipoint Virtual Private Network (DMVPN)

This chapter covers the following subjects:

- **DMVPN Overview:** This section provides an overview of the advantages DMVPN provides and compares DMVPN to the legacy site-to-site crypto map solution.
- **Network Components:** This section examines the components of DMPVN and how they work together to create a dynamic solution.
- **DMVPN Design Considerations:** This section discusses design issues that must be considered before deploying a DMVPN solution as well as the differences between DMVPN Phase 2 and DMVPN phase 3 configuration.
- **DMVPN Hub-and-Spoke Implementation (IPv4 and IPv6):** This section steps through a basic DMVPN hub-and-spoke (IPv4/IPv6) configuration. Examples demonstrate how the DMVPN components interact to provide a comprehensive three-router solution.
- **DMVPN Troubleshooting:** This section discusses how to troubleshoot DMVPN components and provides potential solutions.

"If you read someone else's diary, you get what you deserve."

—David Sedaris

This chapter covers the following exam objectives:

- 1.0 Site-to-site Virtual Private Networks on Routers and Firewalls
  - 1.2 Describe DMVPN
- 3.0 Troubleshooting using ASDM and CLI
  - 3.1 Troubleshoot IPsec

- 3.2 Troubleshoot DMVPN

- 4.0 Secure Communications Architectures
  - 4.1 Describe functional components of GETVPN, FlexVPN, DMVPN, and IPsec for site-to-site VPN solutions
  - 4.3 Recognize VPN technology based on configuration output for site-to-site VPN solutions
  - 4.6 Design site-to-site VPN solutions

In earlier chapters of this book, you have seen that secure VPN technology varies and has been adapted to be used in many different architectures by vastly different organizations. This chapter explores a dynamic adaptation of the site-to-site VPN solution. Traditional site-to-site VPNs did not scale easily, and Dynamic Multipoint Virtual Private Network (DMVPN) was designed to dynamically establish connections with minimal administrative overhead. Furthermore, traditional site-to-site VPNs had various challenges in supporting dynamic routing protocols, voice over IP (VoIP), and streaming video. All of these technologies are needed to support large-scale telecommuter and remote branch networks. In addition, the dynamic nature of DMVPN enables optimization of network paths, which in turn reduces latency and jitter, which are detrimental to VoIP and video. Organizations are finding that dedicated WAN circuits are no longer necessary for remote connectivity. In its place, organizations are using the Internet and secure communication through VPN technology to achieve the same benefits at a fraction of the cost.

A short summary of the value of DMVPN is that it can lower capital and operation expenses, simplify branch communications, reduce deployment complexity, and improve business resiliency. This is why DMVPN is a widely used VPN option and one you will need to master before attempting the SVPN exam. The SVPN exam expects you to be able to describe the components within a DMVPN deployment, recognize DMVPN configuration components, and troubleshoot a DMVPN deployment.

Note

On the exam, you might see a configuration that includes a misconfigured or broken DMVPN solution. In such a situation, you will need to be able to determine what is wrong, and you will need to know the proper commands to fix the configuration. One of the best ways to learn and prepare for the exam is by getting hands-on experience. Reading this book and working with three routers to try out the examples shown in this chapter is a good way to prepare for the exam.

Learning beyond the SVPN concepts:

- DMVPN Overview
- DMVPN Foundational Concepts
- DMVPN Design Considerations

"Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz enables you to assess whether you should read the entire chapter. If you miss no more than one of these self-assessment questions, you might want to move ahead to the "Exam Preparation Tasks" section of the chapter. Table 5-1 lists the major headings in this chapter and the "Do I Know This Already?" quiz questions related to the material in each of those sections to help you assess your knowledge of these specific areas. The answers to the "Do I Know This Already?" quiz appear in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes."

Table 5-1 "Do I Know This Already?" Foundation Topics Section-to-Question Mapping

Foundation Topics Section	Questions
DMVPN Overview	1–3
DMVPN Network Components	4–6
DMVPN Design Considerations	7–10
DMVPN Hub-and-Spoke Implementation (IPv4 and IPv6)	11, 12
DMVPN Troubleshooting	13

1. What are some of the benefits of DMVPN technology compared to legacy site-to-site VPN solutions? (Choose three.)

   a. Multicast support

   b. Crypto map enhancement

   c. QoS support

   d. Dynamic routing protocol capabilities

   e. Complex administrative overhead

2. What is the primary reason companies select DMVPN over a legacy crypto map VPN solution?

   a. Static Internet addresses

   b. Dynamic Internet addresses

   c. Complex configuration overhead

   d. GRE support

3. What advantages does DMVPN offer that a crypto map–based VPN does

not? (Choose two.)

a. Scalability

b. Lack of routing protocol support

c. Reduced configuration overhead

d. Increased bandwidth requirements

4. What are the key components of DMVPN? (Choose all that apply.)

a. mGRE

b. OSPF

c. NHRP

d. Static routes

e. IPsec

f. Routing protocols

5. Which DMVPN component is responsible for mapping the tunnel IP address to an external IP address?

a. OSPF

b. NHRP

c. ISAKMP

d. mGRE

6. Which DMPVN component enables the use of dynamic routing protocols across an IPsec tunnel?

a. OSPF

b. NHRP

c. IPsec

d. GRE

7. Which of the routing protocols used with DMVPN face a split-horizon

issue? (Choose two.)

a. OSPF

b. EIGRP

c. BGP

d. RIP

8. Which routing protocol for use with DMVPN faces a non-broadcast multiple-access (NBMA) challenge that must be addressed?

a. OSPF

b. EIGRP

c. BGP

d. RIP

9. Which design considerations must you consider for DMVPN? (Choose two.)

a. The number of IP address ranges

b. The number of remote sites

c. External IP addresses

d. The need for quality of service (QoS) in applications

10. What is the difference between DMVPN Phase 2 and DMVPN Phase 3?

a. There is no difference; they both support only hub-and-spoke solutions.

b. DMVPN Phase 2 supports hub-and-spoke solutions, and DMVPN Phase 3 also supports spoke-to-spoke.

c. DMVPN Phase 2 has smaller routing tables.

d. DMVPN Phase 3 has smaller routing tables.

11. What key word on a hub router enables connections from any remote spokes?

a. multicast

b. dynamic

c. host

d. map

12. Which command for EIGRP prevents a hub router from setting the router advertisement out to a spoke to its own IP address?

a. no ip split-horizon eigrp 1

b. ip eigrp 1 non-broadcast

c. no ip broadcast eigrp 1

d. no ip next-hop-self eigrp 1

13. Which command would show whether the spoke router is registered with the NHS?

a. show ip nhrp detail

b. show ip nhs detail

c. show ip nhrp nhs detail

d. show ip nhrp client

Foundation Topics

Dynamic Multipoint Virtual Private Network (DMVPN) enables different branch locations to communicate in a direct and secure manner using either a public or a private network. DMVPN accomplishes this by utilizing a centralized architecture to ease implementation and management. This enables branch locations to communicate directly with one another, such as when using voice or video between offices, while also not requiring a permanent VPN tunnel between offices.

DMVPN creates a mesh VPN network that is applied selectively based on the connections being utilized by the organization. Each different location, or “spoke,” can connect to any another location in a secure manner. The components involved include GRE tunnel interfaces, IPsec tunnel endpoint

discovery, routing protocols for dynamically building the network, and NHRP for locating spokes. We dive into all these topics in this chapter, including supporting both IPv4 and IPv6 as well as troubleshooting your deployment.

The following highlight some of the key benefits of using DMVPN compared to a traditional MPLS network.

- It has the potential for high-performance Internet speed and reliable performance.
- It reduces the cost of secure communications and connections between branch locations by integrating VPN with communication technology (voice and video).
- The centralized system simplifies branch-to-branch connections.
- It reduces the risk of downtime by securing routing with IPsec technology.

DMVPN Overview

Many companies use DMVPN for their wide area network connectivity for one primary reason: It enables remote sites to have dynamic Internet addressing and yet still cryptographically access corporate data. In legacy VPN solutions, companies had to order static IP addresses at each remote site, thereby incurring an extra charge from the ISP and adding to the overall cost of the solution. Furthermore, as you added remote sites to such a solution, the hub router configuration grew exponentially. The days of configuring crypto maps, access control lists (ACLs), policies, and generic routing encapsulation (GRE) tunnels for each remote site have been replaced by the use of more mature and flexible VPN solutions. DMVPN specifically resolved the issues of static routing and cumbersome configuration with the use of an IPsec profile. In the legacy VPN configurations shown in Chapter 3, "Site-to-Site VPNs," you had to configure one crypto map with multiple policies, each with its own ACL, to indicate which traffic was permitted to go to which destination through the tunnel and what transform set was configured. Each time you added another site-to-site VPN, you added to the

policy and, potentially, to the non-NAT ACL.

Legacy Crypto Map VPN Solutions

Figure 5-1 shows an example of a legacy crypto map VPN tunnel solution. This solution requires specific configuration for each site; DMVPN does not require this much configuration. In addition, the legacy solution does not support spoke-to-spoke communication, whereas DMVPN does.

Figure 5-1 Legacy VPN Tunnels

Modern VPN Needs

As shown in Figure 5-2, companies today are using VPNs for a variety of services. In this diagram you can see a mobile user who may be using a video conferencing software package on a laptop in order to communicate. In addition, you can see a remote office that might have multiple users that all have VoIP phones behind the main router; they might need to be able to use the DMVPN solution for not only data but voice and video conferencing. We could expand this diagram by adding another remote office on the DMVPN network, and users from one office would be able to call users in another office by using VoIP rather than traditional dedicated phone circuits from the local provider.

Figure 5-2 A Telecommuter and a Remote Office with VoIP

DMVPN Risks

Although DMVPN provides secure connectivity, it does not make you immune to attacks. Simply adding remote sites to a corporate network increases your organization's security risk. For example, if a teleworker's remote machine is infected with ransomware, it might be possible for that ransomware to find other clients to infect through the network. In a fully meshed DMVPN solution, such an attack could cripple an organization's capability to run its business (see Figure 5-3). So, as you are building out a VPN security solution, you should consider best practices for restricting, monitoring, and policing VPN traffic. Some examples of best practices would be to establish east–west access control and to monitor using traffic capture or NetFlow. In terms of packet monitoring security, implementing breach detection capabilities such as IPS/IDS technology should be considered essential.

Figure 5-3 Ransomware Infection

DMVPN Core Concepts

The features available in a DMVPN solution are similar to those available with both GETVPN and FlexVPN. However, like those types of VPN architectures, DMVPN has its own components and terminology. For example, you need to know and understand GRE tunnels and *Next Hop Resolution Protocol (NHRP)*, which enable DMVPN to scale up to thousands of remote connections and reduce the need for complex administration.

DMVPN Example

Figure 5-4 shows an example of a DMVPN solution where each spoke can communicate with the hub router. In addition, Spoke1 and Spoke2 establish a VPN tunnel directly between themselves.

Figure 5-4 A Full-Mesh DMVPN Tunnel

A critical piece of this solution is that GRE and NHRP work together to resolve the peer destination IP address. In essence, the NHRP configuration on a spoke router forces a registration process that maps the GRE tunnel IP address to the Internet destination IP address for the spoke on the hub NHRP database. Another critical piece of this solution is *multipoint Generic Routing Encapsulation (mGRE)*. We will look more closely at these two components in the next section.

DMVPN, as its name implies, also supports IPsec. The configuration combinations for IPsec are quite extensive, and this chapter covers only some of the key ones; in other chapters, you will see many other configurations that include IPsec. Let's look at the components of a DMVPN deployment.

Network Components

As mentioned in the last section of this chapter, DMVPN uses several components to achieve either a hub-and-spoke or a spoke-to-spoke solution: mGRE, NHRP, and IPsec. This section examines these components as well as the routing protocols that DMVPN supports. Make sure you are familiar with each of these components before moving to the next part of this chapter. First, we need to understand mGRE.

mGRE

mGRE enables routers to support multiple GRE tunnels on a single interface. This single interface can receive inbound GRE connections from dynamically addressed remote site locations and simultaneously support dynamic routing protocols, IP Multicast, and non-IP protocols. Both GRE and mGRE have a 24-bit header; in some situations, this header can impact application functionality. (We will examine this later in this chapter.) The advantage of using mGRE is that it enables the DMVPN network to replicate the function of a non-broadcast multiple-access (NBMA) multipoint Frame Relay solution (see Figure 5-5). Such solutions were more common in the past, when companies would purchase a Frame Relay WAN architecture from a telephone company and request that it be configured as multipoint. In Figure 5-5, which provides an example of the components in a DMVPN configuration, you can see that, in addition to a VPN tunnel, there are also GRE tunnels configured between sites.

Figure 5-5 GRE Tunnels

GRE and mGRE Advantages

GRE and mGRE have many advantages both with DMVPN and in other solutions. For example, you can use a GRE tunnel to repair network routing links between OSPF areas that have become disconnected, causing routing updates between them to stop. Because GRE uses the IP protocol 47 and

encapsulates the entire original IP payload, it supports nontraditional protocols as well as multicast and the use of routing protocols across a VPN tunnel.

GRE has a few limitations, but they are significant:

- GRE is not a cryptographic protocol, and it does not provide data protection.
- GRE can be CPU intensive, and you need to consider this during design.
- The IP MTU and fragmentation issue mentioned earlier might occur with some applications.
- Vendor GRE solutions are not all alike, and integration can be challenging.

NHRP

NHRP is used as the primary communication system for DMVPN hubs to inform spoke devices about other registered spokes. This is a classic client and server protocol: The server (hub) maintains the database of the spokes (clients) that have successfully registered. During the registration process, each spoke provides the server with its public IP address and the internal IP address of its GRE tunnel. The NHRP hub stores that information in the NHRP database so that other spokes can query the database for that information. Notice in Figure 5-6 that the NHRP registration occurs over the tunnel, and the NHRP packet includes the source address of the device that sent the tunnel, the destination address of the tunnel, and the NBMA address (public) of the destination device.

Figure 5-6 NHRP Registration Process

NHRP Example

Figure 5-6 shows IPsec tunnels, the GRE tunnel, and NHRP configured. It shows that the NHRP database on the NHRP server provides both the tunnel and the external IP address of a spoke router. This information is gathered during the spoke registration process.

Remaining DMVPN Components

IPsec is used to secure traffic going across a tunnel. Depending on the architecture of a DMVPN topology, it is possible for spokes to dynamically establish VPN tunnels with other spokes.

Routing is an often-overlooked piece of a DMVPN solution. However, routing is key because it enables a remote site to reach another remote spoke network that it did not initially have in its routing table prior to registration. Understanding DMVPN routing configuration comes down to understanding the shortfalls of routing protocols such as EIGRP and the split-horizon feature. With OSPF, an engineer would need to address the issue of NBMA with either a multipoint OSPF configuration or set up a broadcast network.

Solution Breakdown

In studying and preparing for the SVPN 300-730 exam, a good approach would be to break down the components of a solution down into sub pieces. When you have mastered all the components, troubleshooting DMVPN will be much easier. Table 5-2 will help you study and focus on the key components of a DMVPN configuration.

Table 5-2 Basic DMVPN Configuration Components

Component	Requirement
Crypto configuration	Commands for ISAKMP and IPSEC
Tunnel configuration	Commands to set up a tunnel interface
Next Hop Resolution Protocol	Commands to configure NHRP on both hub and spoke routers
Routing protocol configuration	Commands to configure a routing protocol for hub-and-spoke or spoke-to-spoke communications

DMVPN Design Considerations

Before you start designing a DMVPN network, it is critical to establish a goal for the solution. Just like with any VPN technology, you first need to understand what business problems you are going to solve. Once you have determined the goal, you can work back from the goal to the solution. We performed a similar exercise in the last chapter when covering design considerations for deploying GETVPN.

This section looks at some of the common design challenges and issues that security engineers must consider. In addition, equipment has a significant impact on a solution, and you might need to upgrade some of your equipment to support DMVPN, especially if you are trying to reuse existing equipment for remote site deployments. (Chapter 3 includes a list of pre-design

questions that a team should consider before deploying DMVPN. Many of them specifically address equipment issues.)

DMVPN Planning

During the DMVPN design phase, a key constraint would be what applications will be running over the DMVPN links. Are you deploying VoIP or video conferencing solutions? Such low-latency applications might require QoS and priority over other applications. In addition, what level of fault tolerance is needed at the headend (hub) site to which the DMVPN remote sites connect? Will multicast traffic need to traverse the VPN links? What type of routing protocol will you use? The routing protocol setup requires some serious consideration. You should think about the following questions before configuring your routing protocol:

- What network IP blocks need to be accessible from the remote sites?
- Do remote site IP blocks need to be accessible from other locations?
- Does traffic need to be filtered for specific IP address ranges?
- Is QoS required?

Based on the answers to these questions, you might need to configure spoke-to-spoke communication across the VPN tunnel. If the objective of your design is to create spoke-to-spoke communication, you will need to answer another question: Will that traffic go through the headend router, or will it travel directly to the spoke? The answer impacts the configuration of your solution.

You need to think about all the questions posed so far, but these are just a few of the many considerations. Later in this chapter, you will see how to configure traffic from one spoke destined for another to be routed through the hub. You will also see how to configure a solution in which the spoke router can establish a direct VPN link to the other spoke router, thus reducing the overhead on the headend router.

Note

Cisco has a DMVPN Design and Implementation guide available at https://www.cisco.com/c/dam/en/us/products/collateral/security/dynamic-multipoint-vpn-dmvpn/dmvpn_design_guide.pdf?dtid=osscdc000283. We highly recommend that you review it before you deploy DMVPN.

DMVPN Fault Tolerance Considerations

We would be remiss if we did not talk about fault tolerance in this or any section that involves design considerations. Even though we do not focus on fault tolerance/high availability in our examples in this chapter, having multiple hub sites should be part of your design for high-availability purposes. Including multiple hub sites will add to the configuration on the spoke routers, but that additional work will not be a significant amount, and it could also increase the bandwidth at the hub site. The level of fault tolerance your organization requires will impact your solution and its cost. As stated in the last chapter, we find cost is the number of factor that impacts how an organization will include fault tolerance within its VPN design.

Key DMVPN Considerations

One best practice we will continue to use in this chapter is creating a design on paper first. We recommend you share your design with your peers to validate and assess the design before moving forward with any deployment. The following are some of the many factors that should be documented and discussed before an implementation. You find this list to be similar to the one used in the last chapter.

- IOS requirements
- Platform capabilities (and upgrade options)
- IP address scheme: IPv4, IPv6, or both
- Tunnel addresses

- External (public) addresses
- DMVPN hub-and-spoke or partial mesh
- Routing requirements
- Authentication method: RSA signature, PKI, or pre-shared key
- Encryption scheme
- Deployment strategy
- Application requirements

DMVPN Phases

DMVPN comes in three different designs, referred to as DMVPN phase 1, DMVPN phase 2, and DMVPN phase 3. The DMVPN phase you choose determines how spokes communicate with one another as well as the routing configuration. In the next three sections we discuss the differences between each phase and the major configuration differences between them.

DMVPN Phase 1

DMVPN is the first phase that was defined when this technology was implemented by Cisco and is strictly designed for hub-and-spoke communications only. Spoke-to-spoke traffic flows will need to reach the hub and then be transported down to the spoke. This is the exact same traffic flow as a hub-and-spoke design in Frame Relay or ATM. For example, consider the topology shown in Figure 5-7.

Figure 5-7 Basic DMVPN Hub and Spoke Example

R1 is acting as the DMVPN hub for this network and is therefore the NHS for NHRP registration of the spokes. In DMVPN phase 1 the GRE tunnels shown are multipoint GRE on the hub and point-to-point on the spokes. This forces hub-and-spoke traffic flows on the spokes. In addition to this, the next-hop value of any routes sent between spokes and hubs should be changed to reflect the topology. Therefore, the same routing issues with frame-relay and ATM apply to DMVPN (Split Horizon, for example). As a high-level configuration on R1 we can see the basic configurations for DMVPN phase 1.

DMVPN Phase 2

In DMVPN phase 2, spoke-to-spoke traffic flow is now permitted, and all spoke routers implement multipoint GRE. Equally, resolution request NHRP messages are now sent to resolve a spoke's VPN address to its NBMA address. However, this function relies heavily on your routing design and in ensuring that the next-hop address is preserved during advertisement from the hub down to other spokes, much like how the next hop is preserved on an ethernet switch to allow more efficient traffic flows. To demonstrate this, the topology in Figure 5-8 has been updated to reflect this change.

Figure 5-8 Spoke-to-Spoke Added

In DMVPN phase 2, when a spoke router wants to communicate with another spoke router it will look at its routing table to determine the next-hop address.

Spokes preserve their next hop address; because the routing table and NHRP tables are unable to exchange information, each spoke has to hold the full network routing table for all spokes on the DMVPN network. In Figure 5-8, if Spoke1 had a change in its routing table with the failed link that triggered an update, Spoke2 would see this change and update its routing table. The reason is that the Spoke2 routing table has received routes from Spoke1 via the hub router, including the next hop of the tunnel address, which is 192.168.1.2 (Spoke1). Spoke1 only knows of Spoke2 through the tunnel address 192.168.1.3; it is not aware of the NBMA address (public) that lies in between. The hub router knows of the Spoke2 NBMA address and would forward the route update to Spoke2. You need to understand that changes or queries by any spoke of another spoke would, at a minimum, generate an NHRP resolution request to the hub. In this example, a failed link would generate not only an NHRP resolution request but also a routing protocol update packet.

Figure 5-9 shows that a link on Spoke1 has failed. This figure demonstrates that in a DMVPN phase 2 solution, a failed link such as the one on Spoke1 will trigger a routing update being sent to Spoke2 to notify that router of the change.

Figure 5-9 DMVPN Phase 2

DMVPN Phase 3

With DMVPN phase 3, Cisco modified the Cisco Express Forwarding (CEF) table and the NHRP table so that they can work together. This enables the NHRP table to resolve the next hop information and the CEF table to route the packets. This change enables the hub router to set the next hop to itself and advertise summarized routes to all of the spokes. This configuration option supports the use of smaller spoke routers by eliminating the need to support the entire corporate routing table.

Now that we have tackled all the design concepts behind DMVPN, we next learn what is involved with deploying DMVPN. Let's first start with a look at a hub-and-spoke implementation.

DMVPN Phase 1 Hub-and-Spoke Implementation

Now it is time to dive into DMVPN implementations. The best way to address learning how technology is configured is to break it down into manageable parts. This section shows the implementation of a basic hub-and-spoke DMVPN design for both IPv4 and IPv6 by breaking down the process

into four parts. We highly recommend that you understand how each part works as you study DMVPN technology because you will see questions about the different parts of a DMVPN configuration on the SVPN exam. The following are the four parts of a DMVPN configuration:

- Crypto IPsec policy configuration
- GRE tunnel configuration
- NHRP hub-and-spoke configuration
- Routing configuration

Breaking down the process into these four parts will make it easier to troubleshoot which part of the configuration is incorrect and which parts are correct. It will also help with identifying wrong answers for questions about specific parts of a DMVPN configuration. For example, if you are dealing with a routing issue, any answer regarding the GRE tunnel configuration could be eliminated.

Figure 5-10 shows the topology and IPv4 design, and Figure 5-11 shows the topology and IPv6 design for the following configuration examples. Use this as a reference for this next section.

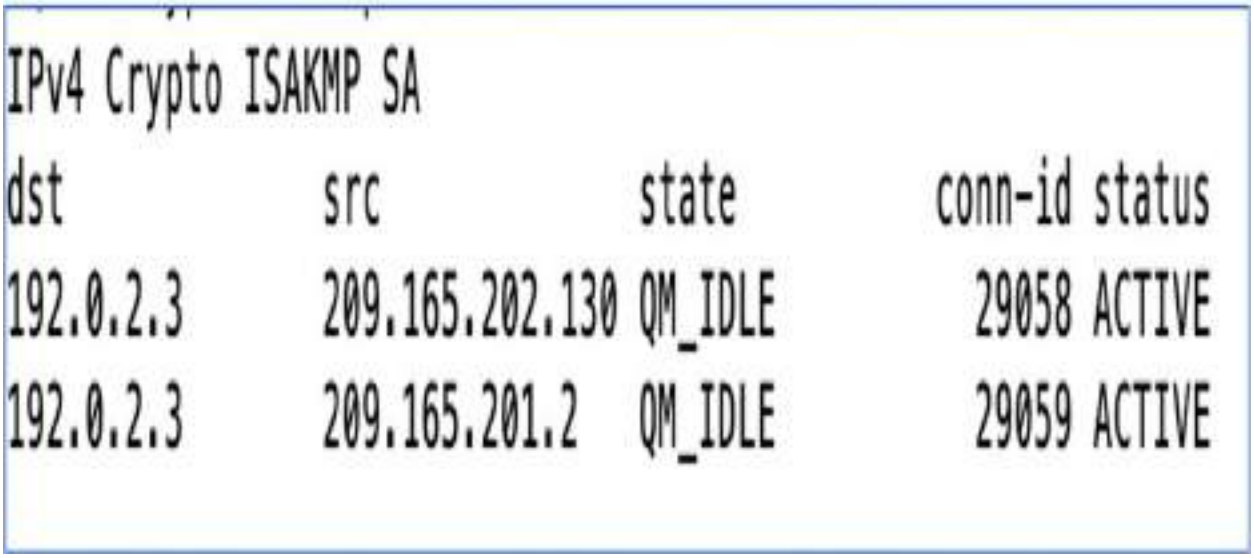


Figure 5-10 DMVPN IPv4 Solution

```
interface: Tunnel1
    Crypto map tag: Tunnel1-head-0, local addr 192.0.2.3

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.0.2.3/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (209.165.201.2/255.255.255.255/47/0)
   current_peer 209.165.201.2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 14592, #pkts encrypt: 14592, #pkts digest: 14592
    #pkts decaps: 28935, #pkts decrypt: 28935, #pkts verify: 28935
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 192.0.2.3, remote crypto endpt.: 209.165.201.2
     path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
     current outbound spi: 0xDFB0D10(234556688)
     PFS (Y/N): Y, DH group: none
```

Figure 5-11 DMVPN IPv6 Solution

Crypto IPsec Policy Configuration

As discussed in earlier chapters, the Internet Key Exchange (IKE) management protocol is primarily used to authenticate IPsec peers. Configuring a crypto IPsec policy can be broken into the following three steps:

- Creating an IKE Policy
- Creating Pre-shared Key Authentication Credentials

- Creating a Profile and Transform Set

This section works through each of these three steps starting with creating an IKE Policy.

Creating an IKE Policy

In Example 5-1, it is used by the two spoke routers and the hub router to authenticate, negotiate, and distribute IPsec encryption keys. Today, this is optional on some Cisco platforms as there is a default IKE policy; however, your organization my require a more secure policy. In this example, this policy will be repeated on the two remote site routers (spokes) and must match the HQ router policy. Let's work through each step of the crypto IPsec policy configuration. We will break this into steps as well to clearly work through how the configuration is performed.

Example 5-1 shows the basic crypto ISAKMP IKE policy used by all the routers in Figures 5-8 and 5-9.

Example 5-1 Creating an IKE Policy

```
HQ-Router(config)# crypto isakmp policy 10
HQ-Router(config-isakmp)# encryption aes 192
HQ-Router(config-isakmp)# hash sha256
HQ-Router(config-isakmp)# authentication pre-share
HQ-Router(config-isakmp)# group 5
```

The policy shown in Example 5-1 is policy number 10. You can have policies from 1 to 65535, ordered by priority. If you establish a VPN with another router that does not have a policy matching this one, your router could potentially find another policy that might match that remote side. If, during troubleshooting, you notice that the IKE policy fails to negotiate, the first place to look is at the IKE policy parameters on both routers.

Example 5-1 shows the use of AES-192 encryption and the hash policy SHA-256. Notice in this example that the authentication in use is pre-shared. This means that you are going to have to manually set up authentication keys on all the DMVPN routers. Another option would be to use certificate authority

(CA) signatures. The third method for authentication would be to use encrypted nonces. (Both forms of certificate authentication are discussed in Chapter 3.) We recommend that you take the time to learn how to use certificates for authentication because this process is critical for large-scale deployments. By using certificates, you remove the need to keep track of pre-shared keys, and that is a security improvement.

Finally, Example 5-1 specifies group 5 for the Diffie-Hellman key algorithm, which uses a 1536-bit modulus, which in turn uses 2048 bits to create a prime and generate numbers as security association (SA) keys. Depending on your router and its IOS version, you might be able to create a more secure solution by increasing the AES encryption to AES-256 with SHA-512. Chapter 8, "Remote Access VPNs," covers encryption in more detail.

Creating Pre-shared Key Authentication Credentials

The next step is creating a pre-shared key. Example 5-2 shows an implementation of IPv4 pre-shared keys for the two remote spoke routers.

Example 5-2 Creating Pre-shared Key Authentication Credentials, IPv4

```
HQ-Router(config)# crypto isakmp key TESTKEY address
209.165.201.2
HQ-Router(config)# crypto isakmp key TESTKEY address
209.165.202.130
```

On the main router, you need to reference the remote site routers or, in this case, the spokes. It is critical that you reference the public IP address of the router or the address that is reachable by the router if you are implementing a DMVPN solution on a private network. The spoke routers at first have just one crypto pre-shared key configuration line. With spoke-to-spoke configuration, this changes, as you'll see later in this chapter.

Example 5-3 shows an implementation of IPv6 pre-shared keys for the two remote spoke routers.

Example 5-3 Creating Pre-shared Key Authentication Credentials, IPv6

```
HQ-Router(config)# crypto isakmp key TESTKEY address ipv6
2001:db8:bbbb:2::2/64
HQ-Router(config)# crypto isakmp key TESTKEY address ipv6
2001:db8:cccc:2::2/64
```

Notice in Example 5-3 that the IPv6 command has similar syntax to the IPv4 command, and both reference the public endpoint IP addresses of the devices that are authenticating.

Example 5-4 shows the IPv4 pre-shared key used by the spoke to authenticate to the hub router.

Example 5-4 Spoke Router Pre-shared Key in IPv4

```
Spoke1(config)# crypto isakmp key TESTKEY address 192.0.2.3
```

Similarly, with IPv6, the spoke would reference the public IPv6 address of the hub router. Example 5-5 shows the IPv6 pre-shared key used by the spoke to authenticate to the hub router.

Example 5-5 Spoke Router Pre-shared Key in IPv6

```
Spoke1(config)# crypto isakmp key TESTKEY address
2001:db8:aaaa:1::1/64
```

Creating a Profile

Next, you need to create a profile and transform set. Example 5-6 shows the implementation of a profile and transform set, which is the same for IPv4 and IPv6 and the same on both the hub and the spoke.

Example 5-6 Creating a Profile and a Transform Set for IPv4 or IPv6

```
HQ-Router(config)# crypto ipsec transform-set MYSET esp-aes
esp-sha-hmac
HQ-Router(cfg-crypto-trans)# mode tunnel
HQ-Router(cfg-crypto-trans)# crypto ipsec profile
MYIPSECPROFILE
HQ-Router(ipsec-profile)# set transform-set MYSET
```

Notice that these two commands are tied together by the crypto profile referencing the transform set. You will see later how the profile is used by the DMVPN configuration. As discussed in Chapter 3, the transform set is for IKE phase 2 negotiation of the encrypted tunnel. As with the crypto policy, some IOS versions now include a default transform set, as you can see with the command **show crypto ipsec profile** in Example 5-7. The key pieces of the transform set are the encryption method, the hash type, and whether Perfect Forward Security (PFS) is used. These must all match except for the security association lifetime. The two sides select the SA lifetime with the smallest size and use that for the tunnel.

In Example 5-7, the command **show crypto ipsec profile** validates your previous profile configuration steps.

Example 5-7 Output Crypto IPsec Profile

```
HQ-Router(config)# show crypto ipsec profile
IPSEC profile MYIPSECPROFILE
        Security association lifetime: 4608000 kilobytes/3600
seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Mixed-mode : Disabled
        Transform sets={
                MYSET:  { esp-aes esp-sha-hmac  } ,
        }
IPSEC profile default
        Security association lifetime: 4608000 kilobytes/3600
seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Mixed-mode : Disabled
        Transform sets={
                default:  { esp-aes esp-sha-hmac  } ,
        }
```

Creating a Transform Set

The transform set is a collection of individual IPsec parameters designed to implement the security policy on the traffic that is transmitted across the

tunnel. During ISAKMP IPsec security association negotiation, the two routers need to agree on the parameters; if the parameters are not the same, the tunnel setup fails. For example, if one side has transport mode set to AH and the other side only supports ESP, the negotiation will fail.

Example 5-8 shows how to verify the transform set configuration. It is important that both sides of the tunnel solution have a match.

Example 5-8 Verifying the IPsec Transform Set

```
HQ-Router(config)# show crypto ipsec transform-set
Transform set default: { esp-aes esp-sha-hmac  }
   will negotiate = { Transport,  },

Transform set MYSET: { esp-aes esp-sha-hmac  }
   will negotiate = { Tunnel,  },
```

In the default configuration, transport mode only protects the upper layer protocols with payload encapsulation mode, and tunnel mode specifies protects the entire IP datagram.

GRE Tunnel Configuration

A GRE tunnel is required for a DMVPN network. If you think about it, the tunnel interface allows the consolidation of numerous remote site point-to-point links into one interface. In some of the legacy Cisco site-to-site configurations, you would have one crypto map on the outside interface with multiple configuration sections for each remote site VPN link. That would cause the router configuration to be extensive and possibly complex to troubleshoot. With the GRE tunnel solution, you have one tunnel interface scaling to support hundreds of remote site locations. The tunnel interface is designated as a multipoint interface, resulting in an NBMA network. Typically, when you configure a GRE tunnel, the source and destination IP addresses are configured so that the tunnel can be established; however, with DMVPN, you do not need this because you use NHRP to solve endpoint address resolution.

Key Points: A GRE tunnel configuration on the hub consists of a single step,

which is creating a multipoint GRE tunnel.

Creating a Multipoint GRE Tunnel on the Hub

Example 5-9 shows how to build a basic DMVPN hub router tunnel configuration. The key to this configuration is the **tunnel** command, which sets the mode to **multipoint**. This tunnel configuration works for both IPv4 and IPv6.

Example 5-9 Creating a Multipoint GRE Tunnel on a Hub Router for IPv4 or IPv6

```
HQ-Router(config)# interface tunnel0
HQ-Router(config-if)# ip address 192.168.1.1 255.255.255.0
HQ-Router(config-if)# ipv6 address 2001:db8:aaaa:1::1/64
HQ-Router(config-if)# tunnel source GigabitEthernet1
HQ-Router(config-if)# tunnel mode gre multipoint
HQ-Router(config-if)# tunnel key 12345
```

Notice that Example 5-9 has both an IPv4 address and an IPv6 address on the tunnel interface. That means you can configure it for either solution, and you can select the one you need for your environment. The tunnel source is the outside interface (that is, the interface of the router in this example).

The command **tunnel mode gre multipoint** in Example 5-9 makes the GRE tunnel a multipoint GRE (mGRE) tunnel, which allows multiple remote sites to be grouped into a single multipoint interface. The **tunnel key** command provides a weak form of security, but it could help prevent misconfiguration of a remote site from impacting a large-scale DMVPN environment.

Creating a GRE Tunnel on the Spoke

Unlike the hub, in DMVPN Phase 1 the spoke uses a point-to-point tunnel. To put another way, the command **tunnel mode gre multipoint** is replaced with the command **tunnel destination** *ip_address*, where *ip_address* is the public IP address of the hub router, as shown in Example 5-10.

Example 5-10 Configuring a Spoke Router for IPv4

```
Spoke1(config)# interface tunnel0
Spoke1(config-if)# ip address 192.168.1.2 255.255.255.0
Spoke1(config-if)# tunnel source GigabitEthernet0
Spoke1(config-if)# tunnel destination 192.0.2.3
Spoke1(config-if)# tunnel key 12345
```

With IPv6, there is a very important command that is often overlooked by VPN administrators. That command is to add **ipv6** to the **tunnel mode** command, as shown in Example 5-11. It is possible to use the **tunnel mode** command without the **ipv6** keyword, but without this keyword, your IPv6 configuration will not work. The other commands are similar to the IPv4 commands.

Note

We cannot stress enough the importance of using the **ipv6** keyword with the **tunnel mode** command for IPv6 because it is critical.

Example 5-11 shows the IPv6 configuration of a spoke router tunnel interface.

Example 5-11 Configuring a Spoke Router for IPv6

```
Spoke1(config)# interface tunnel0
Spoke1(config-if)# ipv6 address 2001:db8:beef:4::2/64
Spoke1(config-if)# tunnel source GigabitEthernet0
Spoke1(config-if)# tunnel destination 2001:db8:aaaa:1::1
Spoke1(config-if)# tunnel key 12345
```

The tunnel configuration for the spoke router references the outside interface with the **tunnel source** command. Next, the tunnel is set to GRE mode so it will support both unicast and multicast traffic. It will be important that the tunnel supports the use of multicast communication mechanisms later, when you want to run routing protocols such as OSPF. As mentioned earlier, the **tunnel key** command provides a weak form of security, preventing misconfiguration of a spoke router from impacting a production DMVPN network.

NHRP Hub-and-Spoke Configuration

The next part of the configuration is the NHRP hub-and-spoke configuration. Configuring NHRP for hub-and-spoke is a three-step process on the hub:

- Configure NHRP
- Configure the tunnel
- Configure tunnel optional parameters

Configure NHRP on the Hub

Let's start by setting up NHRP using IPv4. Example 5-12 shows the required commands for NHRP on a hub router tunnel interface with IPv4.

Example 5-12 Setting Up NHRP IPv4 Server Parameters on the mGRE Tunnel

```
HQ-Router(config)# interface tunnel0
HQ-Router(config-if)# ip nhrp authentication KEY123
HQ-Router(config-if)# ip nhrp map multicast dynamic
HQ-Router(config-if)# ip nhrp network-id 1
```

Example 5-13 shows the required commands for NHRP on a hub router tunnel interface for IPv6. Notice that these two examples are almost the same; the only difference is the addition of **ipv6** at the start of the commands in Example 5-13.

Example 5-13 Setting Up NHRP IPv6 Server Parameters on the mGRE Tunnel

```
HQ-Router(config)# interface tunnel0
HQ-Router(config-if)# ipv6 nhrp authentication KEY123
HQ-Router(config-if)# ipv6 nhrp map multicast dynamic
HQ-Router(config-if)# ipv6 nhrp network-id 1
```

The tunnel interface is set up as NBMA. You need a mechanism to allow the remote sites to communicate with the hub router. NHRP acts like dynamic DNS, as it allows remote sites to communicate and register with the DMVPN hub router. The command **map multicast dynamic** in Example 5-12 and Example 5-13 enables the DMVPN hub router to receive inbound registration requests from any spoke router IP address. Furthermore, the **dynamic** command enables the replication of multicast packets to each of the spoke routers through the single tunnel interface. Think of this in terms of the hub router referencing the NHRP database, and for each entry, it sends a unicast/multicast packet to that spoke IP address. It does this until each spoke has received the routing update. This way, the router is able to establish dynamic routing protocol adjacencies by utilizing the database to map the multicast endpoints.

Configure NHRP on the Spoke

The configuration of NHRP on the spoke router is different from the configuration on the hub router. Notice that there are a few more commands, and you must specify the IP address of the next hop server. In this case, you provide the tunnel IP address for the hub router. In addition, you add an NBMA address that can receive the broadcast or multicast packets you send out the tunnel interface. Finally, the key to mapping the NHRP tunnel address to the outside public address is to provide the mapping of the NHS tunnel IP address (192.168.1.1) to the NBMA IP address (192.0.2.3).

Example 5-14 shows a basic IPv4 NHRP configuration setup.

Example 5-14 Configuring NHRP on a Spoke Router for IPv4

```
Spoke1(config)# interface tunnel0
Spoke1(config-if)# ip nhrp authentication KEY123
Spoke1(config-if)# ip nhrp network-id 1
Spoke1(config-if)# ip nhrp nhs 192.168.1.1
Spoke1(config-if)# ip nhrp map multicast 192.0.2.3
Spoke1(config-if)# ip nhrp map 192.168.1.1 192.0.2.3
```

The IPv6 configuration of NHRP on the spoke is different from the configuration on the hub router, just as it is for IPv4. You use a few more commands and must specify the IP address of the NHS. In this case, you provide the tunnel IP address for the hub router (2001:db8:beef:1::1). In addition, you add an NBMA address that can receive the broadcast or multicast packets you send out the tunnel interface. Finally, it is critical to provide the mapping of the NHS tunnel IP address (192.168.1.1) to the NBMA IP address (192.0.2.3).

Example 5-15 shows a basic IPv6 NHRP configuration setup.

Example 5-15 Configuring NHRP on a Spoke Router for IPv6

```
Spoke1(config)# interface tunnel0
Spoke1(config-if)# ipv6 nhrp authentication KEY123
Spoke1(config-if)# ipv6 nhrp network-id 1
Spoke1(config-if)# ipv6 nhrp nhs 2001:db8:beef:1::1
Spoke1(config-if)# ipv6 nhrp map multicast 2001:db8:aaaa:1::1
Spoke1(config-if)# ipv6 nhrp map 2001:db8:beef:1::1/64
2001:db8:aaaa:1::1
```

Configure Tunnel Protection

Now we need to configure the tunnel interface. Example 5-16 shows the configuration required to encrypt the traffic passing through the tunnel. This same configuration should be applied to both the hubs and spokes

Example 5-16 Configuring the Tunnel Interface with IPsec Profile Protection

```
HQ-Router(config)# interface tunnel0
HQ-Router(config-if)# tunnel protection ipsec profile
MYIPSECPROFILE
```

The **tunnel protection ipsec profile** command applies the IPsec profile created previously to the tunnel interface. No crypto map is required. All traffic that passes through the tunnel will be encrypted with IPsec, and traffic outside the tunnel will not be encrypted. The use of tunnel protection and an IPsec profile significantly simplifies of the IPsec configuration when compared to crypto maps.

Configure Tunnel Optional Parameters

Next, we need to address issues such as MTU size and the maximum segment size that is negotiated during the TCP synchronization handshake. For any TCP packet going through the tunnel, the router will adjust the maximum segment size (MSS) in the TCP header to match the value you have set it to. This will force the end hosts to also adjust their setting to this value. The **mtu** and **adjust-mss** commands help resolve issues with most TCP-based applications that need to traverse the DMVPN tunnel.

Example 5-17 shows additional commands to prevent applications from failing to function across the DMVPN tunnel.

Example 5-17 Configuring the mGRE Interface with Optional IP Parameters

```
HQ-Router(config)# interface tunnel0
HQ-Router(config-if)# ip mtu 1400
HQ-Router(config-if)# ip tcp adjust-mss 1360
```

IPv6 has a different header than with IPv4. You still have to be concerned about the MTU size, but with IPv6, the fragmentation and reassembly process is improved; thus, most hops can handle average IP datagrams along the path without needing to fragment packets.

IPv6 has built-in solutions to address fragmentation, and Example 5-18 shows that you only need to adjust the MTU size.

Example 5-18 Sample IPv6 Configuration of the mGRE Interface

```
HQ-Router(config)# interface tunnel0
HQ-Router(config-if)# ipv6 mtu 1400
```

Routing Protocol Configuration

Routing protocol configuration is the final part in setting up a DMVPN solution. During the design phase, you needed to determine which routing protocol you would select. There are a few options, such as EIGRP or OSPF.

This section walks you through an example of configuring EIGRP. (For other configuration examples, such as OSPF, please refer to the documentation links included at the end of this chapter.)

Configure Routing on the Hub

With DMVPN, the NHRP database enables the hub router to replicate the individual multicast packets needed by the routing protocol to each site, one-by-one. In DMVPN, the routing protocol neighbor relationship is only established between the hub and the spoke routers. Thus, the hub is responsible for distributing routes learned from one spoke back out to another spoke. Thus you run into an issue where a feature in the link state routing protocols, split horizon, works against you. With split horizon, any network learned on an EIGRP interface is not advertised back out the same interface. With DMVPN, you must disable this so that routes propagate successfully to all of the spoke routers.

Example 5-19 shows how to configure EIGRP for IPv4. Notice the commands **no auto-summary** and **no ip split-horizon eigrp 1**.

Example 5-19 IPv4 Hub Router Configuration

```
HQ-Router(config)# router eigrp 1
HQ-Router(config-router)# no auto-summary
HQ-Router(config-router)# network 10.1.1.0 0.0.0.255
HQ-Router(config-router)# network 192.168.1.0 0.0.0.255

HQ-Router(config-router)# interface tunnel 0
HQ-Router(config-router)# no ip split-horizon eigrp 1
```

Notice that Example 5-19 includes a command under the tunnel interface that disables split horizon. In addition, you disable route summarization on the hub so that the hub router will send complete spoke route information out to each spoke rather than summarizing it.

Configure Routing on the Spoke Using IPV4

Example 5-20 shows the IPv4 spoke router configuration for EIGRP.

Example 5-20 IPv4 Spoke Router Configuration

```
Spoke1(config)# router eigrp 1
Spoke1(config-router)# no auto-summary
Spoke1(config-router)# network 10.2.2.0 0.0.0.255
Spoke1(config-router)# network 192.168.1.0 0.0.0.255
```

The spoke routers have a simple EIGRP configuration that identifies the GRE tunnel IP network and the inside network that you need propagated to the hub routing table.

Example 5-21 shows the IPv6 configuration of EIGRP on the hub router.

Example 5-21 IPv6 Hub Router Configuration

```
HQ-Router(config)# ipv6 unicast routing
HQ-Router(config)# ipv6 cef
HQ-Router(config)# ipv6 router eigrp 1
HQ-Router(config-rtr)# eigrp router-id 192.0.2.3
HQ-Router(config-rtr)# Interface tunnel 1
HQ-Router(config-if)# ipv6 eigrp 1
```

Configure Routing on the Spoke Using IPV6

For the IPv6 configuration, we show you an example of enabling IPv6 unicast routing on the router and then configuring the IPv6 router with an EIGRP router ID. It is a good practice to control the router ID; in this case, you are using the outside IPv4 address of the HQ router, which is 192.0.2.3. (Yes, in an IPv6 configuration, you can use an IPv4 address as an identifier.)

Next, on the interface tunnel, you enable EIGRP routing by specifying IPv6 EIGRP with the autonomous system number you set up, which in this case is 1.

Example 5-22 shows the IPv6 EIGRP configuration on the spoke router.

Example 5-22 IPv6 Spoke Router Configuration

```
Spoke1(config)# ipv6 unicast routing
```

```
Spoke1(config)# ipv6 cef
Spoke1(config)# ipv6 router eigrp 1
Spoke1(config-rtr)# eigrp router-id 2.2.2.2
Spoke1(config-rtr)# Interface tunnel 1
HQ-Router(config-if)# ipv6 eigrp 1
```

For the IPv6 configuration, you configure the spoke with IPv6 unicast routing and then configure the IPv6 router with the EIGRP router ID 2.2.2.2. Again, in this case, you do this simply to identify the router when looking at the EIGRP neighbors.

That wraps up our DMVPN hub-and-spoke configuration walkthrough. Next, let's look at a DMVPN spoke-to-spoke configuration.

DMVPN Phase 2 Spoke-to-Spoke Implementation

To enable spoke-to-spoke communication, you need to focus on two configuration changes versus what we worked through when deploying a hub-and-spoke DMVPN deployment. First, you need to make sure that the two routers can communicate via IPsec. This means that any spoke that needs to talk to another spoke needs to include an additional **crypto isakmp key** statement. You also need to enabled routing to use the correct next hop IP address. Let's first look at the IPsec configuration.

IPsec for Spoke-to-Spoke

Example 5-23 shows the addition of extra IPv4 ISAKMP keys on Spoke1. You need to add these keys on both spokes so that they can encrypt and decrypt the traffic when they communicate directly with one another. After adding the second crypto map statement to the Spoke1 router, you need to also add it to the Spoke2 router.

Example 5-23 IPv4 Additional Spoke Crypto Keys

```
Spoke1(config)# crypto isakmp key TESTKEY address 209.0.2.3
Spoke1(config)# crypto isakmp key TESTKEY address
209.165.202.130
```

In IPv6, you do a similar configuration. Example 5-24 shows the addition of extra IPv6 ISAKMP keys on Spoke1.

Example 5-24 IPv6 Additional Spoke Crypto Keys

```
Spoke1(config)# crypto isakmp key TESTKEY address
2001:db8:aaaa:1::1/64
Spoke1(config)# crypto isakmp key TESTKEY address
2001:db8:cccc:2::2/64
```

Spoke-to-Spoke Routing

In spoke-to-spoke routing configuration, spokes do not directly exchange routing information with each other, even though they may be on the same logical subnet (that is tunnel IP address range) with each other. You need to enable a few commands to ensure that routing functions correctly and spokes use the correct next hop IP address.

Example 5-25 expands the EIGRP configuration for spoke-to-spoke communications by resolving the issue of the hub router setting the next hop address to its own IPv4 address.

Example 5-25 IPv4 Additional EIGRP Configuration

```
HQ-Router(config)# router eigrp 1
HQ-Router(config-router)# no auto-summary
HQ-Router(config-router)# network 10.1.1.0 0.0.0.255
HQ-Router(config-router)# network 192.168.1.0 0.0.0.255

HQ-Router(config-router)# interface tunnel 0
HQ-Router(config-router)# no ip split-horizon eigrp 1
HQ-Router(config-router)# no ip next-hop-self eigrp
```

Notice the addition of the command **no ip next-hop-self eigrp**. This command tells the hub router that, when it redistributes the subnets received from one spoke back out to other spokes, it should not replace its own next hop address but should leave the original address provided by the spoke.

IPv6 Spoke-to-Spoke Routing Configuration

The IPv6 spoke-to-spoke routing configuration is not very complex in terms of DMVPN Phase 3 support. You only need to add a command to disable the split horizon associated with EIGRP. Example 5-26 also includes the **ipv6 summary** command to expose some options for simplifying routing tables.

As you can see in Example 5-26, with IPv6 you address the split horizon issue but do not have to address the next-hop-self challenge that occurs in IPv4.

Example 5-26 IPv6 Additional EIGRP Configuration

```
HQ-Router(config)# interface tunnel 1
HQ-Router(config-if)# no ipv6 split-horizon eigrp 1
HQ-Router(config-if)# ipv6 summary-address eigrp 1
2001:db8:AAAA::/48
```

DMVPN Phase 3 Spoke-to-Spoke Implementation

As mentioned earlier in this chapter, DMVPN phase 2 suffers from scale limitations that are addressed in DMVPN phase 3. To transition from DMVPN Phase 2 to DMVPN Phase 3, we will make two simple changes on the hub and spoke routers.

Enable NHRP Redirects on the Hub

On the hub router, enable NHRP redirects with the command **ip nhrp redirect**. The **redirect** command enables the hub to issue redirects, informing the spoke of a better path if such a path exists. Example 5-27 shows an example of doing this on the hub router.

Example 5-27 Enabling NHRP Redirects on the Hub Router

```
HQ-Router(config)# interface tunnel 1
HQ-Router(config-if)# ip nhrp redirect
```

Enable NHRP Shortcuts on the Spoke

On the spoke router, enable NHRP shortcuts with the command **ip nhrp shortcut**. The **shortcut** command enables the spoke to accept redirect messages issues by the hub. Example 5-28 shows an example of doing this on a spoke router.

Example 5-28 Enabling NHRP Shortcuts on the Spoke Router

```
HQ-Router(config)# interface tunnel 1
HQ-Router(config-if)# ip nhrp shortcut
```

DMVPN Troubleshooting

This final section of the chapter discusses troubleshooting DMVPN in terms of the same four steps used to configure DMVPN earlier in this chapter. You are expected to not only be able to build DMVPNs but also identify why a DMVPN is not working, which is why we stress how important it is for you to understand troubleshooting. We concluded Chapter 4 with steps to validate whether the VPN deployment is running, but in this chapter we skip validation and move right into troubleshooting because there are many overlapping steps with validation and troubleshooting. Know that the process used in this section is similar to validating or troubleshooting other site-to-site VPN deployments.

You can break troubleshooting into four parts that mirror the four configuration parts covered earlier in this chapter:

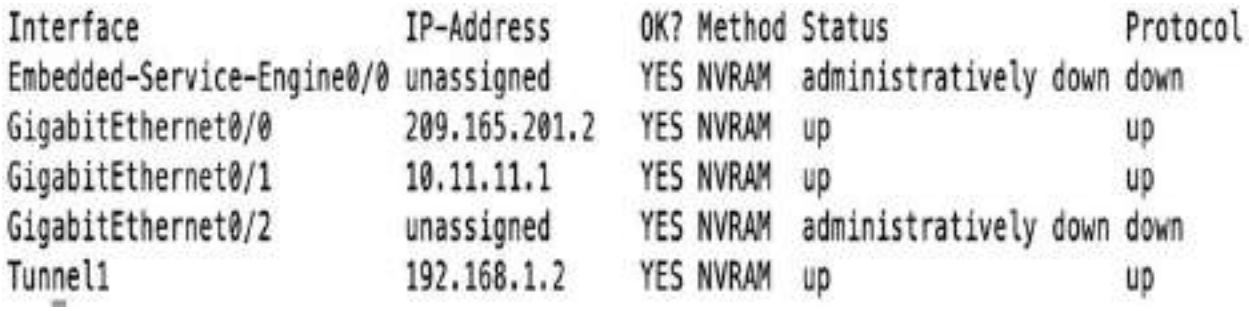
- Troubleshooting the crypto IPsec policy configuration
- Troubleshooting the GRE tunnel configuration
- Troubleshooting the NHRP hub-and-spoke configuration
- Troubleshoot the routing configuration

Note

An interesting thing about configuring DMVPN is that you must have at least three of the steps done on the hub and spoke routers before you start troubleshooting your configuration. So, for example, if you configure just the crypto policy on both the hub and spoke, you do not see either side attempt to establish the VPN tunnel.

Troubleshooting the Crypto IPsec Policy Configuration

There are some key commands you can use to determine whether the crypto configuration is functioning correctly. To see whether IKE phase 1 or IKE phase 2 of the ISAKMP process is working, you issue the command **show crypto isakmp sa** on the hub router as shown in Figure 5-12. This command determines whether IKE phase 1 of the IPsec tunnel is up.



Interface	IP-Address	OK?	Method	Status	Protocol
Embedded-Service-Engine0/0	unassigned	YES	NVRAM	administratively down	down
GigabitEthernet0/0	209.165.201.2	YES	NVRAM	up	up
GigabitEthernet0/1	10.11.11.1	YES	NVRAM	up	up
GigabitEthernet0/2	unassigned	YES	NVRAM	administratively down	down
Tunnel1	192.168.1.2	YES	NVRAM	up	up

Figure 5-12 Output of the Command **show crypto isakmp sa**

The output **QM_IDLE** indicates that the tunnel has completed quick mode, and the policy between the two devices has been accepted. This indicates that there is a match. If you see **MM_Active**, IKE phase 1 failed, and you must validate your ISAKMP policy on both sides of the link.

Troubleshooting IKE Phase 2

To troubleshoot IKE phase 2, use these two commands:

- **show crypto ipsec sa**
- **show crypto session detail**

Figure 5-13 demonstrates the use of the first command, **show crypto ipsec sa**, to learn some important information, such as the crypto endpoints of both sides of the tunnel configuration. Data encapsulating (**encaps**) but not returning (**decaps**) indicates that you have a one-way tunnel, which typically means an ACL or NAT on either side of the tunnel is misconfigured.

```
R2#sh ip nhrp nhs detail
Legend: E=Expecting replies, R=Responding, W=Waiting
Tunnel1:
192.168.1.1  RE priority = 0 cluster = 0  req-sent 281  req-failed 1  repl-recv 206 (00:03:05 ago)
```

Figure 5-13 Output of the Command **show crypto ipsec sa**

With each of the commands shown in Figure 5-12 and Figure 5-13, if you add the word **detail** at the end, the output shows more detailed counters. (For more troubleshooting commands and techniques, see the IPsec troubleshooting documentation listed at the end of the chapter.)

Troubleshooting the GRE Tunnel Configuration

The configuration of a tunnel in a DMVPN solution is somewhat different from the configuration of a tunnel used to repair a discontinuous OSPF area. In DMVPN tunnel configuration, you only have a tunnel source and not a tunnel destination. This is because the tunnel is configured to support NHRP configuration. The hub is dynamic, so it is waiting for inbound registrations and does not need a tunnel destination. The spokes have the destination of the tunnel endpoint mapped to the public IP address in the **nhrp** command in

Example 5-12 for IPv4 and Example 5-13 for IPv6.

Validating the Tunnel

You must validate that the tunnel state is up/up, and after you apply the **tunnel source** command and enable the tunnel interface. You need to make sure you have selected the correct tunnel source interface. In Example 5-11, it is the outside IP address. (This is a common mistake in configuring tunnel interfaces.) In addition, you need to make sure you have the tunnel configured as an mGRE tunnel, especially on the hub side. If you're using a tunnel key, both sides need to be the same.

Figure 5-14 shows the command **show ip interface brief** executed on the Spoke1 router. This validates that the Tunnel1 interface is in the up/up state.

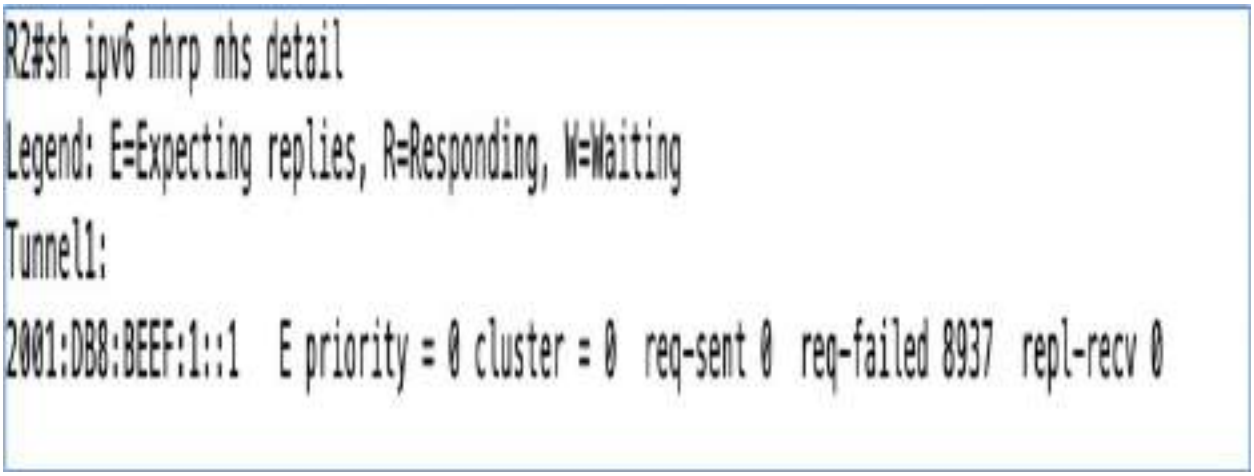


Figure 5-14 Output of the Command **show ip interface brief** on an IPv4 Interface

Troubleshooting the NHRP Hub-and-Spoke Configuration

NHRP troubleshooting starts with issuing two basic commands on the spoke router. First, you need to determine if the VPN tunnel is up and functioning correctly. If it isn't, you need to determine whether IKE phase 1 or IKE phase 2 is failing. If the tunnel is up when you issue **show crypto isakmp sa**, you

should see **QM_IDLE**. If you see only encapsulations and not decapsulations, you know you have either a crypto ISAKMP Phase 2 problem or an NHRP registration issue.

NHRP Registration

You must determine whether the NHRP spoke is registering. The command **show ip nhrp nhs detail**, shown in Figure 5-15, tells you whether you have both sent and received packets from the NHRP NHS. If you see that the request has been sent (**req-sent**) but no replies have been received (**repl-recv**) and the request failed (**req-failed**) count is increasing, then you know you have an NHRP spoke that is unable to register with the NHS.

```
Jan 20 18:21:56.326: NHRP: Receive Registration Request via Tunnel1 vrf 0,
packet size: 104
Jan 20 18:21:56.326:  (F) afn: AF_IP(1), type: IP(800), hop: 255, ver: 1
Jan 20 18:21:56.326:      shtl: 4(NSAP), sstl: 0(NSAP)
Jan 20 18:21:56.326:      pktsz: 104 extoff: 52
Jan 20 18:21:56.326:  (M) flags: "unique nat ", reqid: 65583
Jan 20 18:21:56.326:      src NBMA: 209.165.201.2
Jan 20 18:21:56.326:      src protocol: 192.168.1.2, dst protocol:
192.168.1.1
Jan 20 18:21:56.326:  (C-1) code: no error(0)
Jan 20 18:21:56.326:        prefix: 32, mtu: 17870, hd_time: 7200
Jan 20 18:21:56.326:        addr_len: 0(NSAP), subaddr_len: 0(NSAP),
proto_len: 0, pref: 0
```

Figure 5-15 Output of the Command **show ip nhrp nhs detail**

Tunnel Configuration

It is important to validate that the configuration of the tunnel interface is

correct. Take a look at Figure 5-15, and make sure you have the correct information on the NHS, which in this example is the IP address of the tunnel interface of the hub router. This is the first area that might be misconfigured. Check your documentation and make sure this address is correct. Then verify that the command **ip nhrp map** references the tunnel address first, followed by the outside IP address (NBMA) of the hub router.

Figure 5-16 shows the command **show ipv6 nhrp nhs detail** executed on the Spoke1 router. The output provides information on the IPv6 address of the tunnel interface for the NHRP server. It validates that the NHRP configuration information on the spoke is valid.

Figure 5-16 Output of the Command **show ipv6 nhrp nhs detail**

Debugging

If you determine that so far everything is correct, you can turn on debugging for NHRP packets on the hub router to see if they are being received by the NHS and why the NHS cannot respond. You can force a registration attempt by shutting down the tunnel interface on the spoke router and then reenabling it. If you have debugging enabled on the hub router, you should see an inbound registration request.

Figure 5-17 shows the command **debug nhrp packet** executed on the NHRP server router. This also validates that the spoke router is attempting to register with the NHRP server. If you do not see inbound registration requests, then

there is probably a misconfiguration of the NHRP server parameters on the spoke router.

Figure 5-17 Output of the Command **debug nhrp packet**

In the debug screen shown in Figure 5-17, you can see that the inbound registration request comes via the tunnel interface and includes the source NBMA IP address (the outside address) and the source protocol IP address (the tunnel address). In addition, it includes the destination protocol addresses. Each of these fields provides a good indication about whether the configuration on the host side is aligned with the hub router configuration.

Troubleshoot the Routing Configuration

Troubleshooting the routing protocol part of the DMVPN tunnel is not very complex. The challenge is whether you are able to see routes of other remote sites in the routing table. The first command to issue is **show ip protocol**. This command shows what IP blocks are being advertised. You should compare the spoke side to what the hub side is seeing in the routing table. If you execute **show ip route** and do not see the route in the table, then you should verify both the EIGRP autonomous system number and whether you have any security on the route exchanges. In addition, you should check to see if the hub router is summarizing the routes into a larger block. Finally, you should check to see what EIGRP neighbors the hub router identifies.

DMVPN Troubleshooting Summary

Table 5-3 consolidates some of the key commands covered so far, as well as a few more that are valuable for troubleshooting. The commands are organized in this table in the same parts as the DMVPN implementation shown in this chapter. Even if you configure your solution correctly the first time, it is good to use these commands to understand what the Cisco routers are doing in each of the phases.

Table 5-3 DMVPN Troubleshooting Commands

Troubleshooting Part	Commands
Crypto configuration (ISAKMP/IPSEC)	
Tunnel configuration	
NHRP configuration	
Routing configuration	

Troubleshooting Part	Commands
Crypto configuration (ISAKMP/IPSEC)	**show crypto isakmp sa** **show crypto ipsec sa** **debug crypto isakmp** **debug crypto ipsec**
Tunnel configuration	**show IP tunnel0 interface** **show IPv6 tunnel0**
NHRP configuration	**show ip nhrp nhs detail** **show ipv6 nhrp nhs detail** **debug nhrp**
Routing configuration	**show IP protocol** **show IP route** **debug routing protocol**

Troubleshooting Part	Commands
Crypto configuration (ISAKMP/IPSEC)	**show crypto isakmp sa** **show crypto ipsec sa** **debug crypto isakmp** **debug crypto ipsec**
Tunnel configuration	**show IP tunnel0 interface** **show IPv6 tunnel0**
NHRP configuration	**show ip nhrp nhs detail** **show ipv6 nhrp nhs detail** **debug nhrp**
Routing configuration	**show IP protocol** **show IP route** **debug routing protocol**

That wraps up troubleshooting DMVPN troubleshooting fundamentals. Keep in mind troubleshooting makes up a major part of the SVPN exam.

Summary

This chapter introduced DMVPN technology and its features. It also described the components needed for DMVPN and looked at two of the key components, mGRE and NHRP. We covered the features, benefits, and limitations of mGRE and NHRP, especially related to routing and security. We discussed both IPv4 and IPv6 DMVPN configuration because both are deployed and could be found within the SVPN exam. Finally, this chapter covered some potential pitfalls and challenges related to deploying a DMVPN solution.

At this point, you should have a strong foundation for planning, configuring and managing GETVPN as well as DMVPN deployments. Next up is a deep dive into FlexVPN, wrapping up our focus on site-to-site VPN concepts.

References

Brandom, Russel (May 12, 2017). UK Hospitals Hit with a Massive Ransomware Attack. Retrieved from https://www.theverge.com/2017/5/12/15630354/nhs-hospitals-ransomware-hack-wannacry-bitcoin

Dynamic Multipoint VPN Configuration Guide, Cisco IOS Release 15M&T. Retrieved from https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dmvpn/configuration/15-mt/sec-conn-dmvpn-15-mt-book/sec-conn-dmvpn-tun-mon.html#GUID-E968E183-0022-4E8C-89A6-69AE3AE2AFF9

Dynamic Multipoint VPN Configuration Guide, Cisco IOS Release 15S. Retrieved from https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dmvpn/configuration/15-s/sec-conn-dmvpn-15-s-book/ip6-dmvpn.html#GUID-AE87E1CC-DF83-426D-885C-2E00CF365833

GRE Tunnel Interface States and What Impacts Them, Retrieved from https://www.cisco.com/c/en/us/support/docs/ip/generic-routing-encapsulation-gre/118361-technote-gre-00.html

IP Addressing: NHRP Configuration Guide. Retrieved from https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nhrp/configuration/xe-3s/nhrp-xe-3s-book/config-nhrp.html

IPsec Troubleshooting: Understanding and using debug Commands. Retrieved from https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/5409-ipsec-debug-00.html

Scalable DMVPN Design and Implementation Guide. Retrieved from https://www.cisco.com/c/dam/en/us/products/collateral/security/dynamic-multipoint-vpn-dmvpn/dmvpn_design_guide.pdf?dtid=osscdc000283

Transform Set Configuration. Retrieved from https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21/IPSec/21_IPSec-Reference/b_21_IPSec_chapter_0100.pdf

Kingsbury, Josh, DMVPN – Concepts & Configuration. Retrieved from https://learningnetwork.cisco.com/s/article/dmvpn-concepts-amp-configuration

Coran, Matt, Design Guide | DMVPN Phases. Retrieved from https://network-insight.net/2015/02/design-guide-dmvpn-phases/

Exam Preparation Tasks

As mentioned in the section "How to Use This Book" in the Introduction, you have a couple of choices for exam preparation: the exercises here, Chapter 11, "Final Preparation," and the exam simulation questions in the Pearson Test Prep software online.

Review All Key Topics

Review the most important topics in the chapter, noted with the key topics icon in the outer margin of the page. Table 5-4 lists these key topics and the page number on which each is found.

Table 5-4 Key Topics for Chapter 5

Key Topic Element	Description	Page Number
Figure 5-4	A Full-Mesh DMVPN Tunnel	
Figure 5-5	GRE Tunnels	
List	GRE Limitations	
Figure 5-6	NHRP Registration Process	
Table 5-2	Basic DMVPN Configuration Components	
Figure 5-9	DMVPN Phase 2	
Figure 5-10	IPv4 DMVPN Solution	
Figure 5-11	DMVPN IPv6 Solution	
Example 5-12	Setting Up NHRP IPv4 Server Parameters on the mGRE Tunnel	
Example 5-14	Configuring NHRP on a Spoke Router for IPv4	
Table 5-3	DMVPN Troubleshooting Commands	

Complete Tables and Lists from Memory

Print a copy of Appendix C, "Memory Tables" (found on the companion website), 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 companion website), 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:

Next Hop Resolution Protocol (NHRP)
multipoint Generic Routing Encapsulation (mGRE)

Chapter 6. FlexVPN Configuration and Troubleshooting

This chapter covers the following subjects:

- **FlexVPN Overview:** This section provides an overview on how FlexVPN is different from previous VPN technologies and what benefits it provides.
- **FlexVPN Components:** This section examines the building blocks of FlexVPN and how they work together to create a comprehensive solution for a variety of architectures.
- **FlexVPN Design Considerations:** This section reviews key requirements and considerations when you design a FlexVPN solution.
- **FlexVPN Implementation: Hub-and-Spoke (IPv4/IPv6):** This section steps through the components of a FlexVPN hub-and-spoke (IPv4/IPv6) configuration. It demonstrates, with examples, how each of the FlexVPN building blocks in a three-router solution operates.
- **FlexVPN Troubleshooting:** This section discusses how to break down your troubleshooting of FlexVPN based on the configuration building blocks.

"Relying on the government to protect your privacy is like asking a peeping tom to install your blinds."

—John Perry Barlow

This chapter covers the following exam objectives:

- 1.0 Site-to-site Virtual Private Networks on Routers and Firewalls
  - 1.3 Describe uses of FlexVPN
- 2.0 Remote access VPNs
  - 2.4 Implement Flex VPN on routers

- 3.0 Troubleshooting using ASDM and CLI
  - 3.1 Troubleshoot IPsec
  - 3.3 Troubleshoot FlexVPN
- 4.0 Secure Communications Architectures
  - 4.1 Describe functional components of GETVPN, FlexVPN, DMVPN, and IPsec for site-to-site VPN solutions
  - 4.3 Recognize VPN technology based on configuration output for site-to-site VPN solutions
  - 4.6 Design site-to-site VPN solutions

Welcome to the last site-to-site VPN topic, which is a deep dive into FlexVPN as well as a look at troubleshooting site-to-site VPN technology. Cisco offers many VPN flavors, and each one requires different configurations, show commands, and debug commands. Of all the options available, FlexVPN is the Cisco option used to simplify VPN deployments and covers all VPN types, including support for site-to-site VPN, hub-and-spoke VPN, and remote access VPN deployments. The only caveat to this statement is that FlexVPN does not cover GETVPN.

FlexVPN is a common configuration template for all VPN types and is based on IKEv2. It is important to point out that FlexVPN does not support IKEv1. Many experts view this as a good thing, as IKEv2 is more secure based on its support of the latest Suite B cryptographic algorithms. As mentioned in Chapters 4 and 5, the Implementing Secure Solutions with Virtual Private Networks (SVPN) exam expects you to be able to identify FlexVPN code as well as plan, deploy, and troubleshoot FlexVPN using Cisco technology. This chapter will help you master these topics.

Learning beyond the SVPN concepts:

- FlexVPN Overview
- VPN Licensing

“Do I Know This Already?” Quiz

The “Do I Know This Already?” quiz enables you to assess whether you should read the entire chapter. If you miss no more than one of these self-assessment questions, you might want to move ahead to the “Exam Preparation Tasks” section of the chapter. Table 6-1 lists the major headings in this chapter and the “Do I Know This Already?” quiz questions related to the material in each of those sections to help you assess your knowledge of these specific areas. The answers to the “Do I Know This Already?” quiz appear in Appendix A, “Answers to the ‘Do I Know This Already?’ Quizzes.”

Table 6-1 “Do I Know This Already?” Foundation Topics Section-to-Question Mapping

Foundation Topics Section	Questions
FlexVPN Overview	1–3
FlexVPN Components	4–6
FlexVPN Design Considerations	13
FlexVPN Implementation: Hub-and-Spoke (IPv4/IPv6)	7–10
FlexVPN Troubleshooting	11, 12

1. What feature does FlexVPN include to speed the configuration process?

a. Predefined templates

b. Predefined defaults

c. Installation script

d. Installation template

2. What are some benefits of FlexVPN compared to legacy VPN solutions? (Choose two.)

a. Support for multiple VPN types

b. Backward compatibility

c. Installation script

d. Support on all platforms

3. What new IKEv2 enhancements does FlexVPN support? (Choose two.)

a. PSK

b. Suite B

c. PKI

d. EAP

4. Which of the following configurations are supplied for FlexVPN? (Choose two.)

a. IKEv2 profile

b. IPsec profile

c. IKEv2 policy

d. IPsec policy

5. What VPN capabilities does FlexVPN support that both DMVPN and crypto maps do not support? (Choose three.)

a. Configuration push

b. Per-peer configuration

c. Remote access

d. Full AAA management

e. Dynamic routing

6. Which FlexVPN hub command block enables IKEv2 parameters to download to the spokes?

a. IKEv2 proposal

b. IKEv2 policy

c. IKEv2 authorization

d. IKEv2 profile

7. Which IPsec configuration piece is optional in FlexVPN?

a. IPsec profile

b. IKEv2 profile

c. Tunnel protection IPsec profile

d. Transform set

8. Which command attaches the IKEv2 authorization policy and the AAA local authentication to the IKEv2 profile?

a. aaa authentication

b. keyring local

c. match identity

d. aaa authorization

9. With which of the following does a spoke have both a FlexVPN tunnel interface and a virtual template interface?

a. Hub-and-spoke communication

b. Spoke-to-spoke communication

c. Never

d. Virtual access interface

10. Which of the following need to be configured for spoke-to-spoke connectivity? (Choose two.)

a. Keyring modification

b. Additional tunnel interface

c. Routing configuration

d. NHRP configuration

11. What command on the hub router enables you to determine whether the IKEv2 process has completed?

a. show crypto ikev2 authorization policy

b. show crypto ikev2 profile

c. show crypto ikev2 sa

d. show ip interface brief

12. What command on the spoke router shows whether spoke-to-spoke resolution has completed?

a. show ip route nhrp

b. show crypto ikev2 sa

c. show ip nhrp redirect

d. show ip protocol

13. Which of the following is *not* true regarding FlexVPN design considerations?

a. You must identify routing requirements

b. You must pick an encryption scheme

c. You must determine whether the deployment is site-to-site and/or remote access–related

d. You need to make sure at least IKEv1 or IKEv2 is supported

Foundation Topics

When you think about FlexVPN, Cisco wants you to think “easy.” One

reason you should think FlexVPN is easy is the value of smart defaults. By using smart defaults, you can leverage predefined values based on industry best practices. Smart defaults can dramatically reduce the number of steps you must manually configure to stand up a VPN. FlexVPN is also very useful for customers looking to manage multiple VPN types. It can address the complexity of multiple solutions targeting remote access, teleworker, site-to-site, mobility, and managed security services, along with other use cases.

SVPN version 1.1 of the exam calls out requirements for understanding FlexVPN on Cisco routers, for remote access, site-to-site VPN for both routers and firewalls, and troubleshooting FlexVPN using both ASDM and command-line options. This is a lot of topics to cover, and this chapter focuses on the site-to-site VPN part of these requirements. Chapter 9, "AnyConnect IKEv2 FlexVPN," covers using FlexVPN for remote access.

Let's start off the FlexVPN conversation with a general overview of how the technology works.

FlexVPN Overview

Previous chapters explore the configuration of several types of VPN solutions. This chapter explores the fundamentals and configuration aspects of FlexVPN. Cisco's FlexVPN is an implementation of the next generation of *Internet Key Exchange (IKEv2)*. IKEv2 enhancements include mutual authentication and the establishment and maintenance of security associations (SAs).

FlexVPN was designed to take advantage of IKEv2, which is a next-generation key management protocol described in RFC 4306. Unlike IKEv1, IKEv2 performs mutual authentication and maintains SAs for both sides. The following are some key benefits of leveraging IKEv2 over IKEv1:

- It is more secure than IKEv1 because it supports the latest Suite B cryptographic algorithms.

- It includes built-in support for dead peer detection (DPD) and NAT Traversal.
- It combines IKEv1 main and aggressive modes into one method called *initial*.
- It supports native routing.
- Besides certificates and PSKs, it supports EAP authentication.
- XAUTH is replaced by EAP tunneling.

Some organizations might want to phase in FlexVPN rather than make a large-scale change. The support for legacy solutions permits a FlexVPN device to support IKEv1 remote sites while an organization is transitioning. However, FlexVPN is not backward compatible, meaning FlexVPN does not support legacy technology that can only leverage IKEv1. In addition, FlexVPN supports both IPv4 and IPv6 for transport and overlay. This means that organizations can use FlexVPN to transition to IPv6 while running IPv4 as the transport protocol or implement a dual stack solution.

A powerful feature included in FlexVPN is the use of a default configuration also known as smart defaults. This helps an engineer get a solution up and running quickly by providing some of the built-in defaults. For example, an engineer can use the default IKEv2 proposal rather than provide all of the configuration information for Diffie–Hellman key exchange, encryption, integrity, and *pseudorandom functions (PRFs)*.

FlexVPN Advantages

FlexVPN has a wide range of support making it a popular option for VPN administrators. Figure 6-1 demonstrates the potential solutions that FlexVPN offers. As you can see, FlexVPN supports AnyConnect clients as well as hub-and-spoke and spoke-to-spoke solutions.

Figure 6-1 FlexVPN Hub-and-Spoke Solution with Remote Access

Modular Framework

FlexVPN architecture offers a modular and relatively simple approach to VPN configuration. For example, the FlexVPN modular framework in Figure 6-1 enables this solution to support hub-and-spoke topologies similar to DMVPN as well as remote access VPN clients.

Note

IKEv2 is not supported on Cisco Integrated Service Router (ISR) Generation 1 (G1).

Configuring Service Parameters

Another key advantage of FlexVPN is the ability to implement per-peer configuration of service parameters such as firewall services, quality of service (QoS) features, and other policies. Therefore, the hub router in a hub-and-spoke solution could implement a QoS policy for a remote site to improve VoIP communication; with another site that is a partner company, the configuration could include a firewall policy. FlexVPN offers improved the integration with external authentication, authorization, and accounting (AAA) databases for multi-tenancy scenarios.

EasyVPN Benefits Summarized

An easy way to view the benefits of EasyVPN is using a summary table. Table 6-2 covers the key benefits of IKEv2.

EXAM NOTE

Be sure to study these benefits for the SVPN 300-730 exam.

Table 6-2 Benefits of IKEv2

Troubleshooting FlexVPN Building Block	Commands
Step 1: IKEv2 proposal and IKEv2 policy troubleshooting	**show crypto ikev2 sa** **show crypto ikev2 proposal** **show crypto ikev2 policy** **debug crypto ikev2 error**
Step 2: IKEv2 authorization policy troubleshooting	**show crypto ikev2 authorization policy** **debug crypto ikev2 error** **debug aaa authorization** **debug aaa protocol local**
Step 3: Keyring and IKEv2 profile troubleshooting	**show crypto ikev2 profile** **debug crypto ikev2 error**
Step 4: IPsec profile troubleshooting	**show crypto ipsec profile** **show crypto ipsec sa**
NHRP troubleshooting	**show ip nhrp detail** **show interface virtual-access 1** **debug nhrp packet**
Routing troubleshooting	**show ip protocol** **show ip route**

Benefit	Description
Dead Peer Detection (DPD) and NAT traversal	DPD and NAT traversal are built in.
Certificate URL	Certificates are referenced through a URL and a hash.
Extensible Authentication Protocol (EAP) support	EAP is supported for authentication.
Asynchronous authentication capabilities	IKEv2 supports a certificate one way and EAP or a pre-shared key the other way.
Multiple crypto engines	One engine can support both IPv4 and IPv6 traffic, or separate engines can be used for each protocol.
Reliability and state management	IKEv2 uses sequence numbers and acknowledgements for reliability and error management.

FlexVPN Versus Other Options

On the SVPN exam, you will find questions that ask you to choose the best VPN option for a specific situation. You could also be provided a small snippet of code and asked to identify which VPN option is being used. To help with these questions, we have created a summary table in Table 6-3 that compares crypto maps, DMVPN, and FlexVPN. Remember, FlexVPN does not support GETVPN, which is why it is not included in this table.

Table 6-3 FlexVPN Capabilities

Capability	Crypto Map	DMVPN	FlexVPN
Remote access	Yes	No	Yes
Configuration push	No	No	Yes
Per-peer configuration	No	No	Yes
Dynamic routing	No	Yes	Yes
Spoke-to-spoke direct	No	Yes	Yes
Per-peer QoS	No	Group	Yes
Full AAA management	No	No	Yes

Figure 6-2 provides a graphical representation of the capabilities of FlexVPN. Notice in this figure that FlexVPN can support both the legacy VPN solutions, remote access clients (Windows and AnyConnect), and site-to-site VPNs on the same device. This is one of the most powerful features of FlexVPN.

Figure 6-2 FlexVPN Capabilities

Benefits of IKEv2

As shown in Table 6-4, IKEv2 provides a number of security enhancements. The major improvements with IKEv2 are National Security Agency (NSA) Suite B and anti-denial of service (anti-DoS) capabilities. Proper implementation of IKEv2 features results in secure key exchange between sites and/or clients.

Table 6-4 IKEv2 Security Enhancements

Enhancement	IKEv2 Solution
Protocol objective	Authentication, integrity, privacy
ISAKMP (RFC 2408) IKE (RFC 2796)	Suite B cryptography (new) Anti-DoS (improved)
Dead Peer Detection (DPD)	Enhancement
Authentication (bidirectional)	AuthC-PSK, RSA-Sig, EAP, hybrid authentication (RFC 2407), DOI (new)
NAT Transversal (NAT-T)	Improved

IKEv2 offers some significant advantages over its predecessor IKEv1. Like IKEv1, IKEv2 negotiates a security association between a pair of communicating peers; however, it is based on the third-generation specifications (RFC 4301 to 4309) and addresses security issues and protocol inefficiencies such as resistance to denial-of-service (DoS) attacks and support for more authentication methods.

FlexVPN Requirements

Cisco FlexVPN relies on IKEv2 and a tunnel interface model. This architecture enables both backward legacy VPN support (that is, crypto

maps) and multi-tenancy support (site-to-site, remote-access, hub-and-spoke, and spoke-to-spoke) in a single hub site. In addition, Figure 6-3 shows that in a hub-and-spoke solution, the hub is able to manage parameters such as firewall features, attributes such as quality of service (QoS), policies, and VRF-related settings. Notice that the graphic shows that the hub router (HQ) is pushing route injection information. You will see configurations related to this later in this chapter.

Note

To be clear about FlexVPN support, backward legacy VPN support is not for VPN options that only support IKEv1. FlexVPN does not support technology that only uses IKEv1.

Figure 6-3 FlexVPN Per-Peer Options

FlexVPN Components

Within the Internet Key Exchange (IKE) version 2 standard are a few key components that are important building blocks which help aid in the configuration of FlexVPN. Some of these key components even have preset

defaults that can be invoked. Figure 6-4 shows these key FlexVPN building blocks and the interdependencies between them. Notice the arrows linking the boxes together. One set of arrows indicates that the IKEv2 proposal is added to the IKEv2 policy. What this means is you need to first create the IKEv2 proposal, then create the policy, and finally add the proposal to it. This process is similar to how a keyring is added to an IKEv2 profile but only after the keyring is created.

Figure 6-4 FlexVPN Building Blocks

FlexVPN Component Roles

To better understand the components shown in Figure 6-4, let's look at the role each of the components plays in a FlexVPN configuration:

- **IKEv2 proposal:** The IKEv2 proposal defines the protection attributes used in the negotiation of IKE SAs. If you are troubleshooting IKEv2, this negotiation happens during the IKE_SA_INIT phase, which you can see in the **debug** command output. This is the first configuration step that you complete when setting up a FlexVPN, and the IKEv2 proposal is

attached to the IKEv2 policy. Cisco provides a default proposal to give you a simple way to configure a FlexVPN solution.

- **IKEv2 policy:** The IKEv2 policy is used to negotiate the encryption, integrity, PRF, and Diffie–Hellman (DH) group and is bound to either the IP address or to a virtual routing and forwarding (VRF) instance. As with the default proposal option, Cisco includes a default IKEv2 policy. Notice in Figure 6-4 that this is where the IKEv2 proposal is attached.

- **IKEv2 authorization:** This policy defines the local authorization policy and provides attributes used by the local IKEv2 device (hub) and what the server provides to the remote peers. In addition, the IKEv2 authorization policy can provide authentication using AAA that is either local or RADIUS based. The authorization policy is called by the IKEv2 profile using the **aaa authorization** command.

- **IKEv2 keyring:** This repository is for the symmetric and asymmetric pre-shared keys and is independent of the IKEv1 keyring.

- **IKEv2 profile:** This is a repository of parameters that are nonnegotiable, such as local or remote identities and the authentication methods and services available to the authenticated peers, based on the profile that was matched. This building block does not have a default, so you must configure one and attach it to the IPsec profile. If a pre-shared key is being used, the IKEv2 profile is where the IKEv2 keyring is attached; otherwise, certificate information is configured.

- **IPsec transform set:** The transform set specifies the cryptographic security protocols and algorithms used to encrypt the traffic payload. You can use the default value or define the value.

- **IPsec profile:** The FlexVPN parameters are consolidated into a single profile that is applied to the interface.

Note

For the SVPN 300-730 exam, it is very important to understand how the IKEv2 command-line interface constructs work.

FlexVPN Smart Defaults

Using the IKEv2 smart defaults is an easy way to use built-in attributes and streamline your configurations. The goal of smart defaults is to minimize the FlexVPN configuration. Note that the IKEv2 smart defaults (listed in Table 6-5) can be customized for different use cases. However, customization is not recommended. Instead, it would be better to create a new configuration block for a specific scenario than to customize a smart default.

Table 6-5 Smart Defaults

Preconfigured Block	Default Attributes
Crypto IKEv2 proposal	Encryption: AES-CEB 256/192/128, 3DES Integrity: SHA-512/384/256; SHA-1, MD-5 DH: Group 1536 MODP, Group 5, Group 2 PRF: SHA-512, SHA-384, SHA-256, SHA-1 MD5
Crypto IKEv2 policy	Match any
Crypto IPsec transform set	Encrypt
Crypto IPsec profile	Default transform set, SA lifetime

Router Smart Defaults

To see the smart defaults on a router, you can enter the command **show crypto ikev2 proposal** or **show crypto ikev2 policy** or **show crypto ipsec transform-set** and then **show crypto ipsec profile**. In addition to modifying the defaults, you can disable the defaults to prevent them from being exploited or used accidentally. You do this by issuing the command shown in

Example 6-1. This command also reenables the default settings.

Example 6-1 Smart Defaults

```
No Crypto ikev2 proposal default
     To return the default
Default Crypto ikev2 proposal
```

FlexVPN Design Considerations

Now that you understand the components associated with a FlexVPN deployment, next you must establish a goal for the solution. Just like with the last two site-to-site VPN technology topics, you first need to understand what business problems you are going to solve. Once you have determined the goal, you can work back from the goal to the solution. This will be the third chapter that covers this concept, and therefore will shorten the focus. Know that the steps for designing a VPN solution are similar regardless of the technology being used.

FlexVPN Planning

For any VPN technology, including FlexVPN, you must consider the objectives for the technology, what available technologies can be used, and possible problems as planning occurs. FlexVPN allows for a few unique considerations, including involving smart defaults and use of its modular framework. If legacy support is needed, FlexVPN can work unless the technology only supports IKEv1, which is not supported by FlexVPN. FlexVPN also offers both site-to-site and remote access VPN capabilities, which make it a good choice when both technologies are needed. Other considerations are similar to planning recommendations for DMVPN and GETVPN, including considering routing requirements, IP blocks, traffic filtering, and what applications will be supported. See Chapters 4 and 5 for more questions and considerations when planning a VPN solution. The same general questions will apply regardless of the VPN technology used. This includes fault tolerance considerations.

Key FlexVPN Consideration

One best practice covered in the last two chapters is creating a design on paper first. We recommend sharing your design with your peers to validate and assess the design before moving forward with any deployment. The following are some of the many factors that should be documented and discussed before an implementation. You fill find this list to be similar to the one used in the last two chapters.

- IOS requirements
- Platform capabilities (and upgrade options)
- IP address scheme: IPv4, IPv6, or both
- Tunnel addresses
- Remote access and site-to-site
- External (public) addresses
- Routing requirements
- Authentication method: RSA signature, PKI, or pre-shared key
- Encryption scheme
- Deployment strategy
- Application requirements

Now that we have covered the necessary ingredients and design considerations for using FlexVPN, we are ready to move into learning how to deploy FlexVPN technology. We first start with a walkthrough of building a hub-and-spoke FlexVPN deployment.

FlexVPN Implementation: Hub-and-Spoke (IPv4/IPv6)

The SVPN 300-730 exam blueprint highlights FlexVPN hub-and-spoke as one of its key learning objectives. Therefore, the implementation part of this chapter will focus on hub-and-spoke configuration and setup. To keep things simple and to help you understand the differences and similarities between FlexVPN and DMVPN, this chapter uses the same solution used in Chapter 5. Figure 6-5 (for IPv4) and Figure 6-6 (for IPv6) show the core IP addressing solution used throughout this section.

Figure 6-5 IPv4 FlexVPN Solution

Figure 6-6 IPv6 FlexVPN Solution

This section shows how to configure FlexVPN hub-and-spoke for both IPv4 and IPv6. Where the IPv6 configuration differs from the IPv4 configuration, this section provides separate examples for the two protocols. In these

examples, the names in IPv6-specific examples have v6 added at the end. For example, whereas the IPv4 local pool is named SpokePool, the IPv6 local pool is named SpokePoolv6.

Hub-and-Spoke Configuration Summary

To make the FlexVPN hub-and-spoke configuration easy to digest and understand, this section follows the building block approach shown in Figure 6-4 and breaks down the process into four steps:

Step 1. IKEv2 proposal and IKEv2 policy configuration

Step 2. IKEv2 authorization policy configuration

Step 3. Keyring and IKEv2 profile configuration

Step 4. IPsec profile configuration

As shown in Figure 6-7, this section uses steps to group the parts of the configuration process together to make the whole process more intuitive. The following sections illustrate the configuration using these steps, and later in this chapter, you will see how to troubleshoot the configuration using the same steps.

Figure 6-7 FlexVPN Building Blocks Configuration Flow

Step 1: IKEv2 Proposal and IKEv2 Policy Configuration

The configuration steps in this section start with using the defaults that are built into FlexVPN and show an example of a proposal attached to a policy. Figure 6-8 shows the two FlexVPN building blocks configured in this section, both of which have defaults associated with them.

Figure 6-8 IKEv2 Profile and Policy Configuration

FlexVPN IKEv2 Proposal

Example 6-2 shows how to create a custom IKEv2 proposal with options that deviate from the defaults.

Note

The IKEv2 proposal and IKEv2 policy building blocks are optional. Depending on your organization's security policy, however, these building blocks may be required pieces of your configuration.

Example 6-2 FlexVPN Building Blocks

```
crypto ikev2 proposal Hub-Proposal
```

```
encryption aes-cbc-256
group 15
integrity sah256
prf sha256
```

Figure 6-9 shows the execution of the command **show crypto ikev2** proposal, whose output displays the default proposal included with FlexVPN. Compare this output with the proposal created in Example 6-2. The default configuration includes several options, but you can override them and even remove them.

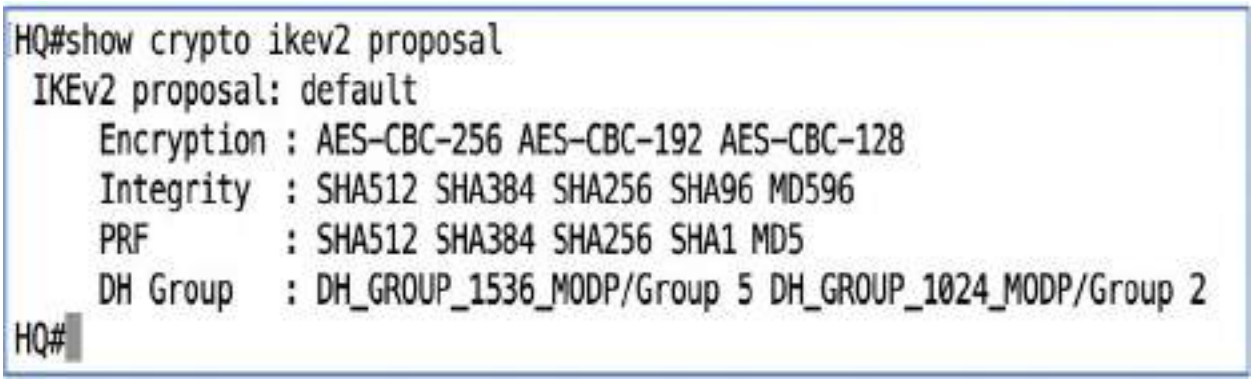


Figure 6-9 FlexVPN Default IKEv2 Proposal

Example 6-3 shows how to build a basic IKEv2 policy on a hub router. This example shows the IKEv2 policy block with the proposal from Example 6-2 attached. Remember that this configuration is optional.

Example 6-3 FlexVPN IKEv2 Policy

```
HQ-Router(config)# crypto ikev2 policy Hub-Policy1
HQ-Router(config-ikev2-policy)# proposal Hub-Proposal
```

Figure 6-10 shows the default policy included on a FlexVPN-capable router.

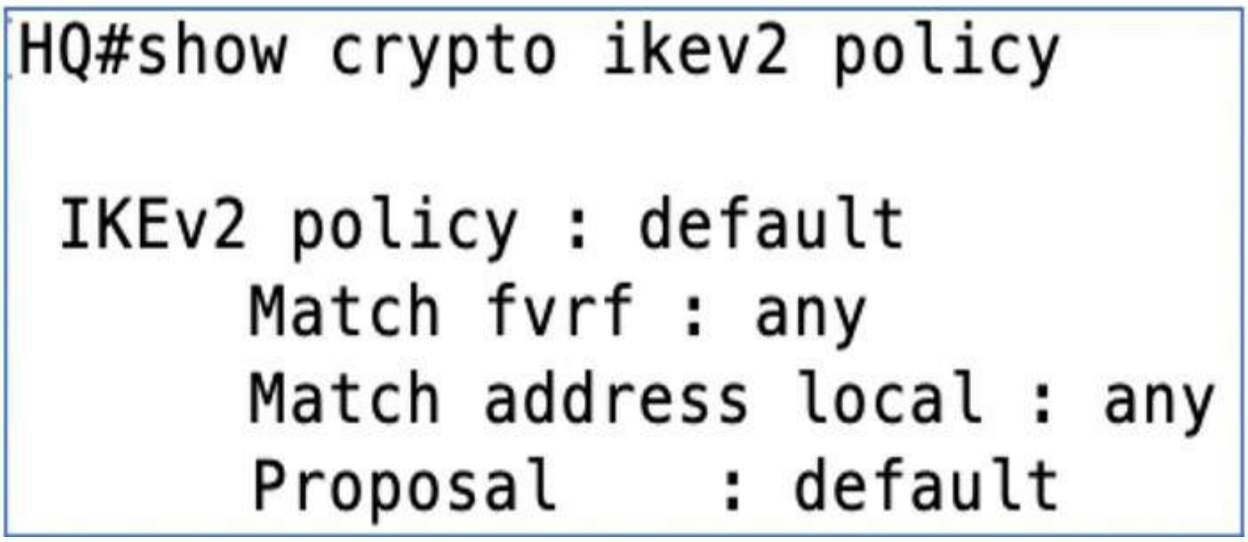


Figure 6-10 FlexVPN IKEv2 Default Policy

When you define an IKEv2 proposal and IKEv2 policy, the peer must match. We show this in Figure 6-7 with the arrow pointing at the IKEv2 policy box that indicates this is where another peer must have a matching proposal and policy.

FlexVPN Transform Set

Another optional configuration component in the FlexVPN building block model is the transform set. Cisco routers include a default version, which you can use to keep the configuration simple. However, you can also configure the transform set yourself.

Example 6-4 shows a simple example of setting a custom transform set named Flex-Transform. Like the IKEv2 policy and proposal, the configuration of the transform set is also optional.

Example 6-4 Crypto IPsec Transform Set

```
crypto ipsec transform-set Flex-Transform esp-aes 192 esp-
sha256-hmac
```

Step 2: IKEv2 Authorization Policy Configuration

This section explores the configuration of the IKEv2 authorization components for a FlexVPN hub-and-spoke solution. First, you need to configure authentication, authorization, and accounting (AAA) on the router. AAA is used to (at a minimum) authenticate the remote spoke's access to the FlexVPN server. The router acts as a server because it has the capability to push the configuration features down to the spoke route. The authorization policy on the hub router needs to include a pool to provide IP addresses to the spoke router.

AAA

Figure 6-11 shows that the AAA, IP pool, and ACL configurations inside the IKEv2 authorization are attached to the IKEv2 profile. In addition, for security purposes, you can use a standard access control list (ACL) to control access to the spokes with the IPv4 or IPv6 routes that they can reach.

Figure 6-11 IKEv2 Authorization Policy Configuration

Example 6-5 shows a configuration that first enables AAA with the command **aaa new-model** and then creates an AAA authentication string for supporting the spokes to authenticate against the local database.

Example 6-5 AAA Authentication

```
HQ-Router(config)# aaa new-model
HQ-Router(config)# aaa authentication network SpokeAuth local
```

Hub Pool

Examples 6-6 (IPv4) and 6-7 (IPv6) show the creation of a local IP pool so that when spoke routers authenticate to the FlexVPN server, they are able to successfully pull an IP address for the tunnel interface. You will see later in this chapter that the FlexVPN server or, as in this case, the HQ router, can role out IP addresses similar to how a DHCP server would.

Example 6-6 Hub IPv4 Pool

```
HQ-Router(config)# ip local pool SpokePool 10.50.50.2
10.50.50.254
```

Example 6-7 Hub IPv6 Pool

```
HQ-Router(config)# ipv6 local pool SpokePoolv6
2001:db8:BEEF:1::2/112 128
```

ACL Permitting Traffic

The configuration in Example 6-8 (IPv4) or Example 6-9 (IPv6) is necessary for the router to advertise to the spoke routers what routes are available on the hub side. That is, it enables the router to show what traffic should be encapsulated through the VPN tunnel. In this case, the network 10.1.1.0/24 is located on the HQ side, so the spoke sending traffic destined for that IP address block passes through the tunnel.

Example 6-8 Hub Standard IPv4 ACL

```
HQ-Router(config)# ip access-list standard HQTraffic
HQ-Router(config-std-acl)# permit 10.1.1.0 0.0.0.255
```

Example 6-9 shows a configuration that advertises the IP block 2001:db8::/32 to all remote devices.

Example 6-9 Hub Standard IPv6 ACL

```
HQ-Router(config)# ipv6 access-list HQTrafficv6
```

```
HQ-Router(config-ipv6-acl)# permit 2001:db8::/32 any
```

Attach to Authorization Policy

After you create the minimum AAA authorization policy and IP pool information needed for the spoke to authenticate and obtain an IP address on the tunnel interface, you need to attach both of these to the IKEv2 authorization policy. Example 6-10 shows the IPv4 pool address that is assigned to the spoke's tunnel interfaces after authentication and the access list used for spoke route table injection.

Example 6-10 IPv4 IKEv2 Authorization Policy

```
HQ-Router(config)# crypto ikev2 authorization policy
SpokePolicy
HQ-Router(config-ikev2-author-policy)# pool SpokePool
HQ-Router(config-ikev2-author-policy)# route set interface
HQ-Router(config-ikev2-author-policy)# route set access-list
HQTraffic
```

Example 6-11 shows the IPv6 configuration, which is identical to the IPv4 configuration except that it references IPv6-specific configuration pieces.

Example 6-11 IPv6 IKEv2 Authorization Policy

```
HQ-Router(config)# crypto ikev2 authorization policy
SpokePolicyv6
HQ-Router(config-ikev2-author-policy)# pool SpokePoolv6
HQ-Router(config-ikev2-author-policy)# route set interface
HQ-Router(config-ikev2-author-policy)# route set access-list
HQTrafficv6
```

Step 3: Keyring and IKEv2 Profile Configuration

Next, you need to configure the keyring on the hub router as shown in Figure 6-12. The keyring is for mutual authentication between the spoke and the hub router. There is IKEv2 documentation that refers to the spoke as the *responder* and the hub router as the *initiator*, which is a good way to look at

things to help remember which does what. This section shows the keyring and IKEv2 profile configuration for both IPv4 and IPv6.

Figure 6-12 IKEv2 Keyring and Profile

Keyring

Example 6-12 (IPv4) and Example 6-13 (IPv6) show the configurations necessary to create a keyring building block that supports authentication for both sides. With IPv4, the use of address 0.0.0.0 0.0.0.0 allows any peer to match this keyring. Notice that with IPv6, the address ::/0 defines all addresses. You need to define a pre-shared key for each side because the keys defined on the two sides do not have to be the same. In addition, one keyring can represent multiple spokes or hosts connecting to the hub because the name under the keyword **peer** defines that peer match. So, you could have another peer match called **peer remote** under the same keyring for AnyConnect authentication.

Example 6-12 IPv4 Keyring Configuration

```
HQ-Router(config)# crypto ikev2 keyring HUB-KR
HQ-Router(config-ikev2-keyring)# peer Spokes
HQ-Router(config-ikev2-keyring)# address 0.0.0.0 0.0.0.0
HQ-Router(config-ikev2-keyring)# pre-shared-key local cisco
HQ-Router(config-ikev2-keyring)# pre-shared-key remote cisco
```

Example 6-13 IPv6 Keyring Configuration

```
HQ-Router(config)# crypto ikev2 keyring HUB-KRv6
HQ-Router(config-ikev2-keyring)# peer Spokesv6
HQ-Router(config-ikev2-keyring)# address ::/0
HQ-Router(config-ikev2-keyring)# pre-shared-key local cisco
HQ-Router(config-ikev2-keyring)# pre-shared-key remote cisco
```

IKEv2 Profile

Example 6-14 (IP4) and Example 6-15 (IPv6) show how to create an IKEv2 profile and attach to it components such as the AAA authorization policy (refer to Example 6-10) and the keyring (refer to Example 6-12). The **aaa authorization group psk** command indicates what authorization will take place when the spoke connects to the hub router. In this example, it says to use the AAA local database on the router and then provides the spoke with that specific policy (SpokePolicy).

Example 6-14 IPv4 IKEv2 Profile

```
HQ-Router(config)# crypto ikev2 profile Hub-Profile
HQ-Router(config-ikev2-profile)# match identity remote address
0.0.0.0
HQ-Router(config-ikev2-profile)# match identity remote fqdn
domain lab.com
HQ-Router(config-ikev2-profile)# identity local address
192.0.2.3
HQ-Router(config-ikev2-profile)# keyring local Hub-KR
HQ-Router(config-ikev2-profile)# authentication remote pre-
share
HQ-Router(config-ikev2-profile)# authentication local pre-share
HQ-Router(config-ikev2-profile)# aaa authorization group psk
SpokeAuth SpokePolicy
HQ-Router(config-ikev2-profile)# virtual-template 1
```

Example 6-15 IPv6 IKEv2 Profile

```
HQ-Router(config)# crypto ikev2 profile Hub-Profilev6
HQ-Router(config-ikev2-profile)# match identity remote address
::/0
HQ-Router(config-ikev2-profile)# match identity remote fqdn
domain lab.com
HQ-Router(config-ikev2-profile)# identity local address
2001:db8:AAAA:1::1
```

```
HQ-Router(config-ikev2-profile)# keyring local Hub-KRv6
HQ-Router(config-ikev2-profile)# authentication remote pre-
share
HQ-Router(config-ikev2-profile)# authentication local pre-share
HQ-Router(config-ikev2-profile)# aaa authorization group psk
SpokeAuth SpokePolicyv6
HQ-Router(config-ikev2-profile)# virtual-template 1
```

Step 4: IPsec Profile Configuration

You are nearing the end of the hub router configuration steps. Figure 6-13 shows that now, in the fourth step, you need to attach the IKEv2 profile from Example 6-14 or 6-15 to the IPsec profile. In this section, you will see how to use the default transform set rather than create a custom one. Know when using FlexVPN, you have the options for using the default or custom transform set.

Figure 6-13 IPsec Profile Configuration

Example 6-16 (IPv4) and Example 6-17 (IPv6) show how to attach the IKEv2 profile to the IPsec profile.

Example 6-16 IPv4 IPsec Profile

```
HQ-Router(config)# crypto ipsec profile Hub-IPsec-Profile
HQ-Router(config-profile)# set ikev2-profile Hub-Profile
```

Example 6-17 IPv6 IPsec Profile

```
HQ-Router(config)# crypto ipsec profile Hub-IPsec-Profile
HQ-Router(config-profile)# set ikev2-profile Hub-Profilev6
```

Create Loopback Address

Example 6-18 (IPv4) and Example 6-19 (IPv6) show how to create a loopback address on the FlexVPN server (hub) router for use by the GRE tunnel interface. In this case, the IPv4/IPv6 pool you use will be the same IP address subnet block you created for the hub spoke pool. This means that when a spoke router authenticates, it will request its IPv4 or IPv6 address from **SpokePool** (which for IPv4 will be 10.50.50.2 through 10.50.50.254) or **SpokePoolv6** and apply it to the GRE tunnel interface.

Example 6-18 IPv4 Loopback

```
HQ-Router(config)# Interface Loopback 0
HQ-Router(config-if)# ip address 10.50.50.1 255.255.255.255
```

Example 6-19 IPv6 Loopback

```
HQ-Router(config)# Interface Loopback 0
HQ-Router(config-if)# ipv6 address 2001:db8:BEEF:1::1/112
```

Virtual Template

Example 6-20 (IPv4) and Example 6-21 (IPv6) show how to create a virtual template and attach the IPsec profile. Notice that you reference the loopback address for the IP address that will be used by the GRE tunnel interface.

Example 6-20 IPv4 Virtual Template

```
HQ-Router(config)# interface virtual-template 1 type tunnel
HQ-Router(config-if)# ip unnumbered loopback 0
HQ-Router(config-if)# tunnel source G0/0
HQ-Router(config-if)# tunnel protection ipsec profile Hub-
IPsec-Profile
```

Example 6-21 IPv6 Virtual Template

```
HQ-Router(config)# interface virtual-template 1 type tunnel
HQ-Router(config-if)# ipv6 unnumbered loopback 0
HQ-Router(config-if)# tunnel source G0/0
HQ-Router(config-if)# tunnel mode gre ipv6
HQ-Router(config-if)# tunnel protection ipsec profile Hub-
IPsec-Profile
```

Pre-shared IKEv2 Keyring

If the local or remote authentication method is a pre-shared key, you need to configure keys in the peer configuration sub mode that defines a peer subblock. An IKEv2 keyring can have multiple peer subblocks. A peer subblock contains a single symmetric or asymmetric key pair for a peer or peer group identified by any combination of the hostname, identity, and IP address. IKEv2 keyrings are independent of IVEv1 keyrings.

FlexVPN Spoke Configuration

This section does not cover the built-in default FlexVPN spoke components. Rather, we will focus on the critical configuration steps you need to take when configuring your FlexVPN spokes.

Spoke AAA Configuration

First, you need to enable AAA and AAA authentication as shown in Example 6-22.

Example 6-22 Spoke AAA Configuration

```
Spoke1(config)# aaa new-model
Spoke1(config)# aaa authentication network FlexAuth local
```

Spoke Access List

The next step is necessary for the spoke router to advertise to the routes that

are available on the spoke side. Basically, you need the router to indicate what traffic should be encapsulated through the VPN tunnel to reach the spoke side, which is network 10.2.2.0/24 for this example. Examples 6-23 and 6-24 show IPv4 and IPv6 examples.

Example 6-23 IPv4 Spoke Access List

```
Spoke1(config)# ip access-list standard SpokeTraffic
Spoke1(config-std-naacl)# permit 10.2.2.0 0.0.0.255
```

Example 6-24 IPv6 Spoke Access List

```
Spoke1(config)# ipv6 access-list SpokeTrafficv6
Spoke1(config-ipv6-acl)# permit 2001:db8:BBBB:2::0/64 any
```

Spoke Keyring

Example 6-25 (IPv4) and Example 6-26 (IPv6) show how to create the keyring building block needed by the spoke for authentication using a pre-shared key.

Example 6-25 IPv4 Spoke Keyring

```
Spoke1(config)# crypto ikev2 keyring Spoke-KR
Spoke1(config-ikev2-keyring)# peer Hub
Spoke1(config-ikev2-keyring)# address 192.0.2.3
Spoke1(config-ikev2-keyring)# pre-shared-key local cisco
Spoke1(config-ikev2-keyring)# pre-shared-key remote cisco
```

Example 6-26 IPv6 Spoke Keyring

```
Spoke1(config)# crypto ikev2 keyring Spoke-KRv6
Spoke1(config-ikev2-keyring)# peer Hub
Spoke1(config-ikev2-keyring)# address 2001:db8:AAAA:1::1
Spoke1(config-ikev2-keyring)# pre-shared-key local cisco
Spoke1(config-ikev2-keyring)# pre-shared-key remote cisco
```

In FlexVPN, configuration works in both directions. That is, the hub router pushes information about its networks to the spoke, and the spoke pushes

information about its local networks to the hub. Another solution might be for HQ-Router to use certificates for authentication and for the spoke routers to use pre-shared keys. Keep this concept in mind for the exam.

Spoke Authorization Policy

Example 6-27 shows how to configure the IKEv2 authorization policy on the spoke to send the route information specified in the **Spoketraffic** access list for IPv4.

Example 6-27 IPv4 Spoke IKEv2 Authorization Policy

```
Spoke1(config)# crypto ikev2 authorization policy SpokePolicy
Spoke1(config-ikev2-author-policy)# route set interface
Spoke1(config-ikev2-author-policy)# route set access-list
Spoketraffic
```

Example 6-28 shows how to configure the IKEv2 authorization policy on the spoke to send the route information specified in the **Spoketrafficv6** access list for IPv6.

Example 6-28 IPv6 Spoke IKEv2 Authorization Policy

```
Spoke1(config)# crypto ikev2 authorization policy SpokePolicyv6
Spoke1(config-ikev2-author-policy)# route set interface
Spoke1(config-ikev2-author-policy)# route set access-list
Spoketrafficv6
```

Spoke IKEv2 Profile

Example 6-29 (IPv4) and Example 6-30 (IPv6) show how to configure an IKEv2 spoke profile attach it to the local keyring. The **aaa authorization** command calls the AAA group **FlexAuth** with the authorization policy from Example 6-27 (**SpokePolicy**) or Example 6-28 (**SpokePolicyv6**).

Example 6-29 IPv4 Spoke IKEv2 Profile

```
Spoke1(config)# crypto ikev2 profile Spoke-Profile
Spoke1(config-ikev2-profile)# match identity remote address
```

```
192.0.2.3
Spoke1(config-ikev2-profile)# identity local address
209.165.201.2
Spoke1(config-ikev2-profile)# authentication remote pre-share
Spoke1(config-ikev2-profile)# authentication local pre-share
Spoke1(config-ikev2-profile)# keyring local Spoke-KR
Spoke1(config-ikev2-profile)# aaa authorization group psk list
FlexAuth SpokePolicy
```

Example 6-30 IPv6 Spoke IKEv2 Profile

```
Spoke1(config)# crypto ikev2 profile Spoke-Profilev6
Spoke1(config-ikev2-profile)# match identity remote address
2001:db8:AAAA:1::1
Spoke1(config-ikev2-profile)# identity local address
2001:db8:BBBB:2::2
Spoke1(config-ikev2-profile)# authentication remote pre-share
Spoke1(config-ikev2-profile)# authentication local pre-share
Spoke1(config-ikev2-profile)# keyring local Spoke-KRv6
Spoke1(config-ikev2-profile)# aaa authorization group psk list
FlexAuth SpokePolicyv6
```

Spoke IPsec Profile

Example 6-31 (IPv4) and Example 6-32 (IPv6) show how to create an IPsec profile.

Example 6-31 IPv4 Spoke IPsec Profile

```
Spoke1(config)# crypto ipsec profile Spoke-IPsec-Profile
Spoke(ipsec-profile)# set ikev2-profile Spoke-Profile
```

Example 6-32 IPv6 Spoke IPsec Profile

```
Spoke1(config)# crypto ipsec profile Spoke-IPsec-Profile
Spoke(ipsec-profile)# set ikev2-profile Spoke-Profilev6
```

Spoke Tunnel Interface

Example 6-33 (IPv4) and Example 6-34 (IPv6) show how to create the tunnel

interface where you attach the IPsec profile.

Example 6-33 IPv4 Spoke Tunnel Interface

```
Spoke1(config)# Interface tunnel 0
Spoke1(config-if)# ip address negotiated
Spoke1(config-if)# tunnel source GigabitEthernet0/0
Spoke1(config-if)# tunnel destination 192.0.2.3
Spoke1(config-if)# tunnel protection ipsec profile Spoke-IPsec-
Profile
```

Example 6-34 IPv6 Spoke Tunnel Interface

```
Spoke1(config)# interface Tunnel 0
Spoke1(config-if)# ip address negotiated
Spoke1(config-if)# tunnel source GigabitEthernet0/0
Spoke1(config-if)# tunnel destination 2001:db8:AAAA:1::1
Spoke1(config-if)# tunnel protection ipsec profile Spoke-IPsec-
Profile
```

The configuration for the hub router and spoke router is now complete. When you enable the tunnel interface on the spoke router and the virtual template on the hub router, you should see the routers initializing IKEv2 and attempting to authenticate. Later in this chapter, you will see how to troubleshoot this configuration using the same four-action process used in this section.

Next, let’s look at a spoke-to-spoke Flex VPN deployment.

FlexVPN Implementation: Spoke-to-Spoke (IPv4/IPv6)

This section discusses how to implement FlexVPN spoke-to-spoke communication. Since we already covered how to build a hub-and-spoke FlexVPN configuration, now you just need to add NHRP so that the spokes can communicate directly with each other. With FlexVPN, NHRP plays a similar role to the one it plays with DMVPN. With shortcut switching (spoke-to-spoke tunnels), the spoke routers are able to use a dynamic virtual tunnel

interface (dVTI) for communication. The spokes will have a main tunnel interface that communicates with the hub and a dynamic virtual interface that will be enabled when traffic must transit between the two spokes directly.

Note

When the FlexVPN virtual tunnel is up and running and tunnels are established from the spoke to the hub router, you can no longer make changes to the hub router's virtual tunnel configuration.

Figure 6-14 shows what the network will look like when the spoke-to-spoke configuration is complete. Notice the flow of the NHRP messages and the shortcut switching established between the two spoke routers over the VTI.

Figure 6-14 FlexVPN Spoke-to-Spoke Solution

FlexVPN NHRP

Example 6-35 shows how to configure the hub router with NHRP. It is important to note two things about the two new lines on the virtual template (highlighted in this example): The network ID must be consistent across the FlexVPN network, and the hub router is the only router that will have the redirect option. NHRP enables the spoke to forward the spoke resolution to another spoke and send back the redirect information to the spoke that

initiated the request. This NHRP redirect information informs the spoke of the other spoke's information.

Note that the same configuration is used for both IPv4 and IPv6.

Example 6-35 Hub Router NHRP for Spoke-to-Spoke Communications

```
HQ-Router(config)# interface virtual-template 1 type tunnel
HQ-Router(config-XXX)# ip unnumbered Loopback0
HQ-Router(config-XXX)# tunnel source GigabitEthernet0/0
HQ-Router(config-XXX)# tunnel protection ipsec profile Hub-
IPsec-Profile
HQ-Router(config-xxx)#  ip nhrp network-id 1
HQ-Router(config-xxx)#  ip nhrp redirect
```

FlexVPN Spoke-to-Spoke Spoke Router

The configuration for the spoke router in the spoke-to-spoke shortcut scenario is a little more complex. It resembles what you did in Chapter 5 when traffic has to traverse the hub. However, on the spoke you need to create a second virtual interface by using the **interface virtual-template type tunnel** command so that the dVTI will clone the tunnel that leads back to the hub. To do so, you need to follow these steps:

Step 1. Add a new keyring for spoke-to-spoke communication.

Step 2. Adjust the IKEv2 profile.

Step 3. Add NHRP commands to the tunnel interface.

Step 4. Create a virtual template tunnel.

Spoke-to-Spoke Keyring

Example 6-36 (IPv4) and Example 6-37 (IPv6) show how to add on to your existing keyring and create a new one for spoke-to-spoke authentication. Note that this example shows how to create a separate keyring for clarity and ease of understanding the configuration.

Example 6-36 IPv4 Spoke Keyring Addition

```
Spoke1(config)# crypto ikev2 keyring S2S-KR
Spoke1(config-ikev2-keyring)# peer Spokes
Spoke1(config-ikev2-keyring)# address 0.0.0.0 0.0.0.0
Spoke1(config-ikev2-keyring)# pre-shared-key local cisco
Spoke1(config-ikev2-keyring)# pre-shared-key remote cisco
```

Example 6-37 IPv6 Spoke Keyring Addition

```
Spoke1(config)# crypto ikev2 keyring S2S-KRv6
Spoke1(config-ikev2-keyring)# peer Spokes
Spoke1(config-ikev2-keyring)# address ::/0
Spoke1(config-ikev2-keyring)# pre-shared-key local cisco
Spoke1(config-ikev2-keyring)# pre-shared-key remote cisco
```

Spoke-to-Spoke Route Injection

Example 6-38 and (IPv4) and Example 6-39 (IPv6) show how to solve the routing issue so that spokes are able to resolve the other remote locations' IP blocks by changing the access list **HQTraffic** to add a static route on both spokes of 10.0.0.0/8 for IPv4 or 2001:db8::/32 for IPv6. Note that although we include this step, most implementations solve the IP connectivity issue with a routing protocol rather than trying to maintain an access list with routes.

Example 6-38 IPv4 Hub-to-Spoke Route Injection

```
HQ-Router(config)# ip access-list standard HQTraffic
HQ-Router(config-std-nacl)# permit 10.0.0.0 0.255.255.255
```

Example 6-39 IPv6 Hub-to-Spoke Route Injection

```
HQ-Router(config)# ipv6 access-list HQTrafficv6
HQ-Router(config-ipv6-acl)# permit 2001:db8::/32 any
```

Spoke-to-Spoke IKEv2 Profile

Example 6-40 (IPv4) and Example 6-41 (IPv6) show how to create a new IKEv2 profile for the spoke-to-spoke authentication. This configuration differs from the one created for hub communication because it includes the **virtual-Template** command. This site-to-site profile needs to be replicated at each spoke that needs to communicate; alternatively, an **any** match can be used.

This example in this section has only have two remote sites, so the configuration is straightforward. Notice that Examples 6-40 and 6-41 call the keyring you created for the other spoke and uses the same **aaa authorization group** command as used in the hub-and-spoke solution (refer to Figure 6-11 and Example 6-5).

Example 6-40 IPv4 Spoke IKEv2 Profile

```
Spoke1(config)# crypto ikev2 profile S2S-Profile
Spoke1(config-ikev2-profile)# match identity remote address
209.165.202.130 255.255.255.255
Spoke1(config-ikev2-profile)# identity local address
209.165.201.2
Spoke1(config-ikev2-profile)# authentication remote pre-share
Spoke1(config-ikev2-profile)# authentication local pre-share
Spoke1(config-ikev2-profile)# keyring local S2S-KR
Spoke1(oncifg-ikev2-profile)# aaa Authorization group psk list
FlexAuth Policy
Spoke1(config-ikev2-profile)# virtual-Tempate 1
```

Example 6-41 IPv6 Spoke IKEv2 Profile

```
Spoke1(config)# crypto ikev2 profile S2S-Profilev6
Spoke1(config-ikev2-profile)# match identity remote address
2001:db8:db8:CCCC:2::2/128
Spoke1(config-ikev2-profile)# identity local address
2001:db8:BBBB:2::2
Spoke1(config-ikev2-profile)# authentication remote pre-share
Spoke1(config-ikev2-profile)# authentication local pre-share
Spoke1(config-ikev2-profile)# keyring local S2S-KRv6
Spoke1(oncifg-ikev2-profile)# aaa authorization group psk list
FlexAuth Policyv6
Spoke1(config-ikev2-profile)# virtual-Tempate 1
```

Spoke-to-Spoke Add NHRP

Example 6-42 (which works for both IPv4 and IPv6) is where things start to get interesting. You need to add to the tunnel interface (Tunnel 0 in our example) to the NHRP network ID so the hub router knows you are part of the same NHRP network. In addition, the **ip nhrp shortcut virtual-template** command supports the setup of the IPsec tunnel between spokes. However, this setup happens only when interesting traffic forces the NHRP resolution process.

Example 6-42 NHRP Added to the Spoke Tunnel Interface

```
Spoke1(config)# interface tunnel 0
Spoke1(config-if)# ip address negotiated
Spoke1(config-if)# tunnel source GigabitEthernet0/0
Spoke1(config-if)# tunnel destination 192.0.2.3
Spoke1(config-if)#  ip nhrp network-id 1
Spoke1(config-if)#  ip nhrp shortcut virtual-template 1
Spoke1(config-if)# tunnel protection ipsec profile Spoke-IPsec-
Profile
```

Spoke-to-Spoke Virtual Template

Example 6-43 (IPv4) and Example 6-44 (IPv6) demonstrate the addition of a virtual template for spoke-to-spoke communication. This template is initialized only when interesting traffic triggers the tunnel. The trigger happens as a result of routing or access list matching. Notice that the IPv6 requires an additional command to enable the GRE tunnel to run over an IPv6 network layer and transport IPv6 packets.

Example 6-43 IPv4 Virtual Template for Spoke-to-Spoke Tunnel Communication

```
Spoke1(config)# interface Virtual-Template1 type tunnel
Spoke1(config-if)# ip unnumbered Tunnel0
Spoke1(config-if)#  ip nhrp network-id 1
Spoke1(config-if)#  ip nhrp shortcut virtual-template 1
Spoke1(config-if)# tunnel protection ipsec profile Spoke-IPsec-
Profile
```

Example 6-44 IPv6 Virtual Template for Spoke-to-Spoke Tunnel Communication

```
Spoke1(config)# Interface Virtual-Template1 type tunnel
Spoke1(config-if)# ip unnumbered Tunnel0
Spoke1(config-if)#  ip nhrp network-id 1
Spoke1(config-if)#  ip nhrp shortcut virtual-template 1
Spoke1(config-if)#  tunnel mode gre ipv6
Spoke1(config-if)# Tunnel protection ipsec profile Spoke-IPsec-
Profile
```

We do not cover routing in this section of the chapter because we have already seen that the IKEv2 authorization policy calling the access list **HQTraffic** results in a summary route being sent to the remote FlexVPN spokes. The authorization policy inserts the summary route into the routing tables of both spokes. Because the two sites' IP address blocks are in that summary (refer to Examples 6-38 and 6-39), they can communicate directly by way of NHRP resolution through the hub via redirection to cause one of the spokes to initiate the tunnel between the two sites. Figure 6-15 shows the routing table on the spoke router; notice that it has the summary address 10.0.0.0/8, pointing to the tunnel interface.

```
      10.0.0.0/8 is variably subnetted, 7 subnets, 3 masks
S        10.0.0.0/8 [2/0] via 0.0.0.0, Tunnel0
D        10.1.1.0/24 [90/26880256] via 10.50.50.1, 00:27:51
C        10.2.2.0/24 is directly connected, GigabitEthernet0/1
L        10.2.2.1/32 is directly connected, GigabitEthernet0/1
S        10.50.50.1/32 [2/0] via 0.0.0.0, Tunnel0
C        10.50.50.2/32 is directly connected, Tunnel0
D        10.50.50.3/32 [90/28160000] via 10.50.50.1, 00:27:20
O     192.0.2.0/24 [110/2] via 209.165.201.1, 08:12:02, GigabitEthernet0/0
      209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
```

Figure 6-15 Showing the IPv4 Route on Spoke1

Note

The configuration of the IKEv2 authorization policy on the hub router allows the push of simple networks or the ones listed in the access list. To enable full functionality, dynamic routing needs to be configured on a FlexVPN network.

That wraps up how to configure both a hub-and-spoke and a spoke-to-spoke FlexVPN deployment. Make sure you are familiar with these steps before taking on the SVPN exam.

Our final topic for this chapter is a review of how to validate and troubleshoot your existing FlexVPN deployment.

FlexVPN Troubleshooting

With FlexVPN, troubleshooting can be very complex, especially when you have a combination of VPN solutions using a single hub. For example, if you are mixing remote access, legacy crypto map hosts, and a hub-and-spoke solution on the same hub router, troubleshooting can be extremely challenging. This chapter limits the configuration to a hub-and-spoke solution with additional capability for spoke-to-spoke communication. For the SVPN exam, you will likely see a FlexVPN configuration that targets one type of deployment, but real-world deployments can be much more complex!

The best way to troubleshoot FlexVPN is to use the blocks from the building block model we have used in the last few chapters to determine where the challenge is. Table 6-6 shows the building blocks on the left and the commands that can be used with each building block on the right. This format follows each section as an action.

Table 6-6 Key FlexVPN Troubleshooting Commands

Troubleshooting FlexVPN Building Block	Commands
Step 1: IKEv2 proposal and IKEv2 policy troubleshooting	
Step 2: IKEv2 authorization policy troubleshooting	
Step 3: Keyring and IKEv2 profile troubleshooting	
Step 4: IPsec profile troubleshooting	
NHRP troubleshooting	
Routing troubleshooting	

Troubleshooting FlexVPN Building Block	Commands
Step 1: IKEv2 proposal and IKEv2 policy troubleshooting	**show crypto ikev2 sa** **show crypto ikev2 proposal** **show crypto ikev2 policy** **debug crypto ikev2 error**
Step 2: IKEv2 authorization policy troubleshooting	**show crypto ikev2 authorization policy** **debug crypto ikev2 error** **debug aaa authorization** **debug aaa protocol local**
Step 3: Keyring and IKEv2 profile troubleshooting	**show crypto ikev2 profile** **debug crypto ikev2 error**
Step 4: IPsec profile troubleshooting	**show crypto ipsec profile** **show crypto ipsec sa**
NHRP troubleshooting	**show ip nhrp detail** **show interface virtual-access 1** **debug nhrp packet**
Routing troubleshooting	**show ip protocol** **show ip route**

Connectivity Troubleshooting

From the spoke router, you must determine whether the **Tunnel0** interface has an IP address or if the VPN tunnel is up and running. If the interface does not have an IP address, you can proceed to determine what part of the configuration is not working correctly. For example, you can check on the

spoke router to see if any Syslog messages are evident. Can you ping the hub's outside IP address from the spoke router? If not, you know you have a basic routing problem. If you can ping that address, then you probably need to determine whether IKEv2 is set up correctly. Figure 6-16 shows a successful ping of the hub router from the spoke that validates connectivity.

```
R2#ping 192.0.2.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.0.2.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

Figure 6-16 Pinging the Hub's IP Address

Figure 6-17 shows how to check that the tunnel has an IP address and that it is from the hub route pool. In this case, you can see that Spoke1 or R2 got an IP address from the **SpokePool**. As shown in Example 6-6, the **SpokePool** IPv4 configuration range is 10.50.50.2 through 10.50.50.254.

```
R2#show ip int brief
Interface                  IP-Address      OK? Method Status                Protocol
Embedded-Service-Engine0/0 unassigned      YES NVRAM  administratively down down
GigabitEthernet0/0         209.165.201.2   YES NVRAM  up                    up
GigabitEthernet0/1         10.2.2.1        YES NVRAM  up                    up
GigabitEthernet0/2         unassigned      YES NVRAM  administratively down down
Loopback0                  unassigned      YES unset  up                    up
Tunnel0                    10.50.50.2      YES NVRAM  up                    up
Virtual-Template1          10.50.50.2      YES unset  up                    down
```

Figure 6-17 Spoke Router IP Address Assignment

Step 1: IKEv2 Proposal and IKEv2 Policy

Troubleshooting

If you have determined that IKEv2 is not working, you need to look at the IKEv2 proposal and IKEv2 policy, using the commands **show crypto ikev2 proposal** and **show crypto ikev2 policy**. You need to make sure that, if you are not using the defaults, the proposal is attached to the policy. Figure 6-18 and Figure 6-19 show default configuration examples. However, the defaults still demonstrate that the proposal is attached to the policy and that the policy matches any local address.

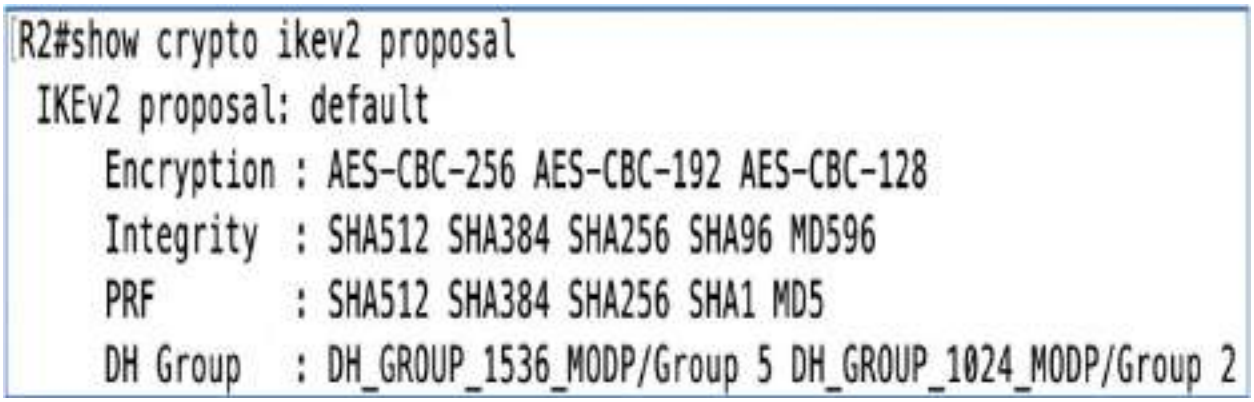


Figure 6-18 show crypto ikev2 proposal Command and Output

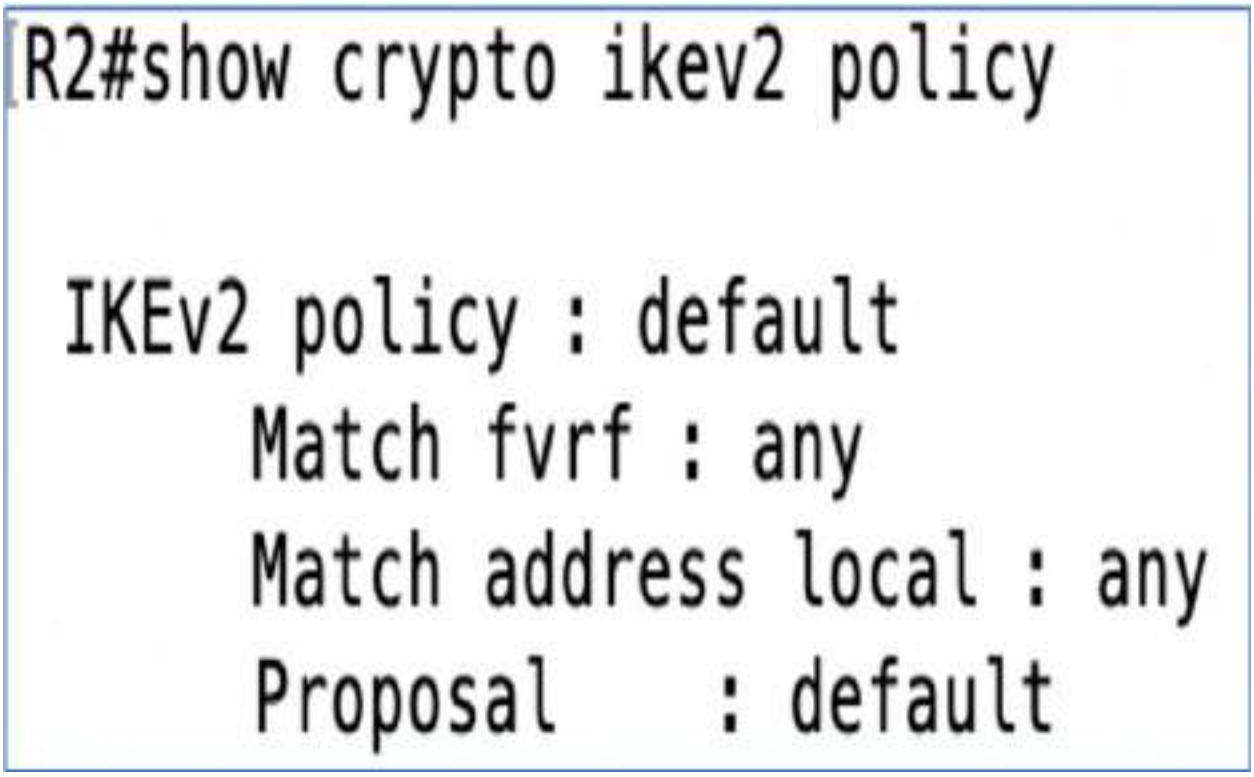


Figure 6-19 show crypto ikev2 policy Command and Output

IKEv2 Debugging

If you cannot determine the issue, then another possible solution is to turn on debugging for IKEv2 with the command **debug crypto ikev2 error**. This will help you determine where IKEv2 is failing. Maybe the issue is that the IKEv2 authorization policy is not defined correctly, or perhaps the match address is not correct; to identify either case, you need to use the command **debug crypto ikev2 error**.

Step 2: IKEv2 Authorization Policy Troubleshooting

If a spoke is unable to get an IP address for the tunnel interface or a route is not in the table, you need to determine whether the IKEv2 authorization policy (that is, the one on the hub router) is misconfigured. Notice in Figure 6-20 that **SpokePool** is the IPv4 pool used for tunnel, and **HQTraffic** is the ACL for route injection. You need to validate that they actually exist on the

hub router. If you use the **debug ikev2** command and the configuration information is incorrect, the command identifies the problem. This command can also let you know if the configuration information is missing or the remote spokes get the wrong IP or route injection.

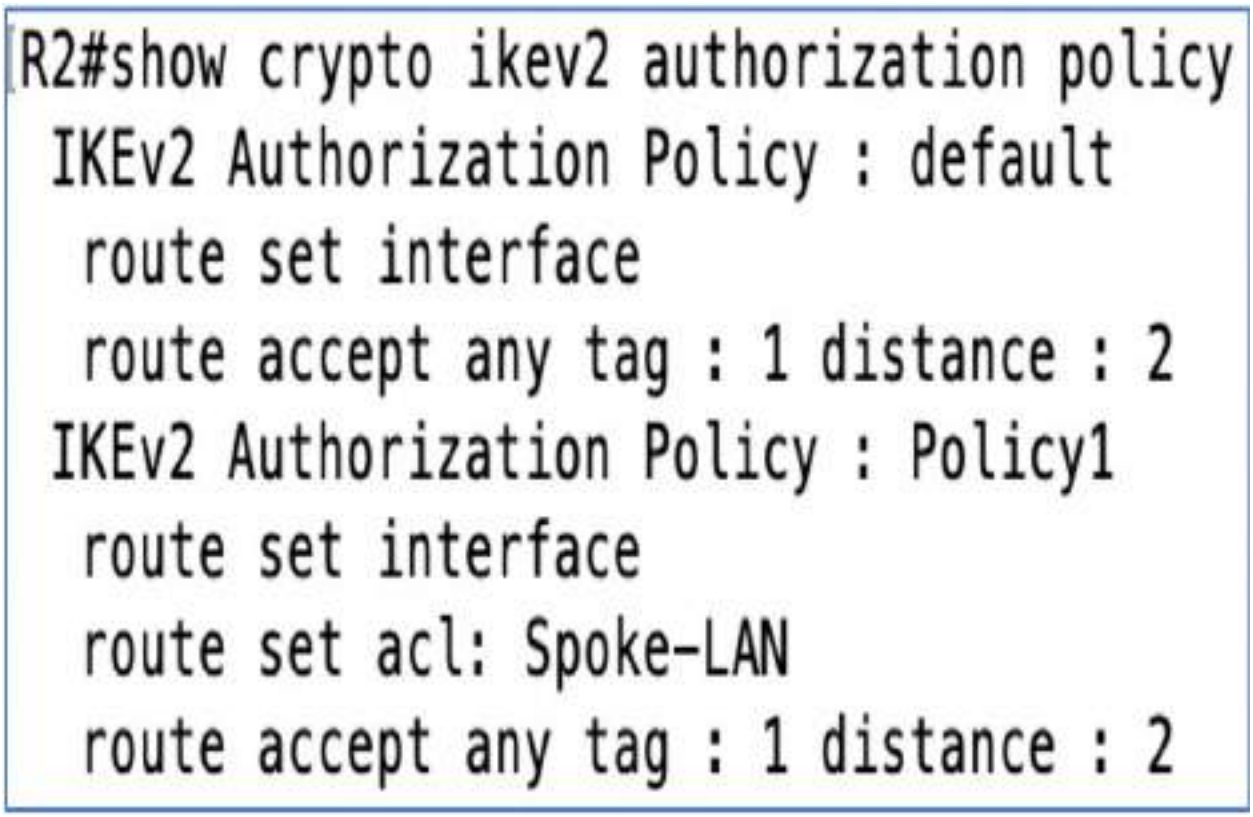


Figure 6-20 show crypto ikev2 authorization policy Command and Output

Step 3: Keyring and IKEv2 Profile Troubleshooting

You can troubleshoot the keyring and the IKEv2 profile by using one command. However, you might have to also use the **show run** command to verify the keyring settings or at least validate them against the other router's keyring configuration. The command **show crypto ikev2 profile** in Figure 6-21 provides some key information for troubleshooting. For example, it shows whether you are using the keyring (**Hub-KR**) or pre-shared authentication. It also includes the identities and the AAA information.

```
HQ#show crypto ikev2 profile

IKEv2 profile: Hub-Profile
 Ref Count: 10
 Match criteria:
  Fvrf: global
  Local address/interface: none
  Identities:
   address 0.0.0.0
   fqdn domain lab3.com
  Certificate maps: none
 Local identity: address 192.0.2.3
 Remote identity: none
 Local authentication method: pre-share
 Remote authentication method(s): pre-share
 EAP options: none
 Keyring: Hub-KR
 Trustpoint(s): none
 Lifetime: 86400 seconds
 DPD: disabled
 NAT-keepalive: disabled
 Ivrf: none
 Virtual-template: 1
 mode auto: No
 AAA AnyConnect EAP authentication mlist: none
 AAA EAP authentication mlist: none
 AAA Accounting: none
 AAA group authorization:
  psk: list FlexAuth, username policy1
 AAA user authorization: none
```

Figure 6-21 show crypto ikev2 profile Command and Output

Step 4: IPsec Profile Troubleshooting

Troubleshooting IPsec for FlexVPN is basically the same as troubleshooting DMVPN (refer to Chapter 5). The command **show crypto ipsec sa** is probably the first place to start your IPsec troubleshooting. You can also use the command **debug ipsec** to see what that output tells you. The command **show crypto ipsec profile** provides a wealth of information and one that can be helpful for troubleshooting IPsec. Figure 6-22 shows that the output provides the profile name and the name of the transform set that is being used. Keep in mind that you need to validate that the profiles on the hub and spoke are in alignment.

```
HQ#show crypto ipsec profile
IPSEC profile Hub-Profile
        IKEv2 Profile: Hub-Profile
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Mixed-mode : Disabled
        Transform sets={
                default:  { esp-aes esp-sha-hmac  } ,
        }

IPSEC profile default
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Mixed-mode : Disabled
        Transform sets={
                default:  { esp-aes esp-sha-hmac  } ,
        }
```

Figure 6-22 show crypto ipsec profile Command and Output

As shown in Figure 6-23, the command **show crypto ikev2 session** displays a concise summary of the tunnels. It is similar to **show crypto ipsec sa** but with fewer details.

```
HQ#sh crypto ikev2 session
 IPv4 Crypto IKEv2 Session

Session-id:2, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                 Remote                fvrf/ivrf            Status
2         192.0.2.3/500         209.165.201.2/500     none/none            READY
      Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/11778 sec
Child sa: local selector  192.0.2.3/0 - 192.0.2.3/65535
          remote selector 209.165.201.2/0 - 209.165.201.2/65535
          ESP spi in/out: 0x50356316/0xA9AC1F96

Session-id:1, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         192.0.2.3/500         209.165.202.130/500   none/none            READY
      Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/11789 sec
Child sa: local selector  192.0.2.3/0 - 192.0.2.3/65535
          remote selector 209.165.202.130/0 - 209.165.202.130/65535
          ESP spi in/out: 0x50067287/0x35D15DFD

 IPv6 Crypto IKEv2 Session
```

Figure 6-23 show crypto ikev2 session Command and Output

NHRP Troubleshooting

If your configuration requires spoke-to-spoke capabilities, you need to understand NHRP resolution and how to troubleshoot this part of the configuration. This section includes the commands you need for this troubleshooting. Make sure to know these commands for the SVPN exam.

The command shown in Figure 6-24 was executed from the spoke router. Note that this command is not included in Table 6-6 because it is only found in spoke-to-spoke communication. As you can see, the spoke (R2) uses

NHRP to resolve 10.50.50.3 information and map its outside address, 209.165.202.130.

```
R2#sh ip nhrp detail
10.3.3.0/24 via 10.50.50.3
   Tunnel0 created 00:02:05, expire 01:57:54
   Type: dynamic, Flags: router rib
   NBMA address: 209.165.202.130
10.50.50.2/32 via 10.50.50.2
   Virtual-Access1 created 00:02:05, expire 01:57:54
   Type: dynamic, Flags: router unique local
   NBMA address: 209.165.201.2
    (no-socket)
  Requester: 10.50.50.3 Request ID: 2
10.50.50.3/32 via 10.50.50.3
   Virtual-Access1 created 00:02:05, expire 01:57:54
   Type: dynamic, Flags: router implicit rib nho
   NBMA address: 209.165.202.130
```

Figure 6-24 show ip nhrp detail Command and Output

Figure 6-25 indicates that interesting traffic initiated the tunnel, and R2 brought up the **Virtual-Access** interface to establish a VPN tunnel to R3. This output comes from using the command **show crypto ipsec sa**. The **Virtual-Access** interface would not exist without NHRP resolving the information about the other spoke.

```
interface: Virtual-Access1
    Crypto map tag: Virtual-Access1-head-0, local addr 209.165.201.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (209.165.201.2/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (209.165.202.130/255.255.255.255/47/0)
   current_peer 209.165.202.130 port 500
     PERMIT, flags={origin_is_acl,ipsec_sa_request_sent}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 14, #recv errors 0

     local crypto endpt.: 209.165.201.2, remote crypto endpt.: 209.165.202.130
     path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
     current outbound spi: 0x0(0)
     PFS (Y/N): N, DH group: none
```

Figure 6-25 Spoke1 **Virtual-Access** Interface

Figure 6-26 shows the command **debug nhrp packet** executed on a spoke router. It shows the resolution process diagramed in Figure 6-14, where by the spoke sends the NHRP resolution request to the hub via the **Tunnel0** interface for destination 10.3.3.1. The hub router sends the redirect message back to the spoke via the **Tunnel0** interface. The information included in the redirect message is src NMBA 209.165.202.130 and src 10.50.50.3. So now the spoke knows to establish a VPN tunnel to 10.50.50.3 and use a **Virtual-Access** interface.

```
Jul 28 09:39:23.407: NHRP: Send Resolution Request via Tunnel0 vrf 0, packet size: 72
Jul 28 09:39:23.407:  src: 10.50.50.2, dst: 10.3.3.1
Jul 28 09:39:23.407:  (F) afn: AF_IP(1), type: IP(800), hop: 255, ver: 1
Jul 28 09:39:23.407:      shtl: 4(NSAP), sstl: 0(NSAP)
Jul 28 09:39:23.407:      pktsz: 72 extoff: 52
Jul 28 09:39:23.407:  (M) flags: "router auth src-stable nat ", reqid: 2
Jul 28 09:39:23.407:      src NBMA: 209.165.201.2
Jul 28 09:39:23.407:      src protocol: 10.50.50.2, dst protocol: 10.3.3.1
Jul 28 09:39:23.407:  (C-1) code: no error(0)
Jul 28 09:39:23.407:        prefix: 32, mtu: 17874, hd_time: 7200
Jul 28 09:39:23.407:        addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref: 0
Jul 28 09:39:23.407: NHRP: Receive Resolution Request via Tunnel0 vrf 0, packet size: 92
Jul 28 09:39:23.407:  (F) afn: AF_IP(1), type: IP(800), hop: 254, ver: 1
Jul 28 09:39:23.407:      shtl: 4(NSAP), sstl: 0(NSAP)
Jul 28 09:39:23.407:      pktsz: 92 extoff: 52
Jul 28 09:39:23.407:  (M) flags: "router auth src-stable nat ", reqid: 2
Jul 28 09:39:23.407:      src NBMA: 209.165.202.130
Jul 28 09:39:23.407:      src protocol: 10.50.50.3, dst protocol: 10.50.50.2
Jul 28 09:39:23.407:  (C-1) code: no error(0)
Jul 28 09:39:23.407:        prefix: 32, mtu: 17876, hd_time: 7200
Jul 28 09:39:23.407:        addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref: 0
```

Figure 6-26 debug nhrp packet Output

That wraps up key commands and concepts you need to know for troubleshooting FlexVPN deployments.

Summary

In this chapter we introduced FlexVPN technology, including the extensive benefits of FlexVPN capabilities. We covered learning objectives included on the SVPN 300-730 exam such as hub-and-spoke and spoke-to-spoke configuration. As you learned in this chapter, FlexVPN supports remote connectivity clients such as AnyConnect. Like the previous chapters, we used

a building block model as the roadmap for configuration and troubleshooting success. Make sure to master both hub-and-spoke as well as spoke-to-spoke deployments and troubleshooting before attempting the SVPN exam.

At this point, we have covered all of the site-to-site VPN topics needed to meet the learning objectives of the SVPN exam. The final site-to-site VPN topic that needs to be covered before we move into remote access VPN concepts is troubleshooting, which makes up the largest learning objective on the SVPN exam. Make sure you have a firm understanding of IPsec, DMVPN, and FlexVPN before moving to the next chapter.

References

FlexVPN IPv6 in Hub and Spoke Deployment Configuration Example. Retrieved from https://www.cisco.com/c/en/us/support/docs/security/flexvpn/116528-config-flexvpn-00.html

Good general info DMVPN vs FlexVPN. Retrieved from https://packetpushers.net/cisco-flexvpn-dmvpn-high-level-design/?doing_wp_cron=1589135866.2408781051635742187500

Great troubleshooting and good example. Retrieved from https://integratingit.wordpress.com/2016/07/10/configuring-cisco-flexvpn-hub-and-spoke/

Introduction to FlexVPN. Retrieved from https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/15-mt/sec-flex-vpn-15-mt-book.pdf

Troubleshooting FlexVPN. Retrieved from https://www.cisco.com/c/en/us/support/docs/security/flexvpn/116032-flexvpn-aaa-config-example-00.html

Exam Preparation Tasks

As mentioned in the section “How to Use This Book” in the Introduction,

you have a couple of choices for exam preparation: the exercises here, Chapter 11, "Final Preparation," and the exam simulation questions in the Pearson Test Prep software online.

Review All Key Topics

Review the most important topics in the chapter, noted with the key topics icon in the outer margin of the page. Table 6-7 lists these key topics and the page number on which each is found.

Table 6-7 Key Topics for Chapter 6

Key Topic Element	Description	Page Number
List	FlexVPN advantages summary	
Table 6-2	Benefits of IKEv2	
Table 6-3	FlexVPN Capabilities	
Figure 6-2	FlexVPN Capabilities	
Figure 6-3	FlexVPN Per-Peer Options	
Figure 6-4	FlexVPN Building Blocks	
List	FlexVPN components	
Table 6-5	Smart Defaults	
Figure 6-7	FlexVPN Building Blocks Configuration Flow	
Table 6-6	FlexVPN Troubleshooting Commands	

Complete Tables and Lists from Memory

Print a copy of Appendix C, "Memory Tables" (found on the companion

website), 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 companion website), 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:

Internet Key Exchange Version 2 (IKEv2)
pseudorandom function (PRF)
Extensible Authentication Protocol (EAP)

Part III: Remote Access Virtual Private Network

Chapter 7. Remote Access VPNs

This chapter covers the following subjects:

- **Remote VPN Architecture:** This section provides an overview of what you need to consider as you develop a remote VPN architecture.
- **Remote Access Components:** This section reviews Cisco technology that supports remote access VPN as well as other possible technology components and configurations commonly used with remote VPN deployments.
- **Encryption Algorithms:** This section covers fundamental concepts behind encryption used within VPN technology.
- **High Availability:** This section takes a quick look at different high availability options for remote VPN deployments.
- **Cisco ASDM Remote Access Configuration:** This section shows how to configure a remote access VPN on a Cisco ASA using Cisco ASDM.
- **Cisco ASA CLI Remote Access Configuration:** This section shows how to configure a remote access VPN on a Cisco ASA using command line.
- **Cisco Secure Firewall Remote Access VPN:** This section shows how to configure a remote access VPN on a Cisco Secure Firewall appliance.
- **Cisco Meraki Remote Access VPN:** This section shows how to configure a remote access VPN on a Cisco Meraki solution
- **Remote Access on Cisco Router:** This section shows how to configure a remote access VPN on a Cisco router.

"When people are free to choose where in the world they want to work, they simply enjoy their day-to-day work more."

—Brian De Haff

We live in a world driven by information. People access social media, make

purchases, and send digital messages at any point from anywhere using mobile devices. According to an article by Pew Research Center, as of early 2019, more than 5 billion people on the planet had mobile devices, and more than half of those devices were smartphones. The workforce expects the same type of access to work-related data as to personal data, and your organization can be exposed to risk if proper security measures are not put in place while providing such access. You need a way to balance the productivity benefits of allowing employees access to corporate data from anywhere in the world while maintaining security that protects that data from unauthorized access. Remote access VPN technology, if implemented properly, can help solve this challenge.

This chapter looks closely at remote access VPN concepts and configuration. It covers the technology you need and how to properly scope a remote access VPN project. This chapter provides examples of how to configure basic remote access VPNs on different Cisco technologies as well as design best practices, such as how to build high availability into your remote access architecture. The format of this chapter similar to the format of Chapter 3, "Site-to-Site VPNs." The chapters that follow go even deeper into specific Cisco remote access VPN concepts. You will want to master this chapter before proceeding to those chapters.

Tip

We highly recommend taking notes and researching any concepts that are new to you to ensure that you fully understand each topic covered.

This chapter covers the following exam objectives:

- 2.0 Remote Access VPNs
  - 2.1 Implement AnyConnect IKEv2 VPNs on ASA and Routers
- 4.0 Secure Communications Architectures
  - 4.2 Describe Functional Components of FlexVPN, IPsec, and Clientless SSL for Remote Access VPN Solutions

- 4.6.a VPN Technology Considerations Based on Functional Requirement

- 4.7 Design Remote Access VPN Solutions
  - 4.7.a VPN Technology Considerations Based on Functional Requirements
  - 4.7.b High Availability Considerations
  - 4.7.c Clientless SSL Browser and Client Considerations and Requirements
- 4.8 Describe Elliptic Curve Cryptography (ECC) Algorithms

Learning beyond the SVPN concepts:

- Remote Access Architectures
- Remote Access Components
- Remote Access Design Considerations
- Cisco Secure Firewall
- Cisco Meraki
- Remote Access on Cisco Router

"Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz enables you to assess whether you should read the entire chapter. If you miss no more than one of these self-assessment questions, you might want to move ahead to the "Exam Preparation Tasks" section of the chapter. Table 7-1 lists the major headings in this chapter and the "Do I Know This Already?" quiz questions related to the material in each of those sections to help you assess your knowledge of these specific areas. The answers to the "Do I Know This Already?" quiz appear in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes."

Table 7-1 "Do I Know This Already?" Foundation Topics Section-to-Question Mapping

Foundation Topics Section	Questions
Remote VPN Architecture	1, 10
Remove VPN Components	2–5
High Availability	6
Cisco ASDM Remote Access Configuration	7
Cisco ASA CLI Remote Access Configuration	13
Firepower Remote Access VPN	12
Cisco Meraki Remote Access VPN	11
Router Configuration	8, 9

1. What are the two fundamental components of a remote access VPN architecture?

a. A VPN concentrator and endpoint

b. A user and client-side software

c. A network access server (NAS) and client-side software

d. Encryption and an endpoint

2. Which of the following is not a Cisco appliance option that offers remote access VPN service?

a. Cisco Adaptive Security Device Manager (ASDM)

b. Cisco Adaptive Security Appliance (ASA) Series

c. Cisco Firepower Series

d Cisco Meraki MX Series

3. Which of the following is not a supported VPN protocol choice for Cisco AnyConnect?

a. SSL

b. TLS

c. DTLS

d. IPsec IKEv2

e. SHA256

4. Which of the following is not an option for deploying Cisco AnyConnect to an endpoint for a VPN setup?

a. Automatically launch installation upon connection

b. Download AnyConnect from cisco.com

c. Use Windows ActiveX to push Cisco AnyConnect to an endpoint

d. Use Java to push Cisco AnyConnect to an endpoint

5. What is the difference between clientless mode and thin client mode?

a. Thin client mode allows for applications such as POP3, SMTP, IMAP, Telnet, and SSH.

b. Thin client mode provides secure access to private web resources and private content.

c. Clientless mode extends cryptographic functions to enable remote access TCP-based applications.

d. Clientless mode allows for a full tunnel, and thin client doesn’t

6. What is a value of using high availability between two standalone ASAs instead of using a cluster?

a. User connections are shared between systems.

b. If an outage occurs, the secondary ASA picks up the VPN connections.

c. If an outage occurs, users do not disconnect.

d. After an outage, users have to reestablish the VPN, which occurs automatically.

7. When using the AnyConnect wizard in ASDM, which of the following is *not* a step in the wizard configuration process?

a. Choose Client image

b. NAT exempt

c. Select VPN protocols

d. Encryption selection

8. Which of the following is *not* a feature included with a SEC-K9 bundle?

a. BGP

b. IKEv1/IPsec/PKI

c. Easy VPN with DVTL

d. DMVPN

9. What step is needed to enable SSLVPN on a Cisco IOS router running Release 15.3 or greater software?

a. Nothing. Cisco IOS Release 15.3 has SSLVPN already enabled.

b. Install a special LIC file along with a SEC-K9 bundle.

c. Install a special LIC file.

d. Nothing is needed. Just boot a SEC-K9 technology package.

10. Which of the following is *not* true?

a. A VAM may be needed to enable FlexVPN.

b. All Cisco routers support FlexVPN with some type of configuration, license, or hardware.

c. Sometimes additional hardware is required, such as an Integrated Services Router adapter, for a router to support FlexVPN.

d. Some Cisco routers require special software to support FlexVPN.

11. Which tunneling protocol is used by a Meraki security appliance for remote access VPN service?

a. PPTP

b. L2F

c. OpenVPN

d. L2TP

12. Which of the following is not true regarding Cisco Firepower Threat Defense support for remote access VPNs?

a. Cisco Firepower Threat Defense supports up to three AAA servers.

b. Cisco Firepower Management Center supports all combinations, such as IPv6 over an IPv4 tunnel.

c. Cisco Firepower Threat Defense supports multiple interfaces.

d. Cisco Firepower Threat Defense supports both SSL and IPsec/IKEv2.

13. What is the CLI command to create a tunnel group on a Cisco ASA?

a. ASA1(config)# **tunnel-group MYTUNNELGROUP type ipsec-ra**

b. ASA1(config)# **tunnel-group type MYTUNNELGROUP ipsec-ra**

c. ASA1(config)# **tunnel-group MYTUNNELGROUP type**

d. ASA1(config)# **tunnel-group ipsec-ra type MYTUNNELGROUP**

Foundation Topics

Demands for simple ways to provide remote access to sensitive systems and

data will continue to grow as organizations move away from having employees work only from a physical office. Every organization, regardless of business sector, is looking at different forms of work-from-anywhere strategies because it not only offers huge benefits but is just what is being expected from the future workforce. Gartner and other analysts have identified work-from-anywhere trends and have made predications that by 2026, 40% of enterprises will be using a cloud-based form of security coined by the industry as Secure Access Services Edge (SASE), pronounced *Sassy*.

One option for delivering cloud security services is using remote access–based VPN technology to force traffic through a range of security features delivered through cloud providers. When most of the planet was forced to work from home during the 2020 COVID-19 pandemic, the work-from-anywhere concept was put to the test for many organizations that had previously offered limited work-from-home flexibility. Today, all major technology providers are looking to the cloud as the future of how they will deliver services, and secure remote connectivity is essentially a foundational requirement. We point this out because the specific remote access VPN concepts covered in this book may change as SASE technology evolves, but the foundational remote access concepts will remain as security technology makes its journey to the cloud.

A remote access VPN enables individual users to establish a secure connection with a remote computer network. The challenge many organizations face is not only provisioning such access but enforcing least-privilege access best practices and providing only the access needed to meet that user's business requirements—and nothing more. However, allowing remote access can be challenging for many organizations as there may be many types of users who need to be authenticated, different levels of access that continuously need to be authorized, and accounting that needs to be included to monitor how resources are accessed. The goals of this chapter and the next few chapters are to give you tools and techniques to address a variety of remote-access VPN challenges and help you answer remote access questions on the SVPN 300-730 exam. This chapter focuses on foundational remote access VPN concepts.

Remote VPN Architecture

Chapter 2, "Introduction to Virtual Private Networks (VPNs)," describes the two categories of VPN technology: site-to-site and remote access VPNs. Remote access VPN technology provides individual users access to remote networks and resources. Individual users could be using various types of devices, ranging from laptops to mobile phones as well as different operating systems and web browsers. Imagine accommodating any type of user, such as an Android phone user who only requires access to a specific internal application or an administrator who requires full access to the inside network from a Windows desktop. Such factors will impact the approach that is recommended for your remote access VPN project. The good news is that proven remote access VPN concepts have been around for a while, and options for provisioning VPNs continuously mature as mobile device technology advances.

The first version of remote access VPN technology relied on dial-up networks. If you are old enough to have experienced dial-up, you have probably heard people talk about the loud screech sounds and the slow and unreliable service. We have come a long way from dial-up networks. VPNs today provide much better performance speed, and reliability—and even options for high availability.

NAS and Client-Side Software

Today's remote access VPN architectures require two fundamental components. First, you need some form of *network access server (NAS)*—also called a media access gateway or remote access server [RAS])—which can be a dedicated server or a software application. A remote user connects to a NAS in order to access the trusted network from an untrusted outside network (typically the Internet). The NAS is responsible for validating user credentials using its own authentication process or by referencing a separate authentication solution. Cisco Adaptive Security Appliance (ASA) is an example of a Cisco NAS option.

The other required component of a remote access VPN is the client-side software, which is the VPN technology on the system attempting to access the NAS. Most modern operating systems have built-in software that supports remote access VPN solutions. However, some operating systems require

additional or alternative software, depending on what and how the VPN technology is configured. Cisco AnyConnect is an example of remote access VPN software that can be deployed on various device types, from tablets, phones, and laptops to desktops and servers. Figure 7-1 provides a high-level diagram of how these components work.

Figure 7-1 Using a NAS and Client-Side Software

Remote Access Technology Considerations

There are many options for the NAS and client software you could use for a remote access VPN project. To determine which remote access VPN is the right option for your project, you need to consider a number of factors. When we consult with customers regarding how to architect their remote access VPN project, we ask a series of questions to narrow down options to the best possible choices. Considering the following questions will give you a good start in determining the remote access VPN project that would be ideal for your VPN needs:

- What is your budget?
- What technology is available for the VPN project?
- What authentication requirements do you face?
- What is the current workload on the devices and the network?

- What types of devices do you expect to connect to the solution?
- What locations in the world need to connect to the solution?
- How many users do you expect to use the solution?
- What kind of growth do you expect in the future?
- What are your high availability and network resilience requirements?
- What are the existing skillsets and technology familiarity in your organization?
- What are your in-house versus external management expectations for the solution?
- What compliance requirements does your organization need to meet?

This list is similar to the questions you need to consider for site-to-site VPNs (refer to Chapter 3) but with slight changes for identifying information about endpoints. Some of the answers to these questions need to be more heavily weighted than others. Available technology is typically a huge influencer because organizations do not want to buy new technology if they have existing technology that will work. Many security tools include remote access VPN capabilities; sometimes they require an additional cost for licenses, and other times it is only necessary to ensure that the remote access VPN is enabled and configured. Available budget and regulatory compliance requirements are very important factors. For example, if a certain level of encryption is required, many lower-end remote access VPN options will not be available for your deployment.

Another important factor is the type of remote access VPNs supported by the technology being used. Answers to questions about the types of endpoints and required encryption will narrow down the possible options for your remote access VPN project.

Sizing requirements are based on the number of expected devices, expected growth, and redundancy requirements. If you don't know the expected growth, using a 20% growth expectancy is a common method. This chapter covers different methods to accommodate growth, including load balancing

and flexible license options. With a flexible license, you can increase the size of a VPN solution only when needed to avoid overspending on unnecessary resources.

Note

It is critical to consider the entire lifecycle of a VPN project as you design the architecture and scope the expected level of effort. The same concepts described for assessing a site-to-site VPN project in Chapter 3 also apply to scoping a remote access VPN project.

Remote Access Components

Chapter 3 groups the hardware required for a site-to-site VPN into two groups: *security appliances* and *network routers*. Many of the same technologies covered for site-to-site VPNs also offer remote access VPN capabilities, depending on available resources, licenses, and configurations. Many network devices and security appliances can fulfill the role of the NAS for a remote access VPN. Each NAS has different options and limitations on the number and types of VPN clients that can be supported. This chapter provides configuration examples for a Cisco ASA acting as the NAS and Cisco AnyConnect acting as the VPN software client. It also covers Cisco IOS routers fulfilling the NAS role and Cisco Firepower as the software client.

Remote Access Capable Routers

Chapter 2 provides an overview of Cisco technologies that offer VPN capabilities. Most of those technologies support both site-to-site and remote access VPNs. When it comes to the NAS role, routers are as popular as security appliances, although security appliances offer more feature-rich NAS capabilities.

The following are some Cisco router series that offer remote access VPN

capabilities:

- 4000 Series Integrated Services Router (ISR)
- 900 Series ISR
- 800 Series ISR
- UC/SR500, 870, 880, and 890 Series routers
- 1800 and 1900 fixed routers
- 1841 and 1941 routers
- 2811, 2821, 2901, 2911, 2921, 2851, and 2951 routers
- 3800 and 3900 series routers
- 1000 Series Aggregation Services Router (ASR)

One or the most common router-based remote access VPN approaches is using *FlexVPN*, which is the focus of Chapter 6, "FlexVPN Configuration and Troubleshooting." Some Cisco routers require certain software images to support FlexVPN, as well as sometimes additional hardware, such as an ISR adapter or a VPN Acceleration Module (VAM). Some routers do not support FlexVPN. Make sure to validate requirements using the associated data sheet with the NAS you plan to use.

Figure 7-2 shows some of the advanced software licenses that are available for the Cisco 1900, 2900, and 3900 Series ISR. Notice that the SEC bundle is required for VPN capabilities. (We cover how to configure an IOS remote access VPN later in this chapter, including how to validate the IOS images that are installed.)

Figure 7-2 IOS Advanced Software Bundle Example

Remote Access Capable Security Appliances

Cisco security appliances also offer both site-to-site and remote access capabilities. Each offering has different hardware limitations and license options, which will determine if and how many VPN sessions are supported. As with routers, the Cisco security appliance hardware limitations can be found by looking at a model's data sheet. Keep in mind that certain licensing may be required to be installed before a security appliance can be configured as a NAS. The Cisco security appliance series that support remote access capabilities include the following:

- Cisco Adaptive Security Appliance (ASA) Series
- Cisco Firepower Series
- Cisco Meraki MX Series

After you select your NAS, you must install and configure which types of VPN clients will be supported. Options could include IKEv2 remote access clients, Android, Apple or Microsoft L2TP/IPsec clients, and Bluefire clients to name a few. The most popular VPN client from Cisco is AnyConnect, which is the VPN software client you are expected to know for the SVPN 300-730 exam.

AnyConnect Secure Mobility Client

Cisco AnyConnect Secure Mobility Client can act as the endpoint client for a remote access VPN deployment and is the client used for most examples in this book. One really cool feature AnyConnect offers is that it can leverage always-on intelligence, which means it can choose to automatically enable or disable the VPN; the VPN can automatically turn on when a device is connected to an untrusted network, which is typically configured with any non-inside network IP address range. Many organizations that allow employees to manually enable the VPN find that the VPN is not always enabled in practice, and remote users are exposed to external threats. People might not understand the technology, and they may either be lazy or fail to understand how important it is to protect themselves while connected to untrusted networks; they also may just not care about security and forget to click the VPN enablement button on their VPN client while they're off the internal network. The best practice is to configure the client to automatically connect.

User Experience

AnyConnect has options to ensure that end users get a very good VPN experience. AnyConnect can select the best network access point and adapt its tunneling protocol to the most efficient method. This allows for maximum performance when there are different connection points/NAS options available for the user to leverage for a VPN connection. Adaptation could include considerations for voice over IP (VoIP) traffic, TCP-based application access, or use of Datagram Transport Layer Security (DTLS) protocol for latency-sensitive traffic. For example, a traveling salesperson might attempt to connect to a NAS while on the road. With AnyConnect, the salesperson doesn't have to know which NAS will provide the best performance from wherever they are in the world because AnyConnect can figure it out automatically.

AnyConnect Protocol Support

AnyConnect-supported VPN protocol choices include SSL for TLS, DTLS, IPsec, and IKEv2. DTLS is an ideal option if AnyConnect will be supporting

latency-sensitive traffic such as VoIP traffic. If IPsec is desired, IKEv2 is also available to accommodate latency-sensitive traffic. Encryption support includes AES-256, 3DES-268, Suite B algorithms, ESPv3 with IKEv2, 4096-bit RSA keys, Diffie–Hellman group 24, and enhanced SHA-2. We will look more closely at VPN encryption later in this chapter.

AnyConnect Security Capabilities

The real value of AnyConnect is its ability host multiple security offerings beyond VPN options. AnyConnect can perform posture checks of endpoints, including assessments and remediations of the status of antivirus, personal firewall, and antispyware products. Validating posture can reduce the risk of permitting onto the network endpoints that are vulnerable because they fail to meet minimum security requirements. AnyConnect can check posture or act as a supplicate for Cisco ISE, with ISE also performing posture checking. (An additional Apex license is required for the ISE posture checking feature.)

Other built-in features in AnyConnect include web security, malware threat defense, phishing protection, and command and control callback blocking. Web security leverages either the premises-based Cisco Secure Web Appliance or cloud-based Cisco Secure Web security. When AnyConnect is not providing VPN protection, a cloud roaming security service called Cisco Umbrella Roaming can be automatically enabled. Cisco AnyConnect has a Network Visibility Module (NVM) that allows tools such as Cisco Secure Network Analytics (formally called Stealthwatch) to gain visibility into the endpoint to add anomaly and behavior-based security capabilities. Another antimalware option in AnyConnect is Cisco Secure Endpoint (formally called Advanced Malware Protection [AMP]), which can act as a signature-based antivirus as well as anomaly behavior-based antimalware. As you can see, Cisco AnyConnect is more than a VPN client, and you can enable a number of capabilities, depending on how you customize your AnyConnect deployment.

Figure 7-3 provides a high-level overview of the features that can be enabled using Cisco AnyConnect. Keep in mind that some of these features require additional licenses and technology.

Key Topic

Figure 7-3 Cisco AnyConnect Options

AnyConnect Platform Support

There are AnyConnect options available for most versions of Windows, macOS X, Linux, and different mobile devices. The different options are associated with AnyConnect client profiles.

When you deploy a remote access VPN offering, you need to consider the types of devices that will be using the VPN solution. Different operating systems, such as Windows or macOS, require different types of installation and support packages.

AnyConnect can be deployed to hosts using a Microsoft installer, automatically launched when a host connects to the NAS, or launched using Windows, ActiveX, and Java. Links to the NAS can be distributed using most communication methods so that employees can simply click a link, be redirected to the NAS, and start the AnyConnect installation process. Admin rights to install software are required to install AnyConnect on a host.

Cisco offers many client packages that are designed for the various types of endpoints you are likely to encounter. Depending on the technology being used, you are likely required to download different packages for the expected device types. For example, you will see later in this chapter how to deploy a remote access VPN solution using a Cisco ASA, with options for downloading Windows, Linux 64-bit, and macOS client packages. Figure 7-4 shows an example of some of the AnyConnect client options that you can download from Cisco.

Figure 7-4 Examples of AnyConnect Client Packages

Some configuration elements must be applied to an installation package, and these elements influence how you set up the client profile. For example, you must tell the installation package where the VPN NAS is located, what types of security protocols to use, what VPN option are available, and many other details that get bundled in with the AnyConnect installation package as you build your remote access VPN setup. For Cisco IOS routers, there isn't a built-in configuration tool to configure the AnyConnect client. Instead, you need to use an editor.

Note

A client profile is required to tell the installation package what it should do.

AnyConnect Profile Editor

The Cisco AnyConnect security mobility client software package includes a profile editor for all operating systems. For example, ASDM activates the profile editor when you load an AnyConnect client image on the ASA. IOS, on the other hand, does not offer this option. Instead, you can use a standalone profile editor that runs on Windows, or you can create a profile in ASDM and export it for your routers.

AnyConnect VPN Profile Example

Let’s look at how to build a customized AnyConnect VPN profile. The result could be used on Cisco security appliances as well as Cisco IOS remote access VPN deployments.

This example uses ASDM rather than the standalone option. You need to first create a client profile before you can edit it. Follow these steps:

Step 1. Log in to ASDM by going to **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **AnyConnect Customization/Localization** > **AnyConnect Client Profile**. Figure 7-5 shows two existing profiles: one that is for a Cisco Umbrella roaming client and an existing SSLVPN profile.

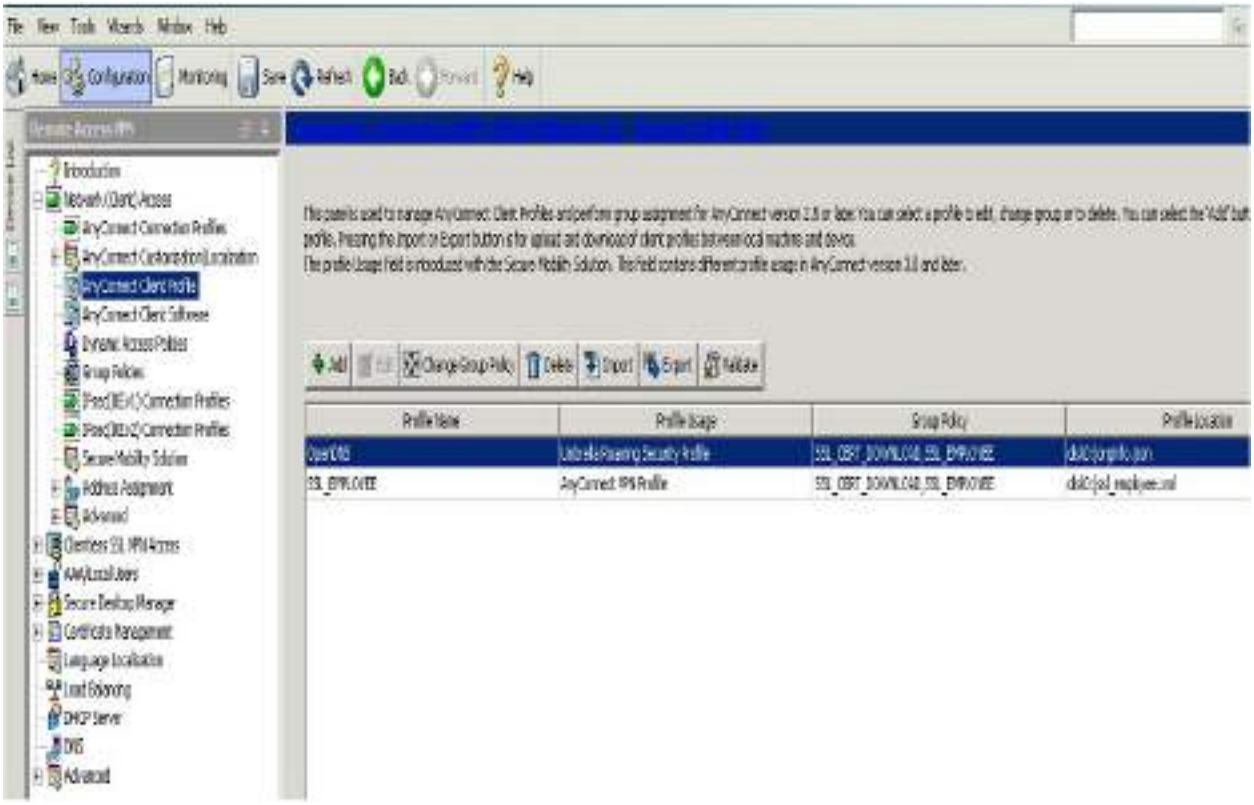


Figure 7-5 Creating a Client Profile

Step 2. Configure a new profile by clicking the **Add** button and specifying a profile name, usage (in this case, AnyConnect VPN), location for the file, and which group policy it should be assigned to (see Figure 7-6). The usage could range from the Umbrella client to what you want in this case, which is an AnyConnect VPN profile.

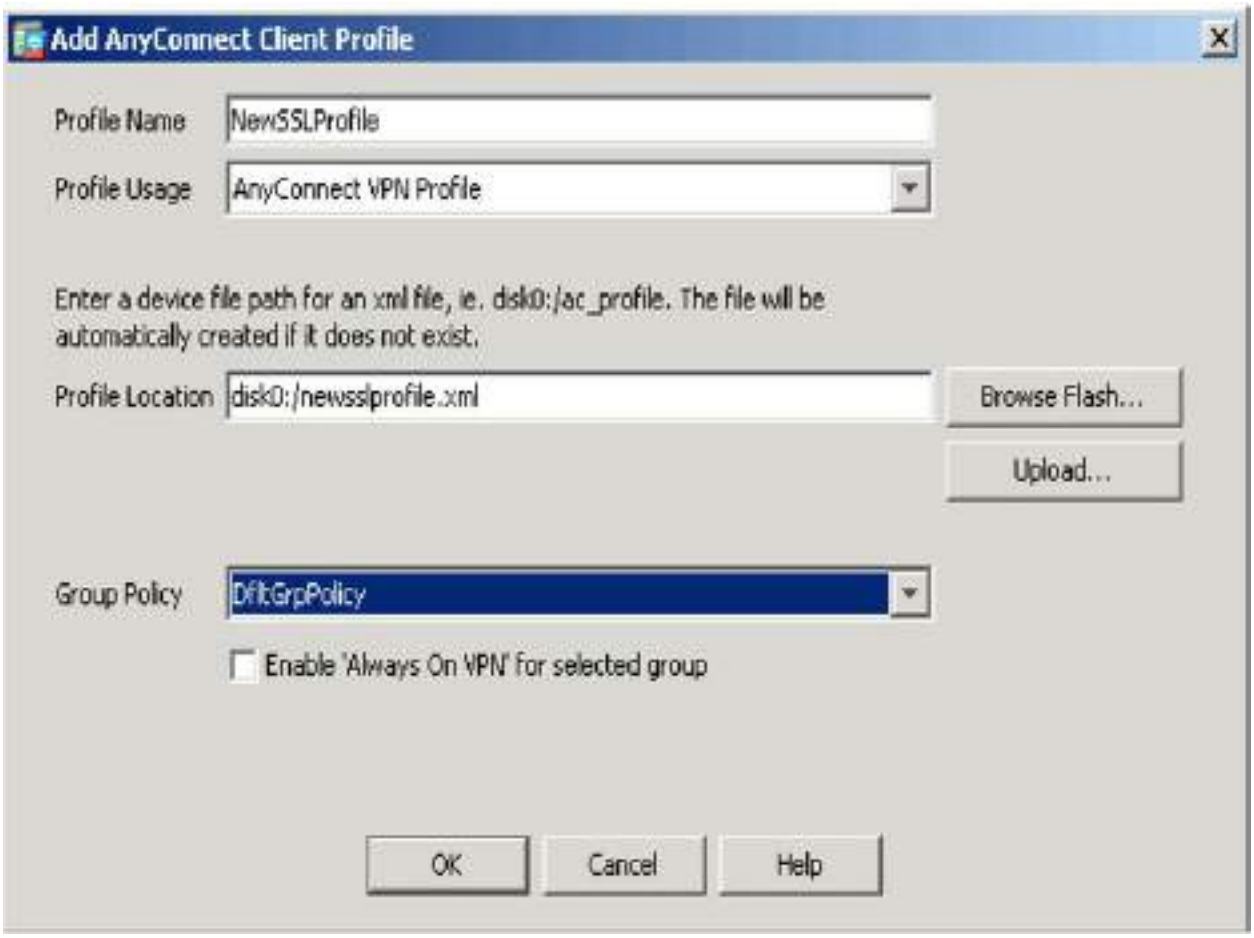


Figure 7-6 Configuring a New Profile

Step 3. Select the new profile and click the **Edit** button. Notice the option to export this as well as import other profiles if you already have a profile ready to go (see Figure 7-7).

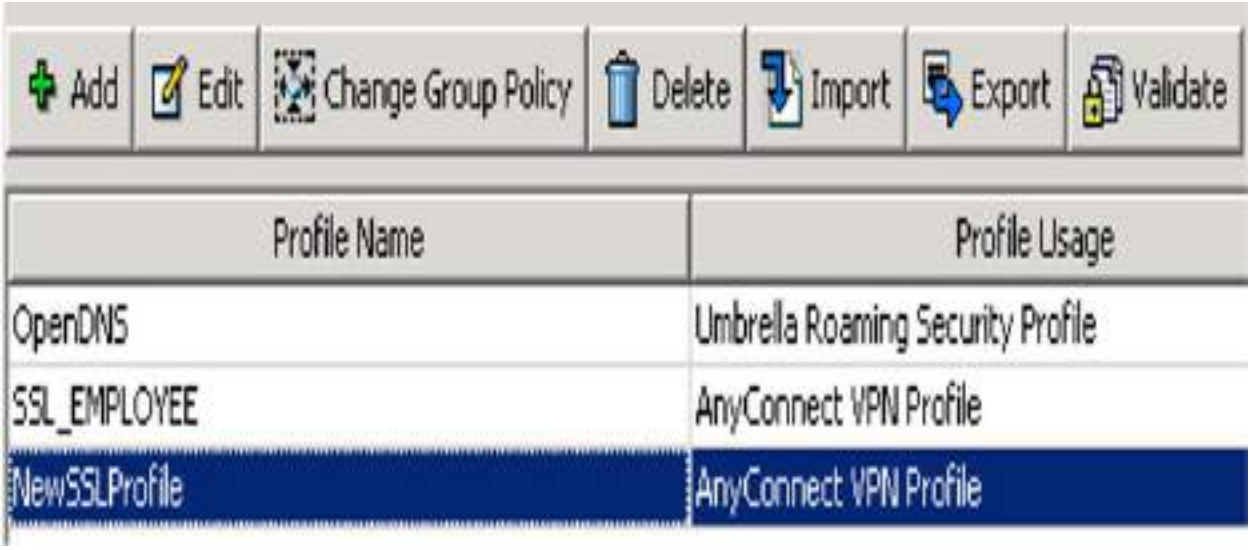


Figure 7-7 Importing and Exporting Profiles

Clicking Edit on a profile will bring up several options. You can find a detailed document covering each specific item on Cisco.com. Here is a summary of the main sections:

- **Preferences Part 1:** Includes various check box options, such as what will be seen before the user logs in, what is controllable by the user, protocol support, auto upgrade options, RSA integration options, and Windows logon and VPN establishment options.
- **Preferences Part 2:** Addresses certificate selection, whether local proxies are permitted, gateway selection, and automatic VPN policies. You can set PPP exclusion options, scripting options, and whether and for how long the VPN remains upon logout.
- **Backup Servers:** Allows a list of backup servers the client would use in case the user-selected server fails.
- **Certificate Pinning, Matching, and Enrollment:** Provide options for configuring how certificates are used by the remote VPN solution.
- **Mobile Policy:** Offers the option to require a device lock as well as some settings for device locking. This is ideal when a mobile device is being used for a remote access VPN.

- **Server List:** Provides where the client should go to find the VPN NAS. If you are using either an appliance option such as a Cisco ASA or a Cisco IOS router as the headend, you need to specify the FQDN that you configured while setting up the router as the NAS device.

Caution

You must include a fully qualified domain name or IP address to ensure that AnyConnect knows where the servers are located. It is highly recommended to include at least one backup server for high-availability purposes.

Once you have configured your AnyConnect client profile, you can save it to ASDM if you are using it on that specific deployment or export it for another deployment. In our previous example using an IOS router as the VPN NAS, you would need to export the new AnyConnect profile and copy it over to the router (see Figure 7-8).

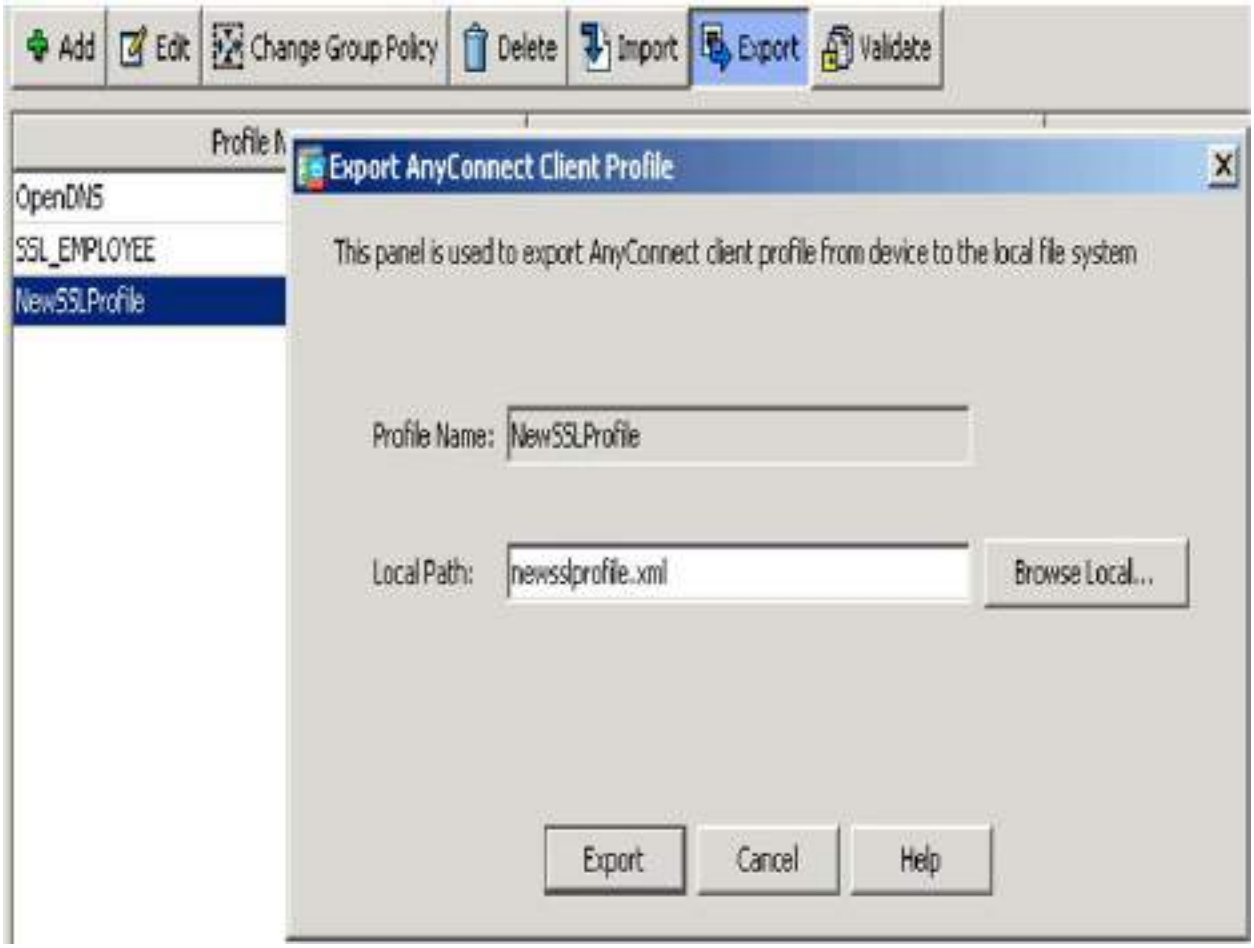


Figure 7-8 Exporting an AnyConnect Client Profile

Client profiles are essential for informing the ASA how to install the proper settings for Cisco AnyConnect. Other profile settings must be configured to provide more details about how the VPN will be used when AnyConnect is installed, and these configurations can be made with the help of connection profiles, groups, and users, discussed next.

VPN Connection Profiles, Group Policies, and Users

One commonly used security practice is to control access to a network that contains sensitive data. The security industry refers to this as a need for AAA, which stands for authentication, authorization, and accounting (and is pronounced “triple A”). With a Cisco VPN, you want to have the ability to

control who can use the VPN and what they will have access to, and you need to be able to log what is accessed. You can be accomplish all this by controlling attributes configured for groups and users.

Group Policies

A *group* is a collection of users treated as a single entry. For example, an organization made up 50 users could group administrators into the admin group, employees into an employee group, and any contractors into a contractor group. As users are placed into one of these three groups, they will get their attributes from the group policy. The Cisco ASA has a generic default group policy that applies any time a group policy isn't assigned to a user; this means all users without a group policy will fall under the generic default group policy.

Connection Profiles

A VPN *connection profile* (formerly called a tunnel group) identifies the group policy for a specific connection. A connection profile consists of a set of records that determines tunnel connection policies. Connection profile records identify the servers to which the VPN tunnel user is authenticated, as well as the accounting servers, if any, to which connection information will be sent. These records also contain protocol-specific connection parameters, including parameters identifying the default group policy for the connection.

Note

The command **tunnel-group** is used to configure connection profiles. For the SVPN 300-730 exam, make sure to remember that the terms *connection profile* and *tunnel group* refer to the same concept.

The Cisco ASA provides a few default connection profiles. You can modify these profiles, but you can't delete them. Connection profiles are local to the ASA and cannot be configured by an external server. The following are the three default connection profiles found within a Cisco ASA:

- **DefaultL2Lgroup:** Default policy for LAN-to-LAN connections
- **DefaultRAgroup:** Default policy for IPsec remote access connections
- **DefaultWEBVPNGroup:** Default policy for both browser-based and AnyConnect client-based SSLVPNs

When using connection profiles, *group policies*, and users, as an administrator, you first configure a connection profile to set the values for the VPN connection. Next, you configure group policies that set values for users, which will be inherited as users are added to the group policy. Finally, you create users and add them to group policies. We will dig into connection profiles and group policies further in configuration examples throughout this book.

Split Tunneling

One very popular VPN concept is *split tunneling*, which enables a mobile user to access dissimilar security domains such as a public untrusted network as well as a local LAN or WAN at the same time, using the same network connection or different connections. Imagine a remote employee having a coffee at a coffeeshop and requiring accessing a local coffee shop printer to print a document while also needing to download the document from the organization's internal network. In order for this to work, the remote employee will need a VPN connection to the internal organization network in order to access the document. However, if all traffic is pushed through the VPN, the user will not have access to any local coffeeshop-owned resources. Allowing this type of connection could help with productivity but could also expose the user to risk. Pushing all traffic through the VPN could also impact the NAS's performance if users consume bandwidth while streaming movies or music over the VPN.

Note

The majority of organizations use some form of split tunneling to maintain proper levels of performance for their VPN deployments.

Split tunneling is commonly designed to push services through a VPN while allowing Internet resources such as public websites or cloud services to flow outside the tunnel. The goal of designing a VPN in this fashion is to alleviate bottlenecks and conserve bandwidth since Internet traffic can be very resource intensive if video and audio streaming traffic is permitted within the organization. Rather than force a remote users' Netflix streaming through a VPN, it makes sense for many organizations to just allow that connection to occur directly from the user's local Internet connection. Another value is providing access to both protected and local resources, much as in the example of the remote employee needing to print a document using a local printer while maintaining connection to the organization's network over a VPN.

Split Tunneling Configuration

To configure split tunneling on a Cisco security solution, you first need to define the traffic for the subnets or hosts that must be encrypted. Then any other traffic can pass through a default policy that does not encrypt the traffic. You can control traffic by using an access control list (ACL) from the NAS end and pushing to the client end. The routes for subnets are installed on the client system's routing table.

Note

Split tunnel configuration occurs in the Group Policies section under Network (Client) Access.

Let's look at how split tunneling can be configured on a Cisco ASA. This example uses ASDM. Follow these steps:

Step 1. Log in to ASDM.

Step 2. Click the **Configuration** tab, select **Remote Access VPN** on the left, and select **Group Policies** in the Network (Client) Access (see Figure 7-9). This is where you will create a split tunneling policy.

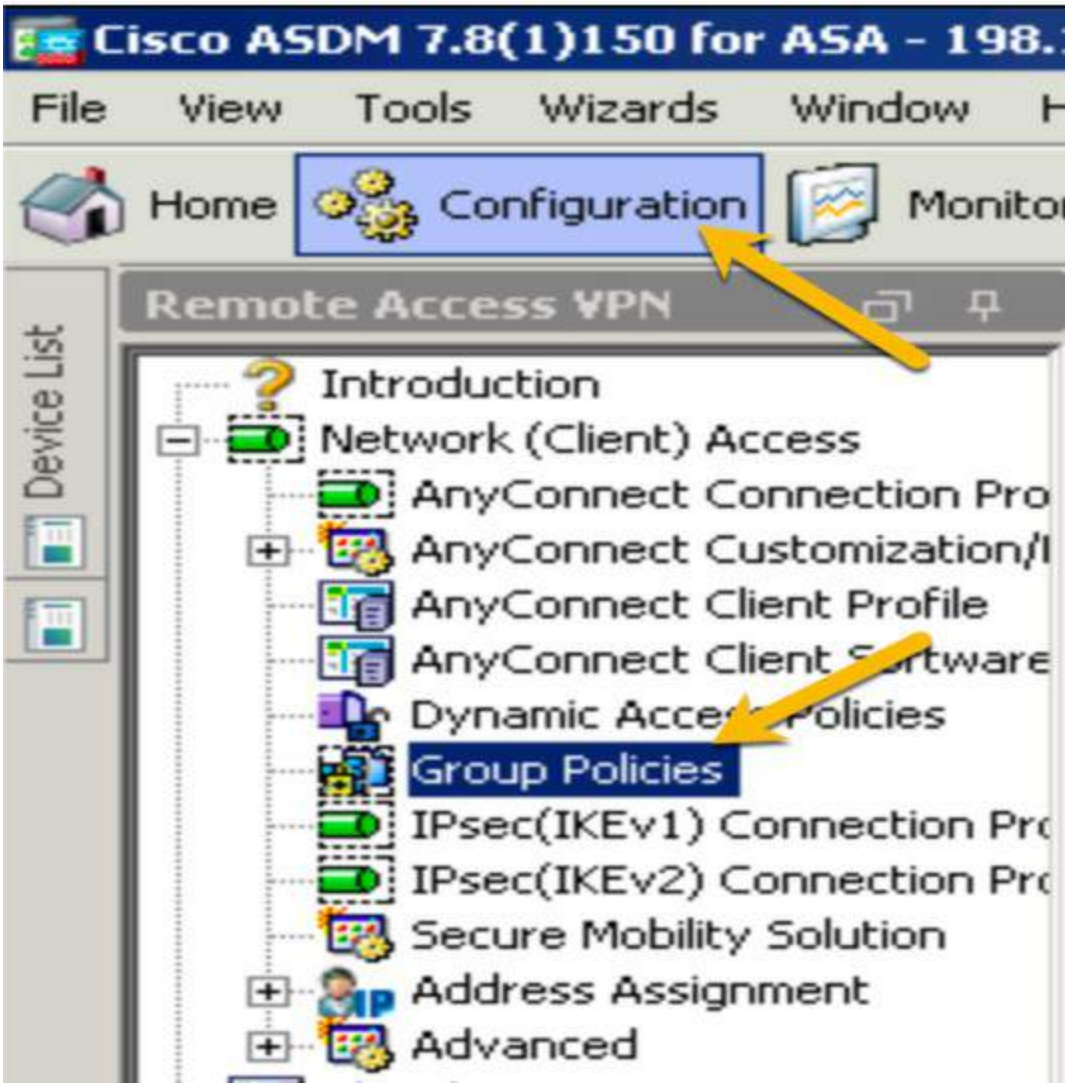


Figure 7-9 Group Policies

Step 3. Click **Edit** (see Figure 7-10) to bring up the edit window and use the navigation tree on the left to select **Advanced** > **Split Tunneling** (see Figure 7-11).

Figure 7-10 Group Policies > Edit

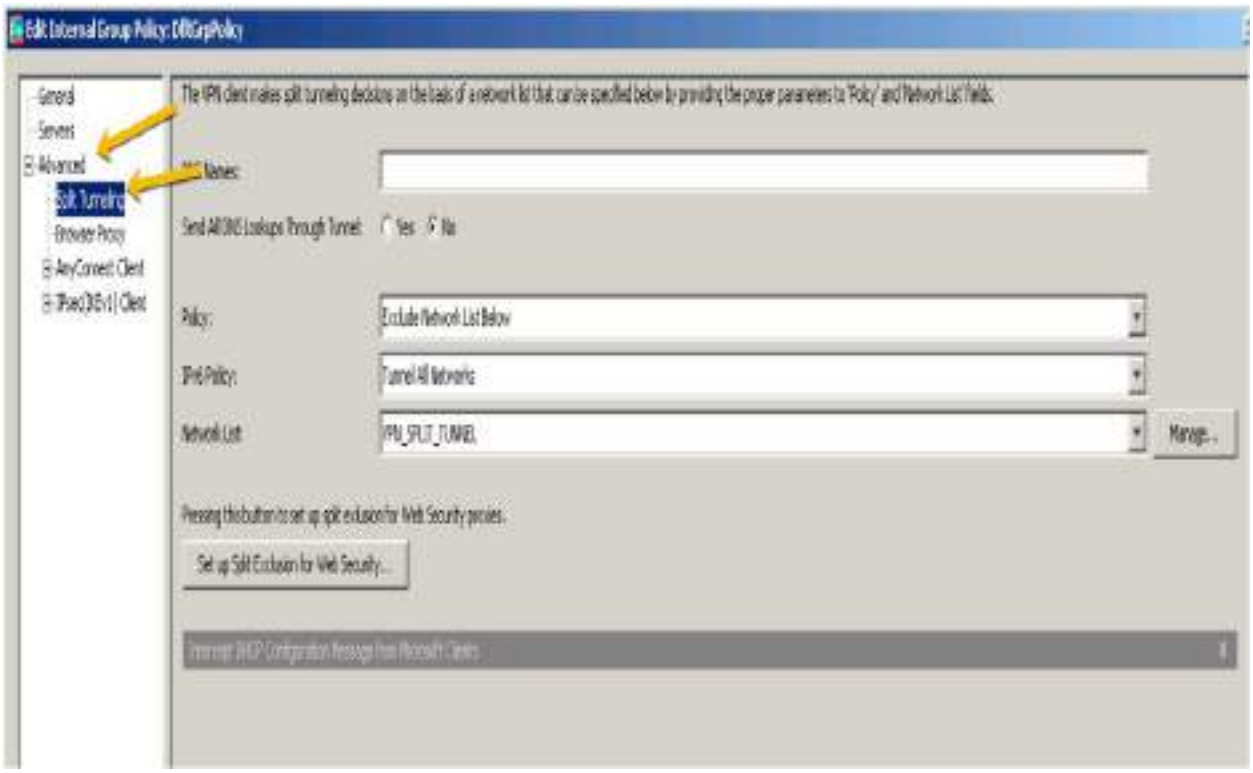


Figure 7-11 Advanced > Split Tunneling

Step 4. Click in the **IPv4 Policy** drop-down and choose **Tunnel Network List Below** (see Figure 7-12).

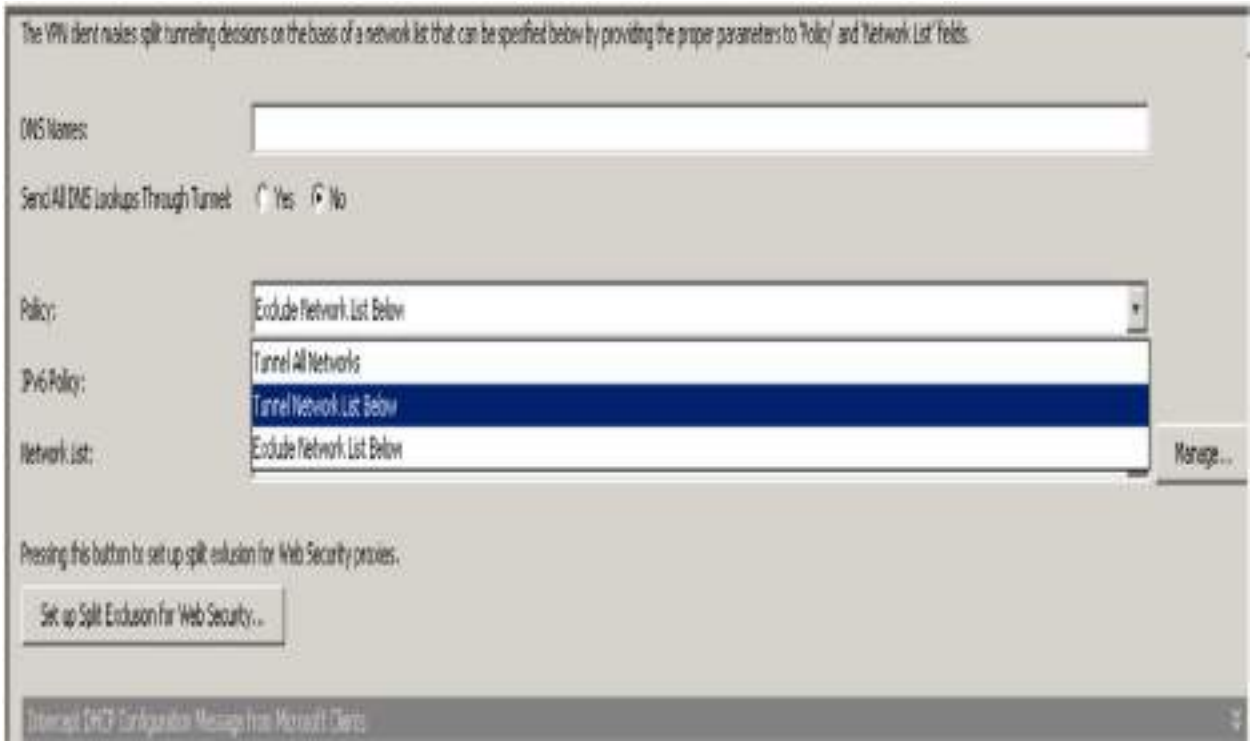


Figure 7-12 IPv4 Policy

Step 5. Click the **Manage** button to bring up the ACL options for this policy. Click **Add** to add a new standard ACL (see Figure 7-13). (This example shows ACLs already associated with the split tunnel deployment. When you create an ACL for a new split tunnel, you will not see these existing ACLs.)

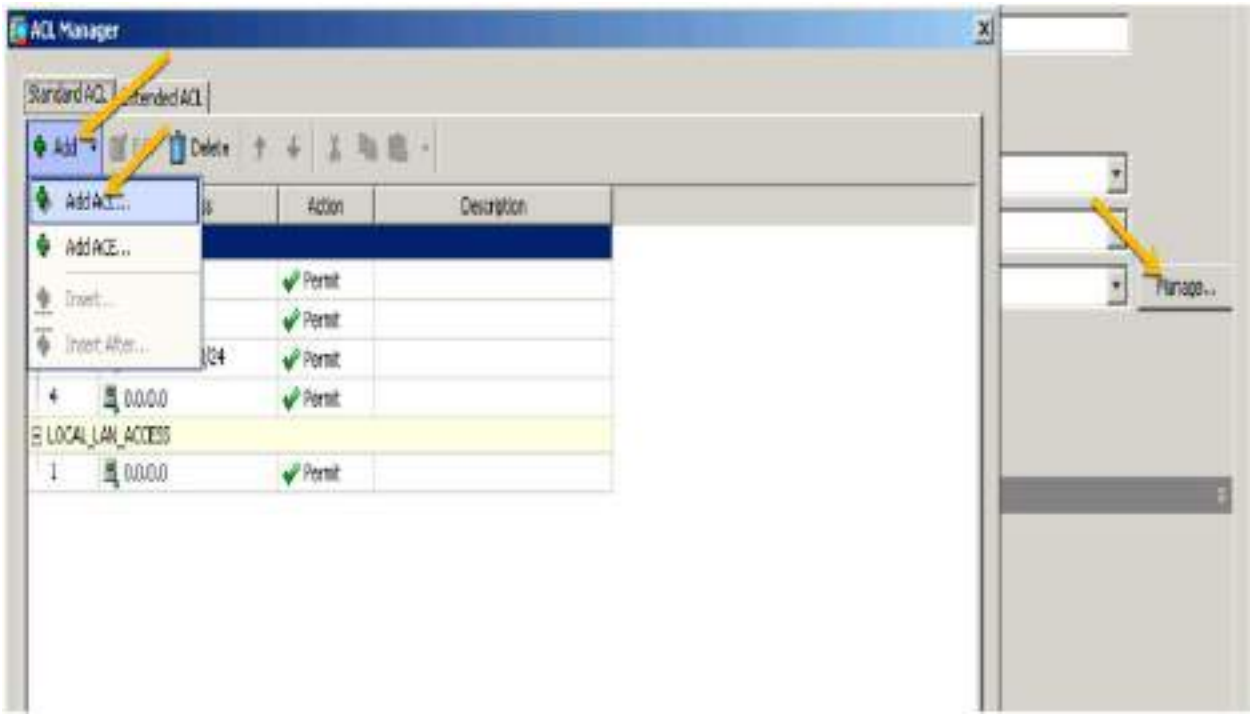


Figure 7-13 Adding an ACL

Step 6. When ASDM asks you to name your ACL, give it a name and click **OK** (see Figure 7-14).

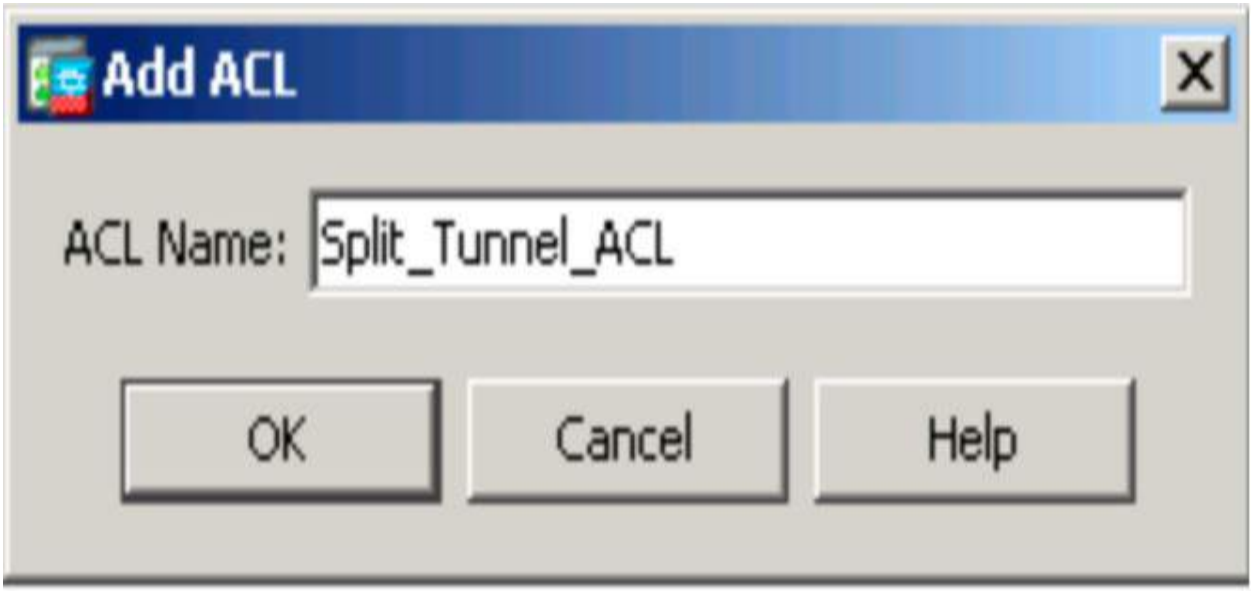


Figure 7-14 Naming the ACL

Step 7. To add access control entries (ACEs) to the ACL policy, click **Add**

while your new ACL policy is highlighted and choose **Add ACE** (see Figure 7-15).

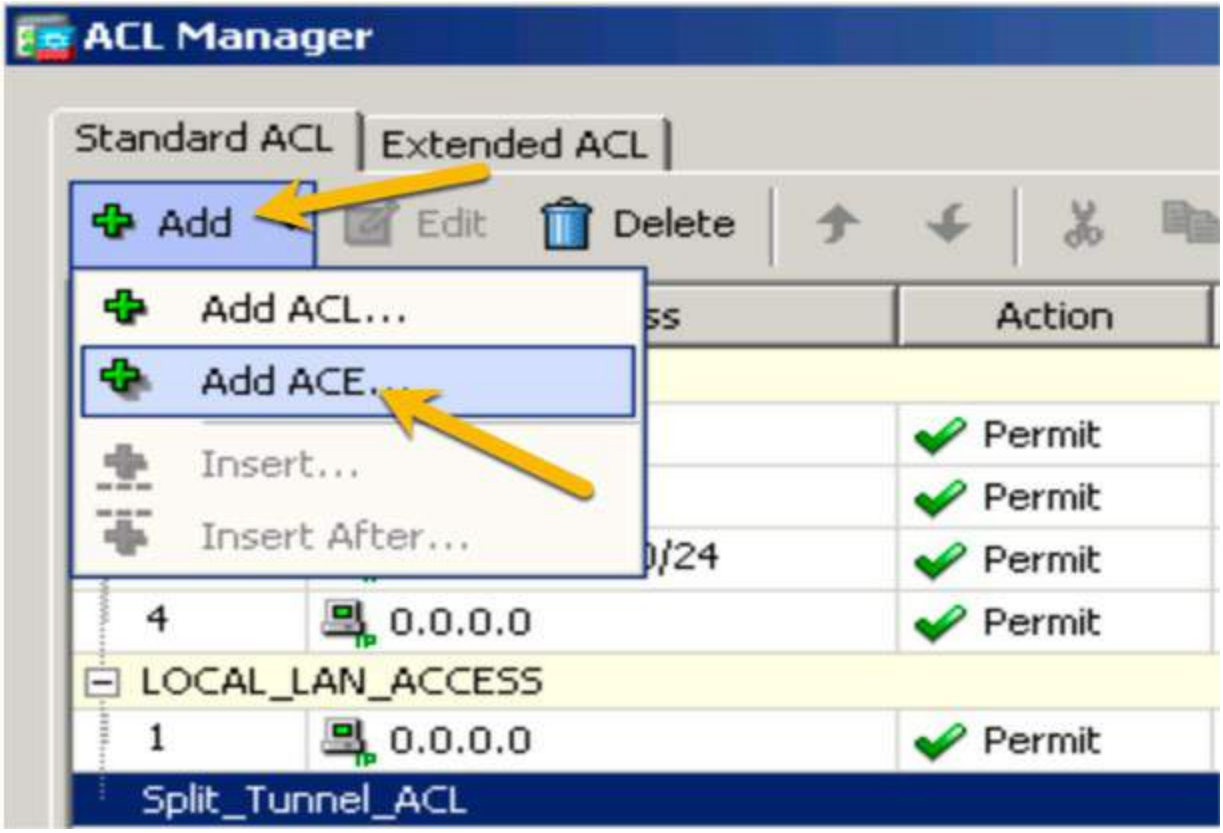


Figure 7-15 Adding an ACE to an ACL

Step 8. To choose what traffic should be encrypted through the VPN, type in the address or, if the objects already exist, click the three-dot button to bring up the network objects and choose the one that represents the network range you want to impact with the ACL. This example shows the 10.64.0.0/10 range. You should include a description regarding what this ACL will do in the event that another administrator needs to understand this ACL. Click **OK** when you are finished (see Figure 7-16).

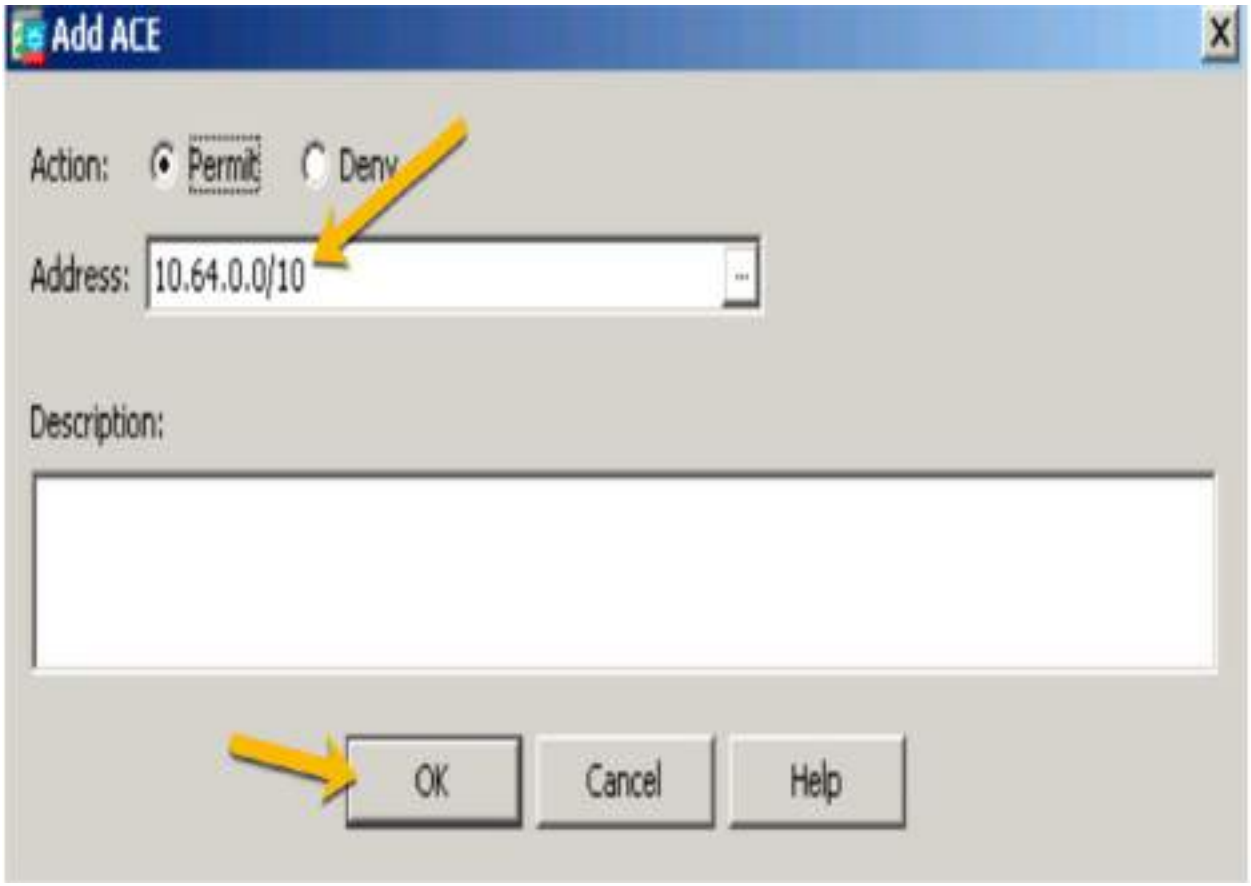


Figure 7-16 Choosing Encrypted Traffic

Step 9. Click **Apply**. Whenever a host connects to a remote access VPN, the routes for the subnets or hosts on the split ACL will be added to the routing table of the client machine. For this example, the 10.64.0.0/10 range would be added to the host routing table.

For the SVPN 300-730 exam, you need to understand how this same configuration would look using the command-line option on the Cisco ASA. Using the CLI preview, Figure 7-17 shows the CLI version of the new split tunnel ACL.

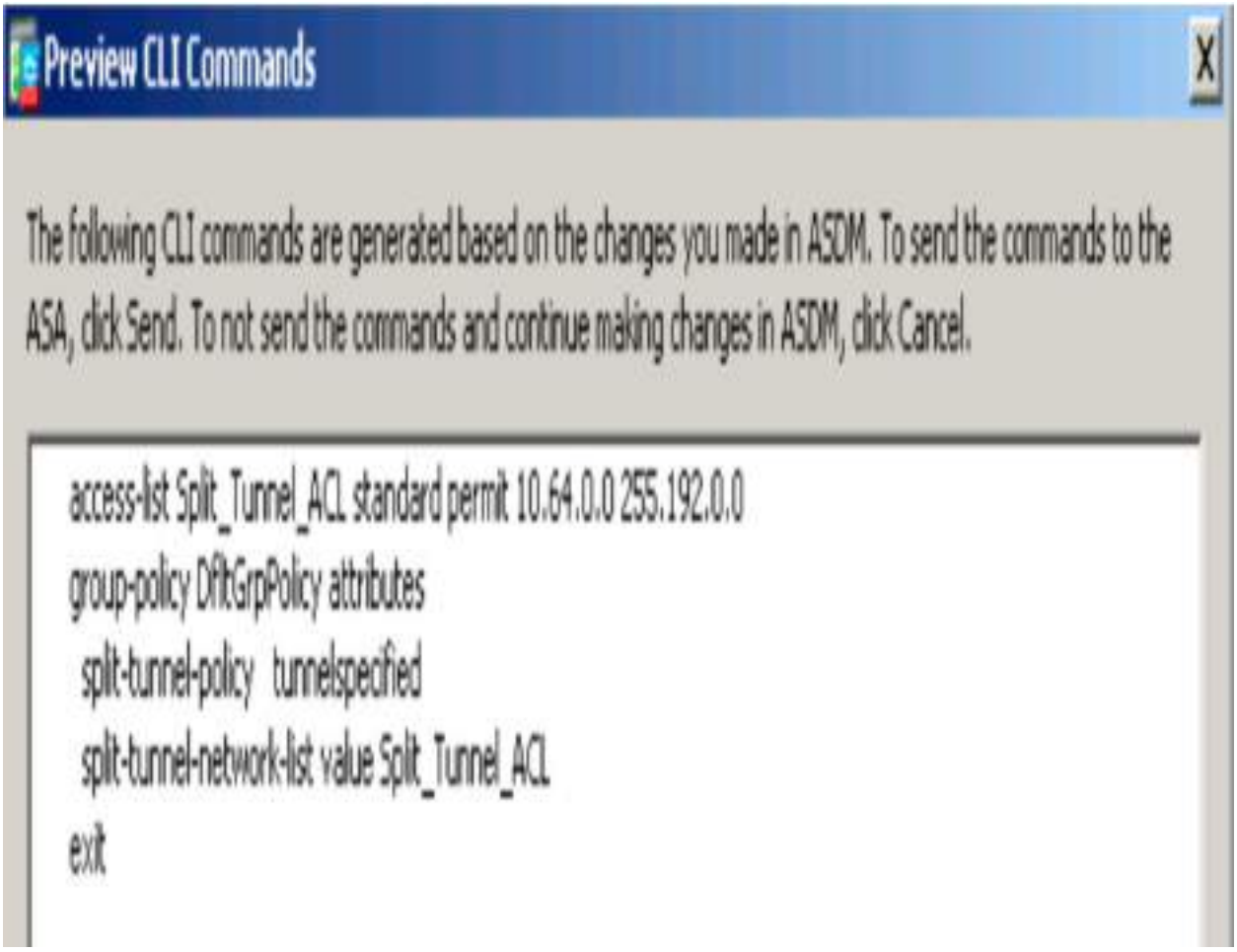


Figure 7-17 CLI for Split Tunnel ACL

You will see more split tunneling configuration examples later in this chapter, when you see how to build a few remote access VPN designs using both Cisco security appliances and IOS routers.

SSLVPN/WebVPN

SSLVPN, or WebVPN, provides remote VPN access through Secure Sockets Layer (SSL) enabled on the VPN gateway. The SSLVPN gateway allows remote users to establish the VPN tunnel using a web browser rather than a software client. The biggest value of this approach is that it simplifies requirements since most mobile devices have a browser that supports SSL and so do not need to install additional software. A remote user can simply launch a web browser and connect directly to a trusted network resource

through the SSLVPN-enabled NAS. SSLVPN also functions over common data ports, reducing the chance that a security tool such as a firewall will prevent the VPN connection from occurring. Figure 7-18 shows an example of a Cisco IOS router providing SSLVPN to a roaming user's mobile device.

Figure 7-18 Remote User SSLVPN Example

WebVPN Example

Figure 7-19 shows a very basic WebVPN portal, which you will build later in this chapter on a Cisco IOS router. Notice that there is a URL search bar, which enables the user to search the VPN. You could set up bookmarks to reach internal servers; this would be helpful, for example, for a contractor who needs access to only specific items in the protected network. Notice on the right the option to launch a full tunnel using Cisco AnyConnect. There are many options available in Cisco portal configurations.

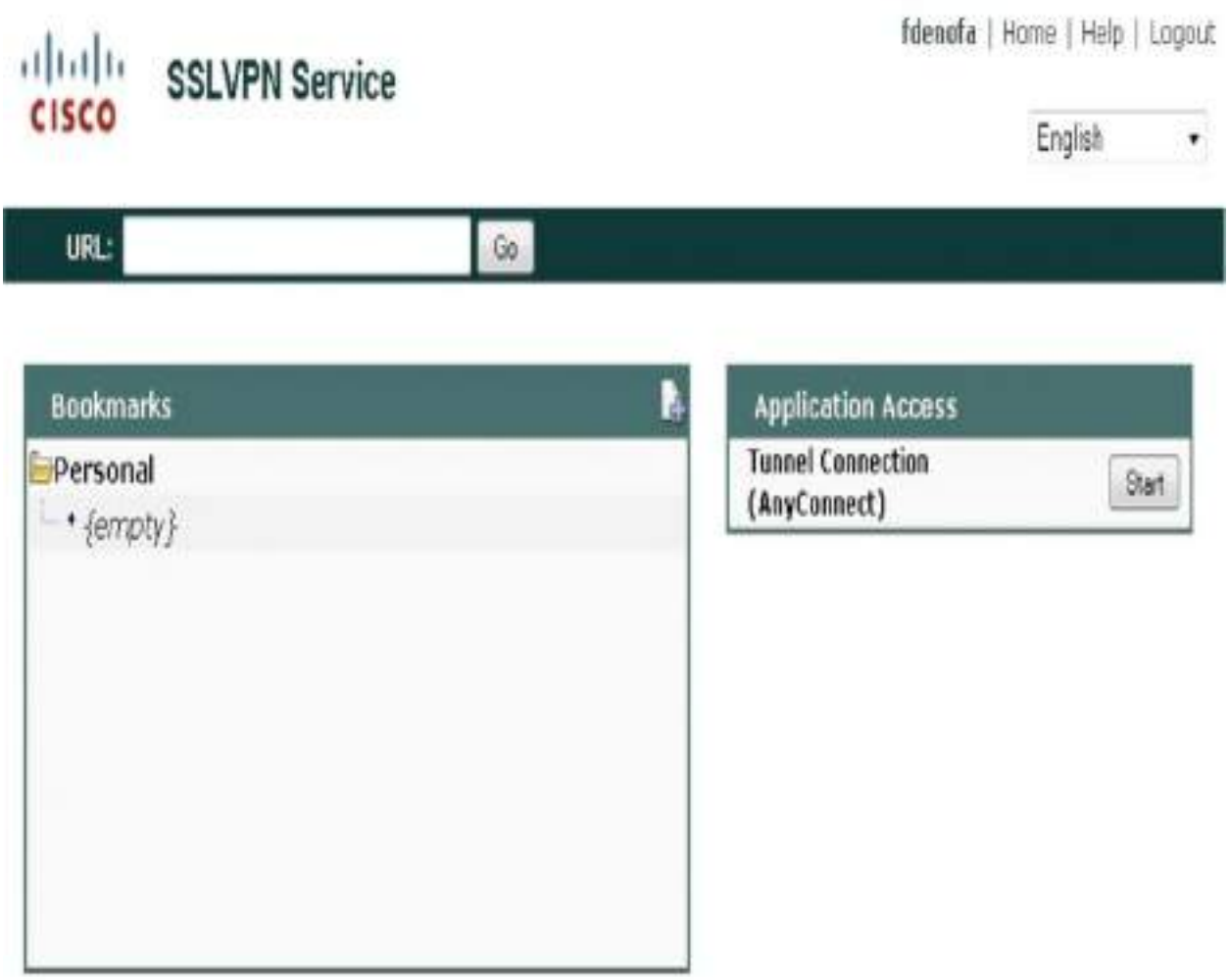


Figure 7-19 Basic WebVPN Portal

SSLVPN traffic flow starts with the remote user accessing the Internet. The user enters the IP address of the VPN NAS and, upon connecting, is redirected to the SSLVPN login page, which, on an ASA, is https://*IP ADDRESS*/index.html. You will see how to build this on a Cisco IOS router later in this chapter. Figure 7-20 provides an example of how the traffic would flow between a user's web browser and VPN NAS.

Figure 7-20 SSLVPN Traffic Flow Diagram

SSLVPN Options

SSLVPN offers a few VPN modes. Clientless mode provides secure access to private web resources and private content. Thin client mode extends the cryptographic functions of the web browser to enable remote access TCP-based applications such as POP3, SMTP, IMAP, Telnet, and SSH. The assumption is that the client application users TCP to connect to a well-known server and port. A Java applet initiates an HTTP request from the remote user client to the SSLVPN NAS. The name and port number of the internal email server are included in the HTTP request. The SSLVPN NAS creates a TCP connection to the internal server and port to allow for access. Finally, with full tunnel mode, a user can flip to a full tunnel by downloading the Cisco AnyConnect VPN client for SSL. For example, a user logged in to a web portal might have the option to select Tunnel Connect (AnyConnect).

The WebVPN GUI can be customized to fit your business requirements. The login page's logo, colors, languages, and text are all customizable. You can add unique messages and images, for example, to provide information to remote users on topics such as your corporate policies for remote VPN access. The SSLVPN portal page is also customizable. As services and other internal links are added to the bookmarks, application access is built, and other details are tuned, the SSLVPN page will begin to look like the one shown in Figure 7-21.

Figure 7-21 SSLVPN Example

SSLVPN Licensing

There are a few SSLVPN license options. A license is consumed when a user creates a VPN session. The same user can create multiple sessions, which would consume a seat count per session. For example, a user working from home and using both a mobile phone and laptop to connect over the SSLVPN would count as two seats. When the maximum license count of the current active license is reached, no new sessions are allowed until seats become available. Seats open up when a user logs out, a session timeout occurs, a session is cleared by the administrator, or another disconnection event occurs.

The following license options are available for SSLVPN:

- **Permanent license:** This type of license does not have a usage period

and node locked.

- **Evaluation license:** This type of licenses is valid for only a short period of time, allowing for the evaluation of the SSLVPN capability. This type of license is not node locked, and it bases its time on the system clock.
- **Extension license:** This type of license is a node locked, metered license. *Metered* means you are billed as the licenses are used. These licenses are ideal when you don't plan to use large license counts but need the option to expand if a special event occurs. An example could be a situation forcing the entire workforce to work from home. It would be ideal to not have to pay for that number of licenses but be able to expand to that count when that event occurs.
- **Grace-rehost license:** This type of license is node locked or metered. It is used in a rehost operation.

You will see how to configure SSLVPN on an IOS router later in this chapter. You will also see SSLVPN configuration examples using a Cisco ASA in next Chapter 8, "Clientless Remote Access SSLVPNs on the ASA."

Encryption Algorithms

So far this chapter has covered the possible options for the NAS and VPN client software required for a remote access VPN deployment. Another component to consider is the type of encryption used by the VPN. Encryption quality and performance are essential to the success of any VPN solution because they determine the VPN experience and level of offered protection.

In Chapter 3, we looked at the technology components of a site-to-site VPN, including various options for encrypting the traffic as it moves between locations. That chapter does not cover encryption concepts, even though they apply to all forms of VPNs, including remote access VPNs. Using the best encryption option for your business is critical to effectively preventing unwanted access to your data. This is especially true with remote access VPNs because remote devices can connect from anywhere in the world, increasing the risk of exposing a VPN session to attack from public networks.

Encryption Trends

Cybersecurity is continuously changing as attack and defense methods adapt to changes in technology and the cyber landscape. The same holds true for cryptography. Over the years, numerous cryptographic algorithms have been developed and used for processes such as encrypting VPN communication. Many older algorithms have been modified or replaced to accommodate modern threats. As you decide which type of encryption you will use to protect your data, it is critical to consider the likelihood that an encryption algorithm could be compromised. Using a deprecated encryption option will lead to a compromise today or a breach in the near future. Computers are constantly becoming faster, and the time required to break an encryption algorithm will continue to decrease. It is critical to understand that encryption is not about permanently preventing attackers from compromising the encryption being used. *Eventually, all encryption algorithms will be compromised.* The goal should be to delay the ability of an adversary to successfully decrypt your VPN.

The cryptography industry considers an encryption acceptable if it can provide security for 10 or more years into the future. Sometimes, acceptable encryption requires a very strong algorithm. Other times, legacy algorithms can be improved by using additional encryption or by including specific configuration and usage, such as enabling short key lifetimes and required password lengths.

Encryption Algorithm Categories

There are four general cryptographic algorithm categories you should be aware of:

- **Symmetric key algorithm:** A *symmetric key algorithm* uses the same key for encryption and decryption. Older symmetric key algorithms can be broken easily due to the small key size. An example of a legacy symmetric key algorithm that should not be used is DES. Triple DES

(3DES) improves DES but is still risky to use unless keys are renewed often. The cryptography industry recommends using AES with 128-bit keys for standard use when using symmetric key algorithms and using AES with 256-bit keys for extremely sensitive information.

- **Public key algorithm:** A *public key algorithm* uses different keys for encryption and decryption. It is common to call these algorithms public/private key algorithms because one key is privately held and kept secret, and the other key is publicly available. These keys are separate and can't be derived from one another. The private key is designed to be used only by its owner, while anybody can use the public key to perform actions with the key owner. However, even if people do not have the private key, data can still be compromised. RSA algorithms for encryption and digital signatures as well as Diffie–Hellman algorithms are becoming more vulnerable to compromise as attack research and technology continue to improve. The cryptography community continues to recommend increasing the key sizes as a countermeasure, but every year RSA and Diffie–Hellman are becoming less effective at protecting encrypted data.

- **Elliptic curve algorithms:** *Elliptic curve algorithms*, or elliptic curve cryptography (ECC), are a relatively new alternative to public key cryptography. These algorithms function on elliptic curves over finite fields, which means ECC is efficient and performs well. ECC can be added to Diffie–Hellman and RSA to create ECDH and ECRSA, which, when used over 284-bit prime modules, can be used for very secure information, such as classified information. The SVPN 300-730 exam covers elliptic curve algorithms.

- **Hash algorithm:** *Hash algorithms*, also known digital fingerprinting algorithms, are irreversible functions that provide a fixed size output based on various inputs. This means you could enter 40 characters for one hash and 20 characters for another statement to be hashed, and both hash outputs would be the same length, such as 30 characters. The strength of hashing is based on the output being irreversible and resistant to collisions. Having two different inputs produce the same hash would violate the value of using a hash to validate that something is authentic. Examples of hash algorithms are Secure Hash Algorithm 1 (SHA-1),

SHA-256, and Message Digest 5 (MD5). Of these examples, MD5 and SHA-1 are legacy algorithms that should be avoided.

Comparing Encryption Options

Table 7-2 is a helpful chart that groups together different encryption algorithms, based on their bit counts. Using 128 bits could be sufficient for encrypting data that isn't extremely sensitive; however, the industry recommends using higher bit levels, such as 256-bit encryption, for protecting sensitive data. The higher the bit count, the harder it is to break the encryption.

Table 7-2 Encryption Strength Summary

Algorithm	Bit Count
AES-128 DH, DSA, RSA-3072 SHA-256 ECDH, ECDSA-256	128 bits
AES-192 SHA-384 ECDH, ECDSA-384	192 bits
AES-256 SHA-512 ECDH, ECDSA-521	256 bits

For remote access VPN encryption, this chapter focuses on the use of ECC. To better understand ECC, let's look more closely at the fundamentals of ECC algorithms.

Elliptic Curve Cryptography Algorithms

ECC is the latest encryption and decryption method for stronger security. It can perform much faster than other options, such as RSA, based on using smaller key sizes (and therefore consuming fewer computational resources). To put things in perspective, a 256-bit ECC key would be similar to a 3072-bit RSA key. Agencies such as the National Security Agency (NSA) have certified ECC, making it a recommended method for encrypting websites and infrastructure; ECC is safer than traditional RSA and DSA options.

Asymmetric encryption such as ECC is used for many things, including bitcoin, X.509/PKI, Transport Layer Security/Secure Sockets Layer (SSL), Internet Key Exchange (IKE), Secure Shell (SSH), Domain Name System Security Extensions (DNSSEC), Secure Multipurpose Internet Mail Extensions (S/MIMI), and most things using digital signatures. ECC is also adaptable to many existing cryptographic schedules and protocols, including Diffie–Hellman (Elliptic Curve Diffie Hellman [ECDH]), Digital Signatures (Elliptic Curve Digital Signatures [ECDSA]), and Integrated Encrypted Scheme (Elliptic Curve Integrated Encryption Scheme [ECIES]). Today many smart cards, cell phones, and Internet of Things (IoT) devices implement ECC for their asymmetric encryption requirements. There is not a known timeline for how long ECC will be effective, but numerous standards define and govern ECC, including the American National Standards Institute (ANSI) X9.62/X9.63/FRP256V1, the Institute of Electrical and Electronics Engineers (IEEE) P1363, the Standards for Efficient Cryptography Group (SECG), NIST's Federal Information Processing Standards (FIPS), and the NSA's Suite B requirements. With this level of support, ECC should remain a trusted option for the foreseeable future.

ECC Threats

ECC does face some potential threats. There is a potential for a side-channel attack, which could result in a leak of information. For example, an attacker

could measure the difference in time between observed peaks in power consumption using a tool such as an oscilloscope. Because there are signification time variances for input values, an attacker could deduce the secret key in a timing attack. A similar approach could be used for measuring power consumption, by mapping changes in power against input to deduce the key. Over time, ECC has developed countermeasures to threats such as side-channel attacks, including the implementation of the Montgomery power ladder, which is designed to mask resource consumption and timing. Unfortunately, not all ECC support ladders and other attack methods will continue to show up as general technology and ECC evolves. Quantum computing is one of the upcoming potential threats to ECC.

Encryption Algorithm Math

Before we dive further into ECC, we need to look at the basics of how asymmetric encryption math works. Public key cryptography is based on the concept that factoring is slow, while multiplication is fast. For example, the easy part of the RSA algorithm is multiplying two prime numbers, and the hard part of the RSA algorithm is factoring the product of the multiplication into two component primes. In the world of mathematics, algorithms that are easy in one direction and difficult in the other are called *trapdoor functions*. Generally, the bigger the difficulty in one direction than in the other, the more secure the algorithm.

As described earlier, asymmetric encryption involves two components—the public key and the private key—that enable two parties to communicate in a secure manner without having to meet each other to exchange a secret key (because only the public key is revealed). The encryption behind this process works by applying to the message a mathematical operation to get a random-looking number. Decryption works by applying another random-looking number, which returns the target number back to its original number. For asymmetric encryption, encrypting with the public key can only be undone by decrypting with the private key.

Limits called maximum wrappers permit the results of calculations to exceed the limits of the computer processing the encryption. Think of a wrapper as a clock; after the value exceeds 12, the next digit is 1. The public and private

keys are special numbers that sit between the maximum number and zero. To encrypt a message, you simply multiply a number times the value of the public key wrapping the value around when it hits the maximum value. For example, say the public key is 10 and you are using the number 4. You would end with a result of 6 based on 4 [ts] 4 = 16. However, you would wrap back to 0 when you hit the wrapper at 10, resulting in the remaining value ending with a result of 6. To decrypt the message, you multiply the number by the private key number, which brings you back to the original number.

RSA and Diffie–Hellman were great options when computing prime factorization was challenging. Specialized algorithms such as the quadratic sieve and general number field sieve algorithms were developed to handle prime factorization, and required key lengths increased to avoid the possibility of an unwanted party breaking the encryption being used. As computers increase in power, applying larger keys obviously does not create a sustainable cryptography system.

ECC Math

Elliptic curve mathematics improves a trapdoor function by applying this mathematic equation:

$E = \{(x,y) \mid y^2 = x^3 + ax + b\}$

When you run numbers through this equation, you end up with different elliptic curve shapes. Figure 7-22 shows an example of a curve that can be produced using this equation.

Figure 7-22 Example Elliptic Curve

By using known variables and seeing where the factors plot the curve, it is easy to solve for the public key; however, it is extremely difficult to construct a seed from the domain parameters, which means you solve a hash inversion to cheat. This difficult part of the logarithm underpins elliptic curve encryption. Despite more than three decades of research and testing, mathematicians around the world have been unable to find an algorithm to function as a shortcut to narrow the gap within the elliptic curve trapdoor, so the trapdoor has maintained its strength as the backbone for EEC. Essentially, solving the elliptic curve logarithm is significantly more difficult than solving the factoring involved with RSA and Diffie–Hellman. The industry has therefore moved away from recommending larger keys for algorithms such as Diffie–Hellman and instead has looked to elliptic curve to improve security.

Combining ECC with Other Algorithms

Now that you have a basic understanding of trapdoor mathematics and why ECC has become the industry recommendation, let’s look at how ECC is used in the real world. Two extremely popular but dated algorithms are digital signatures and Diffie–Hellman. To overcome their weaknesses, many security products offer a combination of ECC with these two algorithms; the combinations, as mentioned earlier, are known as ECDH and the ECDSA.

Diffie–Hellman (DH) is a public key cryptography protocol that enables two parties to establish a shared secret over an insecure communications channel.

It is used in IKE to establish session keys. DH can be configured to support its default of 768 bits or to go as high as 4096 bits. The industry recommends at least 2048 bits, but changes in technology are causing the bit recommendations to continually increase. Adding elliptic curve mathematics to Diffie–Hellman, ECDH, dramatically improves security, allowing a 256-bit ECDH key to meet industry recommendations. It is estimated that a DH 3072-bit key could provide similar protection to an ECDH 256-bit key. Increasing an ECDH key to 384 bits would equate to around the same protection as a 7680-bit DH key. A 512-bit ECDH key would increase the standard asymmetric key's equivalent protection to around 15,360 bits. The bottom line is that ECDH can get you the same level of protection as DH but with much smaller keys. You can see why the industry is moving toward ECC.

ECC can also be applied to digital signatures. The industry has used RSA for a number of years, but now ECDSA is being used for increased performance and security. RSA uses a public key that is a product of two prime numbers, plus a smaller number. Applying elliptic curve mathematics can allow a 256-bit ECDSA key to provide as much protection as a 3248-bit asymmetric key. An average website uses a 2048-bit RSA key, and an ECDSA key of around 256 bits would perform faster and be much stronger than that. As with DH, you could use a large digital signature key to improve security or leverage ECDSA, which can provide high security with a much smaller key. For use cases such as remote access VPNs, this can be critical for performance and protection.

Applying Elliptic Curve Cryptography to a VPN

This section applies what you have learned about elliptic curve cryptography to VPN technology. We look first at generating IPsec keys. When you configure a remote access VPN, you can use different Diffie–Hellman key derivation algorithms to generate IPsec security association (SA) keys. Different group options have different modulus sizes. Cisco set things up so that the larger the group number, the better the security applied; however, better security may require more processing time. As discussed earlier, elliptic curve mathematics has helped improve performance and increase security. When you create a VPN, you need to select certain minimum levels

of security, depending on the type of encryption being used. For example, if you use AES encryption, you should use group 5 or higher. IKEv1 policies allow only groups 1 and 5. Groups specify the level of security being applied.

Diffie Hellman Groups

The Diffie–Hellman group options are as follows:

- **Diffie–Hellman Group 1:** 768-bit modulus. DH group 1 is considered insecure; do not use it.
- **Diffie–Hellman Group 2:** 1024-bit modulus. This option is no longer considered good protection.
- **Diffie–Hellman Group 5:** 1536-bit modulus. Formerly considered good protection for 128-bit keys, this option is no longer considered good protection.
- **Diffie–Hellman Group 14:** 2048 bit modulus. Considered good protection for 192-bit keys.
- **Diffie–Hellman Group 19:** 256-bit elliptic curve.
- **Diffie–Hellman Group 20:** 384-bit elliptic curve.
- **Diffie–Hellman Group 21:** 521-bit elliptic curve.
- **Diffie–Hellman Group 24:** 2048-bit modulus and 256-bit prime order subgroup. This option is no longer recommended.

You can see that DH bit sizes start at 768 bits and increase to more than 2,000 bits. With groups 19 and higher, elliptic curve is applied (that is, ECDH), which reduces the bit size. As mentioned earlier, the current recommendation is either a large-bit-size DH option or an ECDH option. The options and recommendations will continue to change as technology and mathematics matures.

When you need to protect classified or extremely sensitive information, it is best to use a 384-bit elliptic curve option for ECDH. Regardless of the security with ECDH, there is no method to authenticate the parties during the exchange. ECDSA is used to sign the content and fill this gap with ECDH.

ECDH is used for establishing a public key. ECDSHA is used for signing certificates. This means you use ECDH to share a secret key and ECDSHA to authenticate parties since ECDH doesn't have the ability to authenticate.

High Availability

Redundancy must be part of your VPN design considerations. For some organizations, remote access VPN capabilities are a luxury; other organizations depend on having remote access to critical resources. Examples of business-critical use cases can include administrators accessing equipment within an organization, sales teams requiring access to internal sensitive applications, and remote systems requiring updates from internal sources.

Load Balancing

Cisco customers have a few options for high availability, as mentioned in Chapter 3. The first option is load balancing VPN traffic between members of a virtual cluster. A virtual cluster is made of two or more headend devices, where one acts as the virtual master, and others are backups. The headend devices do not have to be the same type or have identical software or configurations to participate in the virtual cluster. All active devices in the virtual cluster are responsible for session loads. Load balancing works by directing traffic to the least-loaded device in the cluster, and that device attempts to balance the distribution of sessions between all headend devices.

Failover Design

Another option is to use a failover design. The most basic of these is a cold failover, which involves having similar hardware available but not powered on. In the event that a VPN system goes down, you could power on the standby unit and redirect traffic to the new unit by copying over the

configuration. If you use a cold standby approach, best practice is to have a system that periodically downloads the most current configuration from the primary headend to prevent the loss of recent configuration changes.

A better failover approach is to use two identical headend devices, such as two Cisco ASAs, and connect them with a dedicated failover link. A heartbeat check takes place between the primary and secondary devices, and certain conditions will trigger failover. For the ASA, active/active and active/standby options are available. Active/active means a high-availability configuration is established and requires multi-context mode to be enabled. This approach allows for balancing traffic between two active systems. Active/standby involves only the primary ASA providing VPN capabilities with a standby system that waits for failover to occur.

Note

One key value of a high-availability design in which each ASA is considered standalone is that if an ASA fails, users do not need to disconnect. With a failover design that clusters the ASAs, if one ASA goes down, the users get disconnected and have to reestablish the VPN connection after the failover occurs.

Load Balancing Considerations

There are a few things to consider that may or may not allow your design to include load balancing. Here is a quick summary of important items:

- Many Cisco offerings do not support load balancing or stateful failover when a security appliance is in multi-context mode. If you are using multi-context mode, check to see if your designed failover and load balancing option is supported. For example, ASAs do not support multi-context mode and load balancing.
- If you have limited IP address pools available for a remote access deployment, you may not want to perform load balancing. The load

balancing algorithm is based on the load that each backup cluster member supplies. This means you can quickly run out of IP addresses if you are using multiple systems in a load balancing cluster. Also, each device must have a unique IP address.

- When clustering devices, all devices are active, which means the maximum number of devices for each device is in play. For example, if one device in a cluster supports 100 devices and another supports 200 remote devices, you could support 300 devices with this cluster.

- Some VPN clients may not be able to participate in load balancing. For example, the Cisco ASA supports IPsec clients, SSLVPN clients, and clientless sessions. The Cisco ASA allows support for LT2P, PPTP clients, or L2TP/IPsec, but they do not participate in load balancing.

Another failover factor to consider is how the clients react during a failover. Cisco AnyConnect offers the ability to configure a backup server, which will be the fallback if the primary server is not available. This is configured within the AnyConnect client profile, which is discussed earlier in this chapter. Within the server list settings is an option to add one or more backup servers. You need to include either a fully qualified domain name (FQDN) or an IP address. Figure 7-23 shows the configuration page for adding a backup server.

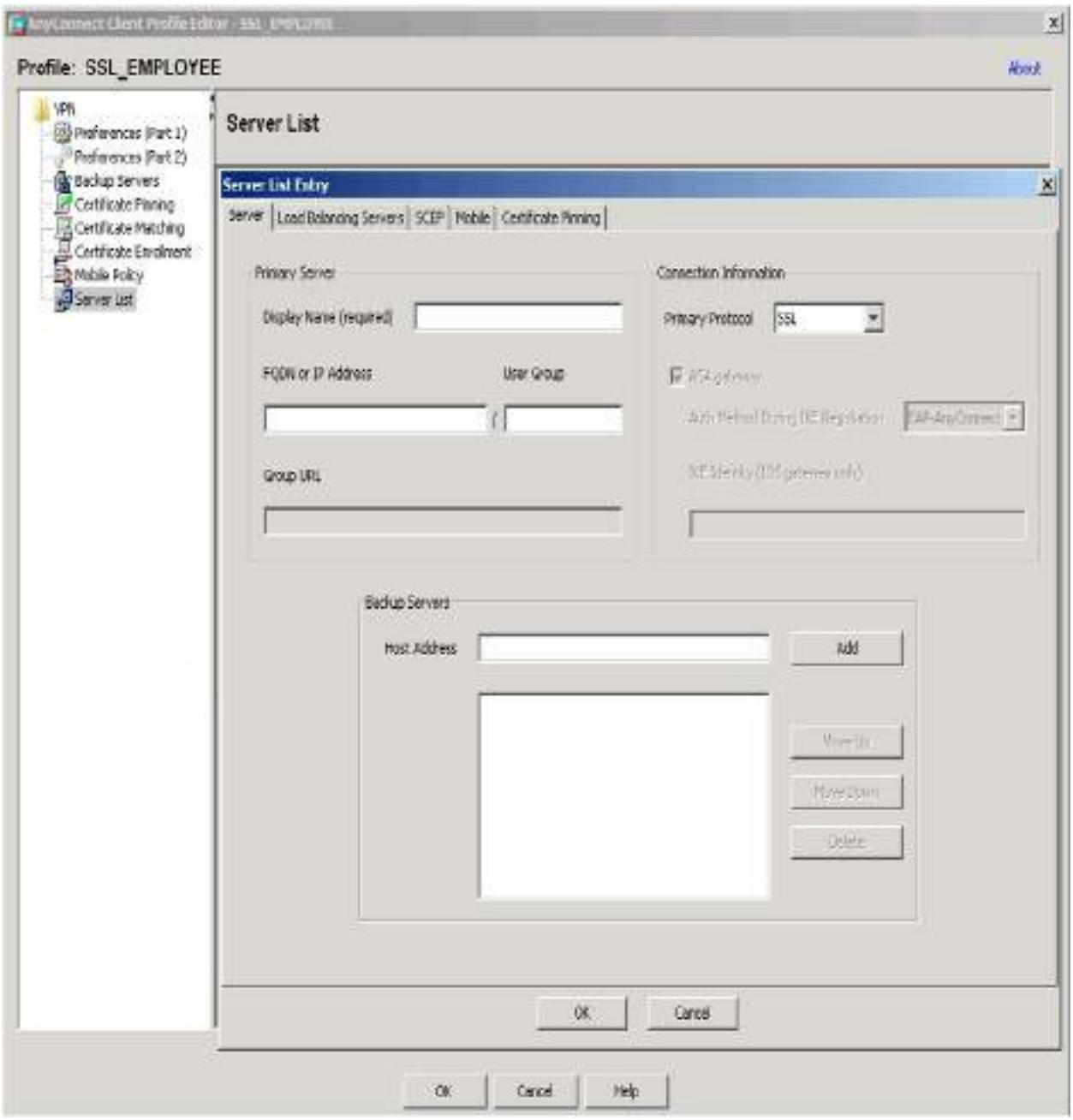


Figure 7-23 Adding a Backup Server in AnyConnect

Cisco ASDM Remote Access Configuration

It’s time to configure a remote access VPN! In the first example, you will see how to configure a Cisco ASA to provide remote access to employees running Cisco AnyConnect. You will see how to build this by using the ASDM VPN wizard and will also see the command-line code that is created

for the configuration. Then you will work through a similar project using the ASA command line to ensure that you understand how to build a basic remote access VPN setup.

The design for this deployment will accommodate a remote user connecting over the public Internet to access the outside interface of the ASA security appliance. Any traffic that crosses the VPN will be routed to the 10.64.0.0/10 network. The outside IP address for the ASA will be 172.16.21.1. Figure 7-24 shows this design.

Figure 7-24 ASA Remote Access Design

Let’s start off this configuration example by accessing Cisco ASDM:

Step 1. Log in to ASDM and select **Wizards** > **VPN Wizards** > **AnyConnect VPN Wizard** (see Figure 7-25).

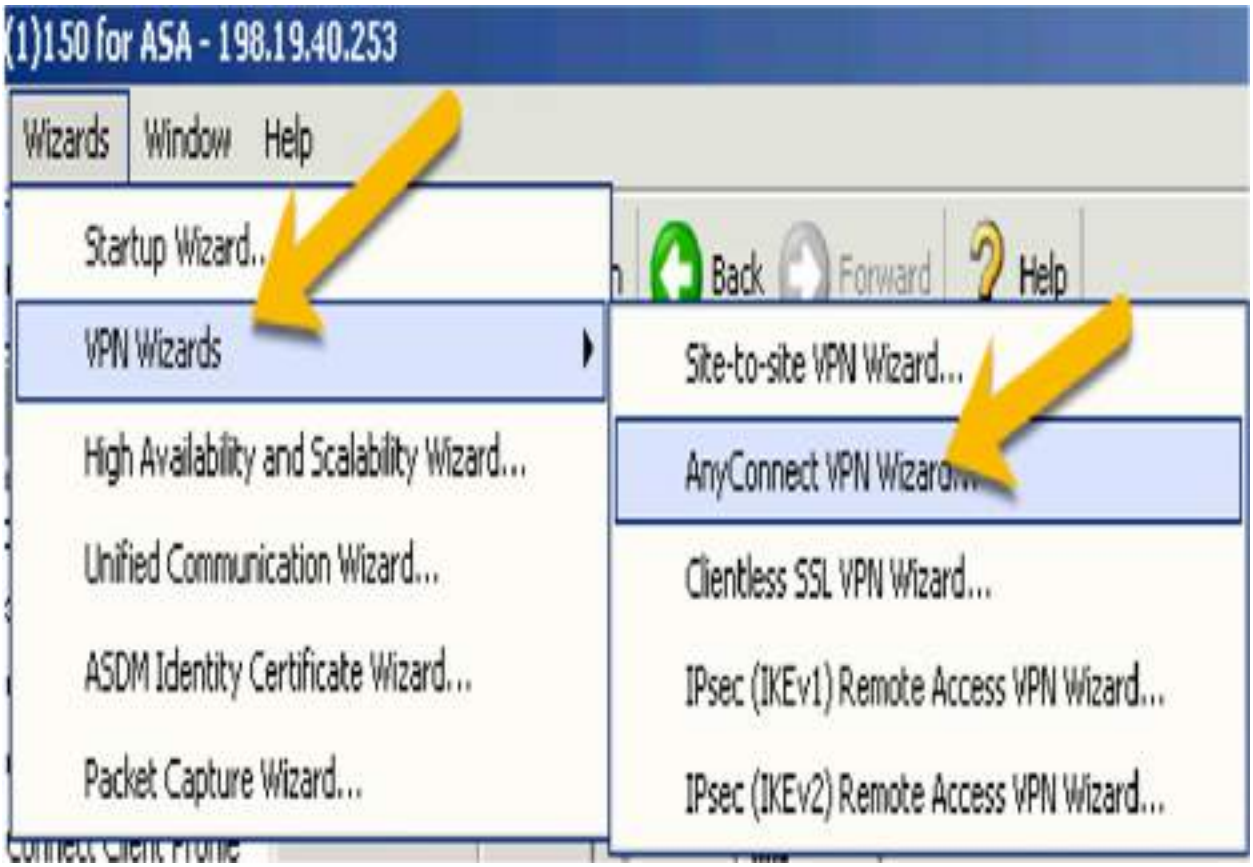


Figure 7-25 Navigating to the AnyConnect VPN Wizard

Step 2. On the introduction page, click **Next**.

Step 3. Give your connection profile a name and choose the outside interface as the termination point (that is, the point to which people will connect from outside the network). Click **Next** (see Figure 7-26).

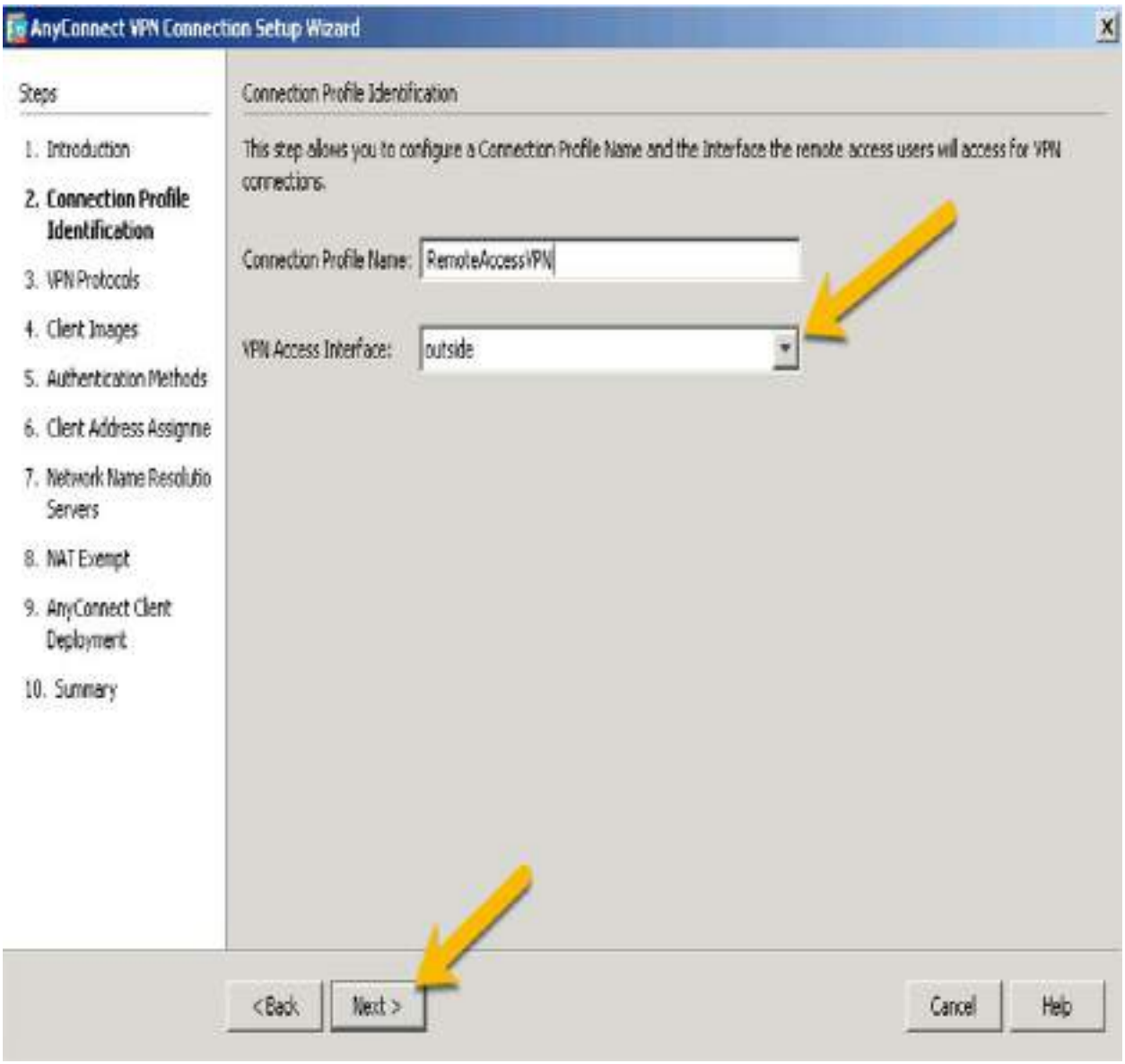


Figure 7-26 Connection Profile Identification

Step 4. Check the **SSL** check box to enable SSL and choose the device certificate. You could use a self-signed certificate, but it is recommended to use a third-party certificate authority (CA), such as Entrust or Verisign, because many companies have approved the trust provided by such CAs. Also, some applications have built-in trust for popular third-party CAs. This example uses a certificate created using Active Directory, as shown in Figure 7-27. If you do not have a certificate available, click **Manage**.

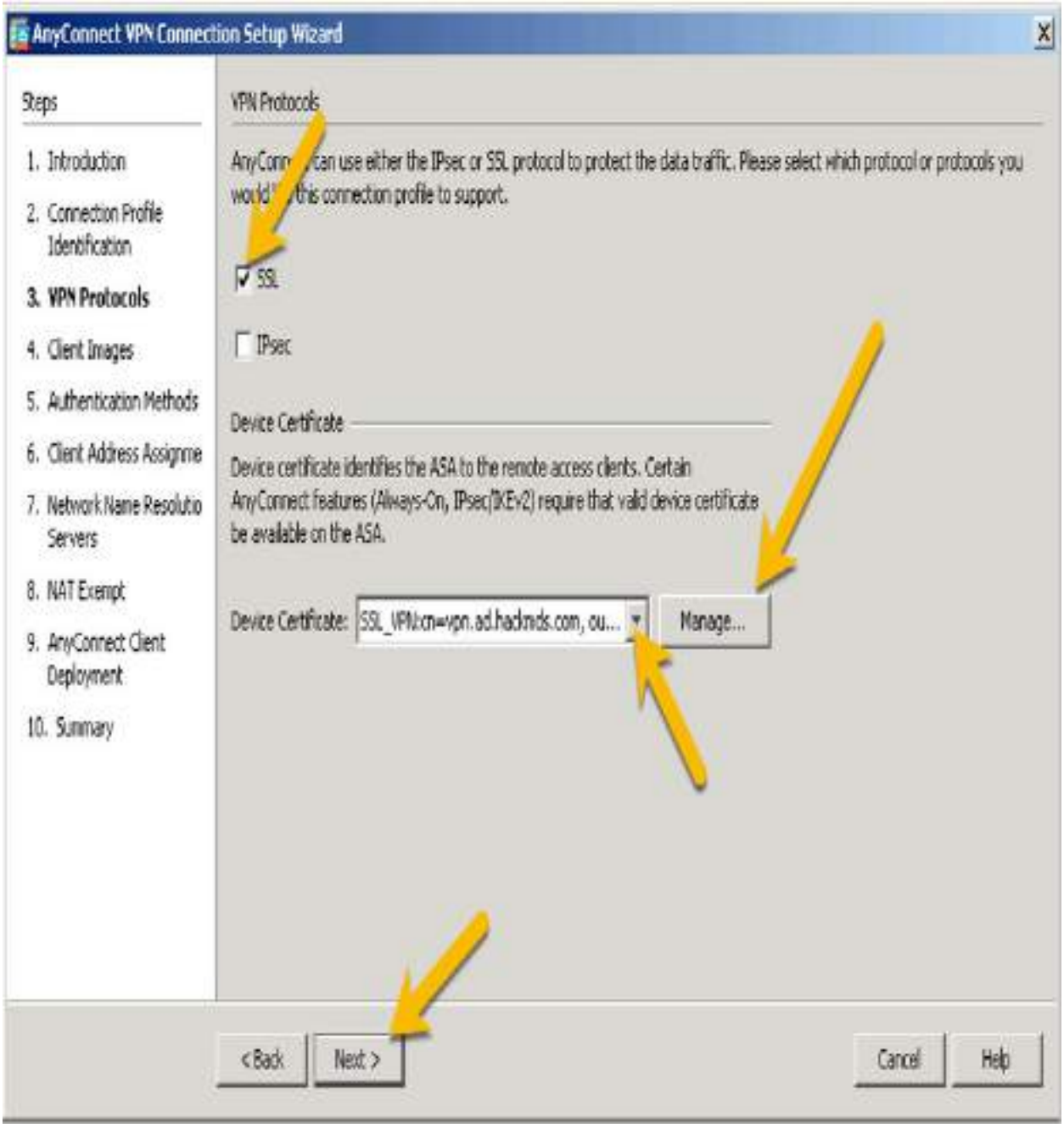


Figure 7-27 VPN Protocols

Step 5. If you needed to create or import a certificate, click **Add** (to import) and choose **Enroll ASA SSL certificate with Entrust** or **Launch ASM Identity Certificate Wizard**, as shown in Figure 7-28. Once you have created your certificate option, select it and click **Next**.

Figure 7-28 Creating or Importing a Certificate

Step 6. On the page that allows you to choose your AnyConnect image, click **Add** if an image isn't already selected. If you have not downloaded an AnyConnect image, you can upload it here or select one that has been downloaded to flash. After you select an AnyConnect image, click **Next** (see Figure 7-29).

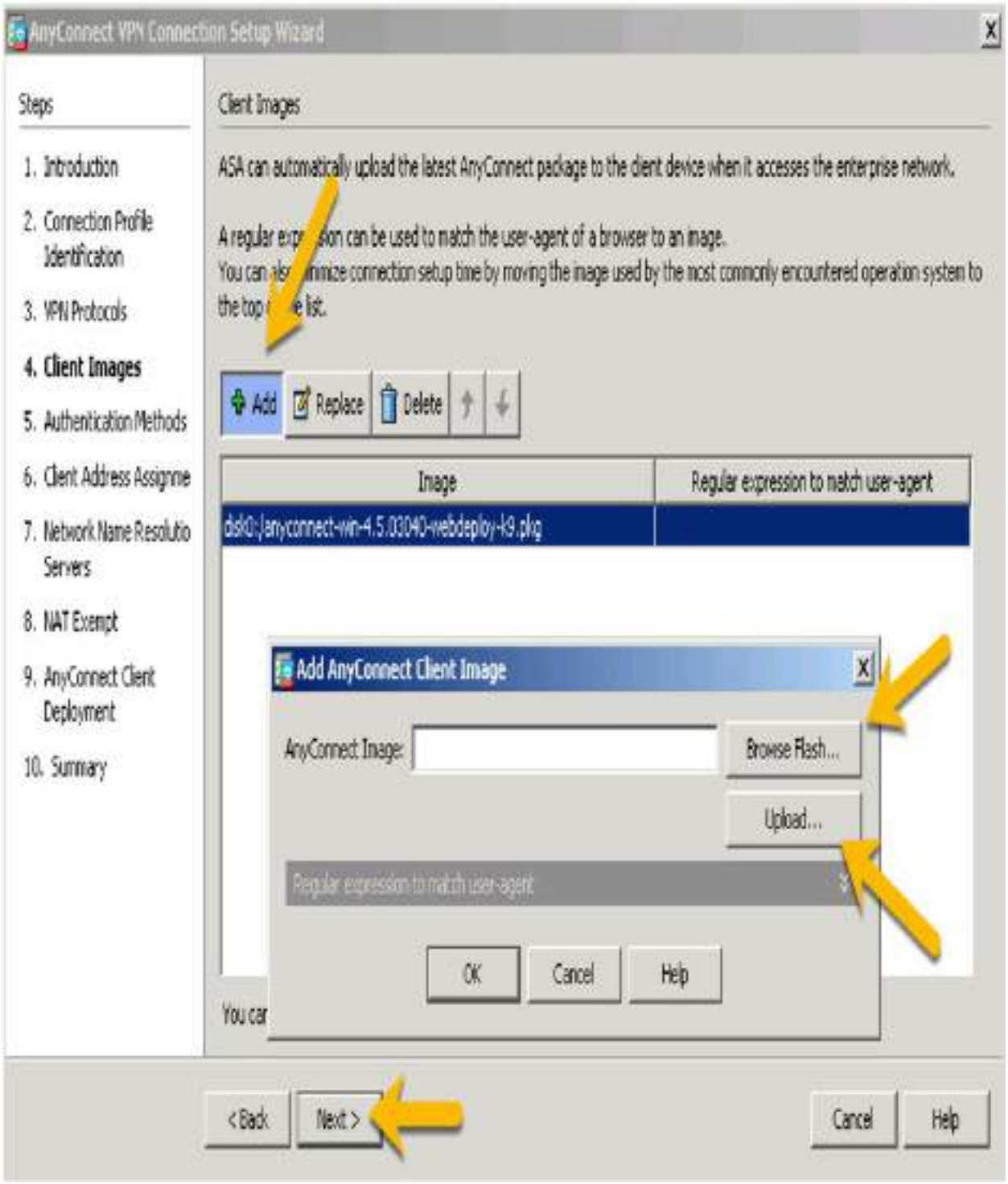


Figure 7-29 Choosing an AnyConnect Image

Step 7. On the next page, where you can select authentication methods used for logins to the VPN, click **New** to add a new authentication option

or select the one you want to use and click **Next** (see Figure 7-30).

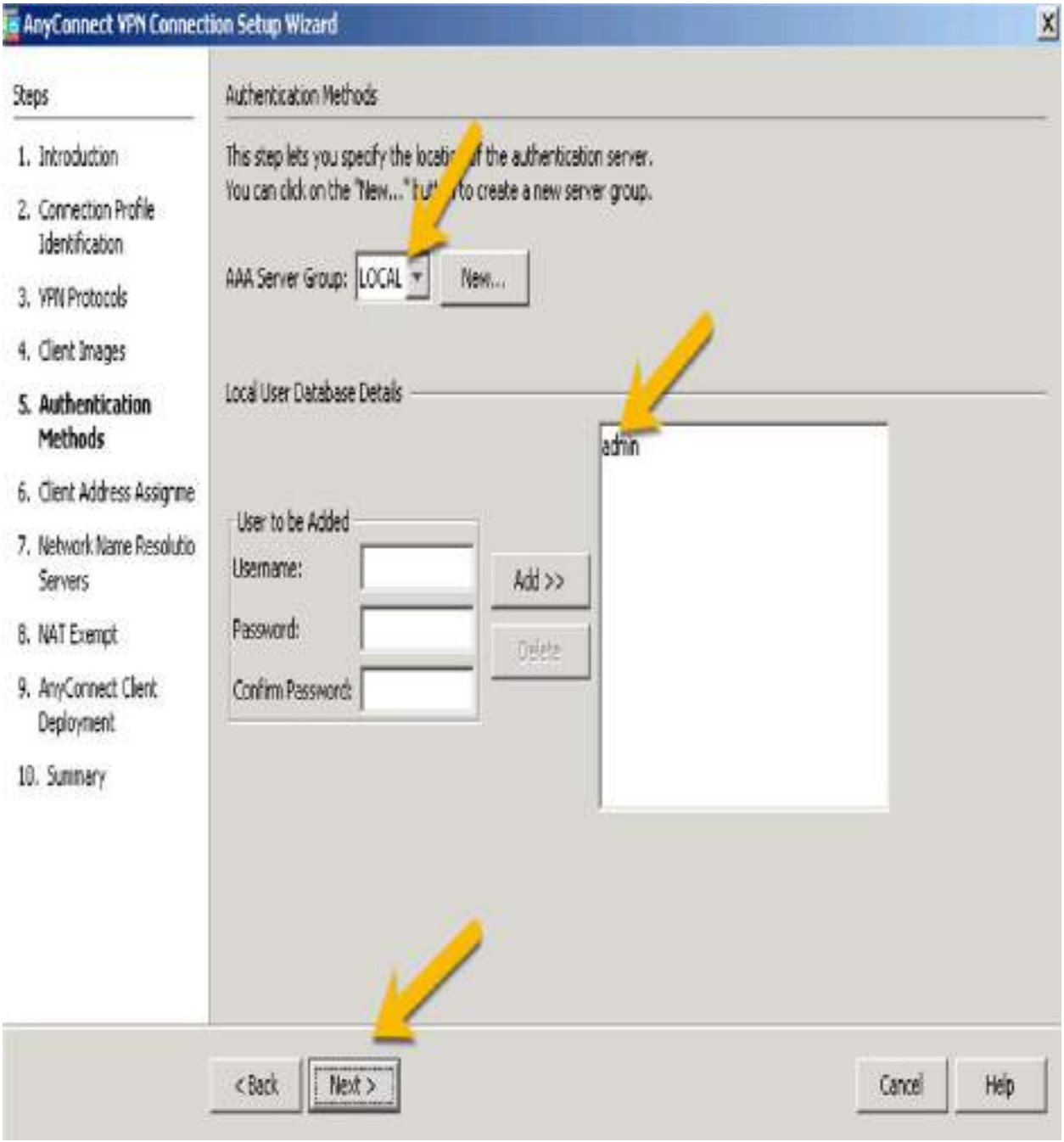


Figure 7-30 Authentication Methods for Login

After you click **New**, you can click the **Authentication Protocol** drop-down to see the options (Figure 7-31).

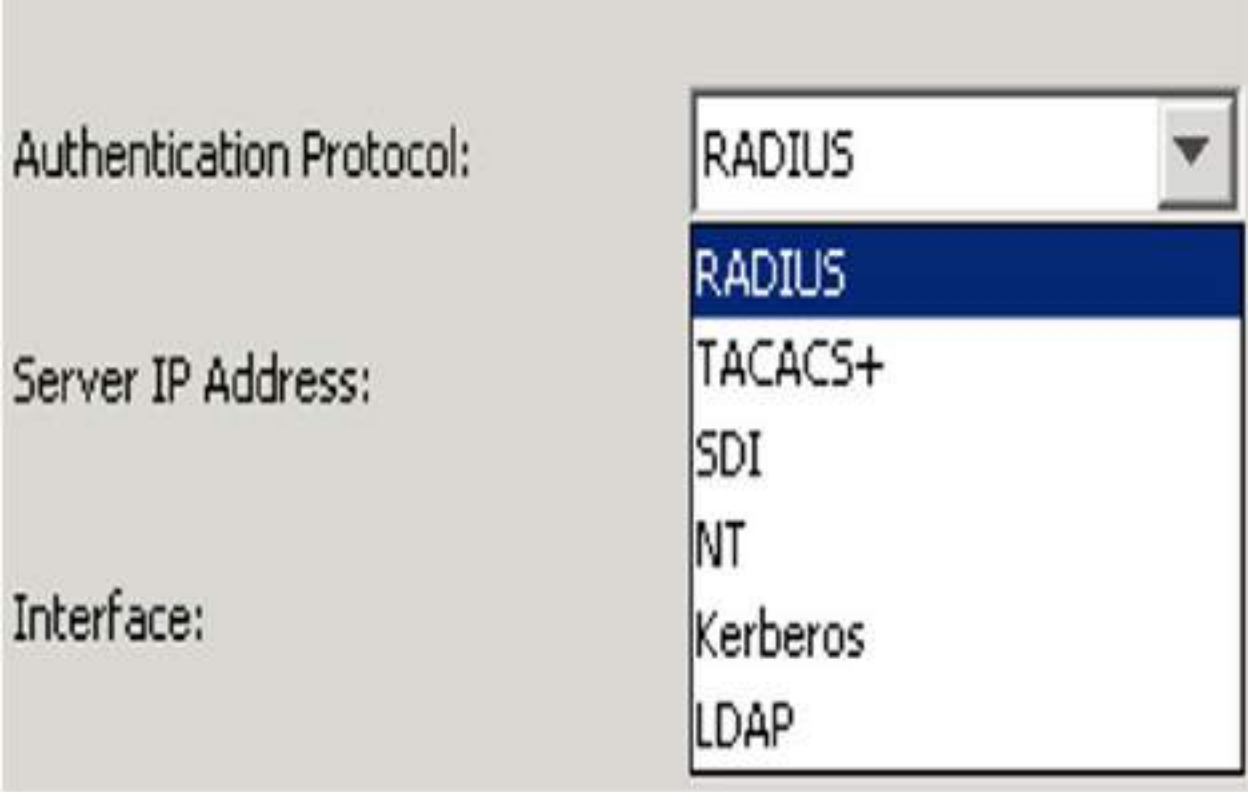


Figure 7-31 Authentication Protocol Drop-down

Figure 7-32 provides an example of using ISE for the authentication protocol. After you have chosen your authentication protocol, click **Next**.

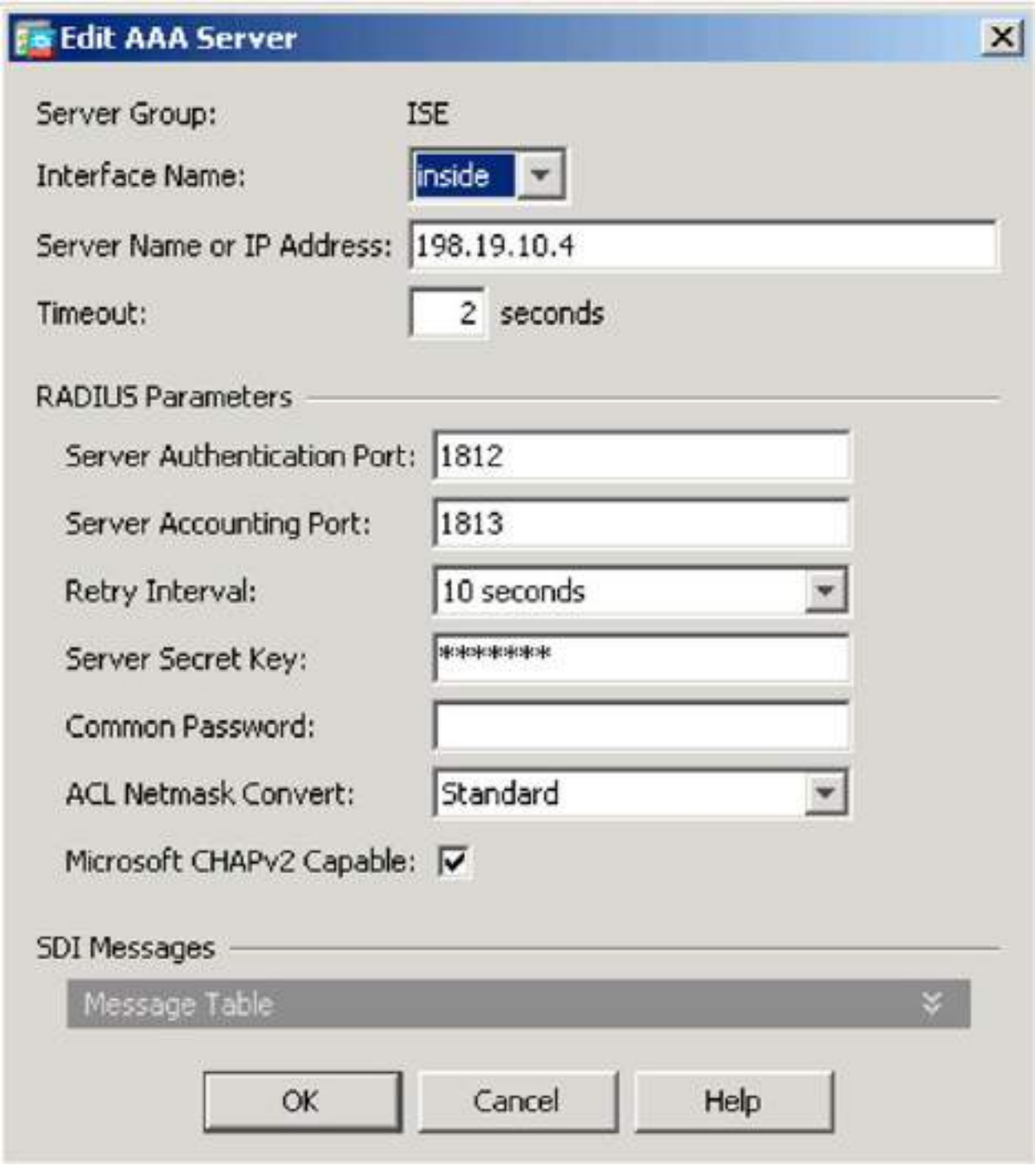


Figure 7-32 ISE as the Authentication Protocol

Step 8. On the Client Address Assignment screen, select an existing IP address pool or create a new pool of IP addresses by clicking the **New** button. Select with IPv4 and IPv6 address pool(s) you want to use, and click **Next**. This example uses VPN-POOL with IP

addresses between 198.19.40.51 and 198.19.40.60 because there will not be very many VPN users (see Figure 7-33).

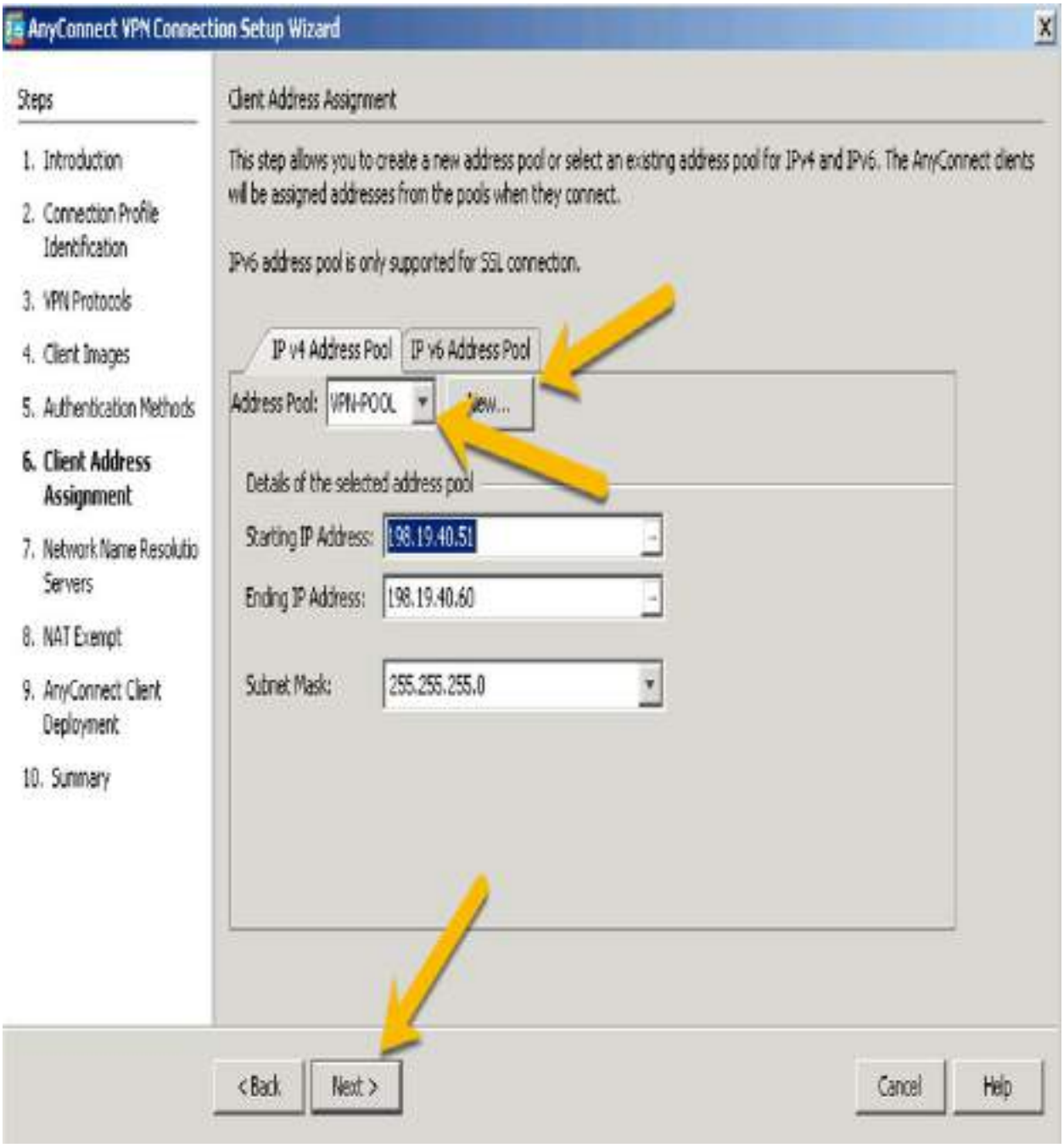


Figure 7-33 Client Address Assignment

Step 9. Specify a DNS server and a domain name, and then click **Next** (see Figure 7-34).

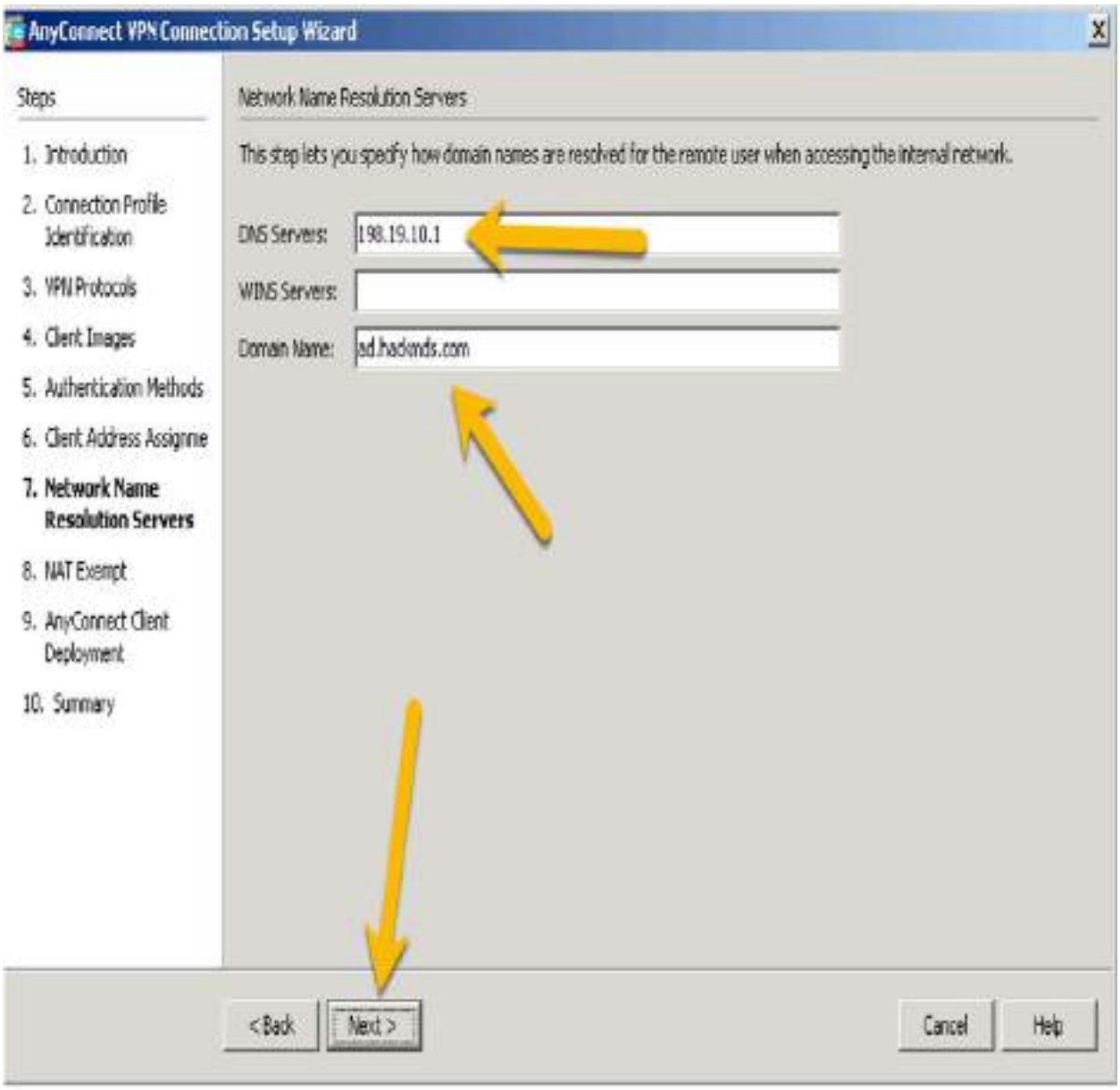


Figure 7-34 Specifying the Network Name Resolution Servers

Step 10. When asked to choose whether to exempt the VPN from NAT, leave the check box unselected and click **Next** (see Figure 7-35).

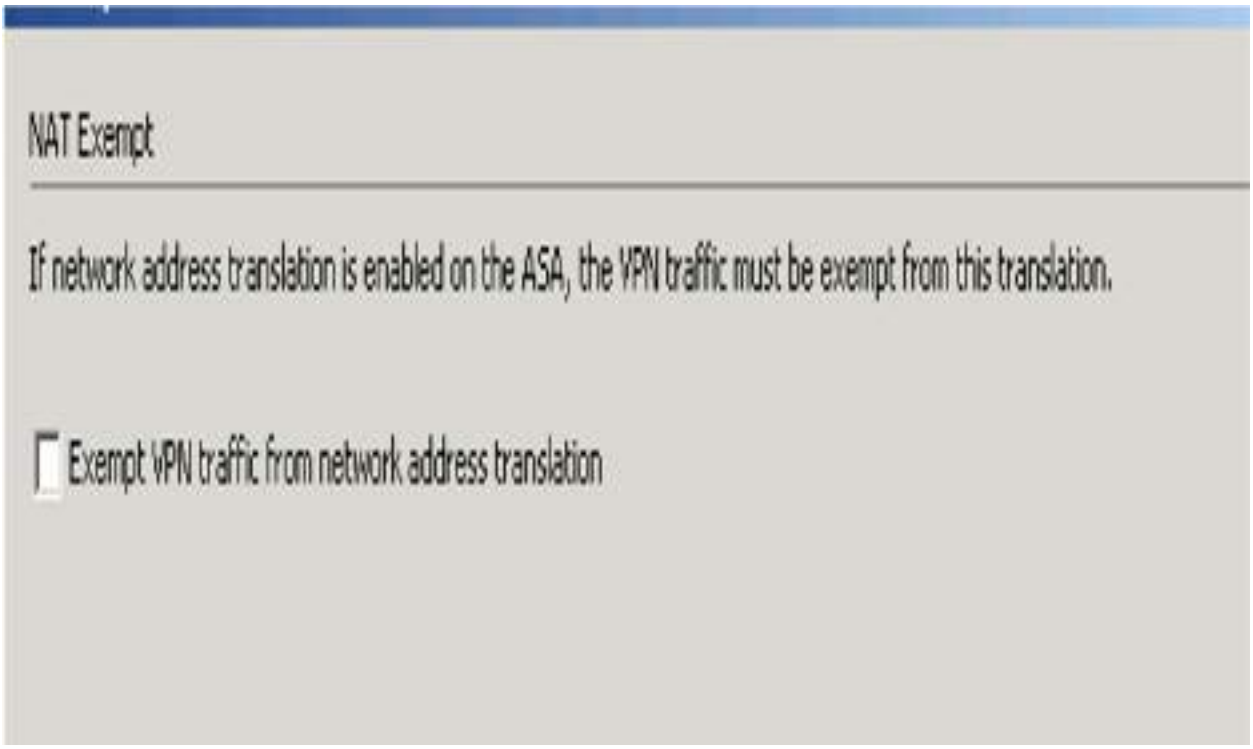


Figure 7-35 Exempting the VPN from NAT

You will see an explanation indicating that there are two options for the AnyConnect client to be installed on hosts. After reading this explanation, click **Next**. Now you see the summary page (see Figure 7-36).

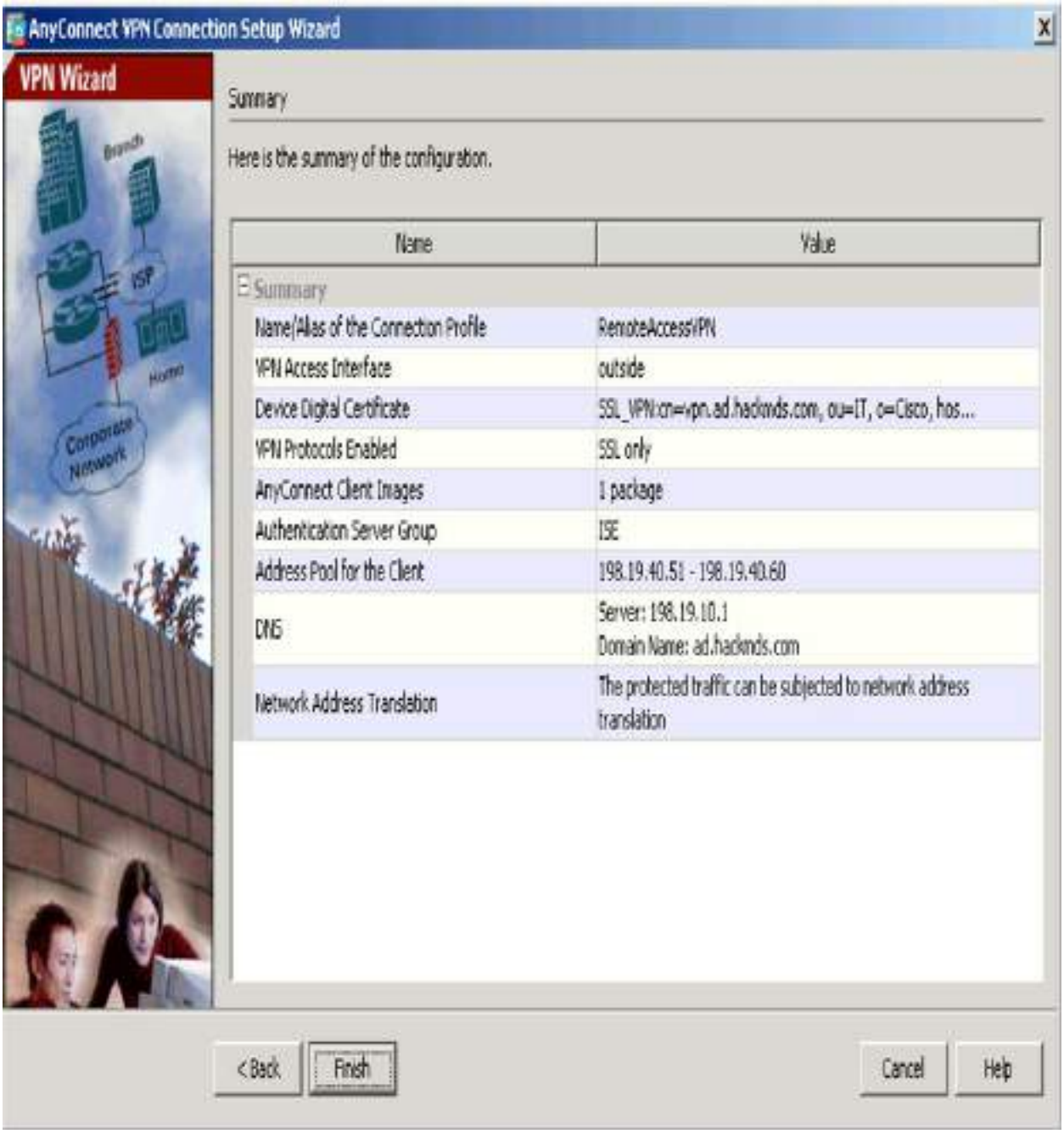


Figure 7-36 Summary Page

If you are studying for the SVPN 300-730 exam, you need to understand the command-line code associated with an ASDM wizard configuration. Figure 7-37 shows a summary of the code used for this configuration. To better understand this command-line code, in the next section, you will build a similar basic remote access VPN setup using the command-line options in a Cisco ASA. You can view the configuration and also use an SSH client and

view the configuration from the command line.

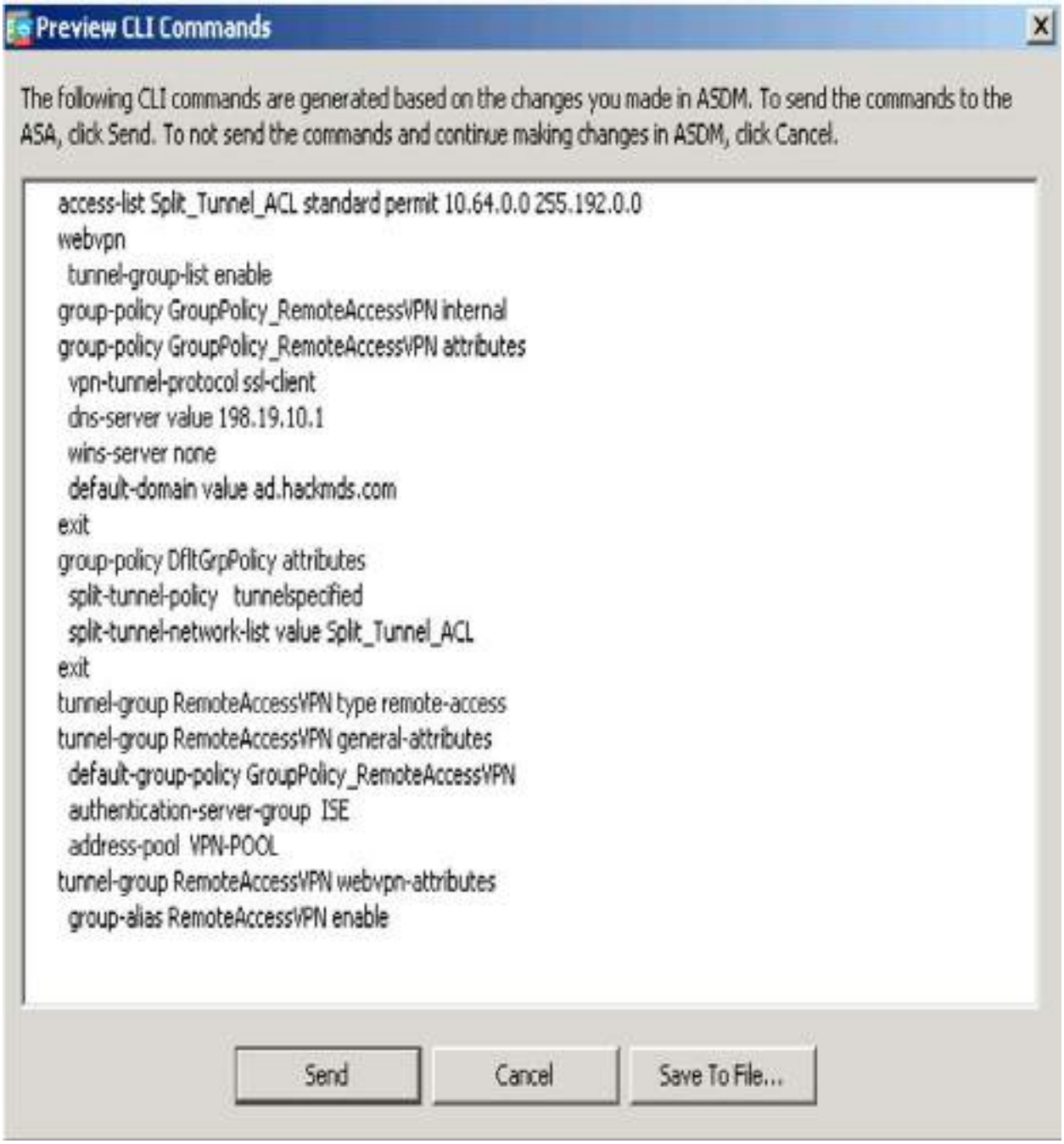


Figure 7-37 Summarized CLI Commands

Cisco ASA CLI Remote Access Configuration

The previous section showed how to use ASDM to configure a remote access

VPN. It also shows the command-line configuration that would be created using the VPN wizard in the GUI. This section shows how to build a remote access VPN by using the command-line interface (CLI) in a Cisco ASA so you have multiple examples of different options.

Note

If you are attempting the SVPN 300-730 exam, you need to understand both the GUI and CLI steps for configuring remote access VPNs.

To build a remote access VPN by using the CLI in a Cisco ASA, follow these steps:

Step 1. Decide which interfaces on the Cisco ASA will act as the management and outside interfaces. The outside interface will be used by remote devices to connect to the VPN headend/NAS. For the outside interface, you access the interface, provide an IP address, and name it **outside**:

```
ASA1(config)# interface ethernet0
ASA1(config-if)# ip address 10.10.5.100
255.255.0.0
ASA1(config-if)# nameif outside
ASA1(config-if)# no shutdown
```

Step 2. Specify the configuration method:

```
ASA1(config)# crypto ikev1 policy 1
encryption aes-256
```

Other options include **aes**, **aes-129**, **aes-256**, **des**, and **3des**. **des** and **3des** are not recommended due to their weak security capabilities.

Step 3. Specify the hash algorithm for the IKE policy (which is also known as the HMAC variant).

```
ASA1(config)# crypto ikev1 policy 1 hash sha
```

Instead of using SHA, you could use MD5.

Step 4. Specify the Diffie–Hellman group for the IKE policy:

```
ASA1(config)# crypto ikev1 policy 1 group 14
```

This is the crypto protocol that allows the IPsec client and the Cisco ASA to establish a shared secret key. It is not recommended to use group 1 due to its weak security.

Step 5. Specify the encryption key lifetime, which is configured using the number of seconds each security association should use before it expires:

```
ASA1(config)# crypto ikev1 policy 1 lifetime
43200
```

This example uses 43200, which equals 12 hours. The available range is 120 to 2147483647.

Step 6. Enable ISAKMP on the interface, which in this case is the outside interface, and save the configuration:

```
ASA1(config)# crypto ikev1 enable outside
ASA1(config)# write memory
```

Step 7. Assign the pool of addresses that will be assigned to remote users as they connect over the VPN, and add a test user and a basic password (or passphrase):

```
ASA1(config)# ip local pool testpool
192.168.0.10-192.168.0.15
ASA1(config)# username testuser password
sftsvpne
```

The passphrase in this case is created from the first letter of each word in the sentence “Studying for the SVPN 300-730 exam,” which equals **sftsvpne**.

Step 8. Create an IKEv1 transform set that specifies the IPsec IKEv1 encryption and hash algorithms used to ensure data integrity:

```
ASA1(config)# crypto ipsec transform set
FirstSet esp-aes esp-sha-hmac
```

You can use **ESP-AES**, **ESP-AES-192**, **ESP-AES-256**, **ESP-DES**,

ESP-3DES, or **ESP-NULL** if you don't want to use encryption. For the hash, you can use **ESP-MD5-HMAC**, **ESP-SHA-HMAC**, or **ESP-NONE** if you don't want to use a HMAC.

Step 9. Specify an IKEv2 proposal set to name the IPsec IKEv2 protocol, encryption, and integrity algorithms that will be used:

```
ASA1(config)# crypto ipsec ikev2 ipsec-
proposal secure_proposal
ASA1(config-ipsec-proposal)# protocol esp
encryption aes integrity sha-1
```

Once again, you can use **DES**, **3DES**, **AES**, **AES-192**, **AES-256**, or **NULL**. For the hash, you also once again use **MD5** or **SHA-1**.

Next, you need to define a tunnel group. Think of a tunnel group as a collection of one or more tunnel policies. Policies might, for example, identify AAA servers, specify connection parameters, and define the default group policy.

Default Tunnels Groups

There are two default tunnel groups on the Cisco ASA. It is okay to change these default groups, but you can't delete them. The ASA needs default tunnel parameters for remote access. The default groups are as follow:

DefaultRAGroup: The default remote-access tunnel group.

DefaultL2Lgrooup: The default LAN-to-LAN tunnel group.

Follow these steps to define a tunnel group:

Step 1. Create a tunnel group:

```
ASA1(config)# tunnel-group MYTUNNELGROUP
type ipsec-ra
```

Step 2. Enter the **general-attributes** mode:

```
ASA1(config)# Tunnel-group MYTUNNELGROUP
general-attributes
ASA1(config-tunnel-general)#
```

Step 3. In the **general-attributes** mode, specify an address pool that will be used for the tunnel group (in this case **TESTPOOL**):

```
ASA1(config-tunnel-general)# address-pool
TESTPOOL
ASA1(config-tunnel-general)# exit
```

Step 4. Enter the IPsec-specific attributes for IKEv1 connections and, if desired, a pre-shared key, which applies only to IKEv1 and can be a string of 1 to 128 characters:

```
ASA1(config)# tunnel-group MYTUNNELGROUP
ipsec-attributes
ASA1(config-tunnel-ipsec)# pre-shared-key
MYPRESHAREDKEY12345
```

Step 5. Create a dynamic crypto map, in this case using **IKEv2** (though you can also use IKEv1):

```
ASA1(config)# crypto dynamic-map
MYDYNAMICMAP 1 set ikev2 ipsec-proposal
SECURE_PROPOSAL
```

Note

Recall that crypto maps are important for defining policy templates when some parameters are not configured. For example, a remote peer that doesn't have a known IP address still needs to connect to establish the remote access VPN.

Optionally, enable a reserve route injection for AnyConnect:

```
ASA1(config)# crypto dynamic-map
MYDYNAMICMAP 1 set reverse route
```

Step 6. Create a crypto map entry that permits the ASA to use the dynamic crypto map to set the parameters of IPsec security associations:

```
ASA1(config)# crypto map mymap 1 ipsec-
isakmp dynamic MYDYNAMICMAP
```

Step 7. Apply the crypto map to the outside interface:

```
ASA1(config)# crypto map mymap 1 ipsec-
isakmp dynamic MYDYNAMICMAP
```

The configuration is now complete. Example 7-1 shows a summary of the code you just built.

Example 7-1 Cisco ASA CLI Remote Access Configuration

```
hostname(config)# crypto ikev1 policy 1 encryption aes-256
hostname(config)# crypto ikev1 policy 1 hash sha
hostname(config)# crypto ikev1 policy 1 group 14
hostname(config)# crypto ikev1 policy 1 lifetime 43200
hostname(config)# crypto ikev1 enable outside
hostname(config)# crypto ikev2 policy 1
hostname(config-ikev2-policy)# group 2
hostname(config-ikev2-policy)# integrity sha512
hostname(config-ikev2-policy)# prf sha512
hostname(config)# crypto ikev2 enable outside
hostname(config)# ip local pool POOL 192.168.0.10-192.168.0.15
hostname(config)# username testuser password 12345678
hostname(config)# crypto ipsec ikev2 ipsec-proposal  AES256-
SHA512
hostname(config-ipsec-proposal)# protocol esp encryption  aes-
256
hostname(config-ipsec-proposal)# protocol esp integrity sha-512
hostname(config)# tunnel-group RAVPN type remote-access
hostname(config)# tunnel-group RAVPN general-attributes
hostname(config-general)# address-pool POOL
hostname(config)# tunnel-group RAVPN ipsec-attributes
hostname(config-tunnel-ipsec)# ikev2 local-authentication
pre-shared-key localravpnkey
hostname(config-tunnel-ipsec)# ikev2 remote-authentication
pre-shared-key remoteravpnkey
hostname(config)# crypto dynamic-map DYNMAP 1 set ikev2
ipsec-proposal AES256-SHA512
hostname(config)# crypto dynamic-map DYNMAP 1 set reverse-route
hostname(config)# crypto map CMAP 1 ipsec-isakmp dynamic DYNMAP
```

```
hostname(config)# crypto map CMAP interface outside
```

Cisco Secure Firewall Remote Access VPN

The next configuration example involves a remote access VPN on a Cisco Secure Firewall (formally called Firepower Threat Defense appliance). Remote access can be accomplished using SSL and IPsec/IKEv2 VPNs. In this example, you will once again be using AnyConnect Security Mobility Client to provide a full tunnel, which could use secure SSL or IPsec/IKEv2 to secure the gateway for remote users.

Cisco Secure Firewall concepts VPN is not a learning requirement for the SVPN exam; however, it is a widely deployed option and concept we believe is very relevant for real-world remote access VPN requirements. If your focus is to pass the SVPN exam, you can skip this section. We highly recommend validating the latest version of the SVPN learning objectives because Cisco Secure Firewall could be added in the near future!

Note

As of Firepower Version 6.2.3, AnyConnect is the only Firepower-supported client.

Cisco Secure Firewall Features

A Cisco Secure Firewall solution provides the following remote access features:

- AnyConnect Security Mobility Client provides SSL and IPsec/IKEv2.
- Cisco Secure Firewall Management Center supports multiple combinations, such as IPv6 over an IPv4 tunnel.
- Cisco Secure Firewall provides configuration support on both Cisco Secure Firewall Management Center and Cisco Secure Device Manager.

- Cisco Secure Firewall provides support for both Cisco Secure Firewall Management Center and Cisco Secure Firewall high-availability options.
- Cisco Secure Firewall provides support for multiple interfaces and multiple AAA servers.

Just as with the Cisco ASA, with Cisco Secure Firewall, if the Cisco AnyConnect client isn't already installed, users can access the IP address of the browser interface for the Cisco Secure Firewall appliance. The browser interface can be configured to accept SSL or IPsec/IKEv2 VPN connections. The user is presented with a login screen (unless they are using HTTP:// and redirected to HTTPS://), and after logging in, the user can download the AnyConnect VPN client, as discussed in the previous section.

Follow these steps to configure a remote access VPN on Cisco Secure Firewall:

Step 1. Log in to Cisco Secure Firewall.

Step 2. Select **Devices** > **VPN** > **Remote Access** (see Figure 7-38).

Figure 7-38 Logging In to Cisco Secure Firewall

Step 3. If this is your first time setting up a remote access VPN on this device, click the **Add** button to add a new configuration (see Figure 7-39).

Figure 7-39 Adding a Configuration

Step 4. Work through the five steps of the Cisco Secure Firewall Remote Access VPN Wizard (see Figure 7-40):

1. On the policy assignment page, give your policy a name and a description and decide whether you want to use SSL and/or IPsec/IKEv2, and select which headend device will offer remote access VPN services. Make your choices and click **Next**.

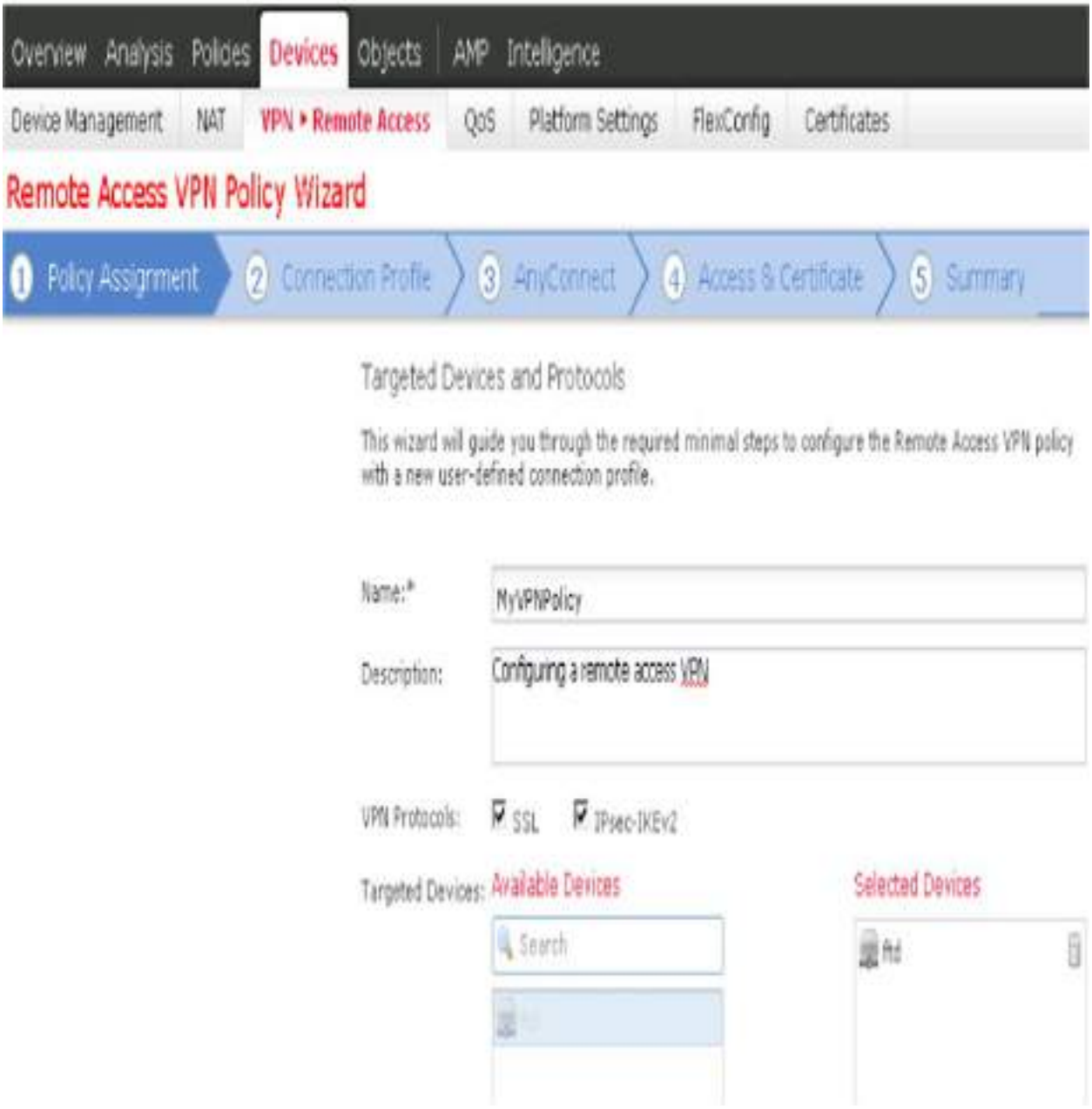


Figure 7-40 Cisco Secure Firewall Remote Access VPN Wizard

2. On the Connection Profile page, choose the authentication method, authentication server (realm or RADIUS), IPv4 and IPv6 IP address pools for remote devices, and the group policy (see Figure 7-41). For this example, use an Active Directory setup called AD and the default group policy called DfltGrpPolicy. You can edit the group policy by clicking the selected group policy or selecting another group policy if one is available. Once you make

your selection, click the **Next** button.

Note

Consider giving your group policies names that are easily identifiable because it makes it easier to locate the appropriate one when you are trying to choose between many of them.

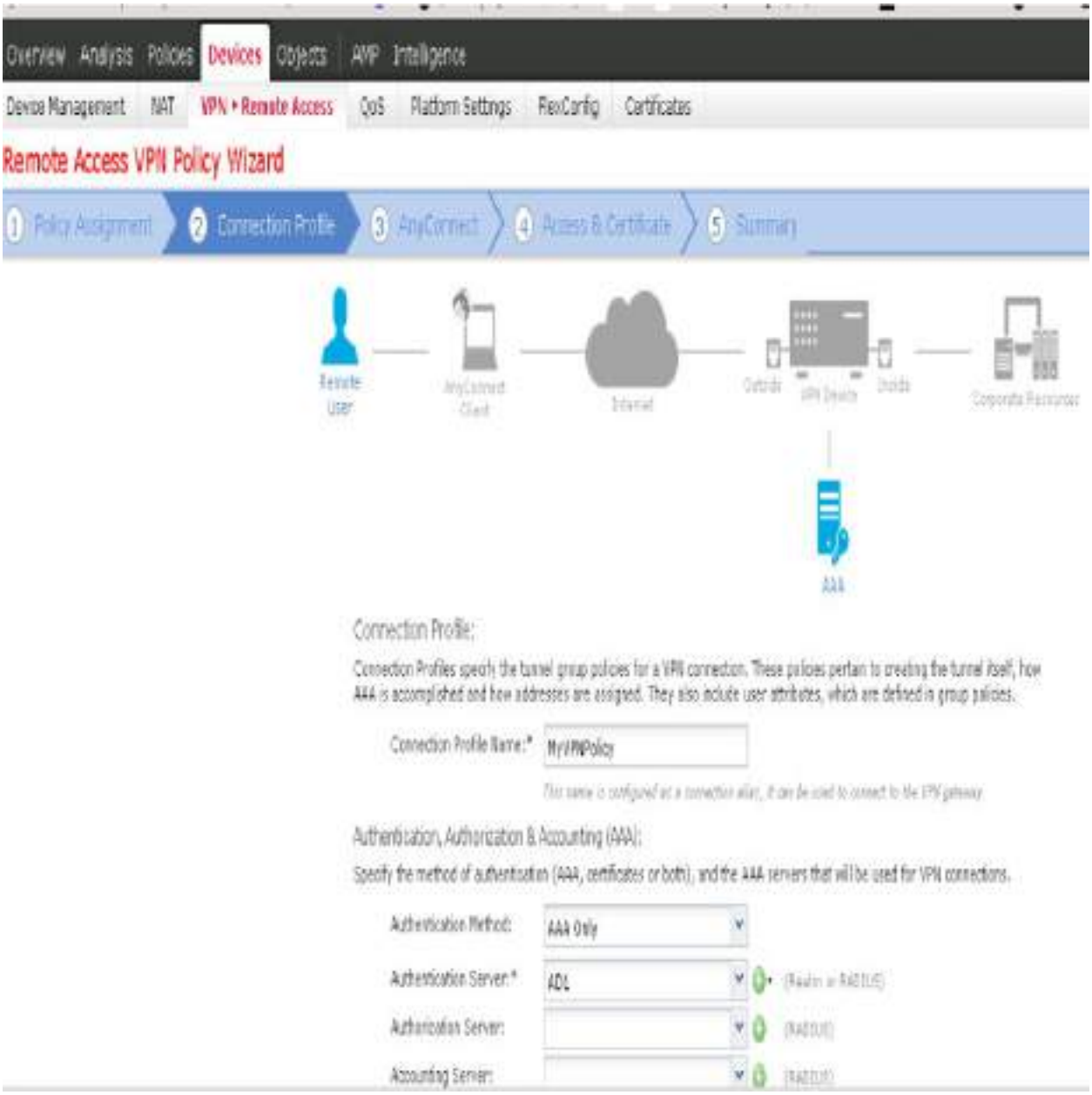


Figure 7-41 Connection Profile Page

3. On the AnyConnect page, select **Mac OS** to choose the macOS AnyConnect package and then click **Next** (see Figure 7-42).

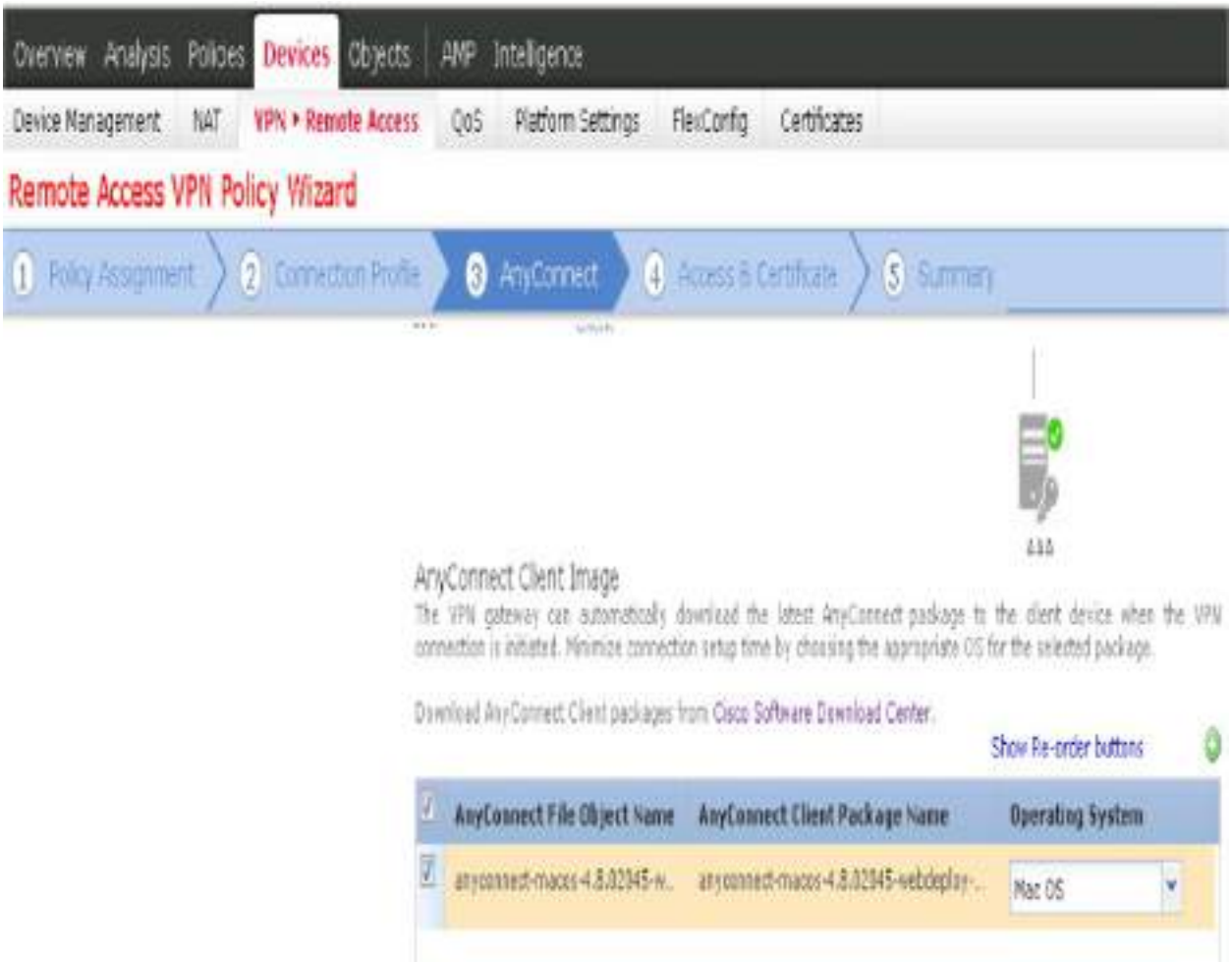


Figure 7-42 AnyConnect Page

If you don’t have the package, you can click the **Cisco Software Download Center** link to quickly access the different packages. Figure 7-43 shows an example of uploading a macOS AnyConnect package to Firepower; it must be a .pkg file.

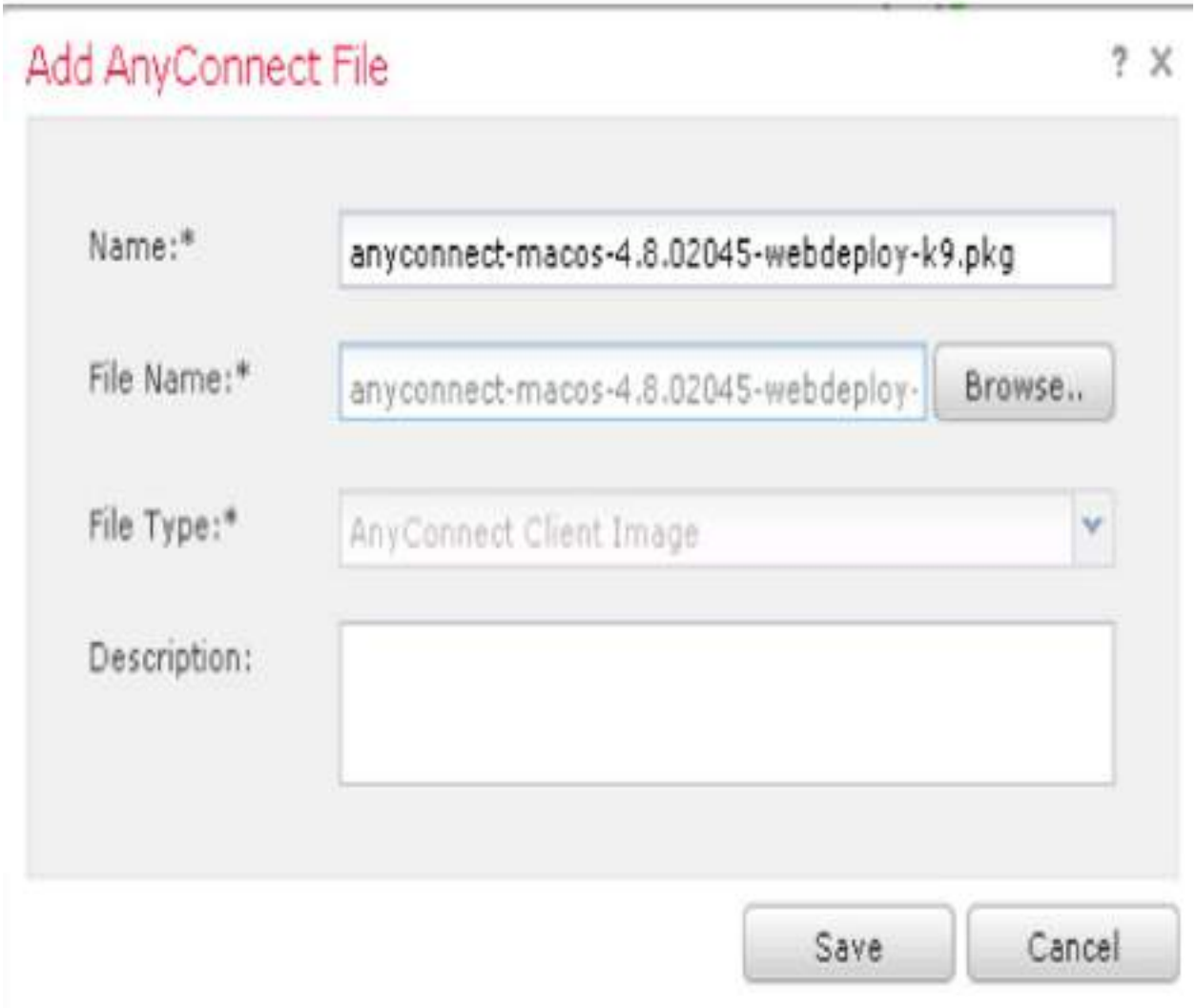


Figure 7-43 Uploading a macOS AnyConnect Package to Firepower

Note

You need a Cisco CCO login and authorized access to download the AnyConnect packages.

4. On the Access & Certificates page, choose **VLAN 1** as the interface group or security zone users will be able to access (which is essentially what a remote user can connect to; see Figure 7-44).

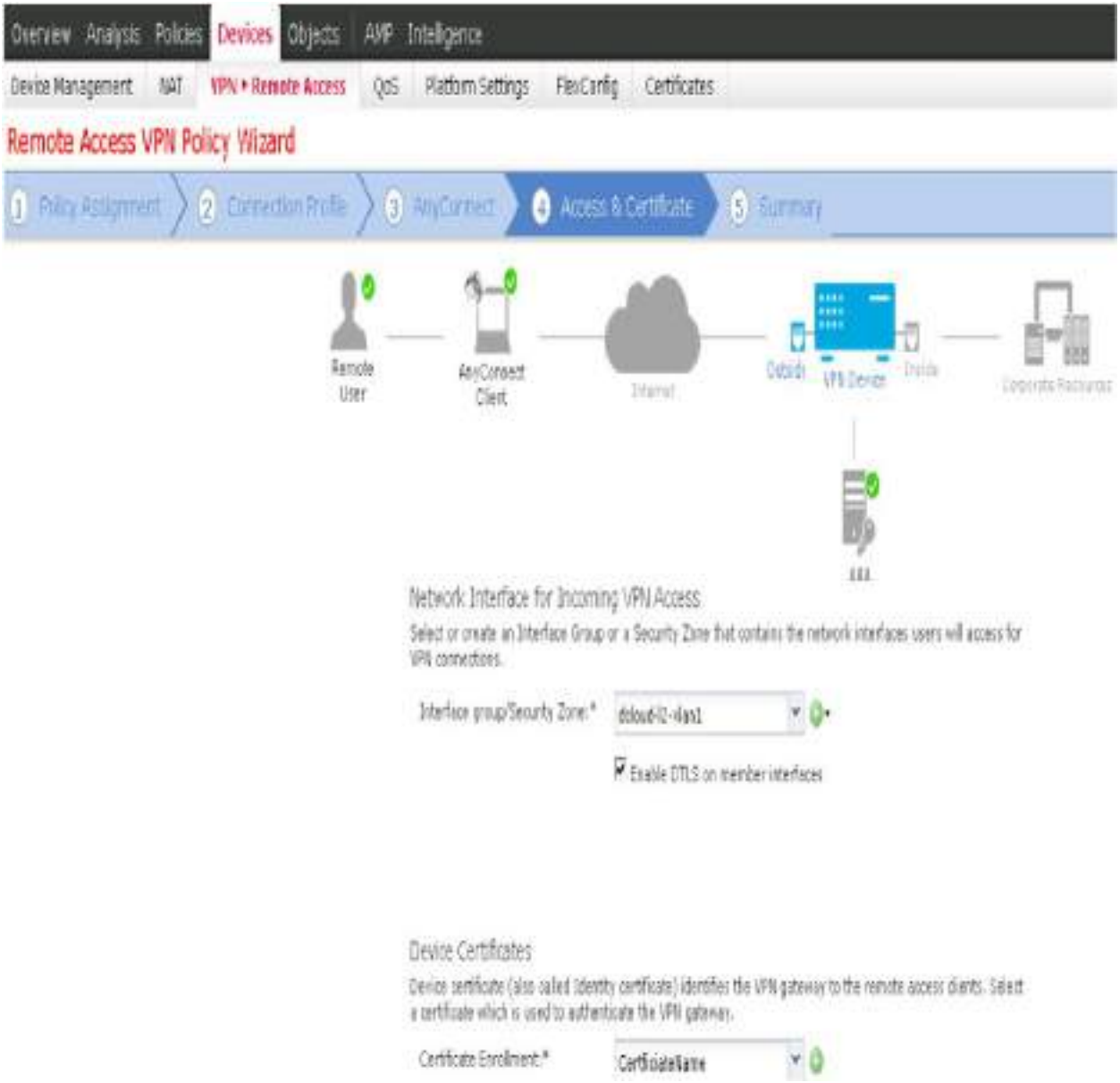


Figure 7-44 Access & Certificates Page

Another item to address is the device certificates that will be used. You can select an existing certificate or configure a new one by clicking the + button. You have the options SCEP, Self-Signed Certificate, Manual Certificate, or PKCS12. For this example, use **Self-Signed Certificate** (see Figure 7-45).

Figure 7-45 Device Certificates

On the Certificate Parameters tab, fill out information about you certificate. If you choose to use an FQDN, you have to provide that name in the Common Name (CN) section (see Figure 7-46).

Figure 7-46 Certificate Parameters Tab

The next tab reviews the security key (see Figure 7-47). You have the option to use RSA or ECDSA (the elliptic curve version).

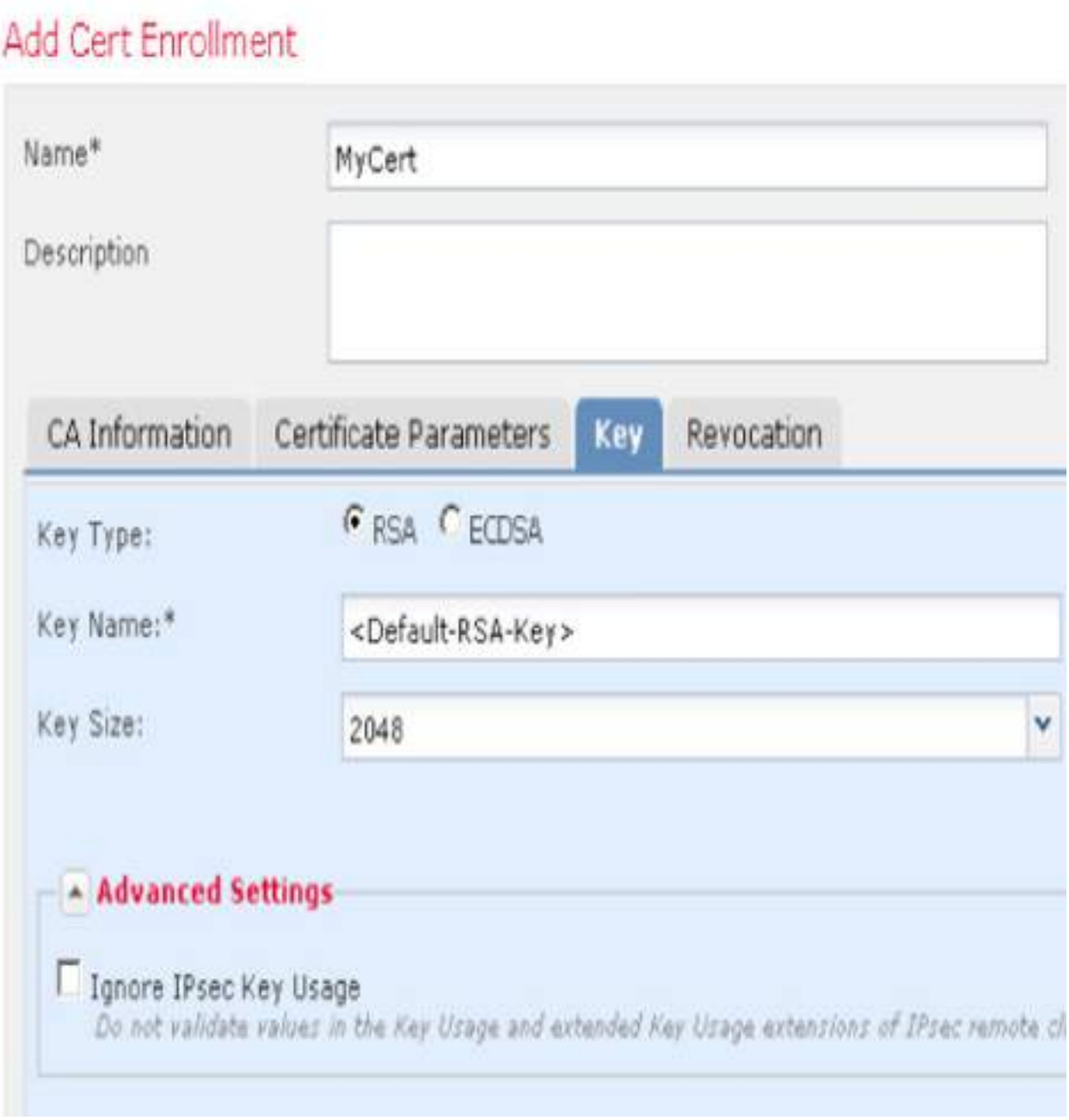


Figure 7-47 Choosing the Security Key

The final tab covers the revocation options (see Figure 7-48).

Figure 7-48 Revocation Options

There is also an option to bypass access control for VPN traffic

available on the Access & Certificates page of the wizard. You can enabled this by selecting the checkbox and then click Next (see Figure 7-49).

Figure 7-49 Bypassing Access Control for VPN Traffic

Step 8. On the last page of the configuration wizard, which provides a summary of what you have set up, if everything looks good, click the **Finish** button (see Figure 7-50).

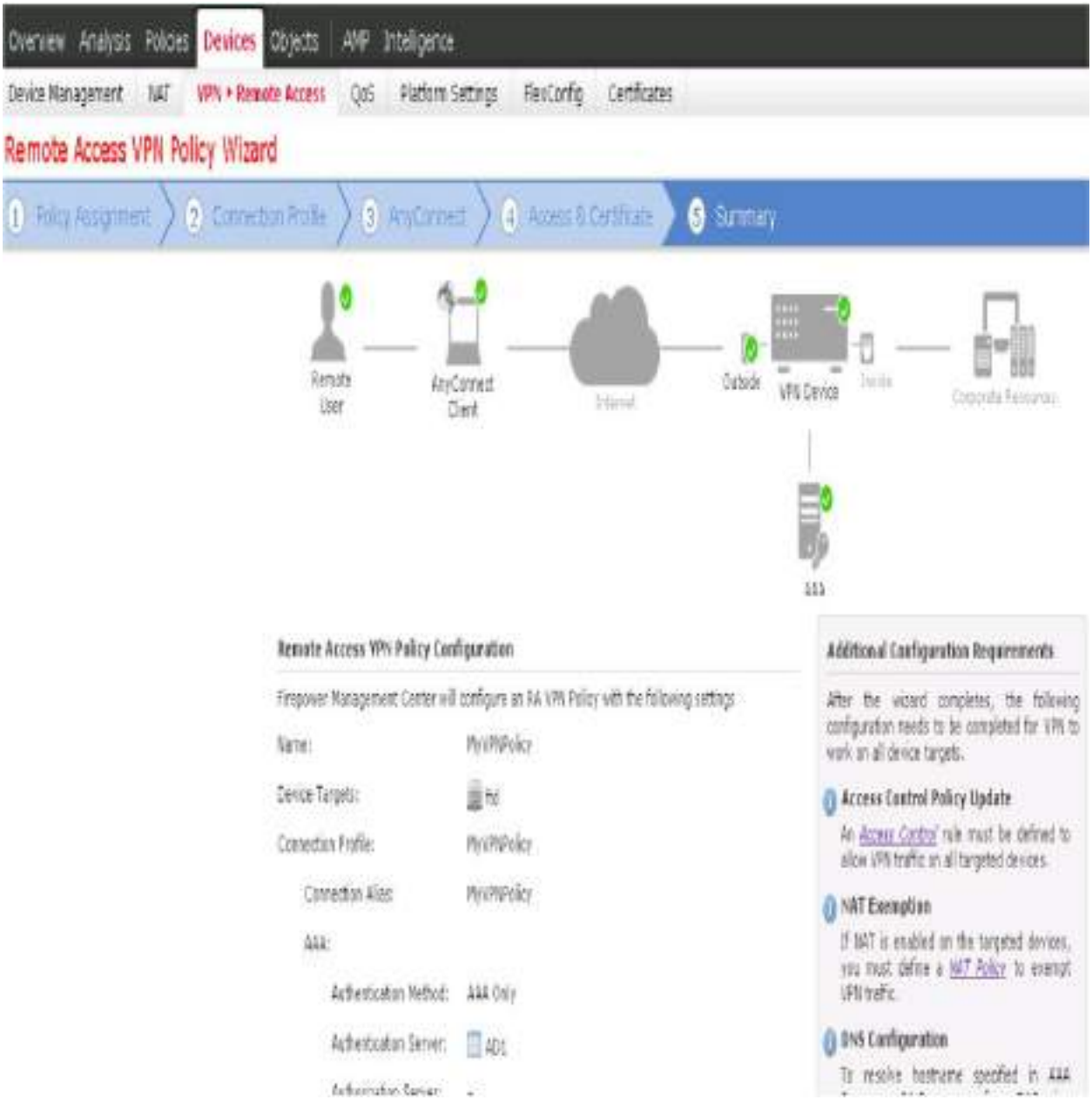


Figure 7-50 Summary Page

You need to deploy your configuration by clicking the **Deploy** button to make remote access VPN services available to users. You can use the User Activity window to monitor VPN users after your VPN configuration is deployed. You can reach this window to selecting **Analysis** > **Users** > **User Activity** > **User Activity** (see Figure 7-51).

Figure 7-51 User Activity for Monitoring VPN Users

Cisco Meraki Remote Access VPN

Another popular Cisco security solution that offers remote access VPN functionality is the Meraki security appliance series. Client VPN services use the L2TP tunneling protocol, which doesn't require any additional software for various device types that have native support for L2TP, including Windows, macOS, iOS, and Android devices. In order to use Linux devices, you need to support L2TP through a third-party package.

Once again, we want to point out that Meraki remote access concepts are not part of the SVPN learning objectives, but we have included a small section based on its popularity within organizations around the world. If your focus is passing the SVPN exam, feel free to skip this section; however, we once again recommend keeping an eye out on the latest SVPN learning objectives. Based on Meraki's popularity, Cisco might add Meraki as a future SVPN

learning objective.

Hash algorithms that are supported along with L2TP are 3DES and SHA-1 for Phase 1 nd AES-128/3DES and SHA-1 for Phase 2. Meraki has disclaimers for offering stronger encryption methods to support PCI-DSS; if you need such encryption, you must contact Meraki support about AES-128 encryption with Diffie–Helman group 5 capabilities.

Meraki Remote Access Configuration Example

Meraki is simple, and the entire remote access VPN configuration is located on one screen, which you reach by selecting **Security & SD-WAN** > **Configure** > **Client VPN** (see Figure 7-52).

Figure 7-52 Meraki Client VPN

Configuration starts with enabling the remote access VPN capability. Next, you specify the client subnet pool that will be used as people use the VPN to access the network. You choose the DNS name server, configure authentication, and add users. Authentication includes a secret as well as the

user password. This setup is very straightforward. Authentication can be local or can use an external source, such as Active Directory or RADIUS. On a mobile device, you choose L2TP as the VPN protocol, put in the server that Meraki generates for you, choose an account that was created, and enter the password and the secret you added to Meraki—and that's it. Figure 7-53 shows an example of an iOS device set up to connect to a Meraki remote access VPN.

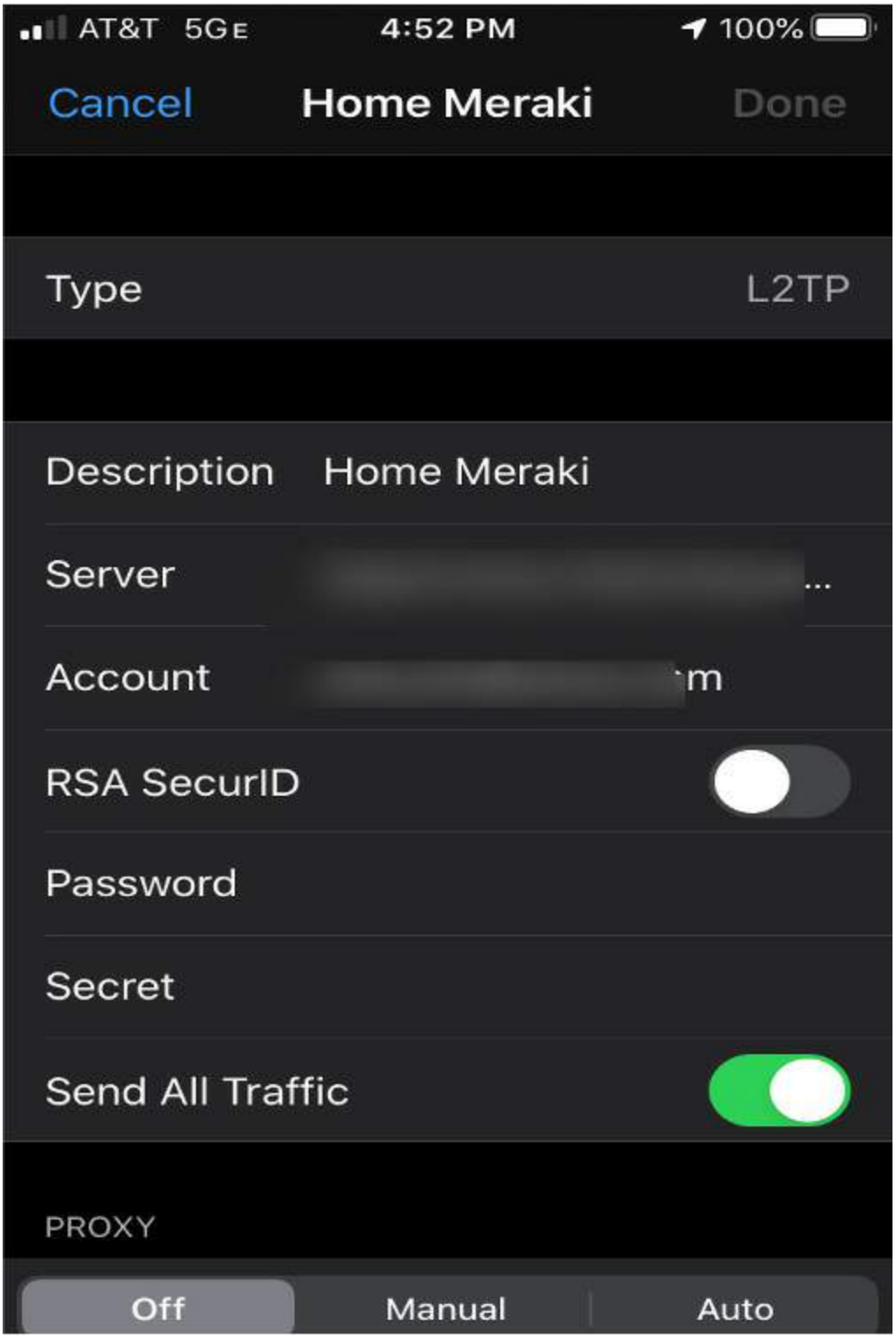


Figure 7-53 Mobile Device Setup to Use a Meraki Remote Access VPN

Router Configuration

To this point in the chapter, you have seen a number of examples of configuring remote access VPNs on Cisco's popular security appliances. In this section, you will see how to configure a remote access VPN on a Cisco IOS router. The concepts here are similar to those you've already seen, but you don't have a pretty GUI or wizards available to help with the configuration.

You can configure a Cisco router to act as an AnyConnect SSLVPN headend. For the router example in this section, we use a Cisco Cloud Services Router (CSR) device running IOS XE 16.9.2 and Cisco AnyConnect 4.6.03049 running on Windows 10. Figure 7-54 provides a diagram of this configuration.

Figure 7-54 AnyConnect IOS XE Router Design Diagram

It is important to know that remote access VPN concepts are not on the SVPN exam, but client based remote access VPN is still an available option for real-world deployments. Clientless SSLVPN on Cisco routers has been marked as end-of-sale, making it a depreciated option that eventually will not be supported. If your focus for this book is passing the SVPN exam, feel free to skip this section.

Key Concepts for Remote Access on Routers

There are a few key points to keep in mind regarding requirements for the Cisco router. First, the Cisco router must have a SEC-K9 feature set in order

to support SSLVPN features, regardless of the IOS version that is installed. SEC-K9 offers additional features that are included with the base router image. Examples of features included when a SEC-K9 bundle is enabled include IKEv1/IPsec/PKI, IPsec/GRE, Easy VPN with DVTI, DMVPN, static VTI, firewall, network foundation protection, and GETVPN. The SSLVPN license is counted, which means you buy a certain number of seats or allowed VPN users. Intrusion prevention and content filtering are also possible, but both of these features require a subscription.

Another key point is the end-of-sale and end-of-life announcement for clientless SSLVPN/WebVPN on Cisco IOS software. This announcement means you should be using only client-based remote access VPN options when using a Cisco router. That announcement can be found at https://www.cisco.com/c/en/us/products/collateral/security/ios-sslvpn/eos-eol-notice-c51-731468.html.

The steps you take to enable the ability to use SSLVPN on a router depend on which version of code or IOS is being used. Anything after IOS Release 15.3 has SSLVPN enabled upon booting the SEC-K9 technology package. Older images may require a special LIC file to be installed, depending on whether the image is older than Release 15.1. It is recommended to verify the version of software you are running and consult with the latest data sheet to ensure that you have the proper level of code and licenses installed.

Remote Access on Router Configuration Example

To configure a Cisco router to act as an AnyConnect SSLVPN headend, follow these steps:

Step 1. Verify that you have the right licenses by using the commands **show license** and **show version**.

Step 2. Enable AAA, configure AAA lists, and add a username to the local database:

```
aaa new-model
!
aaa authentication login a-eap-authen-local
```

```
local
aaa authorization network a-eap-author-grp
local
!
username test password PASSWORD123
```

Step 3. Configure a trust point that will hold the router certificate (in this case, **pkcs12**):

```
Router(config)# crypto pki import IKEv2-TP
pkcs12
bootflash:IKEv2-TP.p12 password PASSWORD123
```

Step 4. Define a local IP address pool to assign addresses to AnyConnect VPN clients:

```
ip local pool ACPOOL 192.168.10.5
192.168.10.10
```

Step 5. Create an IKEv2 local authorization policy:

```
crypto ikev2 authorization policy ikev2-
auth-policy pool
ACPOOL
dns 10.0.1.1
```

Step 6. Optionally, create an IKEv2 proposal and policy (otherwise, smart defaults will be used):

```
crypto ikev2 proposal IKEv2-prop1
  encryption aes-cbc-256
  integrity sha256
  group 14
!
crypto ikev2 policy IKEv2-pol
  proposal IKEv2-prop1
```

Step 7. Create an AnyConnect profile that will be delivered to the client machine by using the AnyConnect profile editor (see Figure 7-55).

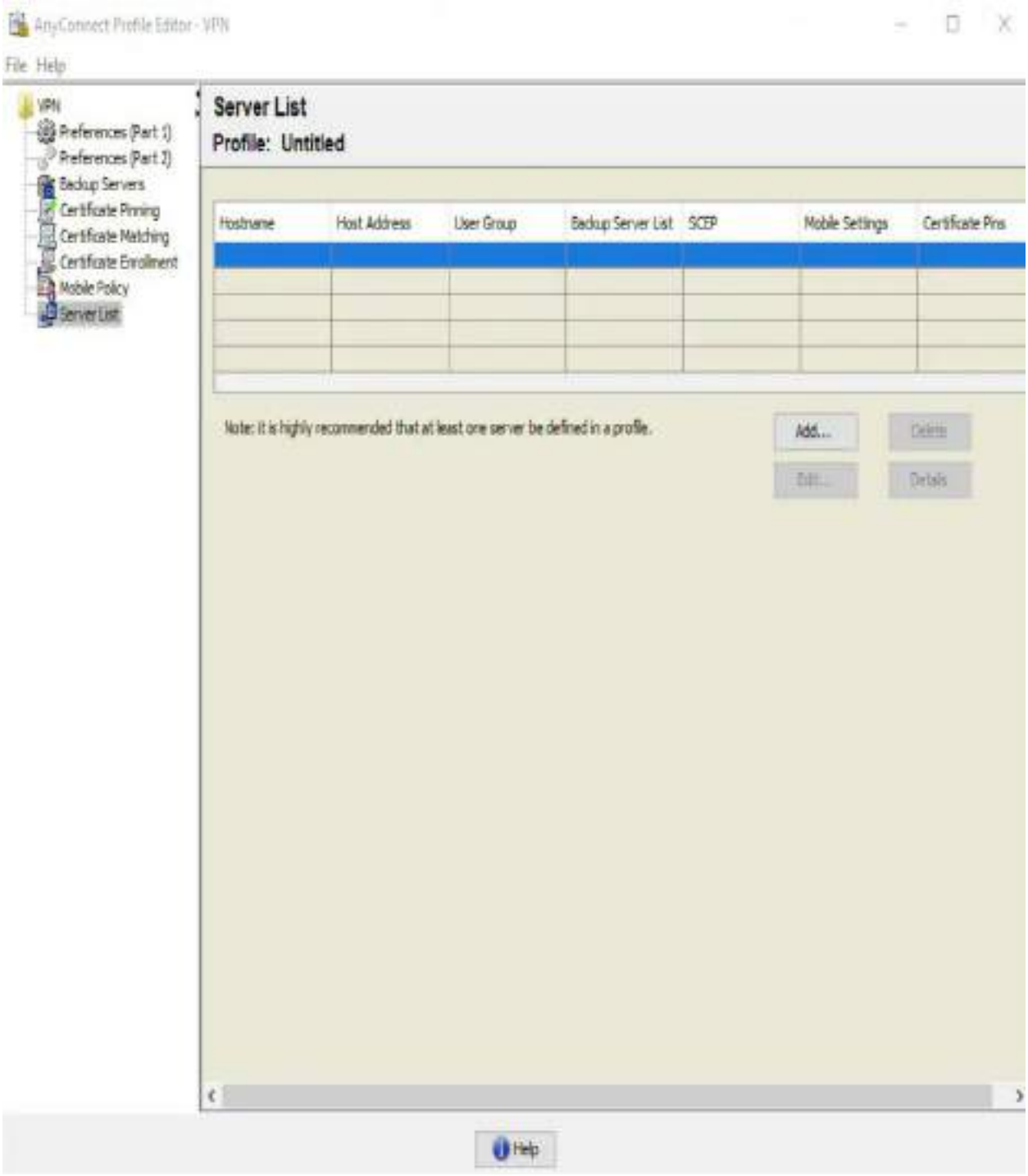


Figure 7-55 Accessing the AnyConnect Profile Editor

Step 8. Click **Add** to create an entry for the VPN gateway, select **IPsec** as the primary protocol, and uncheck the **ASA gateway** option (see Figure 7-56).

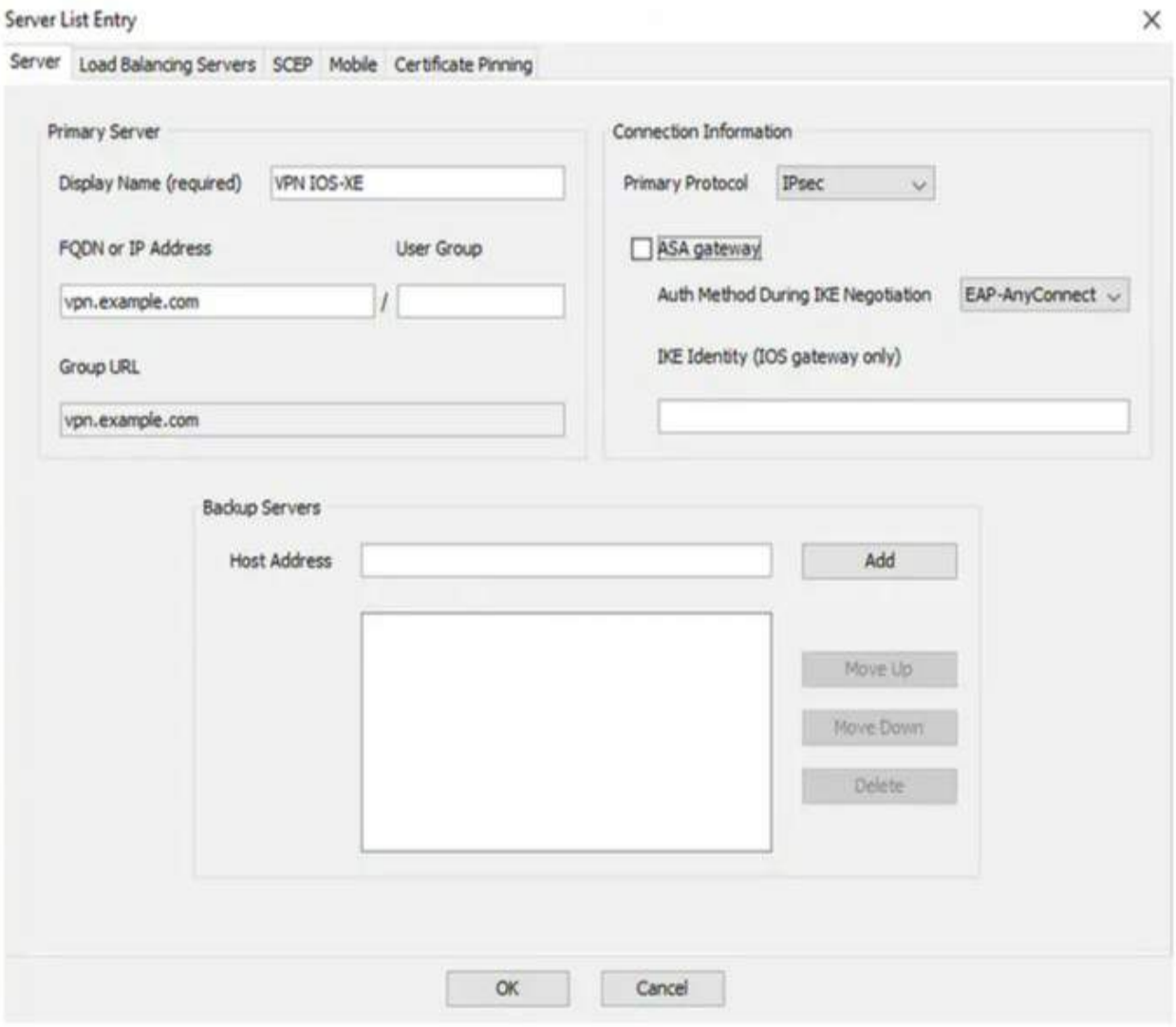


Figure 7-56 Configuring the AnyConnect Profile Editor

Step 9. Save the profile by selecting **File** > **Save As** and using the filename **acvpn.xml**.

Step 10. Create an IKEv2 profile for the AnyConnect-EAP method of client authentication:

```
crypto ikev2 profile AnyConnect-EAP
    match identity remote key-id
*$AnyConnectClient$*
    authentication local rsa-sig
    authentication remote anyconnect-eap
aggregate
```

```
    pki trustpoint IKEv2-TP
    aaa authentication anyconnect-eap a-eap-
authen-local
    aaa authorization group anyconnect-eap
list a-eap-author-grp   ikev2-auth-policy
    aaa authorization user anyconnect-eap
cached
    virtual-template 100
    anyconnect profile acvpn
```

Step 11. Disable HTTP-URL-based certificate lookup and the HTTP server on the router:

```
no crypto ikev2 http-url cert
no ip http server
no ip http secure-server
```

Step 12. Define the encryption and hash algorithms used to protect data that will travel over the VPN:

```
crypto ipsec transform-set TS esp-aes 256
esp-sha256-hmac
 mode tunnel
```

Step 13. Configure a loopback interface with a dummy IP address (in this case, **10.0.0.1**), from which the Virtual-Access interfaces will borrow the IP address:

```
interface loopback100
 ip address 10.0.0.1 255.255.255.255
```

Step 14. Configure a virtual template (associated in the IKEv2 profile):

```
interface Virtual-Template100 type tunnel
   ip unnumbered Loopback100
   ip mtu 1400
   tunnel mode ipsec ipv4
   tunnel protection ipsec profile
AnyConnect-EAP
```

Step 15. Optionally, enable split tunneling (such as if you don’t want all traffic to be sent through the tunnel):

```
ip access-list standard split_tunnel
 permit 10.0.0.0 0.255.255.255
!
crypto ikev2 authorization policy ikev2-
auth-policy
 route set access-list split_tunnel
```

Step 16. If all traffic is going through the VPN, use NAT to allow Internet connectivity for remote clients:

```
ip access-list extended NAT
 permit ip 192.168.10.0 0.0.0.255 any
!
ip nat inside source list NAT interface
GigabitEthernet1 overload
!
interface GigabitEthernet1
 ip nat outside
!
interface Virtual-Template 100
 ip nat inside
```

Step 17. Test the configuration. Using a fresh installation of the AnyConnect client (with no XML profiles added), ensure that the user is able to manually enter the FQDN of the VPN gateway in the address bar of AnyConnect client. This should result in an SSL connection being made to the gateway. The AnyConnect client does not attempt to establish the VPN tunnel with IKEv2/IPsec protocols by default. Having the XML profile installed on the client is mandatory to establish the IKEv2/IPsec tunnel with IOS XE VPN gateway.

To use a particular profile, select its name from the drop-down list in the AnyConnect address bar. The name that appears is the same name as specified with Display Name in the AnyConnect profile editor. In this case, select the newly configured profile, as shown in Figure 7-57, and click **Connect**.

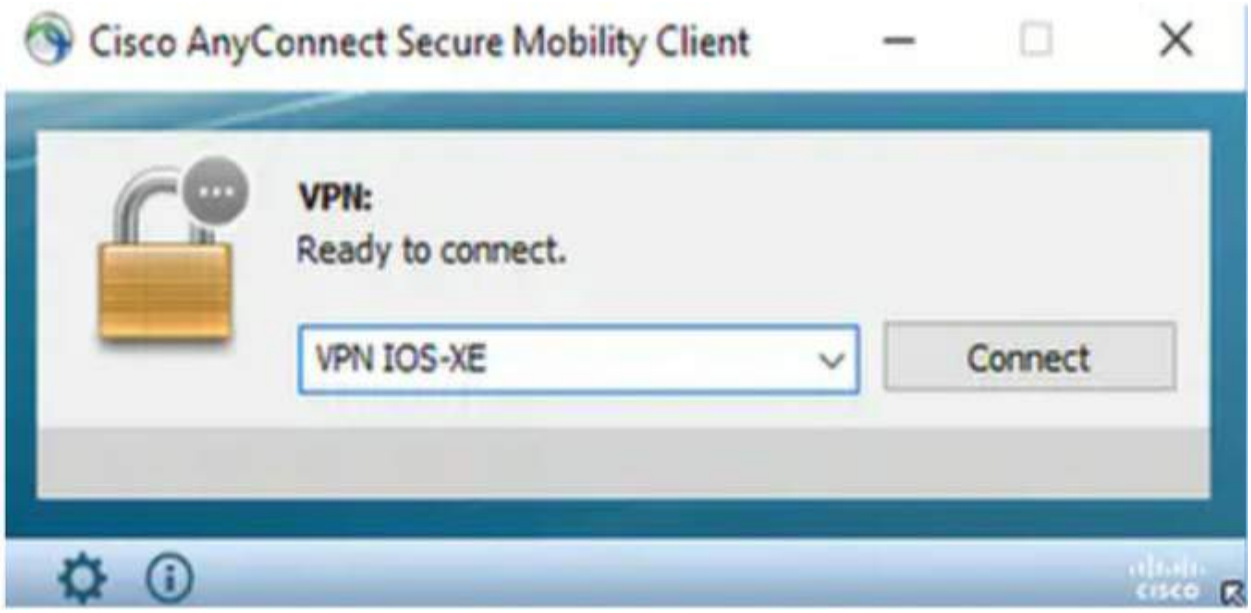


Figure 7-57 Selecting a Profile in AnyConnect

Note

If you are using IOS XE software older than Release 16.9.1, you need to disable the AnyConnect downloader capabilities. Before that release, it was not possible to upload an XML profile to a router. If a profile is not available, the connection will fail. Disabling the AnyConnect downloader capability is a workaround.

Step 18. Verify that the VPN is established:

```
show crypto ikev2 sa detailed
```

You should see details such as the following information about the status being ready:

```
1     192.0.2.1/4500      192.0.2.100/50899
  none/none             READY
```

That wraps up our overview of remote access with Cisco technology. The SVPN exam will focus on remote access within a Cisco ASA using both the command line and ASDM. We dive deeper into remote access VPN deployment options in the remaining chapters. We also included additional

learning topics, such as Cisco Secure Firewall, Meraki, and client-based remote access on Cisco routers as additional learning topics that won't be on the SVPN exam but are leveraged in organizations around the world. Know that any of these topics could one day be added to future versions of the SVPN exam learning objectives.

Summary

This chapter kicks off our review of remote access VPNs. It discusses planning for a remote access deployment, including the questions to consider during VPN design sessions. This chapter also looks at the different components involved with remote access VPN deployments, including hardware, software, encryption, and everything in between. This chapter examines the different forms of encryption, including the value of elliptic curve cryptography. This chapter provides a handful of basic remote access VPN configuration examples, including using the Cisco ASA CLI, Cisco ASA GUI (ASDM), Cisco IOS, Cisco Secure Firewall, and Cisco Meraki.

Now that you have a basic understanding of how remote access VPN technology works, it's time to look more closely at the different VPN frameworks Cisco offers that support remote access VPN capabilities. Topics moving forward will be focused on remote access VPN and related to what is required in the SVPN version 1.1 of the exam.

Next up, we will dive into clientless Access SSLVPNs on the ASA.

References

2017 Cisco AnyConnect Secure Mobility Client. Retrieved from https://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-secure-mobility-client/at_a_glance_c45-578609.pdf

Anand, Adity (July 14, 2018). SSL Strip & How Awesome It Is! Retrieved from https://medium.com/bugbountywriteup/ssl-strip-how-awesome-it-is-a0eb79e28bcc

AnyConnect: Configure Basic SSLVPN for IOS Router Headend With the

User of CLI. Retrieved from https://www.cisco.com/c/en/us/support/docs/security/anyconnect-secure-mobility-client/200533-AnyConnect-Configure-Basic-SSLVPN-for-I.html

Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 4.0 Retrieved from https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect40/administration/guide/b_AnyConnect_Administrator_Guide_4-0/anyconnect-profile-editor.html#ID-1430-0000000c

Cisco AnyConnect Secure Mobility Client Data Sheet. Retrieved from https://www.cisco.com/c/en/us/products/collateral/security/anyconnect-secure-mobility-client/datasheet-c78-733184.html

CLI Book 3: Cisco ASA Series VPN CLI Configuration Guide, 9.5. Retrieved from https://www.cisco.com/c/en/us/td/docs/security/asa/asa95/configuration/vpn/asa-95-vpn-config/vpn-remote-access.html#ID-2444-00000088

Configure AnyConnect Secure Mobility Client with Split Tunneling on an ASA. Retrieved from https://www.cisco.com/c/en/us/support/docs/security/anyconnect-secure-mobility-client/119006-configure-anyconnect-00.html

FlexVPN: AnyConnect IKEv2 Remote Access with Local User Database, https://www.cisco.com/c/en/us/support/docs/security/flexvpn/200555-FlexVPN-AnyConnect-IKEv2-Remote-Access.html

Next Generation Cryptography. Retrieved from https://tools.cisco.com/security/center/resources/next_generation_cryptography

Silver, Laura (February 5, 2019). Smartphone Ownership Is Growing Rapidly Around the World, but Not Always Equally. Retrieved from https://www.pewresearch.org/global/2019/02/05/smartphone-ownership-is-growing-rapidly-around-the-

world-but-not-always-equally/

Smeets, Marten (July 4, 2017). How to Choose Your Cipher Suite. Retrieved from https://technology.amis.nl/2017/07/04/ssltls-choose-cipher-suite/#prettyPhoto

Snyder, Joel (March 21, 2011). Retrieved from https://www.networkworld.com/article/2200809/cisco-has-long-history-with-vpns.html

Sullivan, Nick (October 14, 2013). A (Relatively Easy to Understand) Primer on Elliptic Curve Cryptography. Retrieved from https://arstechnica.com/information-technology/2013/10/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/3/

Exam Preparation Tasks

As mentioned in the section "How to Use This Book" in the Introduction, you have a couple of choices for exam preparation: the exercises here, Chapter 11, "Final Preparation," and the exam simulation questions in the Pearson Test Prep software online.

Review All Key Topics

Review the most important topics in the chapter, noted with the key topics icon in the outer margin of the page. Table 7-3 lists these key topics and the page number on which each is found.

Table 7-3 Key Topics for Chapter 7

Key Topic Element	Description	Page Number
Figure 7-3	Cisco AnyConnect Options	
List	Default connection profiles	
List	Cryptographic algorithm categories	
Table 7-2	Encryption strength summary	
List	The Diffie–Hellman group options	
List	Default tunnel groups options	

15%	1.0 Site-to-site Virtual Private Networks on Routers and Firewalls 1.1 Describe GETVPN 1.2 Describe uses of DMVPN 1.3 Describe uses of FlexVPN
20%	2.0 Remote access VPNs 2.1 Implement AnyConnect IKEv2 VPNs on ASA and routers 2.2 Implement AnyConnect SSLVPN on ASA 2.3 Implement Clientless SSLVPN on ASA 2.4 Implement Flex VPN on routers
35%	3.0 Troubleshooting using ASDM and CLI 3.1 Troubleshoot IPsec 3.2 Troubleshoot DMVPN 3.3 Troubleshoot FlexVPN 3.4 Troubleshoot AnyConnect IKEv2 on ASA and routers 3.5 Troubleshoot SSL VPN and Clientless SSLVPN on ASA
30%	4.0 Secure Communications Architectures 4.1 Describe functional components of GETVPN, FlexVPN, DMVPN, and IPsec for site-to-site VPN solutions 4.2 Describe functional components of FlexVPN, IPsec, and Clientless SSL for remote access VPN solutions 4.3 Recognize VPN technology based on configuration output for site-to-site VPN solutions 4.4 Recognize VPN technology based on configuration output for remote access VPN solutions 4.5 Describe split tunneling requirements for remote access VPN solutions 4.6 Design site-to-site VPN solutions 4.6.a VPN technology considerations based on functional requirements 4.6.b High availability considerations 4.7 Design remote access VPN solutions 4.7.a VPN technology considerations based on functional requirements 4.7.b High availability considerations 4.7.c Clientless SSL browser and client considerations and requirements 4.8 Describe Elliptic Curve Cryptography (ECC) algorithms

Complete Tables and Lists from Memory

There are no memory tables in this chapter.

Define Key Terms

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

network access server (NAS)
FlexVPN
connection profile
group policy
split tunneling
symmetric key algorithm
public key algorithm
elliptic curve algorithm
hash
trapdoor function
Diffie–Hellman (DH)

Chapter 8. Clientless Remote Access SSLVPNs on the ASA

This chapter covers the following topics:

- **Clientless SSLVPN Overview:** This section covers the basics of clientless SSLVPNs and how they compare to client-based AnyConnect VPNs.
- **Clientless SSLVPN Prerequisites:** This section covers the licensing, operating system, browser, and other software required to implement clientless SSLVPNs with the ASA.
- **Basic Clientless SSLVPN Configuration:** This section describes the basic steps involved in configuring a basic clientless SSLVPN, including certificates, group policies, connection profiles, and authentication.
- **Extended Clientless SSLVPN Configuration Options:** This section describes how to configure optional, but common, features of clientless SSLVPNs, including bookmarks, web ACLs, port forwarding, smart tunnels, and client/server plug-ins.

"Details make perfection, and perfection is not a detail."

—Leonardo Da Vinci

This chapter covers the following objective:

- 2.0 Remote access VPNs
  - 2.3 Implement Clientless SSLVPN on ASA
- 4.0 Secure Communication Architectures
  - 4.2 Describe functional components of FlexVPN, IPsec, and Clientless SSL for remote access VPN solutions
  - 4.4 Recognize VPN technology based on configuration output for

remote access VPN solutions

- 4.7 Design remote access VPN solutions
  - 4.7.c Clientless SSL browser and client considerations and requirements

Chapter 7, "Remote Access VPNs," explored remote access VPNs at a conceptual level. Now that you have the remote access VPN foundational concepts under your belt, it is time to dig deeper into key learning objectives for the SVPN exam regarding remote access VPN technology. This chapter looks at the basic steps to configure a clientless SSLVPN on the ASA in addition to key features available with clientless SSLVPNs, such as bookmarks, web ACLs, port forwarding, smart tunnels, and client/server plug-ins.

Learning beyond the SVPN concepts:

- Clientless VPN Overview
- VPN Licensing

"Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz enables you to assess whether you should read the entire chapter. If you miss no more than one of these self-assessment questions, you might want to move ahead to the "Exam Preparation Tasks" section of the chapter. Table 8-1 lists the major headings in this chapter and the "Do I Know This Already?" quiz questions related to the material in each of those sections to help you assess your knowledge of these specific areas. The answers to the "Do I Know This Already?" quiz appear in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes."

Table 8-1 "Do I Know This Already?" Foundation Topics Section-to-Question Mapping

Foundation Topics Section	Questions
Clientless SSLVPN Overview	1
Clientless SSLVPN Prerequisites	2
Basic Clientless SSLVPN Configuration	3–6, 8, 10
Extended Clientless SSLVPN Configuration Options	7, 9

1. A clientless SSLVPN uses which of the following protocols?

a. SSL

b. TLS

c. IKEv2

d. IPsec

2. Which of the following licenses does *not* support clientless SSLVPNs?

a. AnyConnect Base

b. AnyConnect Plus

c. AnyConnect Apex

d. AnyConnect VPN Only

3. What is the recommended minimum RSA key size for certificates from a publicly trust CA?

a. 512 bits

b. 1024 bits

c. 2048 bits

d. 4096 bits

4. What type of VPN is *not* allowed by the default in the default group policy (DfltGrpPolicy)?

a. Clientless SSLVPN

b. IPsec/IKEv2

c. L2TP/IPsec

d. SSLVPN client

5. Which of the following is required when configuring a connection profile?

a. Tunnel group

b. Domain name

c. DNS server

d. Aliases

6. Which attributes take precedence over all others?

a. Dynamic access policy (DAP) attributes

b. User attributes

c. Group policy attributes

d. Connection profile default group policy attributes

7. Which of the following requires Java to function?

a. Clientless SSLVPN

b. Port forwarding

c. Smart tunnel

d. AnyConnect SSLVPN

8. Which of the following bookmark types is not supported by Cisco ASA by default?

a. CIFS

b. RDP

c. HTTP

d. DNS

9. Which of the following is an optional configuration parameter for smart tunnels?

a. Application ID

b. Operating system

c. Process name

d. Hash

10. Which of the following is not an available client/server plug-in?

a. RDP

b. VNC

c. CIFS

d. SSH

Foundation Topics

Our first remote access deep dive topic is clientless remote access SSLVPNs on the Cisco ASA. Why do organizations care about clientless SSL? Remote access VPN technology is used to secure data transferred between a client and a server. The client might not want to install a VPN client, for many reasons:

- The host user might not have administration rights to install software on a host system
- An end user might be leveraging a shared computer
- The user might be operating from a terminal or publicly used computer
- There is a policy against hosts having direct access to internal resources
- Security tools that prevent a client VPN from functioning might exist
- Contractors or other temporary users might not want to install VPN

software

- Various host types exist that could make it difficult to ensure that a client is available to match their system requirements
- Some users might have challenges installing VPN software

An alternative to using a VPN client is using the host's web browser and built-in SSL/TLS capabilities to protect traffic, which is one form of clientless VPN. Most modern web browsers include SSL/TLS capabilities, allowing for a VPN experience without the need to install any software or require special privileges. Clientless VPN opens the door for supporting use cases such as not having administration rights on the host system or having users who don't want to install software.

As with client-based VPN, once the user authenticates with the VPN gateway, preconfigured network resources can be made available but the host does not have direct access to the internal network, meaning the VPN concentrator acts as a proxy to the provisioned resources. It is common for organizations to leverage both client and clientless VPN technologies, for which different levels of sensitive data and connection types are permitted based on which option is used. For example, users might be able to access unclassified but sensitive resources using a clientless VPN; however, classified data is held within a more secured part of the network and requires a client-based VPN. Part of this sample configuration can include different assessment features that are enabled, such as ensuring host systems have antivirus installed, evaluating the version of web browser being used, and many other characteristics that make up a security policy that can be applied to a VPN deployment.

You learn how to build the previous example VPN deployment using the concepts covered in this and the next chapter. This chapter focuses on clientless VPN concepts and the next chapter dives deep into the Cisco flagship VPN client AnyConnect.

Let's start off by reviewing the general concepts associated with a clientless SSLVPN technology.

Clientless SSLVPN Overview

Clientless SSLVPN creates a secure remote access VPN tunnel to an ASA using a web browser without requiring a software or hardware client. It provides secure and easy access to a broad range of web resources, including both web-enabled and legacy applications from almost any device that can connect to the Internet via HTTPS. The previous section provided an example of clientless VPN based on using an Internet browser. There are other ways SSL VPN technology can be applied.

The following are some of the applications that can use a clientless SSLVPN:

- Internal websites
- Web-enabled applications
- Windows file shares
- Other TCP applications (via port forwarding)

Think ASA as a Proxy

The Cisco ASA allows users to access internal resources by acting as a proxy. In a traditional VPN, application TCP connections are directed and established directly from the client device to the internal server being accessed and are forwarded by the ASA unmodified after decryption/encryption. Unless NAT is used, the internal server being accessed sees the IP address assigned to the client tunnel. With a clientless SSLVPN, the application TCP connections from the client device are directed to the ASA, and they are then proxied with a second TCP connection created to the internal server. The internal server being accessed sees the IP address of the ASA interface. As a result, users using a clientless SSLVPN having no direct access to resources on the internal network. For users who need to be kept at an arm’s distance, such as contractors, this can be ideal.

Note

Despite its name, a clientless SSLVPN no longer uses the Secure Sockets Layer (SSL) protocol. As of ASA Release 9.4(1), a clientless SSLVPN instead uses the successor to SSL, Transport Layer Security (TLS), to provide a secure connection between remote users and specific supported internal resources that you configure.

Cisco VPN Options

Before deploying a clientless SSLVPN, you should consider the needs of your users to determine the type of clientless SSLVPN connectivity that will best suite them or whether a client-based solution, such as the AnyConnect Secure Mobility Client, would be a better fit:

- **Clientless SSLVPN:** A clientless SSLVPN enables end users to securely access resources on the corporate network from anywhere by using a TLS-enabled web browser. The user first authenticates with the ASA, which then allows the user to access preconfigured network resources. The user does not have network layer access; instead, all connections are proxied by the ASA. Web browser–enabled applications using protocols such as HTTP, HTTPS, CIFS, and FTP can be supported with only the browser on the user's device. More complex applications and protocols, such as POP3, SMTP, IMAP, SSH, and Telnet, can be supported with port forwarding, smart tunnels, and plug-ins.

- **AnyConnect VPN (TLS, DTLS, or IKEv2):** An AnyConnect VPN provides users highly secure access to the enterprise network, from any device, at any time, in any location. In contrast to clientless SSLVPNs, AnyConnect VPNs require the installation of the AnyConnect client before a user can obtain access. AnyConnect VPNs support a much broader range of applications, including almost any application that uses TCP, UDP, or ICMP, and provide network layer access to resources without the ASA serving as a proxy. To protect communications over the Internet, AnyConnect can be configured to encapsulate traffic in either TLS, DTLS, or IKEv2 tunnels. Table 8-2 summarizes the key differences between the clientless SSLVPN solution and the AnyConnect client solution.

Table 8-2 Comparison Between a Clientless SSLVPN and an AnyConnect VPN

Feature	Clientless SSLVPN	Client VPN
Common use cases		
Client		
Installation		
Protocols used		
Connectivity to resources		
IP address seen on internal servers		
Applications supported		

Feature	Clientless SSLVPN	Client VPN
Common use cases	Contractors, partners	Employees
Client	Web browser	Cisco AnyConnect Secure Mobility Client
Installation	None required	Via web, manually, or software distribution (for example, SCCM)
Protocols used	TLS	TLS, DTLS, and IKEv2
Connectivity to resources	ASA proxied connection	Direct IP layer connection
IP address seen on internal servers	ASA IP address	Client tunnel IP address
Applications supported	TCP applications only	All IP protocols, including TCP, UDP, and ICMP

Feature	Clientless SSLVPN	Client VPN
Common use cases	Contractors, partners	Employees
Client	Web browser	Cisco AnyConnect Secure Mobility Client
Installation	None required	Via web, manually, or software distribution (for example, SCCM)
Protocols used	TLS	TLS, DTLS, and IKEv2
Connectivity to resources	ASA proxied connection	Direct IP layer connection
IP address seen on internal servers	ASA IP address	Client tunnel IP address
Applications supported	TCP applications only	All IP protocols, including TCP, UDP, and ICMP

Clientless SSLVPN solutions are most often used when users are accessing a limited set of resources (for example, contractors) or accessing resources from untrusted systems (such as kiosks). AnyConnect is most often used when users need access to a large array of applications, such as from a corporate PC.

This chapter focuses on the clientless SSLVPN options, and Chapter 9, "AnyConnect VPNs on the ASA and IOS," covers client-based VPNs using the AnyConnect. You will need to know both options for the SVPN exam.

Clientless SSLVPN Prerequisites

Before deploying a clientless SSLVPN in your environment, you need to meet a number of prerequisites, such as those related to licensing, operating system, browser, and other supporting software. The following sections describe the details of each of these prerequisites.

Note

Cisco uses the term SSLVPN and WebVPN interchangeably.

First, let's review software license requirements for SSL VPN deployments.

Software Licenses

For VPN capabilities to function on the ASA, the ASA requires the appropriate licenses. For a lab and very small deployments, the ASA includes a two-user complimentary license. For deployments larger than two concurrent users, additional licenses are needed.

Note

If more than two users attempt to access an ASA without the necessary additional licenses, users receive the error message "AnyConnect was not

able to establish a connection to the specified secure gateway. Please try connecting again." Know this error message not only for troubleshooting questions on the exam, but also for real support problems with world deployments. We have encountered tickets with this error message when the administrator has not applied licensing to the ASA, licensing on the ASA has expired, and other situations where the administrator believes the ASA is properly licensed when it is not.

License Options

Chapter 7 introduced the possible VPN license options for a Cisco ASA. The license options were simplified into two categories, Apex and Plus. Chapter 7 also pointed out that there are two flavors of these license options, purchasing the licenses as a subscription or as a perpetual license. This means the following are ways organizations can purchase VPN licenses for their ASAs:

- AnyConnect Apex subscription
- AnyConnect Plus subscription
- AnyConnect Plus perpetual
- AnyConnect VPN Only perpetual

Let's further define what each of these license options offers.

AnyConnect Plus Subscription and Perpetual

AnyConnect Plus includes basic VPN services, such as device and per-application VPN services (including third-party IKEv2 remote access VPN headend support), trusted network detection, basic device context collection, and Federal Information Processing Standards (FIPS) compliance. AnyConnect Plus also includes other non-VPN services, such as the AnyConnect Network Access Manager 802.1X supplicant, the Cloud Web Security module, and the Cisco Umbrella roaming module.

AnyConnect Plus is licensed based on the total number of unique users and

can be purchased as a subscription license or as a perpetual license. The license is delivered with a multiuse product activation key (PAK), which allows for the activation of AnyConnect Plus functionality on all VPN headends in the organization.

AnyConnect Apex Subscription

AnyConnect Apex includes more advanced services, such as endpoint posture checks (HostScan via ASA VPN or ISE Posture via the Cisco Identity Services Engine), network visibility, next-generation VPN encryption (including Suite B), and clientless remote access VPN services, as well as all the capabilities of AnyConnect Plus.

Like AnyConnect Plus, AnyConnect Apex is licensed based on the total number of unique users. However, it differs in that it can only be purchased as a subscription license. The AnyConnect Apex license is similarly delivered with a multiuse PAK for the activation of AnyConnect Apex functionality on all VPN head ends in the organization.

AnyConnect VPN Only Perpetual License

AnyConnect VPN Only includes basic VPN services such as device and per-application VPN services (including third-party IKEv2 remote access VPN headend support), trusted network detection, basic device context collection, and FIPS compliance. It also includes more advanced VPN services, such as endpoint posture checks (HostScan via ASA VPN), next- generation VPN encryption (including Suite B), and clientless remote access VPN services. No other AnyConnect function or service (such as the Web Security Module, Cisco Umbrella roaming, ISE Posture, Network Visibility, or Network Access Manager) is available with the AnyConnect VPN Only licenses.

AnyConnect VPN Only is licensed based on the number of simultaneous connections (rather than unique users) for a single headend device. The license is delivered as a single-use PAK for activation of AnyConnect VPN Only functionality on a single VPN headend.

License Option Summary

Table 8-3 compares the AnyConnect Plus, AnyConnect Apex, and AnyConnect VPN Only license options. You will not have to know how Cisco licenses an ASA for the SVPN; however, it is important to understand licensing options when designing a real-world deployment. Also know that in order of cost, Apex is the highest cost, followed by Plus, which is less expensive than Apex but a higher cost than VPN only. The price you pay can vary due to different factors, including using a subscription versus perpetual licensing, bundling technologies, or using discounts that might be available depending on where you purchase the licenses.

Table 8-3 Supported Features by License Type

Feature	AnyConnect Plus	AnyConnect Apex	AnyConnect VPN Only
License type(s)	Subscription and perpetual	Subscription	Perpetual
License usage	Multiple VPN headends	Multiple VPN headends	Single VPN headend
Device or system VPN (including Cisco phone VPN)	Yes	Yes	Yes
Third-party IPsec IKEv2 remote access VPN clients (non-AnyConnect client)	Yes	Yes	Yes
Per-application VPN	Yes	Yes	Yes
Cloud Web Security and Web Security Appliance	Yes	Yes	Not supported
Cisco Umbrella roaming	Yes	Yes	Not supported
Network Access Manager	Yes	Yes	Not supported
Cisco AMP for Endpoints Enabler	Yes	Yes	Not supported
Network Visibility Module	Not supported	Yes	Not supported
Unified endpoint compliance and remediation (posture)	Not supported	Yes	Not supported
Suite B or next-generation encryption	Not supported	Yes	Yes
Third-party IPsec/IKEv2 remote VPN clients	Not supported	Yes	Yes
Clientless (browser-based) VPN connectivity	Not supported	Yes	Yes
ASA multicontext-mode remote access	Not supported	Yes	Yes
SAML authentication	Not supported	Yes	Yes

SSLVPN Support Requirements

When planning an SSLVPN deployment, you must consider what type of hosts will be using the VPN. We have pointed out that SSVPN is clientless, which means one benefit is not needing to install VPN software. There are still specific technologies that must exist in order for a clientless VPN to function properly. Many of these requirements should exist within the native operating system used by the clients leveraging the VPN; however, there can be situations where a key technology is not functioning or available, leading to a failure in VPN service.

Successful and reliable use of the clientless SSLVPN functionality depends on the use of supported operating systems, browsers, and supporting software. Without these, the client will not be able to successfully connect to the VPN. The following list explains these requirements in more detail:

- **OS:** Clientless SSLVPN from Cisco is tested and supported on macOS and Windows. Apple iOS and Android are not supported except for Citrix Receiver for Mobile at the time of publication.

- **Browser:** The client must use a TLS-enabled browser, such as Microsoft Edge, Firefox, or Chrome. Table 8-4 provides a list of operating systems and browsers supported as of ASA Release 9.14. Non supported browsers could still possibly work but are not recommended or supported by Cisco TAC.

- **Java:** The browser must be enabled with Java Runtime Environment (JRE) Version 6u151 b10, 7u141 b11, 8u131 b11, or later for SSLVPN features such as port forwarding and smart tunnels. On macOS X, Apple's JRE is supported.

- **ActiveX:** When using Internet Explorer on Windows operating systems, the browser must be enabled with ActiveX for SSLVPN features such as smart tunnels.

The SVPN exam could include host troubleshooting SSLVPN concepts. For example, a user could find attempting to connect to an SSLVPN fails because Java or ActiveX is not available. You will not be tested on the specific versions of OS or browsers that are or are not supported by Cisco VPN technology, but Table 8-4 does outline which are supported.

Table 8-4 Supported Operating Systems and Browsers for Clientless SSLVPN

OS/Browser	Chrome	Firefox	Internet Explorer	Safari
macOS 10.15	Yes	Yes	Not supported	13.0
macOS 10.14	Yes	Yes	Not supported	12.0
macOS 10.13	Yes	Yes	Not supported	12.0
macOS 10.12	Yes	Yes	Not supported	12.0
Windows 10	Yes	Yes	11	Not supported
Windows 8.1	Yes	Yes	11	Not supported
Windows 8	Yes	Yes	11	Not supported
Windows 7	Yes	Yes	11	Not supported
Apple iOS	Not supported	Not supported	Not supported	Not supported
Android	Not supported	Not supported	Not supported	Not supported

SSL VPN Prerequisites Summary

To summarize what is required for a Cisco ASA SSLVPN deployment, you need an ASA that is licensed for the SSLVPN features that meet your

technical goals. If you are working in a lab, you can use the two licenses that are available by default. If you are supporting more than two users, you will need to choose either a Plus or an Apex version of license. Next, you must validate whether the host system support meets the requirements to support an SSLVPN, which are a supported OS and browser as well as a browser with Java and ActiveX enabled. With the requirements covered, we are ready to move into our first basic clientless SSLVPN configuration example.

Basic Clientless SSLVPN Configuration

Now that you understand the prerequisites for deploying SSLVPN on a Cisco ASA, you are ready to configure a basic clientless remote access VPN. Doing so involves the following steps, which are explained in detail in the following sections:

Step 1. Install an identity certificate.

Step 2. Apply an identity certificate to the interface(s).

Step 3. Enable clientless SSLVPN access.

Step 4. Configure group policies.

Step 5. Configure connection profiles.

Step 6. Configure user authentication.

The examples in this chapter use the lab environment shown in Figure 8-1, which uses the following software and hardware versions:

- Adaptive Security Virtual Appliance (ASAv) Release 9.12(4)
- Adaptive Security Device Manager (ASDM) Release 7.12(2)
- AnyConnect Security Mobility Client Release 4.8.03052 running on Windows 10

Figure 8-1 Clientless SSLVPN on ASA Lab Diagram

Step 1: Installing an Identity Certificate

For an SSLVPN to function, the ASA must have a digital certificate to identify it to connecting clients. This can be accomplished with a self-signed certificate or a certificate from a certificate authority (CA). For basic testing, the self-signed certificate generated by the ASA upon startup may suffice. For production deployments, the use of a certificate from a publicly trusted CA is the preferred approach. The process to obtain and install a certificate from a CA is called *enrollment* and can be broken into three steps:

Step 1. Generate a new RSA key pair.

Step 2. Create an identity certificate request.

Step 3. Install a signed identity certificate.

Generating a New RSA Key Pair Using ASDM

Before requesting an identity certificate, you must generate an RSA key pair via ASDM or via the CLI. If you are requesting an identity certificate from a publicly trusted CA, the RSA key pair should have a size of at least 2048 bits, as this is the minimum acceptable size as of the press time of this book. Alternatively, you can use an existing key pair if it meets the requirements.

To generate a new RSA key pair via ASDM, follow these steps:

Step 1. Navigate to **Configuration** > **Remote Access VPN** > **Certificate Management** > **Identity Certificates**.

Step 2. Click **Add** to open the Add Identity Certificate dialog box.

Step 3. Select **Add a new identity certificate**.

Step 4. Click **New** to open the Add Key Pair dialog box.

Step 5. Select **Enter a new key pair name** and specify a name for the key pair.

Step 6. Select the desired Size for the key pair, in bits.

Step 7. Click **Generate Now** to generate the new RSA key pair and close the Add Key Pair dialog box.

Figure 8-2 shows the creation of a new RSA key pair with the name EXAMPLE_KEY_PAIR and the key size 2048 bits.

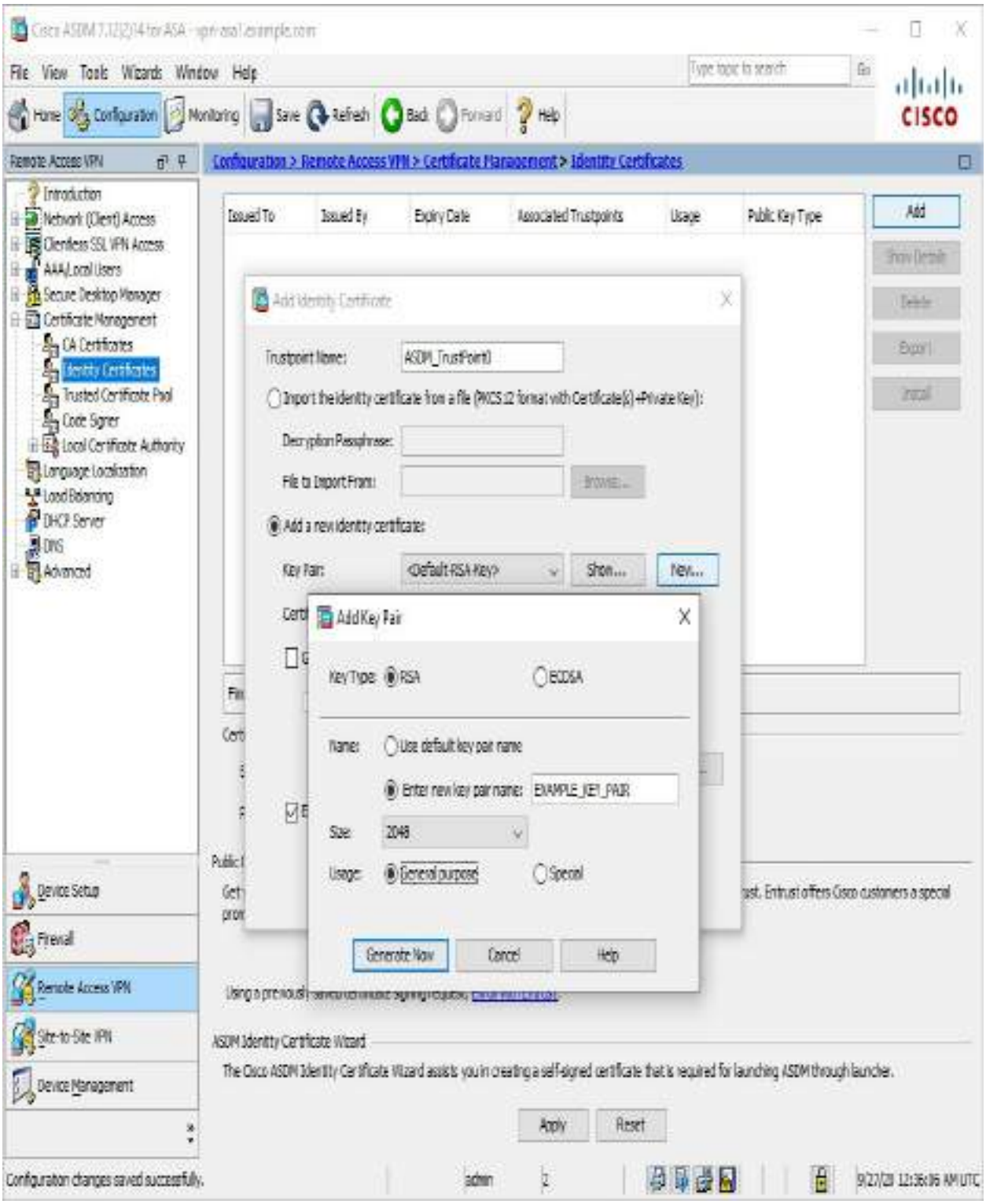


Figure 8-2 Generating a New RSA Key Pair via ASDM

Generating a New RSA Key Pair Using CLI

To generate a new RSA key pair via the CLI, use the **crypto key generate rsa** command. Example 8-1 shows an example of generating a new RSA key pair via the CLI that mirrors the configuration in Figure 8-2.

Example 8-1 Generating a New RSA Key and Creating an Identity Certificate Request via the CLI

```
VPN-ASA1(config)# crypto key generate rsa label
EXAMPLE_KEY_PAIR modulus 2048
INFO: The name for the keys will be: EXAMPLE_KEY_PAIR
Keypair generation process begin. Please wait...
```

Creating an Identity Certificate Request Using ASDM

With the RSA key pair generated, you can now create a certificate signing request (CSR) for the identity certificate.

To create an identity certificate request via ASDM, follow these steps:

Step 1. Navigate to **Configuration** > **Remote Access VPN** > **Certificate Management** > **Identity Certificates**.

Step 2. Click **Add** to open the Add Identity Certificate dialog box.

Step 3. Specify a trustpoint name.

Step 4. Select **Add a new identity certificate**.

Step 5. Select the desired key pair.

Step 6. Specify the certificate subject DN, which is typically the fully qualified domain name (FQDN) of the ASA, in the form CN=<*FQDN*>.

Step 7. Click **Add Certificate** to generate the CSR and open the Identity Certificate Request dialog box.

Step 8. Click **Browse** to open the Save As dialog box.

Step 9. Specify a filename and click **Save As** to close the Save As dialog box.

Step 10. Click **OK** to save the CSR to the specified file and close the Identity Certificate Request dialog box.

Figure 8-3 shows the creation of a new identity certificate named EXAMPLE_IDENTITY_CERT. The identity certificate will use the key pair named EXAMPLE_KEY_PAIR and will contain the FQDN VPN-ASA1.EXAMPLE.COM in the CSR. The generated CSR will be stored in C:\Example_CSR.csr.

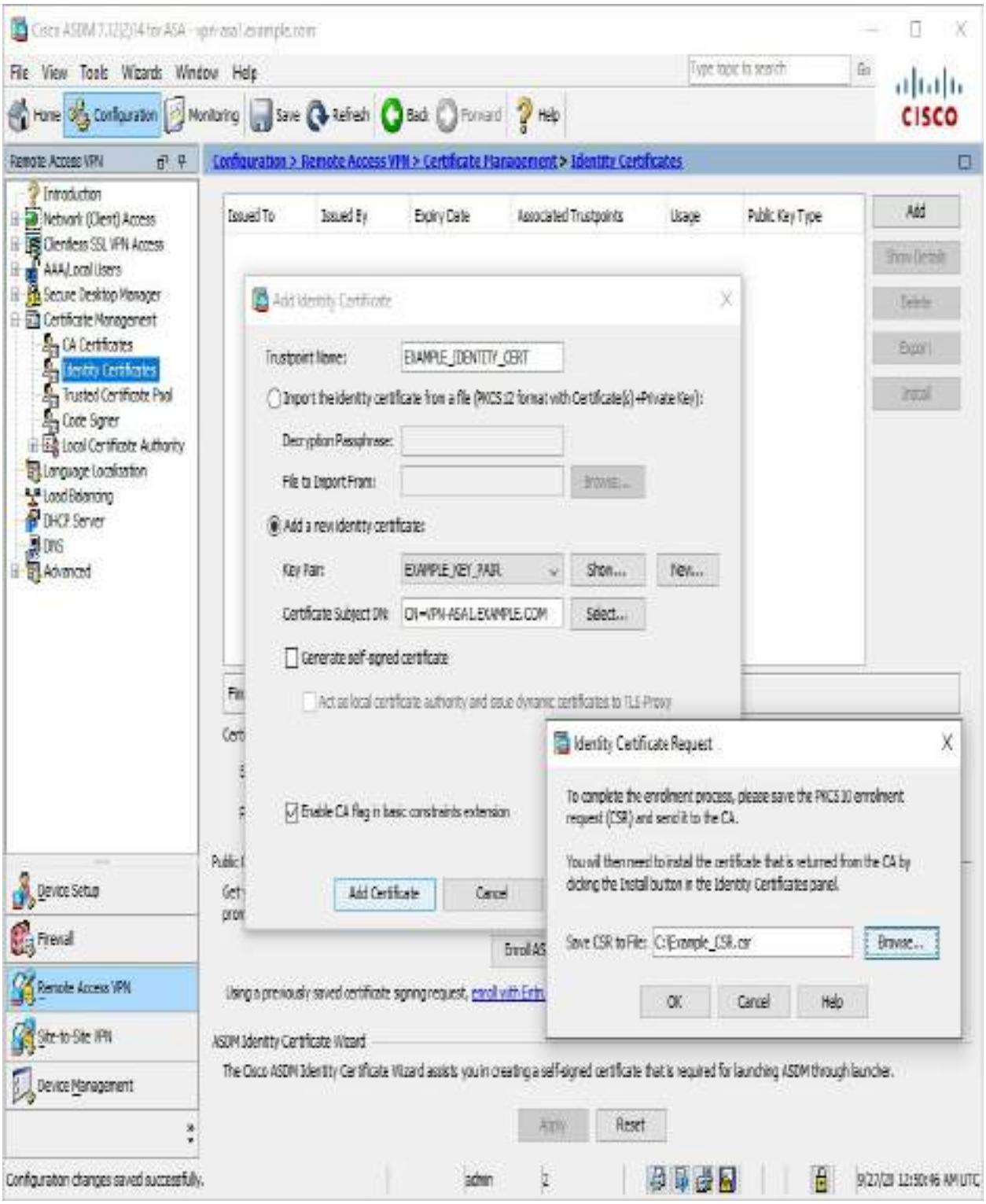


Figure 8-3 Creating an Identity Certificate Request via ASDM

Creating an Identity Certificate Request Using CLI

To create an identity certificate request via the CLI, you first use the **crypto ca trustpoint** command to create a new trustpoint and then use the **crypto ca enroll** command to create the CSR. Example 8-2 shows an example of generating a new RSA key pair and creating an identity certificate request via the CLI. It mirrors the configuration in Figure 8-3.

Example 8-2 Generating a New RSA Key and Creating an Identity Certificate Request via the CLI

```
VPN-ASA1(config)# crypto ca trustpoint EXAMPLE_IDENTITY_CERT
VPN-ASA1(config-ca-trustpoint)# keypair EXAMPLE_KEY_PAIR
VPN-ASA1(config-ca-trustpoint)# subject-name CN=VPN-
ASA1.EXAMPLE.COM
VPN-ASA1(config-ca-trustpoint)# no fqdn
VPN-ASA1(config-ca-trustpoint)# enrollment terminal
VPN-ASA1(config-ca-trustpoint)# exit
VPN-ASA1(config)# crypto ca enroll EXAMPLE_IDENTITY_CERT
% Start certificate enrollment ..
% The subject name in the certificate will be: CN=VPN-
ASA1.EXAMPLE.COM

% Include the device serial number in the subject name?
[yes/no]: no

Display Certificate Request to terminal? [yes/no]: yes
Certificate Request follows:
-----BEGIN CERTIFICATE REQUEST-----
MIICszCCAZsCAQAwODEdMBsGA1UEAxMUVlBOLUFTQTEuRVhBTVBMRS5DT00xFzA
V
BgkqhkiG9w0BCQIWCFZQTi1BU0ExMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMII
B
CgKCAQEAoyPeBeusNbdUh/NVZ1c0drOdsXCpShz6GbrUyp0teMns5M1+UahWFSw
5
PXtVP88d09QS/E9wWyWW0RSgFT6DG8B3nfjUUbPfDrpFFkwX8Ft3OfH00K8oSVu
e
e5uiJgFAAa+XmmcogbzA7+HpVhyWO/y9JpTYu9Belqgv0eQ3ijy00n0rC/8XG3j
D
lRQ+1xBmrYTbR8FWfgqeGILlm2aAftvTgqyB7FrwZWRT/+v+7q9HEU71N8e/Nm7
S
1Q3QV/r724wUx91LFBWTi9SQF2c/TDYrYJmj15R//Wvv32KA8Gpp3Omxi6g8PGu
k
/IJcQ67if+80WhAP4Eij7y5ZV8jl+QIDAQABoDYwNAYJKoZIhvcNAQkOMScwJTA
O
BgNVHQ8BAf8EBAMCBaAwEwYDVR0RBAwwCoIIVlBOLUFTQTEwDQYJKoZIhvcNAQE
F
```

```
BQADggEBAHzW6KZOI0oVsOToq1yV65/7KwYh6DdHfg6v2uCf/XUAhW22ocwraJk
O
WwGYSQsnzLazqpuj2P3qrfld63ulnOzYrZ8dFT+aE1lR4KFmjm4JJiy0m4u2NFd
t
Xghu8Rj/yd0APg3spfdcThu46fe/bZDc/Uc0vkEsXIh+zibsaxjF0VTn0EvQRQd
0
mcPiF0iMJ82+Li0lK5y3y2KBjRN3TX0i3WvnJgLZlZRe2BJ1G9HxYVSzdE0Oo9c
1
ZqeTU0Fe2a/k3ndqg9yFi1dfNBHqZb9B5wV+KTZtpTLD2URTYxleCbVn4B8es62
B
DCtMS6q2BLyf0ysYvPyRFIkWEztoh/o=
-----END CERTIFICATE REQUEST-----

Redisplay enrollment request? [yes/no]: no
```

After generating the CSR for the identity certificate, you need to submit the certificate request to the CA. How this is done varies by CA, but it typically involves uploading or pasting the CSR into a web form.

Installing a Signed Identity Certificate Using ASDM

Once the CSR for the identity certificate has been approved by the CA administrator, you need to download the signed certificate in base-64 format for installation on the ASA.

To install the signed identity certificate via ASDM, follow these steps:

Step 1. Navigate to **Configuration** > **Remote Access VPN** > **Certificate Management** > **Identity Certificates**.

Step 2. Select the certificate with the associated trustpoint name specified earlier.

Step 3. Click **Install** to open the Install Identity Certificate dialog box.

Step 4. Click **Browse** to browse to the Install ID Certificate File dialog box.

Step 5. Select the signed certificate file.

Step 6. Click **Install ID certificate file** to close the Install ID Certificate File dialog box.

Step 7. Click **Install Certificate** to install the signed certificate and close the Install Identity Certificate dialog box.

Figure 8-4 shows the installation of a signed identity certificate for the trustpoint named EXAMPLE_IDENTITY_CERT. The signed identity certificate will be installed from the file C:\ VPN-ASA1.EXAMPLE.COM_cert.pem.

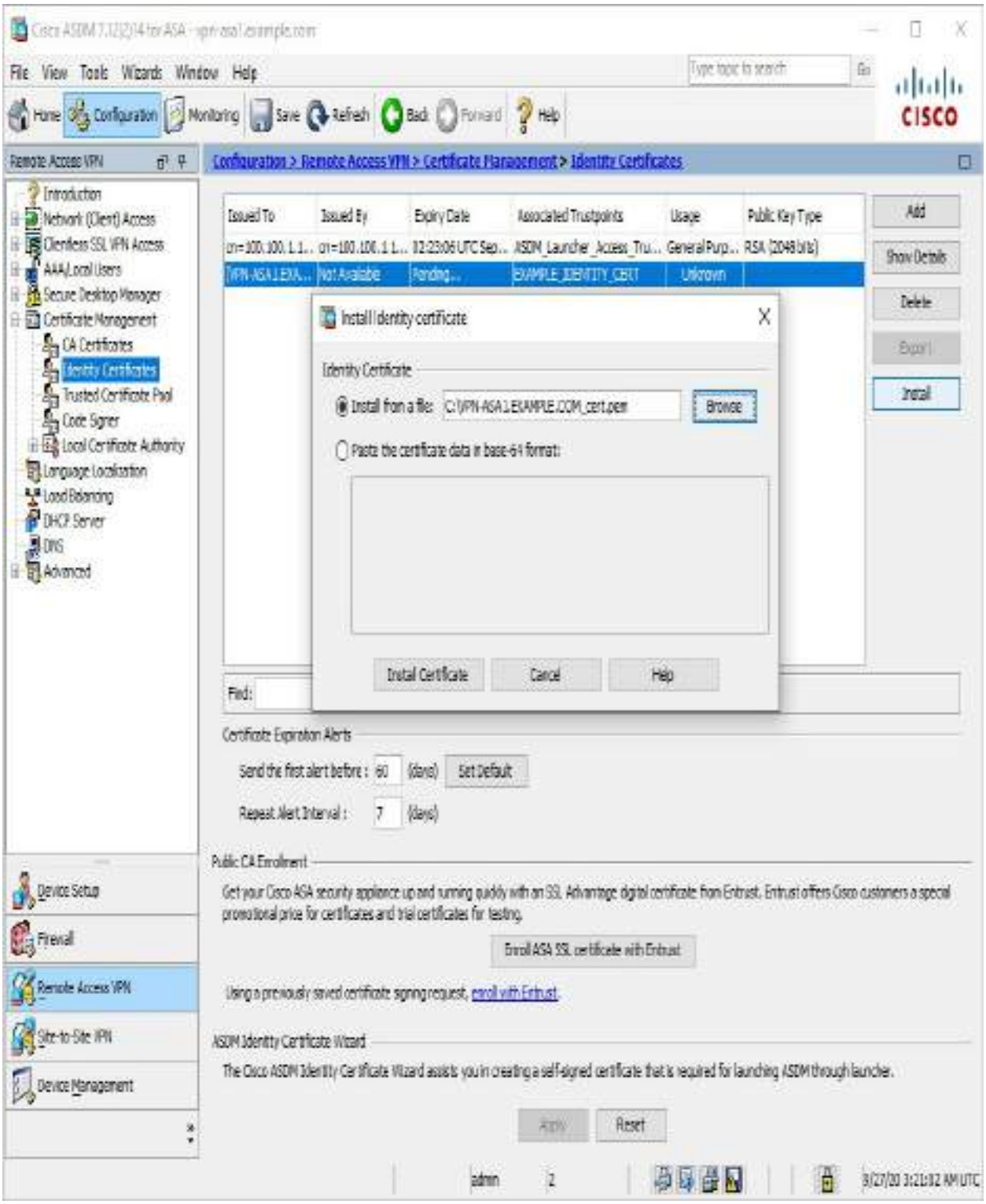


Figure 8-4 Installing a Signed Identity Certificate via ASDM

Installing a Signed Identity Certificate Using CLI

To install a signed identity certificate via the CLI, use the **crypto ca import** command to import the base-64-encoded certificate. Example 8-3 shows an example of installing a signed identity certificate via the CLI that mirrors the configuration in Figure 8-4.

Example 8-3 Installing a Signed Identity Certificate via the CLI

```
VPN-ASA1(config)# crypto ca import EXAMPLE_IDENTITY_CERT
certificate

% The fully-qualified domain name in the certificate will be:
VPN-ASA1


Enter the base 64 encoded certificate.
End with the word “quit” on a line by itself

MIIDODCCAiCgAwIBAgIGAXTNj66hMA0GCSqGSIb3DQEBCwUAMCcxCzAJBgNVBAY
T
AlVTMRgwFgYDVQQDDA9FeGFtcGxlIFJvb3QgQ0EwHhcNMjAwOTI3MDMxNjE5Whc
N
MjEwOTI3MDMxNjIwWjAfMR0wGwYDVQQDDBRWUE4tQVNBMS5FWEFNUExFLkNPTTC
C
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKMj3gXrrDW3VIfzVWdXNHa
z
nbFwqUoc+hm61MqdLXjJ7OTNflGoVhUsOT17VT/PHdPUEvxPcFsllltEUoBU+gxv
A
d5341FGz3w66RRZMF/Bbdznx9NCvKElbnnuboiYBQAGvl5pnKIG8wO/h6VYcljv
8
vSaU2LvQXpaoL9HkN4o8tNJ9Kwv/Fxt4w5UUPtcQZq2E20fBVn4KnhiC5ZtmgH7
b
04Ksgexa8GVkU//r/u6vRxFO9TfHvzZu0tUN0Ff6+9uMFMfdSxQVk4vUkBdnP0w
2
K2CZo9eUf/1r799igPBqadzpsYuoPDxrpPyCXEOu4n/vNFoQD+BIo+8uWVfI5fk
C
AwEAAaNyMHAwHwYDVR0jBBgwFoAUgxKw2Q3vg/G4gxwZ3Nr+3JsJyxkwCQYDVR0
T
BAIwADATBgNVHREEDDAKgghWUE4tQVNBMTAOBgNVHQ8BAf8EBAMCBaAwHQYDVR0
O
BBYEFIzXjLDM23Fxfyo1Xsdsbvv8WI5XMA0GCSqGSIb3DQEBCwUAA4IBAQC8X2v
c
edrb4MsSuliFmX+yPGJ/iHxgcR1hTYpbc/PhP2fBZ6C4uptbEPQ7UPIqz4V799z
/
wpdbaC8dJ1ZF4VZa6WG8rSO4x+LcgkICcZp5eoAElZK7tBsXriskjdwls28pHiH
C
dDrVD+YRUs4H8pCdPO4uXZOZhkYdYIp9HHTF8J4fiLS0NTLf8+b+pHXCsOfPdML
```

```
9
SDu0UvKolNONVZGk9uFHTuHAicrvfGw4Jj2tWehZFujebg6UN93LVYGghQInMHO
g
NiKdLiFmOUcdvoUVseMrexydfj7JkdFCDG2b8hg+xON4qioEyN1iWmvbZ8KCi5K
d
yFrBv9mAQtl41sXT
quit
INFO: Certificate successfully imported
```

Step 2: Applying an Identity Certificate to the Interface(s)

After the identity certificate is imported, it needs to be associated with the interfaces that will be used to terminate SSLVPN connections to become active. The method shown here assigns the certificate to all interfaces of the ASA.

Applying the Identity Certificate Using ASDM

To apply the identity certificate to all interfaces via ASDM, follow these steps:

Step 1. Navigate to **Configuration** > **Clientless SSLVPN Access** > **Connection Profiles**.

Step 2. Click **Device Certificate** to open the Specify Device Certificate dialog box.

Step 3. Select the desired device certificate.

Step 4. Click **OK** to apply the identity certificate to all interfaces and close the Specify Device Certificate dialog box.

Figure 8-5 shows the application of the identity certificate from the trustpoint name EXAMPLE_IDENTITY_CERT to all interfaces.

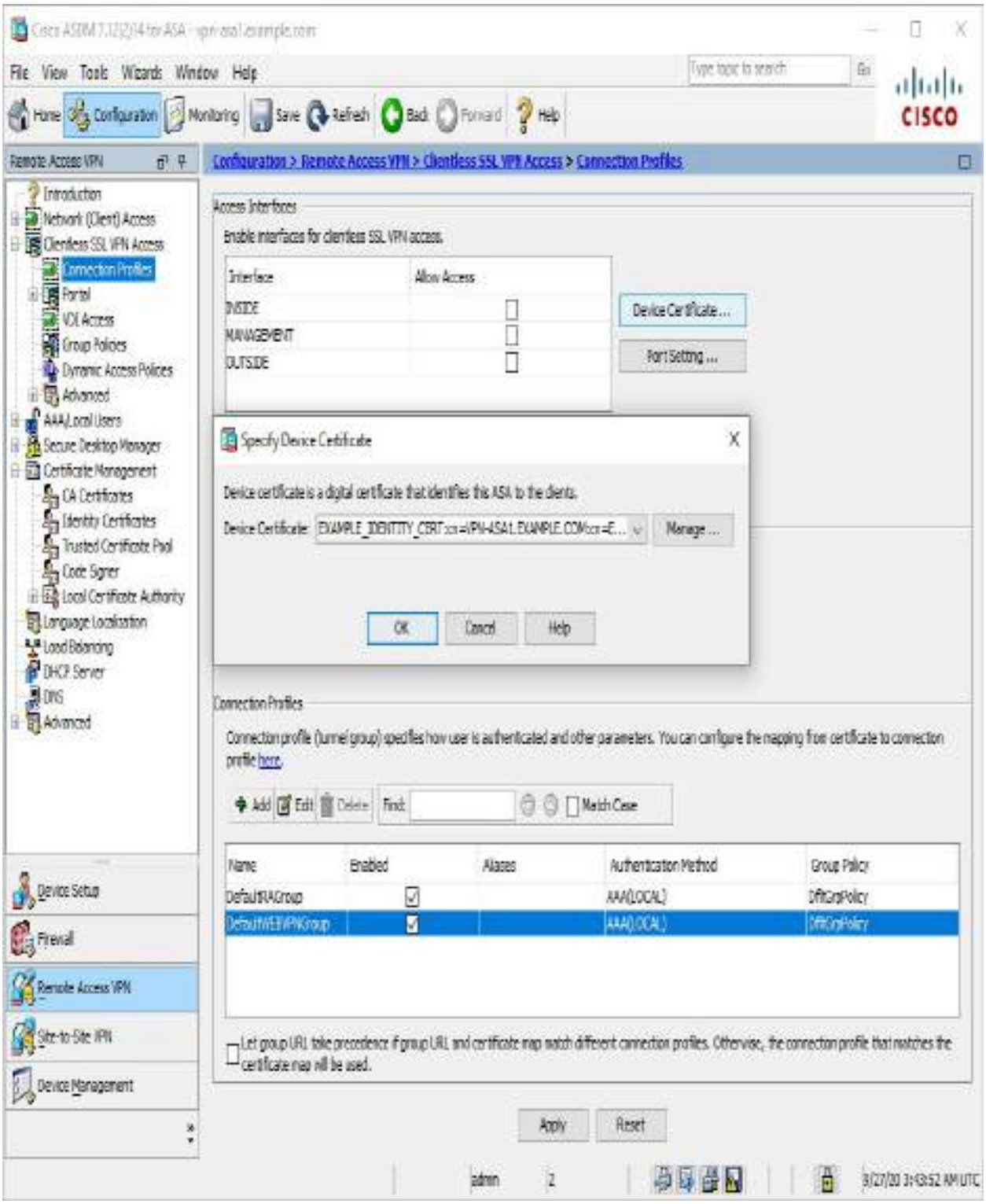


Figure 8-5 Applying an Identity Certificate to All Interfaces via the CLI

Applying the Identity Certificate Using CLI

To apply an identity certificate via the CLI, use the **ssl trust-point** command to associate the identity certificate with each desired interface. Example 8-4 shows an example of applying the identity certificate EXAMPLE_IDENTITY_CERT to the INSIDE, MANAGEMENT, and OUTSIDE interfaces. It mirrors the configuration in Figure 8-5.

Example 8-4 Applying an Identity Certificate to All Interfaces via the CLI

```
VPN-ASA1(config)# ssl trust-point EXAMPLE_IDENTITY_CERT
MANAGEMENT
VPN-ASA1(config)# ssl trust-point EXAMPLE_IDENTITY_CERT OUTSIDE
VPN-ASA1(config)# ssl trust-point EXAMPLE_IDENTITY_CERT INSIDE
```

Step 3: Enabling Clientless SSLVPN on an Interface

With the identity certificate successfully enabled on the client interfaces, the next step in setting up a clientless SSLVPN is to enable SSLVPN on the interface that will terminate the user traffic. If SSLVPN is not enabled on the interface, the security appliance does not accept any connections, even if SSLVPN is globally enabled.

Enable Clientless SSLVPN Interface using ASDM

To enable a clientless SSLVPN on an interface via ASDM, follow these steps:

Step 1. Navigate to **Configuration** > **Remote Access VPN** > **Clientless SSLVPN Access** > **Connection Profiles**.

Step 2. Check **Allow Access** for the interface on which you want to enable clientless SSLVPN.

Figure 8-6 shows an example of enabling a clientless SSLVPN on the OUTSIDE interface. The clientless SSLVPN remains disabled on the INSIDE and MANAGEMENT interfaces.

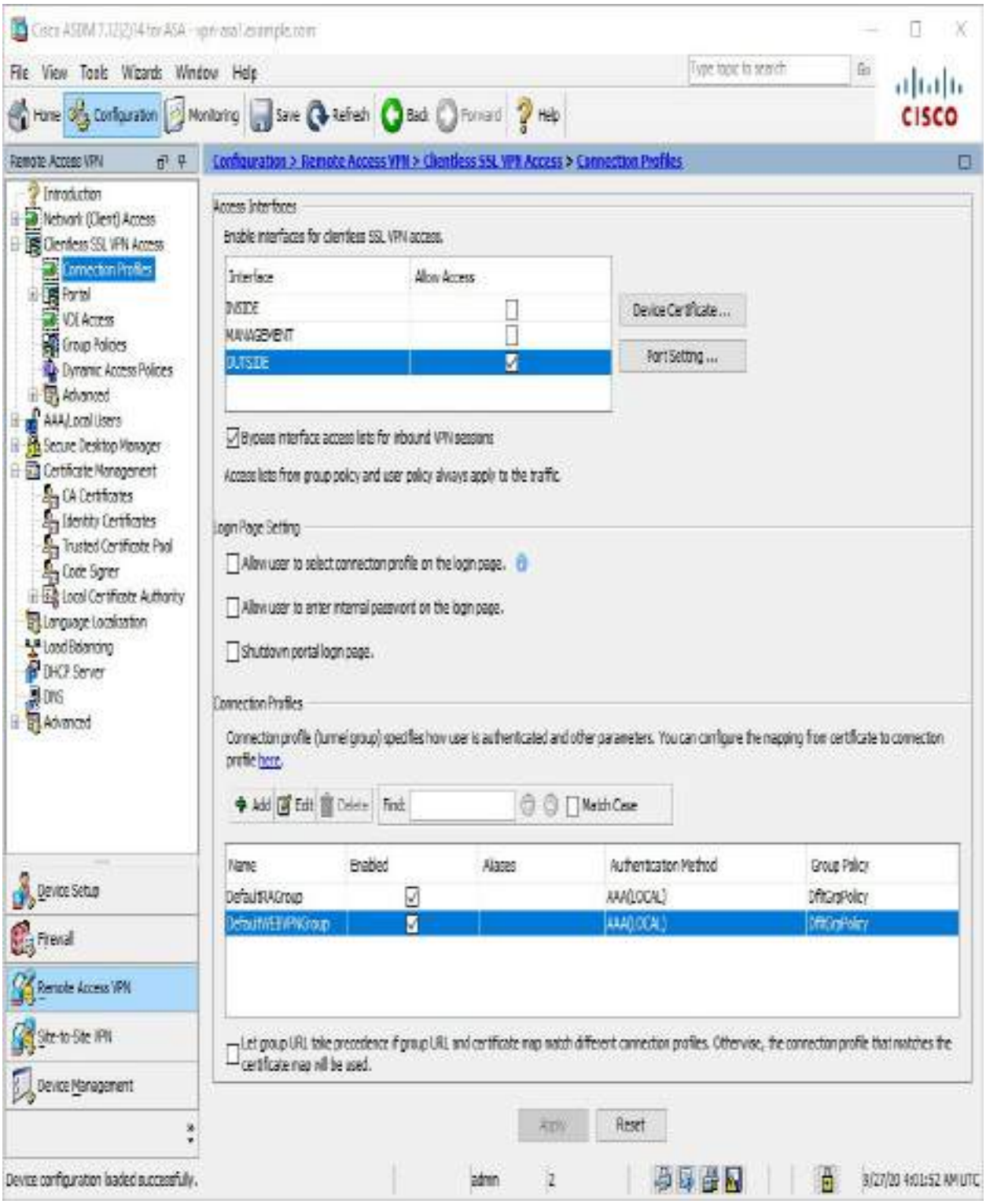


Figure 8-6 Enabling a Clientless SSLVPN on the OUTSIDE Interface via ASDM

Enable Clientless SSLVPN Interface using CLI

To enable a clientless SSLVPN via the CLI, use the **enable** command in webvpn configuration mode. Example 8-5 shows and example of enabling a clientless SSLVPN on the OUTSIDE interface. It mirrors the configuration in Figure 8-6.

Example 8-5 Enabling a Clientless SSLVPN on the OUTSIDE Interface via the CLI

```
VPN-ASA1(config)# webvpn
VPN-ASA1(config-webvpn)# enable OUTSIDE
INFO: WebVPN and DTLS are enabled on 'OUTSIDE'.
```

After you enable a clientless SSLVPN on an interface and click Apply to push the configuration to the device, the security appliance accepts clientless SSLVPN connection requests. The next step is to configure user authentication.

Step 4: Configuring Group Policies

Groups and users are core concepts in managing the security of VPNs and in configuring the ASA. They specify attributes that determine user access to and use of the VPN. A *group* is a collection of users treated as a single entity. *Users* get their attributes from *group policies*. If you do not assign a particular group policy to a user, the default group policy for the connection applies.

Group policies simplify system management. To streamline configuration, the ASA provides the default group policy DfltGrpPolicy. The default group policy provides settings that are likely to be common for many users. As you add users, you can specify that they inherit parameters from a group policy. Thus, you can quickly configure VPN access for large numbers of users.

Group Policy Selection

This capability to inherit parameters enables the ASA to accommodate the

complex and dynamic nature of VPN environments. If the ASA receives attributes from multiple sources, the attributes are evaluated, merged, and applied to the user policy. If there are conflicts between attributes, an ordered ranking determines which attribute takes precedence (see Figure 8-7).

Figure 8-7 Attribute Inheritance

The following breaks down how precedence is determined for a group policy:

1. **Dynamic access policy (DAP) attributes:** These attributes take precedence over all others. If you set a bookmark or URL list in DAP, it overrides a bookmark or URL list set in the group policy.
2. **User attributes:** These are user-specific attributes.
3. **Group policy attributes:** These are group policy–specific attributes that are associated with a user's group policy.
4. **Connection profile default group policy attributes:** A default group policy is applied to the connection profile. All users connecting to the ASA initially belong to this group, which provides any attributes that are missing from the DAP, user attributes, or the group policy assigned to the user.

5. **Default group policy assigned by the ASA (DfltGrpPolicy):** System default attributes provide any values that are missing from the DAP, user attributes, group policy, or connection profile.

Creating Group Policies Using ASDM

If you decide to grant identical rights to all VPN users, you do not need to configure specific group policies. However, VPNs seldom work that way. For example, you might allow a finance group to access one part of a private network, a customer support group to access another part, and a sales group to access other parts. In addition, you might allow specific users within sales to access systems that other sales users cannot access. Connection profiles and group policies provide the flexibility to do grant rights in this way.

To create and modify a group policy via ASDM, follow these steps:

Step 1. Navigate to **Configuration** > **Remote Access VPN** > **Clientless SSLVPN Access** > **Group Policies**.

Step 2. Click **Add** to open the Add Internal Group Policy dialog box.

Step 3. Specify a name for the group policy.

Step 4. Uncheck **Inherit** next to the attributes you wish to modify and specify a non-inherited value for each of these attributes.

Step 5. Click **OK** to close the Add Internal Group Policy dialog box.

Figure 8-8 shows an example of creating a clientless SSLVPN only group policy named CONTRACTOR_GROUP. Inheritance for the tunneling protocols attribute has been disabled, and only clientless SSLVPN connections are allowed. For users or connections mapped to this group policy, all other connection types will be denied.

Note

The default group policy DfltGrpPolicy allows clientless SSLVPNs as well as IPsec/IKEv1, IPsec/IKEv2. and L2TP/IPsec by default. It does not allow

SSLVPN client connections by default.

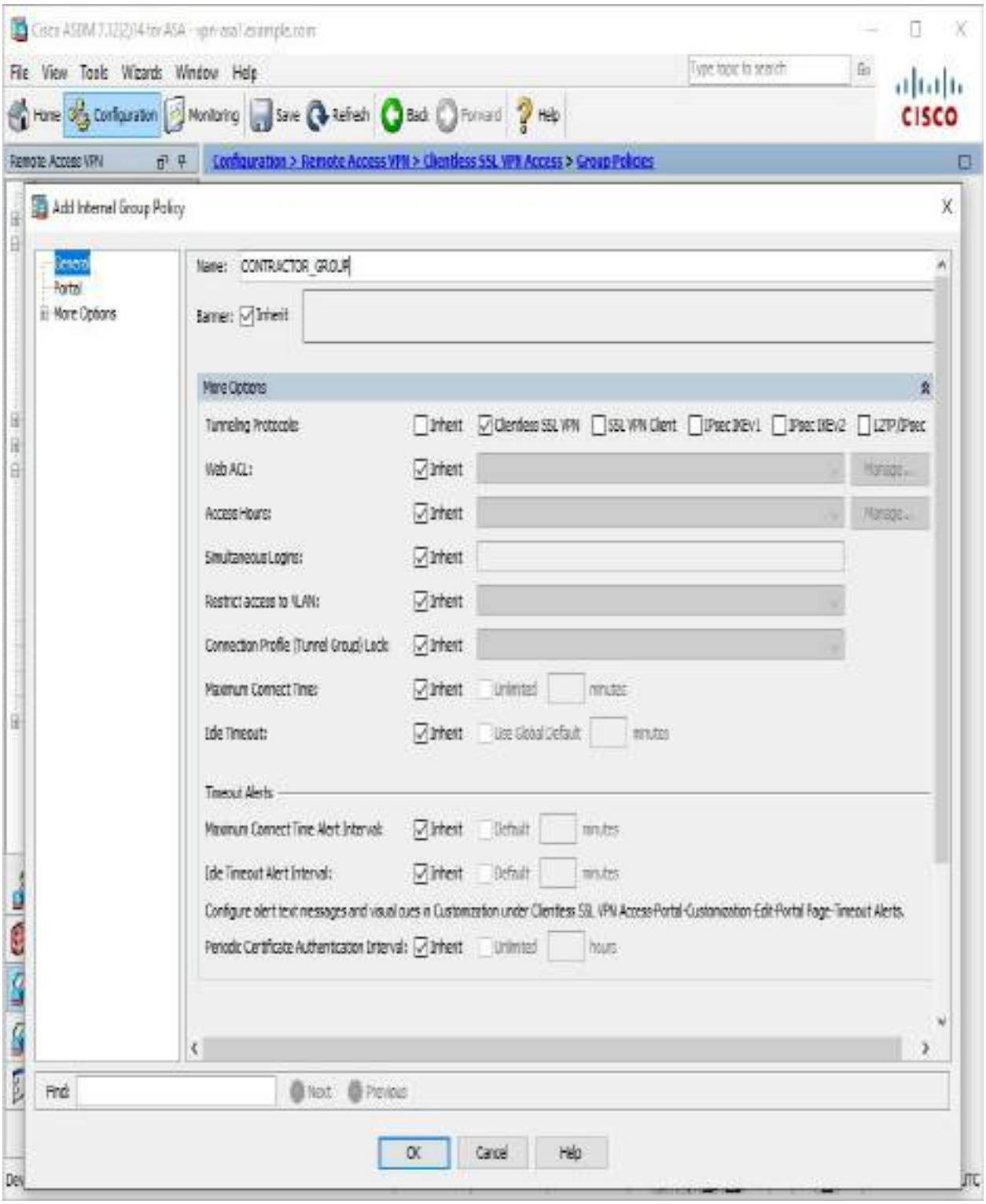


Figure 8-8 Creating a Clientless SSLVPN Group Policy via ASDM

Creating Group Policies Using CLI

To create and modify a group policy via the CLI, you first use the **group-policy** name **internal** command to create the group policy. Then you use the **group policy** *name* **attributes** command to enter **group-policy** configuration mode. Finally, you use the commands listed in Table 8-5 modify the desired attribute(s) or use the **webvpn** command to enter group policy **webvpn** configuration mode and use the commands in Table 8-6 to modify the desired attributes(s). Example 8-6 shows an example of creating a clientless SSLVPN group policy via the CLI; it mirrors the configuration in Figure 8-8.

Example 8-6 Creating a Clientless SSL Group Policy via the CLI

```
VPN-ASA1(config)# group-policy CONTRACTOR_GROUP internal
VPN-ASA1(config)# group-policy CONTRACTOR_GROUP attributes
VPN-ASA1(config-group-policy)# vpn-tunnel-protocol ssl-
clientless
```

Group Policy Attributes for Clientless SSLVPNs

Group policy attributes are parameters you can apply to group of hosts leveraging the VPN technology. This can make things easier regarding standardizing the user experience across large groups of people. This also enables you to create templates to speed up configuring new groups of users. For example, you could copy one user group, tweak a few attributes, and call it a new user group rather than building a new user group from scratch. It is important to know what parameters are available, which are shown in Table 8-5.

Table 8-5 Group Policy Attributes for Clientless SSLVPNs

Command	Description
	Creates a banner or welcome text to be displayed on the VPN remote client
	Specifies the name of an existing tunnel group that users are required to connect with
	Configures periodic authentication
	Specifies the VLAN onto which VPN traffic for this group will be forwarded.
	Specifies the name of a configured time-range policy
	Specifies the idle timeout period, in minutes
	Specifies the maximum user connection time, in minutes, or none for unlimited time
	Specifies the maximum number of simultaneous logins allowed
	Specifies the permitted tunneling protocols
	Configures additional group policy attributes for the WebVPN

Command	Description
banner	Creates a banner or welcome text to be displayed on the VPN remote client
group-lock	Specifies the name of an existing tunnel group that users are required to connect with
periodic-authentication	Configures periodic authentication
vlan	Specifies the VLAN onto which VPN traffic for this group will be forwarded.
vpn-access-hours	Specifies the name of a configured time-range policy
vpn-idle-timeout	Specifies the idle timeout period, in minutes
vpn-session-timeout	Specifies the maximum user connection time, in minutes, or none for unlimited time
vpn-simultaneous-logins	Specifies the maximum number of simultaneous logins allowed
vpn-tunnel-protocol	Specifies the permitted tunneling protocols
webvpn	Configures additional group policy attributes for the WebVPN

Command	Description
banner	Creates a banner or welcome text to be displayed on the VPN remote client
group-lock	Specifies the name of an existing tunnel group that users are required to connect with
periodic-authentication	Configures periodic authentication
vlan	Specifies the VLAN onto which VPN traffic for this group will be forwarded.
vpn-access-hours	Specifies the name of a configured time-range policy
vpn-idle-timeout	Specifies the idle timeout period, in minutes
vpn-session-timeout	Specifies the maximum user connection time, in minutes, or none for unlimited time
vpn-simultaneous-logins	Specifies the maximum number of simultaneous logins allowed
vpn-tunnel-protocol	Specifies the permitted tunneling protocols
webvpn	Configures additional group policy attributes for the WebVPN

WebVPN Group Policy Attributes

In group policy WebVPN configuration mode, you can specify whether to inherit or customize the parameters as shown Table 8-6. This is similar to the concept covered in Table 8-5, meaning you are creating parameters that will be applied to anybody within the group policy.

Table 8-6 WebVPN Group Policy Attributes for Clientless SSLVPNs

Command	Description
	Lets a user who has established a clientless SSLVPN session use a browser to launch Microsoft Office applications. The applications use the session to download and upload ActiveX. The ActiveX relay remains in force until the clientless SSLVPN session closes.
	Sets values for auto sign-on, which requires that the user enter username and password credentials only once for a clientless SSLVPN connection.
	Assigns a customization object to a group policy or user.
	Specifies the message delivered to a remote user who logs in to clientless SSLVPN successfully but has no VPN privileges.
	Enables CIFS file browsing for file servers and shares. Browsing requires NBNS (Master Browser or WINS).
	Allows users to enter names of file servers to access.
	Sets the name of the web type access list.
	Controls the visibility of hidden shares for CIFS files.
	Sets the URL of the web page that displays upon login.
	Configures the content and objects to filter from the HTML for this group policy.
	Configures compression.
	Configures the ASA to use an external proxy server to handle HTTP requests.
	Sets the maximum object size to ignore for updating the session timer.
	Applies a list of clientless SSLVPN TCP ports to forward. The user interface displays the applications in this list.
	Sets the maximum object size to post.
	Configures a list of programs and several smart tunnel parameters to use a smart tunnel.
	Configures storage objects for the data stored between sessions.
	Configures SSLVPN client attributes.
	Sets the UNIX group ID.
	Sets the UNIX user ID.
	Controls the ability of the user to enter any HTTP/HTTPS URL.
	Applies a list of servers and URLs that the clientless SSLVPN portal page displays for end-user access.
	Configures a location for storing user data between sessions.

Command	Description
activex-relay	Lets a user who has established a clientless SSLVPN session use a browser to launch Microsoft Office applications. The applications use the session to download and upload ActiveX. The ActiveX relay remains in force until the clientless SSLVPN session closes.
auto-sign-on	Sets values for auto sign-on, which requires that the user enter username and password credentials only once for a clientless SSLVPN connection.
customization	Assigns a customization object to a group policy or user.
deny-message	Specifies the message delivered to a remote user who logs in to clientless SSLVPN successfully but has no VPN privileges.
file-browsing	Enables CIFS file browsing for file servers and shares. Browsing requires NBNS (Master Browser or WINS).
file-entry	Allows users to enter names of file servers to access.
filter	Sets the name of the web type access list.
hidden-shares	Controls the visibility of hidden shares for CIFS files.
homepage	Sets the URL of the web page that displays upon login.
html-content-filter	Configures the content and objects to filter from the HTML for this group policy.
http-comp	Configures compression.
http-proxy	Configures the ASA to use an external proxy server to handle HTTP requests.
keep-alive-ignore	Sets the maximum object size to ignore for updating the session timer.
port-forward	Applies a list of clientless SSLVPN TCP ports to forward. The user interface displays the applications in this list.
post-max-size	Sets the maximum object size to post.
smart-tunnel	Configures a list of programs and several smart tunnel parameters to use a smart tunnel.
storage-objects	Configures storage objects for the data stored between sessions.
svc	Configures SSLVPN client attributes.
unix-auth-gid	Sets the UNIX group ID.
unix-auth-uid	Sets the UNIX user ID.
url-entry	Controls the ability of the user to enter any HTTP/HTTPS URL.
url-list	Applies a list of servers and URLs that the clientless SSLVPN portal page displays for end-user access.
user-storage	Configures a location for storing user data between sessions.

Command	Description
activex-relay	Lets a user who has established a clientless SSLVPN session use a browser to launch Microsoft Office applications. The applications use the session to download and upload ActiveX. The ActiveX relay remains in force until the clientless SSLVPN session closes.
auto-sign-on	Sets values for auto sign-on, which requires that the user enter username and password credentials only once for a clientless SSLVPN connection.
customization	Assigns a customization object to a group policy or user.
deny-message	Specifies the message delivered to a remote user who logs in to clientless SSLVPN successfully but has no VPN privileges.
file-browsing	Enables CIFS file browsing for file servers and shares. Browsing requires NBNS (Master Browser or WINS).
file-entry	Allows users to enter names of file servers to access.
filter	Sets the name of the web type access list.
hidden-shares	Controls the visibility of hidden shares for CIFS files.
homepage	Sets the URL of the web page that displays upon login.
html-content-filter	Configures the content and objects to filter from the HTML for this group policy.
http-comp	Configures compression.
http-proxy	Configures the ASA to use an external proxy server to handle HTTP requests.
keep-alive-ignore	Sets the maximum object size to ignore for updating the session timer.
port-forward	Applies a list of clientless SSLVPN TCP ports to forward. The user interface displays the applications in this list.
post-max-size	Sets the maximum object size to post.
smart-tunnel	Configures a list of programs and several smart tunnel parameters to use a smart tunnel.
storage-objects	Configures storage objects for the data stored between sessions.
svc	Configures SSLVPN client attributes.
unix-auth-gid	Sets the UNIX group ID.
unix-auth-uid	Sets the UNIX user ID.
url-entry	Controls the ability of the user to enter any HTTP/HTTPS URL.
url-list	Applies a list of servers and URLs that the clientless SSLVPN portal page displays for end-user access.
user-storage	Configures a location for storing user data between sessions.

WebVPN Group Policy vs. Group Policy Attributes

Know that for WebVPN group policy and group policy attributes the concepts behind how they work are the same. The difference between WebVPN group policies and group policies is where you apply the commands, meaning the commands are located in different places as you configure your VPN. You use the commands listed in Table 8-5 to modify the desired attribute(s) or use the **webvpn** command to enter group policy webvpn configuration mode, and use the commands in Table 8-6 to modify the desired attributes(s).

Know that the user, group, and default group policies can be applied to clientless, AnyConnect, and IPsec-based remote access VPN tunnels. Some of the most commonly used clientless SSLVPN-specific attributes are discussed in detail in the next few sections of this chapter.

Step 5: Configuring Connection Profiles

A connection profile, also known as a tunnel group, consists of a set of records that determines tunnel connection policies. These records identify the servers to which the user is authenticated, as well as the accounting servers, if any, to which connection information is sent. They also identify a default group policy for the connection, and they contain protocol-specific connection parameters. Connection profiles include a small number of attributes that pertain to creating a tunnel. A connection profile includes a pointer to a group policy that defines user-oriented attributes.

Default Connect Profiles

The ASA provides the following default connection profiles: DefaultL2Lgroup for LAN-to-LAN connections, DefaultRAgroup for IPsec remote access connections, and DefaultWEBVPNGroup for SSLVPN (browser-based and AnyConnect-based) connections. You can modify these default connection profiles, but you cannot delete them. You can also create one or more connection profiles specific to your environment. Connection profiles are local to the ASA and are not configurable on external servers.

Creating a Connection Profile Using ASDM

To create and modify a connection profile via ASDM, follow these steps:

Step 1. Navigate to **Configuration** > **Remote Access VPN** > **Clientless SSL VPN Access** > **Connection Profiles**.

Step 2. Click **Add** to open the Add Clientless SSL VPN Connection Profile dialog box.

Step 3. Specify a name for the connection policy.

Step 4. Specify one or more servers for DNS, if not already configured.

Step 5. Specify a domain name, if not already configured.

Step 6. Make any other desired changes.

Step 7. Click **OK** to create the clientless SSLVPN connection profile and close the Add Clientless SSL VPN Connection Profile dialog box.

While not strictly required, you must configure the Domain Name System (DNS) server(s) if:

- Users will be allowed to browse and access internal websites by using FQDNs
- Administrators configure bookmarks that use FQDNs

Figure 8-9 shows an example of creating a simple connection profile for contractors named CONTRACTOR_CONNECTION. The alias CONTRACTORS has been configured to allow users to select this connection group via a drop-down on the login page (if enabled). After a user connects, the ASA will use the DNS server 172.20.1.50 to resolve FQDNs and will append the domain example.com to unqualified names. The attributes from the group policy of CONTRACTORS will be applied to users connecting with this connection; the attributes enable the clientless SSLVPN protocol that has been selected. Users will be authenticated to the local database.

Note

To enable users to select their desired connection profile on the login page, check the Allow user to select connection profile on the login page option on the Connection Profiles page.

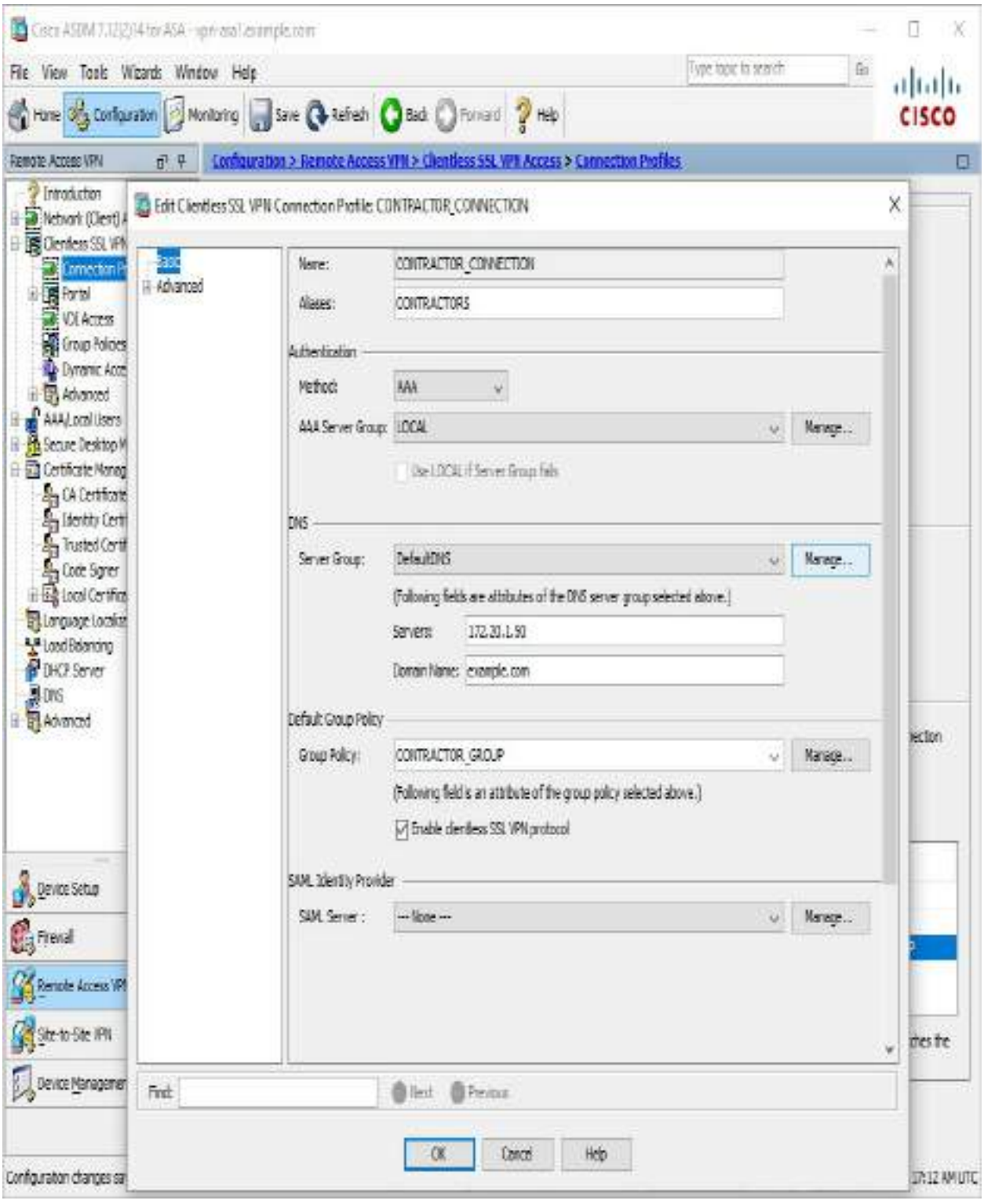


Figure 8-9 Creating a Simple Connection Profile for Contractors via ASDM

Creating a Connection Profile Using CLI

To create and modify a connection profile via the CLI, use the **tunnel-group** *name* **type remote-access** command to create the tunnel group. Then use the **tunnel-group** *name* **general-attributes** command to enter the **tunnel-group general-attributes** configuration mode. Finally, configure the attributes shown in Table 8-7 or use the **tunnel-group** *name* **webvpn-attributes** command to enter the **tunnel-group webvpn-attributes** configuration mode to configure the attributes shown in Table 8-8. Example 8-7 shows an example of creating a simple connection profile for contractors, setting the alias attribute to CONTRACTORS, and setting the default group policy to CONTRACTOR_GROUP. Example 8-8 shows an example of setting the domain name and name server for the device if they were not already configured. The configuration in Example 8-7 and Example 8-8 mirrors the configuration in Figure 8-9.

Example 8-7 Creating a Simple Connection Profile for Contractors via the CLI

```
vpn-asa1(config)# tunnel-group CONTRACTOR_CONNECTION type
remote-access
vpn-asa1(config)# tunnel-group CONTRACTOR_CONNECTION general-
attributes
vpn-asa1(config-tunnel-general)# default-group-policy
CONTRACTOR_GROUP
vpn-asa1(config-tunnel-general)# tunnel-group
CONTRACTOR_CONNECTION webvpn-attributes
vpn-asa1(config-tunnel-webvpn)# group-alias CONTRACTORS enable
vpn-asa1(config-tunnel-webvpn)# exit
```

Example 8-8 Setting DefaultDNS Settings if Not Already Configured

```
vpn-asa1(config)# dns server-group DefaultDNS
vpn-asa1(config-dns-server-group)# domain-name example.com
vpn-asa1(config-dns-server-group)# name-server 172.20.1.50
```

Connection Profile General Attributes

There are a handful of options you can choose for a connection profile. Table 8-7 provides a summary of those options. Think of a connection profile as the security guard at an airport who is responsible for moving passengers to the

proper checkpoint line. Attributes can be used to determine how the client will be authenticated, which policies you want to apply to the user upon authentication, and other connection parameters. Just as we explained earlier in this chapter, attributes are a powerful way to group users into a specific experience. We recommend being familiar with the general attributes available for a connection profile for the SVPN exam.

Table 8-7 Connection Profile General Attributes for Clientless SSLVPNs

Command	Description
	Specifies the name of the accounting server group
	Indicates that the authenticated username will be associated with the session
	Specifies the authentication server that provides an authorization attribute for the session
	Specifies the name of the authentication server group
	Requires users to authorize successfully in order to connect
	Specifies the name of the authorization server group
	Specifies the name of the default group policy
	Enables password management
	Enables SCEP proxy enrollment
	Specifies the name of the secondary authentication server group
	Specifies the DN of the peer certificate used as the secondary username for authorization
	Enables strip-group processing
	Enables strip-realm processing
	Specifies the DN of the peer certificate used as the username for authorization and/or authentication

Command	Description
accounting-server-group	Specifies the name of the accounting server group
authenticated-session-username	Indicates that the authenticated username will be associated with the session
authentication-attr-from-server	Specifies the authentication server that provides an authorization attribute for the session
authentication-server-group	Specifies the name of the authentication server group
authorization-required	Requires users to authorize successfully in order to connect
authorization-server-group	Specifies the name of the authorization server group
default-group-policy	Specifies the name of the default group policy
password-management	Enables password management
scep-enrollment	Enables SCEP proxy enrollment
secondary-authentication-server-group	Specifies the name of the secondary authentication server group
secondary-username-from-certificate	Specifies the DN of the peer certificate used as the secondary username for authorization
strip-group	Enables strip-group processing
strip-realm	Enables strip-realm processing
username-from-certificate	Specifies the DN of the peer certificate used as the username for authorization and/or authentication

Command	Description
accounting-server-group	Specifies the name of the accounting server group
authenticated-session-username	Indicates that the authenticated username will be associated with the session
authentication-attr-from-server	Specifies the authentication server that provides an authorization attribute for the session
authentication-server-group	Specifies the name of the authentication server group
authorization-required	Requires users to authorize successfully in order to connect
authorization-server-group	Specifies the name of the authorization server group
default-group-policy	Specifies the name of the default group policy
password-management	Enables password management
scep-enrollment	Enables SCEP proxy enrollment
secondary-authentication-server-group	Specifies the name of the secondary authentication server group
secondary-username-from-certificate	Specifies the DN of the peer certificate used as the secondary username for authorization
strip-group	Enables strip-group processing
strip-realm	Enables strip-realm processing
username-from-certificate	Specifies the DN of the peer certificate used as the username for authorization and/or authentication

Connection Profile WebVPN Attributes

Another group of attributes you can configure for a connection profile are the WebVPN attributes. These attributes are more specific to the SSLVPN

experience, meaning they are options for this point of building your WebVPN solution. Know that the difference between general attributes and WebVPN attributes is where you configure them. Both are essentially the same thing but are configuration options located at different places. Table 8-8 shows the WebVPN attribute options.

Table 8-8 Connection Profile WebVPN Attributes for Clientless SSLVPNs

Command	Description
	Specifies the authentication method (either AAA or certificate).
	Specifies the name of a previously defined customization to apply. Customizations determine the appearance of the windows that the user sees upon login. You configure the customization parameters as part of configuring a clientless SSLVPN.
	Specifies the DNS server group, which indicates the DNS server name, domain name, name server, number of retries, and timeout values for a DNS server to use for a connection profile.
	Specifies the name of the NetBIOS name service server (nbns-server) to use for CIFS name resolution.
	Specifies the one or more alternate names by which the server can refer to a connection profile. At login, the user selects the group name from a drop-down menu.
	Specifies the one or more group URLs. If you configure this attribute, users coming in on a specified URL need not select a group at login.
	Specifies the VPN feature policy if you use the Cisco Secure Desktop Manager to set the Group-Based Policy attribute to Use Failure Group-Policy or Use Success Group-Policy, if Criteria Match.
	Specifies the username-to-certificate binding on this tunnel group.
	Flags this tunnel group as a specific proxy authentication tunnel group.
	Overrides download of the group policy or username attributes configured for downloading the AnyConnect VPN client to the remote user.
	Enables the display of the RADIUS reject message on the login screen when authentication is rejected.
	Configures SAML service.
	Configures a secondary username-to-certificate binding on this tunnel group.
	Disables CSD for a tunnel group.

Command	Description
authentication	Specifies the authentication method (either AAA or certificate).
customization	Specifies the name of a previously defined customization to apply. Customizations determine the appearance of the windows that the user sees upon login. You configure the customization parameters as part of configuring a clientless SSLVPN.
dns-group	Specifies the DNS server group, which indicates the DNS server name, domain name, name server, number of retries, and timeout values for a DNS server to use for a connection profile.
nbns-server	Specifies the name of the NetBIOS name service server (nbns-server) to use for CIFS name resolution.
group-alias	Specifies the one or more alternate names by which the server can refer to a connection profile. At login, the user selects the group name from a drop-down menu.
group-url	Specifies the one or more group URLs. If you configure this attribute, users coming in on a specified URL need not select a group at login.
hic-fail-group-policy	Specifies the VPN feature policy if you use the Cisco Secure Desktop Manager to set the Group-Based Policy attribute to Use Failure Group-Policy or Use Success Group-Policy, if Criteria Match.
pre-fill-username	Specifies the username-to-certificate binding on this tunnel group.
proxy-auth	Flags this tunnel group as a specific proxy authentication tunnel group.
override-svc-download	Overrides download of the group policy or username attributes configured for downloading the AnyConnect VPN client to the remote user.
radius-reject-message	Enables the display of the RADIUS reject message on the login screen when authentication is rejected.
saml	Configures SAML service.
secondary-pre-fill-username	Configures a secondary username-to-certificate binding on this tunnel group.
without-csd	Disables CSD for a tunnel group.

Command	Description
authentication	Specifies the authentication method (either AAA or certificate).
customization	Specifies the name of a previously defined customization to apply. Customizations determine the appearance of the windows that the user sees upon login. You configure the customization parameters as part of configuring a clientless SSLVPN.
dns-group	Specifies the DNS server group, which indicates the DNS server name, domain name, name server, number of retries, and timeout values for a DNS server to use for a connection profile.
nbns-server	Specifies the name of the NetBIOS name service server (nbns-server) to use for CIFS name resolution.
group-alias	Specifies the one or more alternate names by which the server can refer to a connection profile. At login, the user selects the group name from a drop-down menu.
group-url	Specifies the one or more group URLs. If you configure this attribute, users coming in on a specified URL need not select a group at login.
hic-fail-group-policy	Specifies the VPN feature policy if you use the Cisco Secure Desktop Manager to set the Group-Based Policy attribute to Use Failure Group-Policy or Use Success Group-Policy, if Criteria Match.
pre-fill-username	Specifies the username-to-certificate binding on this tunnel group.
proxy-auth	Flags this tunnel group as a specific proxy authentication tunnel group.
override-svc-download	Overrides download of the group policy or username attributes configured for downloading the AnyConnect VPN client to the remote user.
radius-reject-message	Enables the display of the RADIUS reject message on the login screen when authentication is rejected.
saml	Configures SAML service.
secondary-pre-fill-username	Configures a secondary username-to-certificate binding on this tunnel group.
without-csd	Disables CSD for a tunnel group.

Step 6: Configuring User Authentication

Authentication is a critical component of a VPN technology. Industry best practice is leveraging multifactor authentication based on a combination of something you know, something you have, and something you are. Best practice also includes using a centralized database to manage all user login details versus creating accounts for individual systems. For example, it is common to create a separate policy for administrators and employees in which employees have less privileges than administrators. It is also common to require employees to use a combination of a password and token to prove their identity.

The ASA supports a number of different authentication protocols and databases to meet the requirements of the previous example as well as many other use cases. The following are options you can use to meet your authentication requirements:

- RADIUS (Remote Authentication Dial-In User Service)
- NT domain
- Kerberos
- SDI (RSA SecureID)
- LDAP (Lightweight Directory Access Protocol)
- Digital certificates
- Smart cards
- Local database
- SAML 2.0 (Security Assertion Markup Language)

Authentication Servers

For small organizations, a local database can be set up for user authentication.

This is fine for supporting a few users; however, as an organization grows, so will its users and resources that need to be secured. There will be a point where the administration overhead of creating individual user accounts on separate systems will overwhelm an administration team, and a centralized solution will be needed.

For medium to large SSLVPN deployments, it is highly recommended that you use an external authentication server, such as a RADIUS, LDAP, or Kerberos server, as the user authentication database. The value of using a centralization authentication system includes the following:

- Having one database that all systems reference for authentication
- Having one place to provision and disable accounts
- Having simplified monitoring and logging of authentication behavior
- Being able to group users with similar policies into categories such as Employees and Contractors
- Having standardized authentication across the organization

While you prepare for the SVPN exam, you might be able to access an ASA or ASA emulator. For a lab environment, you can practice creating a local account for user authentication purposes. Next, we work through how to do that using both ASDM and CLI.

Configuring Authentication Using ASDM

To create a VPN-only local user via ASDM, follow these steps:

Step 1. Navigate to **Configuration** > **Remote Access VPN** > **AAA/Local Users** > **Local Users**.

Step 2. Click **Add** to open the Add User Account dialog box.

Step 3. Specify a username.

Step 4. Specify a password and confirm the password.

Step 5. Select **No ASDM**, **SSH**, **Telnet** or **Console** access to block admin access.

Step 6. Click **OK** to create the user account and close the Add User Account dialog box.

Figure 8-10 shows an example of creating a VPN only local user with the username vpnuser2. No ADSM, SSH, Telnet, or console access has been selected, which will result in the user only being able to log in to the VPN. There were two users accounts, admin and vpnuser, previously configured on the ASA. The admin account can both administer the ASA via ASDM/CLI and log in to the VPN; vpnuser can only log in to the VPN.

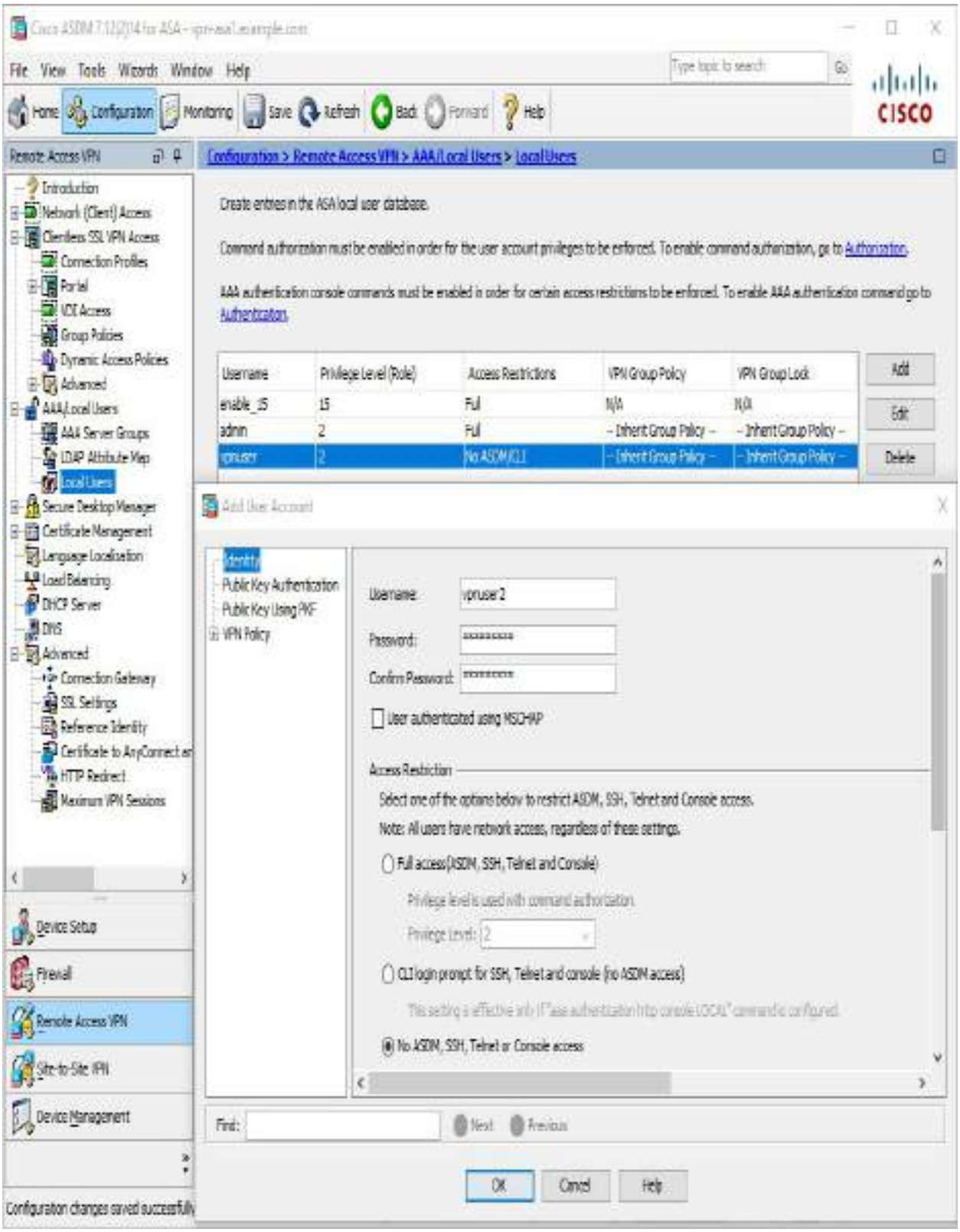


Figure 8-10 Creating a VPN Only Local User via ASDM

Configuring Local Authentication Using CLI

To create a VPN only local user via the CLI, use the **username** command to create the user. Then use the **username** *name* **attributes** command to enter username configuration mode and use the **service-type** command to specify the allowed service type(s) for the user. Example 8-9 shows an example of creating a VPN only user with the service-type remote-access that mirrors the configuration in Figure 8-10.

Example 8-9 Creating a VPN Only Local User via the CLI

```
vpn-asa1(config)# username vpnuser2 password cisco123 privilege
2
vpn-asa1(config)# username vpnuser2 attributes
vpn-asa1(config-username)# service-type remote-access
```

With authentication configured, users can now log in to the VPN by navigating to https://vpn-asa1.example.com/ from any standard web browser. Upon doing so, they will be greeted by the login page. While the VPN is now functional and will provide users access to browse internal resources via the explorer bar, the next section discusses how the functionality of the clientless SSLVPN can be extended beyond the default configuration and functionality.

The majority of organizations we work with have some form of centralized authentication system. For this reason, you will need to know how to configure a VPN solution to work with an external authentication solution. This chapter gave you an example of using local authentication. In Chapter 9, you see how to use an external authentication solution. Make sure you know how to use both local and external authentication options.

That wraps up configuring a basic SSLVPN using both ASDM and CLI. Now that you can build a basic SSLVPN, we will look at configuration options that impact the users who successfully connect through the VPN solution.

Extended Clientless SSLVPN Configuration Options

The previous section discusses the basic steps required to enable a clientless SSLVPN on the ASA. With users able to successfully access the clientless SSLVPN, we turn our focus to enabling their access to specific applications and controlling which applications they can access. To accomplish that goal, we explore the following topics:

- Configuring bookmarks
- Configuring web ACLs
- Configuring application access via port forwarding
- Configuring application access via smart tunnels
- Configuring client/server plug-ins

Configuring Bookmarks

By default, users can browse for resources by using the explorer bar within the clientless SSLVPN portal. Administrators can also define bookmarks to provide users with predefined servers to access. Both of these options are illustrated in Figure 8-11.

Figure 8-11 Clientless SSLVPN Portal with Explorer Bar and Bookmarks

Defining bookmarks serves two primary purposes. If the explorer bar remains

enabled, bookmarks make it easy for users to access commonly used resources. If the administrator chooses to disable the explorer bar, bookmarks serve as a way to restrict the resources users can easily access.

Bookmark Support

Bookmarks are supported for multiple different application types and protocols, including these:

- Websites (HTTP and HTTPS)
- File servers (CIFS and FTP)
- RDP (Remote Desktop Protocol)
- VNC (Virtual Network Computing)
- SSH and Telnet

Note

You will not see an option for RDP, VNC, SSH, and/or Telnet unless the appropriate client/server plug-in has been installed first. Installing client/server plug-ins is covered later in this chapter.

Configuring a bookmark is a two-step process:

Step 1. Create a bookmark list.

Step 2. Apply the bookmark list (for example, via a group policy).

Creating a Bookmark List

To create a simple bookmark via ASDM, follow these steps:

Step 1. Navigate to **Configuration** > **Remote Access VPN** > **Clientless SSL VPN Access** > **Portal** > **Bookmarks**.

Step 2. Click **Add** to open the Add Bookmark List dialog box.

Step 3. Specify a bookmark list name that will later be referenced in a group policy.

Step 4. Click **Add** to open the Select Bookmark Type dialog box.

Step 5. Select **URL** with a GET or POST method.

Step 6. Click **OK** to close the Select Bookmark Type dialog box and open the Add Bookmark dialog box.

Step 7. Specify a bookmark title that will be the name for the bookmark that is visible to the user.

Step 8. Specify **URL** for the bookmark.

Step 9. Click **OK** to add the bookmark and close the Add Bookmark dialog box.

Step 10. Click **OK** to add the bookmark list close the Add Bookmark List dialog box.

Figure 8-12 shows an example of creating a simple bookmark list for contractors called CONTRACTOR_BOOKMARKS. There is a single bookmark named HR Web Server that points to the URL http://hr.example.com.

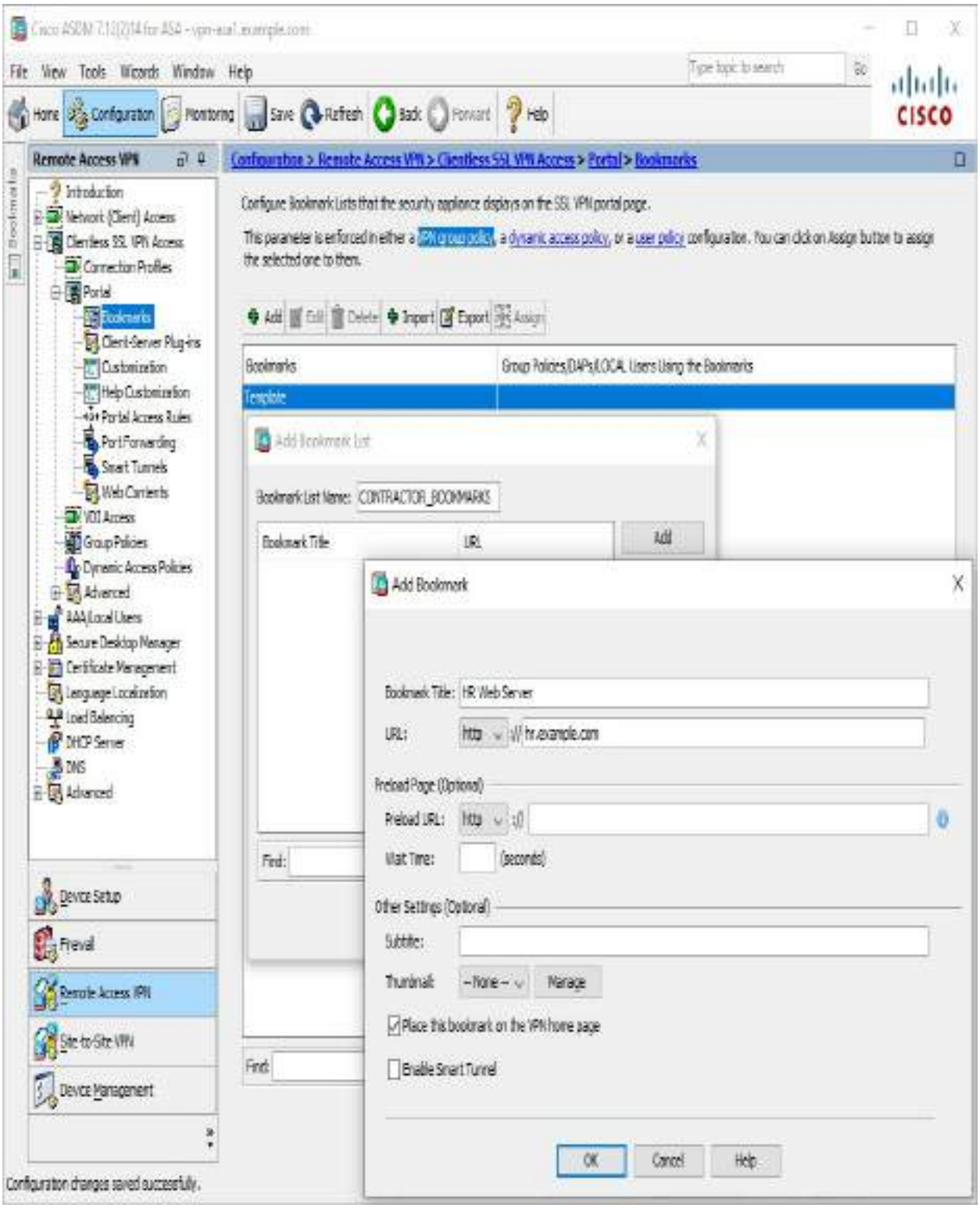


Figure 8-12 Configuring a Simple Bookmark List for Contractors via ASDM

Note

You must use ASDM to create bookmarks. Creating bookmarks via the CLI is not currently supported.

Applying the Bookmark List to a Group Policy Using ASDM

To apply a bookmark list to a group policy via ASDM, follow these steps:

Step 1. Navigate to **Configuration** > **Remote Access VPN** > **Clientless SSL VPN Access** > **Group Policies**.

Step 2. Select a group policy and click **Edit** to open the Edit Internal Group Policy dialog box.

Step 3. Click **Portal**.

Step 4. Uncheck the **Inherit** next to Bookmark List and select the desired bookmark list in the drop-down.

Step 5. Click **OK** to close the Edit Internal Group Policy dialog box.

Figure 8-13 shows an example of setting the bookmark list attribute to CONTRACTOR_BOOKMARKS for the group policy CONTRACTOR_GROUP.

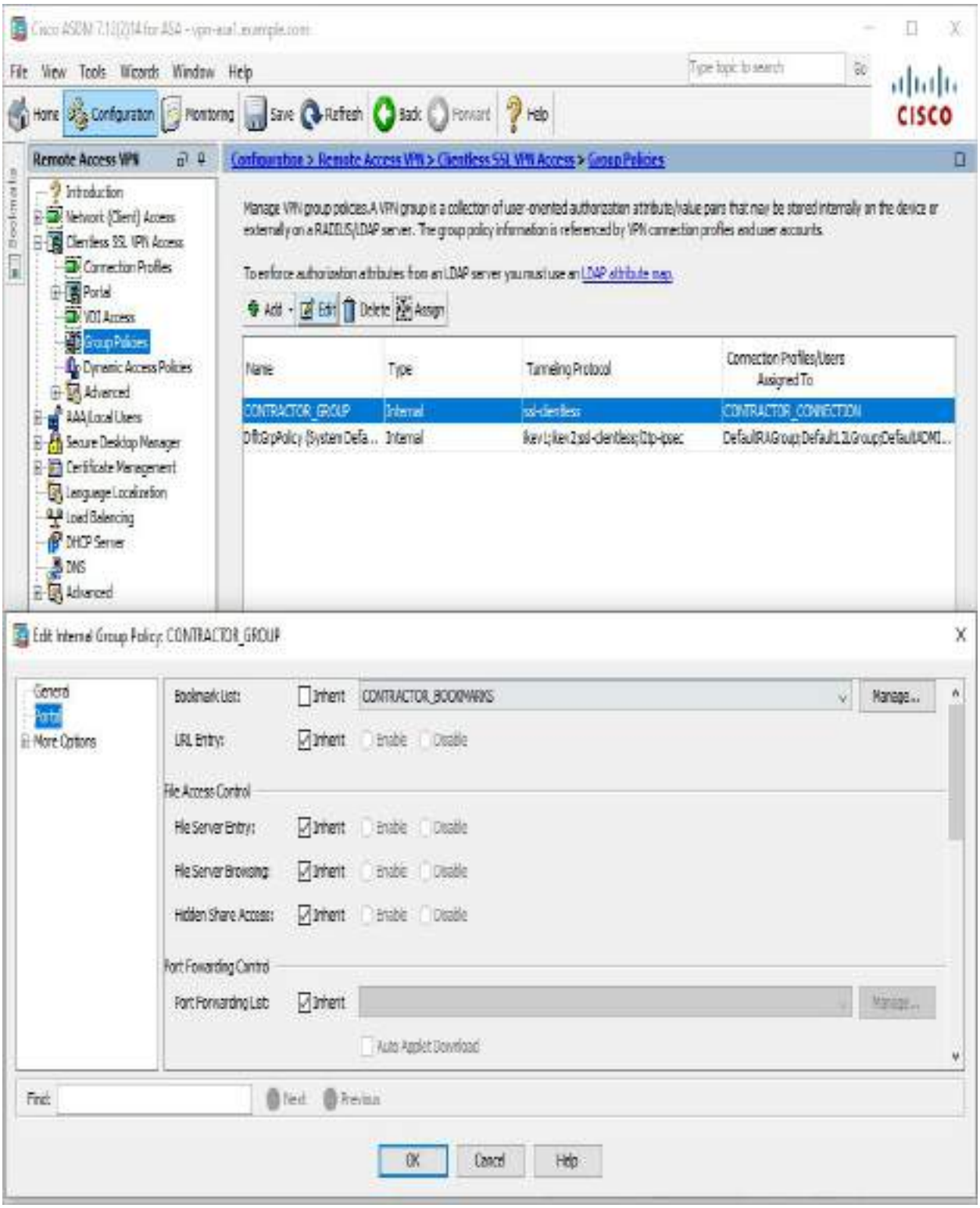


Figure 8-13 Setting the Bookmark List Attribute for a Group Policy via ASDM

Applying the Bookmark List to a Group Policy Using CLI

To set the bookmark list attribute in a group policy via the CLI, use the **url-list** command in group policy webvpn configuration mode. Example 8-10 shows an example of setting the bookmark list attribute to CONTRACTOR_BOOKMARKS in the group policy CONTRACTOR_GROUP. It mirrors the configuration in Figure 8-12 and Figure 8-13.

Example 8-10 Setting the Bookmark List Attribute in a Group Policy via the CLI

```
vpn-asa1(config)# group-policy CONTRACTOR_GROUP attributes
vpn-asa1(config-group-policy)# webvpn
vpn-asa1(config-group-webvpn)# url-list value
CONTRACTOR_BOOKMARKS
```

Configuring Web ACLs

Web ACLs allow administrators to control the resources users are able to access when making access requests through a clientless SSLVPN. Unlike network ACLs, though, web ACLs only affect clientless SSLVPN traffic.

Web ACL Support

The ASA supports the following types of web ACLs:

- CIFS, FTP, and NFS
- Citrix and Citrixs
- HTTP and HTTPS
- IMAP4, POP3, and SMTP

- SSH and Telnet
- RDP and VNC
- Smart tunnel
- Any type of traffic

Note

You must import the RDP, VNC, and SSH/Telnet plug-ins to be able to filter those protocols via a web ACL. Plug-ins are discussed later in this chapter.

By default, there is no web ACL applied to group policies, and all traffic is allowed through a clientless SSLVPN. Once an ACL is defined and applied to the group policy, the behavior changes: If traffic is not explicitly allowed, it will be blocked.

Configuring a web ACL is a two-step process:

Step 1. Create a web ACL.

Step 2. Apply the web ACL list (for example, via a group policy).

Creating a Web ACL Using ASDM

To create a web ACL via ASDM, follow these steps:

Step 1. Navigate to **Configuration** > **Remote Access VPN** > **Clientless SSL VPN Access** > **Advanced** > **Web ACLs**.

Step 2. Click **Add** > **Add ACL** to open the Add ACL dialog box.

Step 3. Specify an ACL name, and click **OK** to create the web ACL and close the Add ACL dialog box.

Step 4. Select the previously created web ACL.

Step 5. Click **Add** > **Add ACE** to open the Add ACE dialog box.

Step 6. In the Filter section, select one of the following:

- **Filter on URL:** To filter based on the application layer URL
- **Filter on Address and Service:** To filter based on TCP layer information

Step 7. Click **OK** to create the ACE and close the Add ACE dialog box.

Figure 8-14 shows the creation of a web ACL named CONTRACTOR_WEBACL. The ACL will have a single ACE that permits traffic to http://hr.example.com.

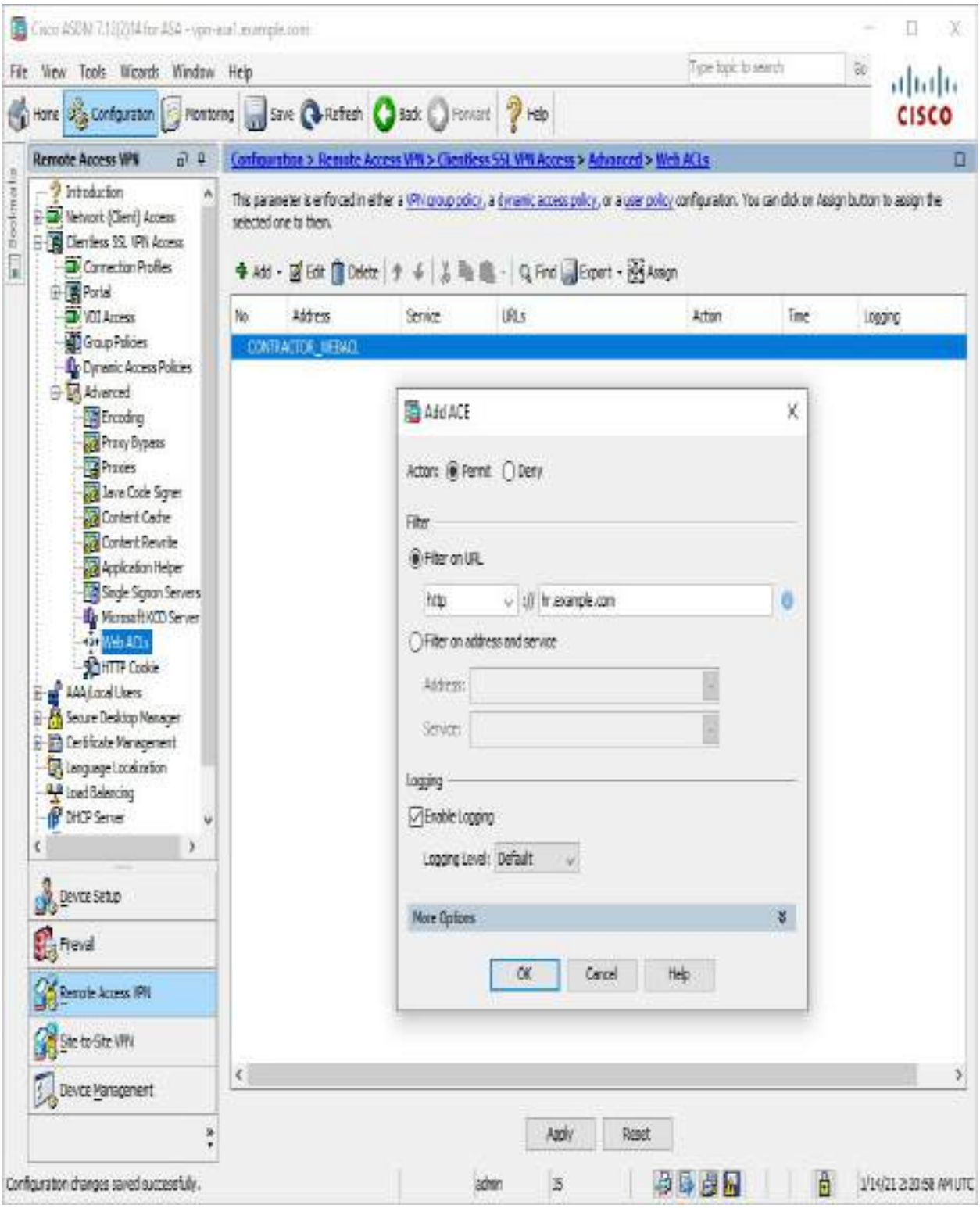


Figure 8-14 Creating a Web ACL via ASDM

Creating a Web ACL Using CLI

To create a web ACL via the CLI, use the **access-list** *name* **webtype** command to create the ACL and ACE. Example 8-11 shows an example of creating the web ACL CONTRACTOR_WEBACL. It mirrors the configuration in Figure 8-14.

Example 8-11 Creating a Web ACL via the CLI

```
vpn-asa1(config)# access-list CONTRACTOR_WEBACL webtype permit
url http://hr.example.com
```

Applying a Web ACL to a Group Policy Using ASDM

To apply a web ACL to a group policy, follow these steps:

Step 1. Navigate to **Configuration** > **Remote Access VPN** > **Clientless SSL VPN Access** > **Group Policies**.

Step 2. Select a group policy and click **Edit** to open the Edit Internal Group Policy dialog box.

Step 3. Click **General**.

Step 4. Click **More Options**.

Step 5. Uncheck the **Inherit** check box next to Web ACL.

Step 6. Select the desired web ACL from the drop-down to apply to the group policy.

Step 7. Click **OK** to close the Edit Internal Group Policy dialog box.

Figure 8-15 shows an example of setting the web ACL attribute to CONTRACTOR_WEBACL for the group policy CONTRACTOR_GROUP.

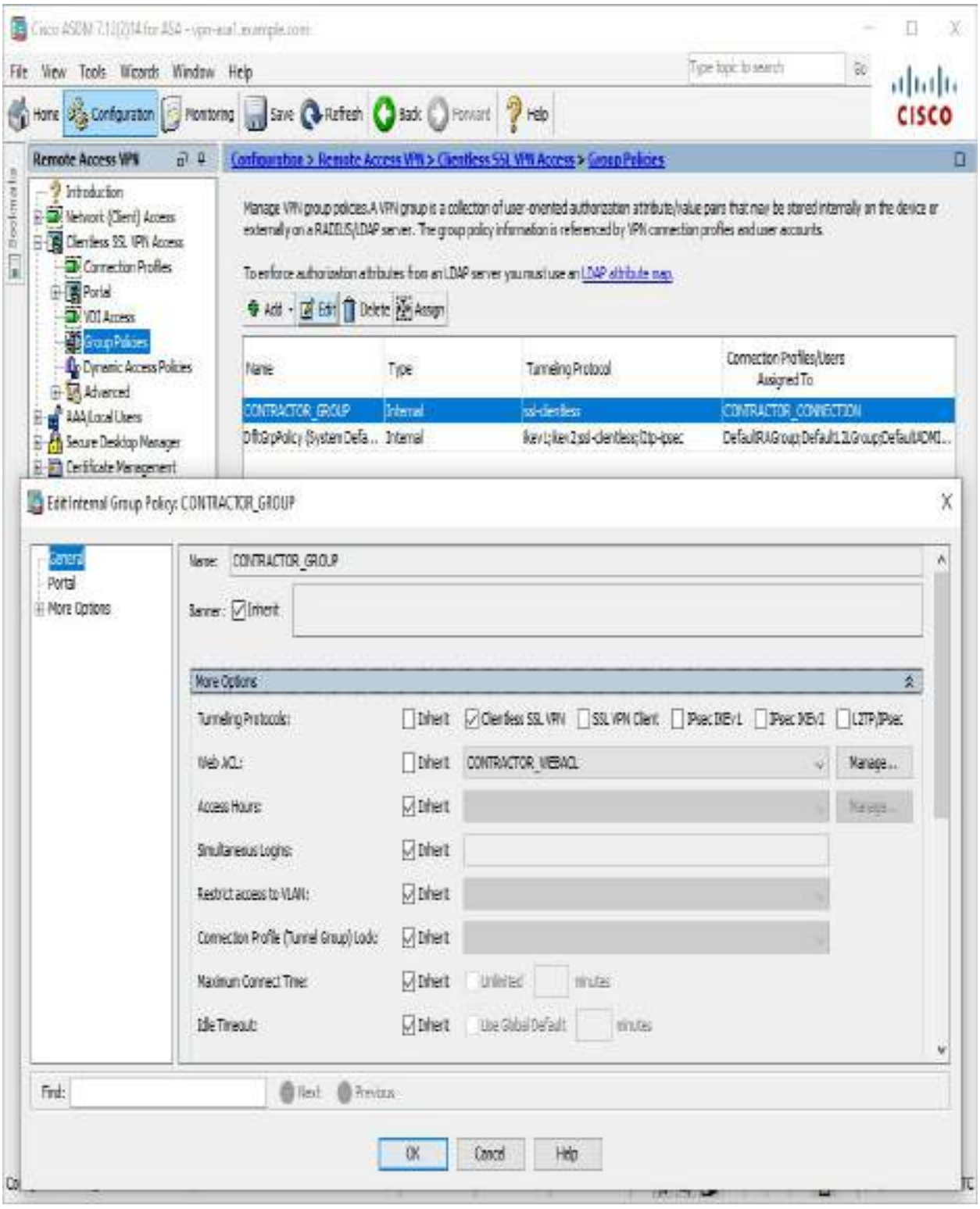


Figure 8-15 Setting the Web ACL Attribute for a Group Policy via ASDM

Applying a Web ACL to a Group Policy Using CLI

To apply a web ACL to a group policy via the CLI, use the **filter value** command in group policy webvpn configuration mode to set the attribute for a group policy. Example 8-12 shows an example of applying the web ACL CONTRACTOR_WEBACL to the group policy CONTRACTOR_GROUP. It mirrors the configuration in Figure 8-15.

Example 8-12 Applying a Web ACL to a Group Policy via the CLI

```
vpn-asa1(config)# group-policy CONTRACTOR_GROUP attributes
vpn-asa1(config-group-policy)# webvpn
vpn-asa1(config-group-webvpn)# filter value CONTRACTOR_WEBACL
```

Configuring Application Access via Port Forwarding

Port forwarding allows users to access TCP-based applications over a clientless SSLVPN connection. Such applications include Secure FTP (FTP over SSH), SSH, Telnet, and Windows Terminal Service.

Port forwarding only works with applications that use a single TCP port. Applications that use UDP, dynamic TCP ports (for example, Active FTP) or multiple TCP ports are not supported. Due to these limitations, port forwarding is primarily a legacy technology for supporting simple TCP applications over a clientless SSLVPN connection. New implementations should use smart tunnels, which are discussed in the next section.

Port forwarding involves using a Java applet to redirect traffic destined to a local IP address and port across the clientless SSLVPN. In Figure 8-16, RDP traffic destined to 127.0.0.1 on port 12345 will be directed across the clientless SSLVPN and forwarded to the server hr.example.com on port 3389. On the RDP client, the user directs the client to connect to 127.0.0.1:12345 rather than hr.example.com.

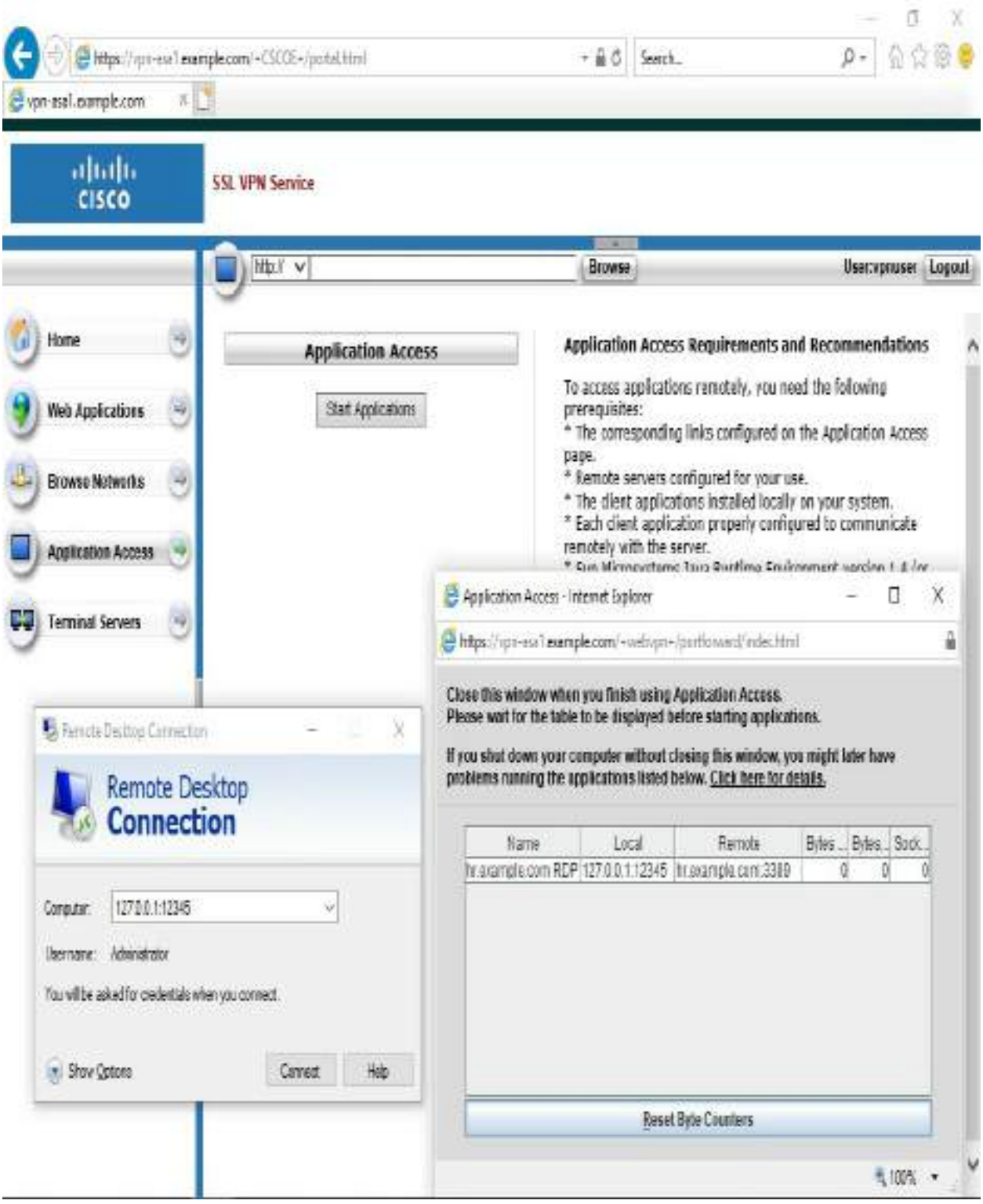


Figure 8-16 Port Forwarding of RDP Traffic

Configuring a port forwarding list is a two-step process:

Step 1. Create a port forwarding list.

Step 2. Apply the port forwarding list (for example, via a group policy).

Creating a Port Forwarding List Using ASDM

To create a port forwarding list via ASDM, follow these steps:

Step 1. Navigate to **Configuration** > **Clientless SSL VPN Access** > **Portal** > **Port Forwarding**.

Step 2. Click **Add** to open the Add Port Forwarding List dialog box.

Step 3. Specify a list name for the port forwarding list.

Step 4. Click **Add** to bring up the Add Port Forwarding Entry dialog box.

Step 5. Specify the local TCP port for the client connection.

Step 6. Specify the remote server the connection should be redirected to.

Step 7. Specify the remote TCP port to which the connections should be redirected.

Step 8. Specify an optional user-visible description for the port forwarding entry.

Step 9. Click **OK** to create the port forwarding entry and close the Add Port Forwarding Entry dialog box.

Step 10. Click **OK** to create the port forwarding list and close the Add Port Forwarding List dialog box.

Figure 8-17 shows an example of configuring the port forwarding entry that matches Figure 8-16. Traffic travels from the local TCP port 12345 to the remote server hr.example.com on port 3389. The user sees the description of hr.example.com RDP in the port forwarding applet. The forwarding entry is added to the port forwarding list CONTRACTOR_PORTFORWARDING.

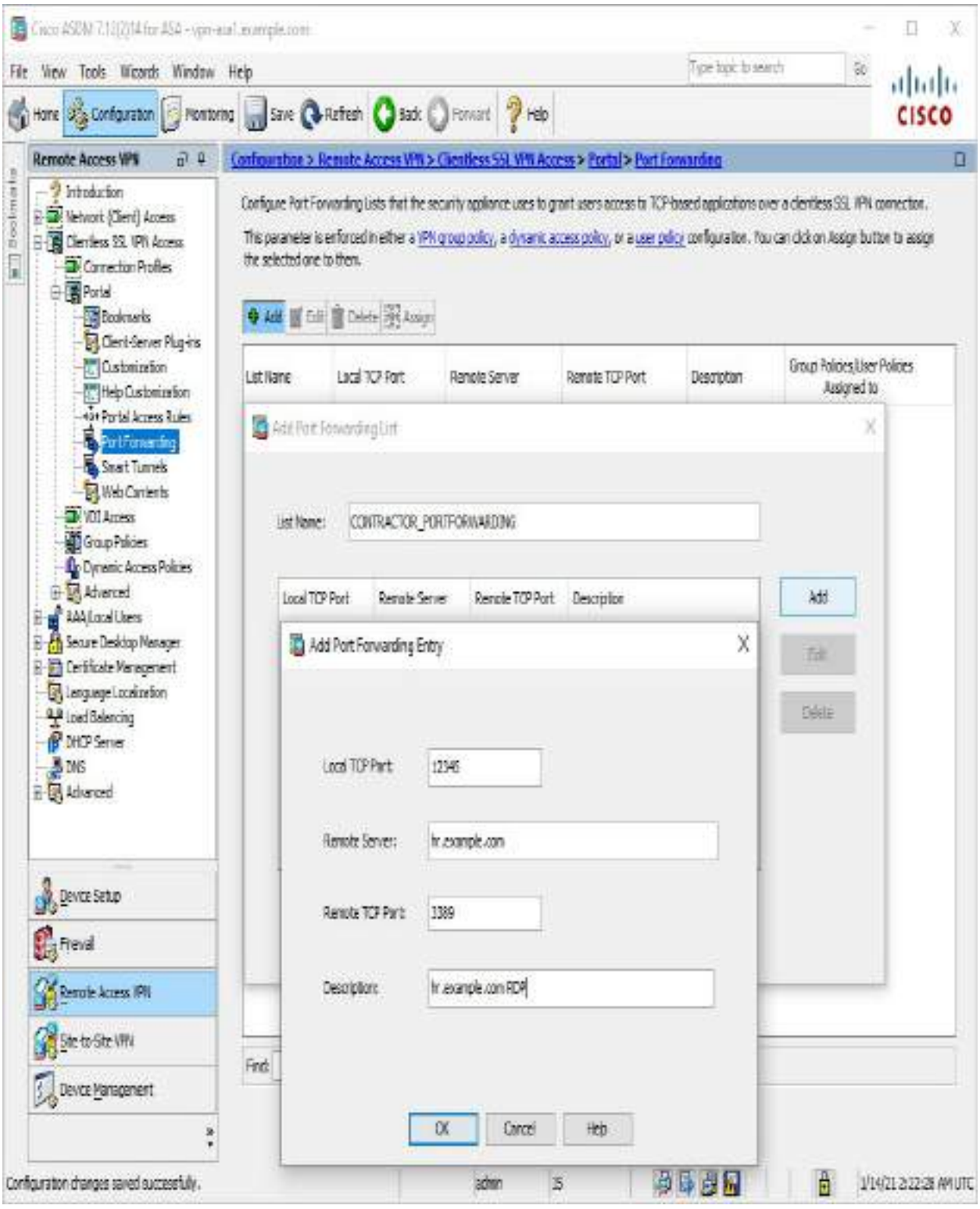


Figure 8-17 Defining a Port Forwarding List

Creating a Port Forwarding List Using CLI

To create a port forwarding list via the CLI, use the **port-forward** command in the webvpn configuration mode. Example 8-13 shows an example of creating a port forwarding list. It mirrors the configuration in Figure 8-17.

Example 8-13 Creating a Port Forwarding List via the CLI

```
vpn-asa1(config)# webvpn
vpn-asa1(config-webvpn)# port-forward CONTRACTOR_PORTFORWARDING
12345 hr.example.com
```

Applying a Port Forwarding List to a Group Policy Using ASDM

To apply a port forwarding list to a group policy via ASDM, follow these steps:

Step 1. Navigate to **Configuration** > **Remote Access VPN** > **Clientless SSLVPN Access** > **Group Policies** and select the desired group policy.

Step 2. Click **Edit** to bring up the Edit Internal Group Policy dialog box.

Step 3. Click **Portal**.

Step 4. Uncheck the **Inherit** check box next to Port Forwarding List and select the previously created port forwarding in the drop down.

Step 5. Click **OK** to close the Edit Internal Group Policy dialog box.

Figure 8-18 shows the port forwarding list CONTRACTOR_PORTFORWARDING applied to the group policy CONTRACTOR_GROUP.

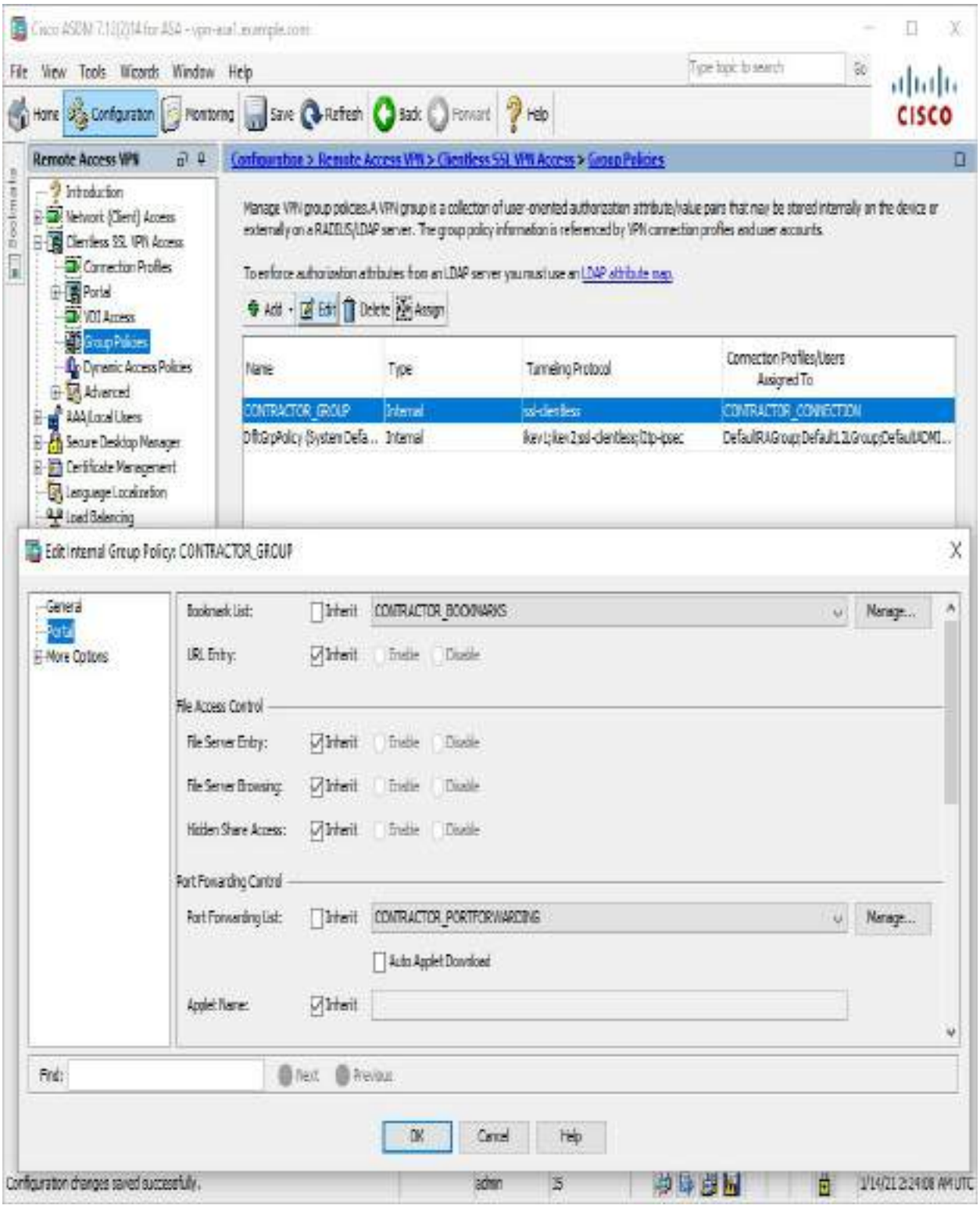


Figure 8-18 Applying a Port Forwarding List to a Group Policy via ASDM

Applying a Port Forwarding List to a Group Policy Using

ASDM

To apply a port forwarding list to a group policy via the CLI, use the **port-forward** command in the group policy webvpn configuration mode. Example 8-14 shows applying a port forwarding list to a group policy. It mirrors the configuration in Figure 8-18.

Example 8-14 Applying a Port Forwarding List to a Group Policy via the CLI

```
vpn-asa1(config-config)# group-policy CONTRACTOR_GROUP
attributes
vpn-asa1(config-group-policy)# webvpn
vpn-asa1(config-group-webvpn)# port-forward enable
CONTRACTOR_PORTFORWARDING
```

Configuring Application Access via Smart Tunnels

A smart tunnel is a connection between a TCP-based application and a private site, using a clientless (browser-based) SSLVPN session with the security appliance as the pathway and the security appliance as a proxy server. You can identify applications to which you want to grant smart tunnel access and specify the local path to each application. For applications that run on Microsoft Windows, you can also require a match of the SHA-1 hash of the checksum as a condition for granting smart tunnel access.

Smart Tunnel Requirements

Depending on whether the application is a client or a web-enabled application, smart tunnel configuration requires one of these procedures:

- Create one or more smart tunnel lists of the client applications and then assign the list to the group policies or local user policies for which you want to provide smart tunnel access.
- Create one or more bookmark list entries that specify the URLs of the web-enabled applications eligible for smart tunnel access and then assign the list to the DAPs, group policies, or local user policies for which you

want to provide smart tunnel access

You can also list web-enabled applications for which to automate the submission of login credentials in smart tunnel connections over clientless SSLVPN sessions.

A smart tunnel table displays the smart tunnel lists, each of which identifies one or more applications eligible for smart tunnel access and its associated operating system. Because each group policy or local user policy supports one smart tunnel list, you must group the non-browser-based applications to be supported into a smart tunnel list. Following the configuration of a list, you can assign it to one or more group polices or local user policies.

Smart Tunnel Benefits

Smart tunnel access offers the following advantages to users:

- A smart tunnel offers better performance than plug-ins.
- Unlike port forwarding, a smart tunnel simplifies the user experience by not requiring the user connection of the local application to the local port.
- Unlike port forwarding, a smart tunnel does not require users to have administrator privileges.
- Unlike port forwarding and smart tunnel access, a plug-in does not require the client application to be installed on the remote computer.

Configuring a smart tunnel list is another two-step process:

Step 1. Create a smart tunnel list.

Step 2. Apply the smart tunnel list (for example, via a group policy).

Creating a Smart Tunnel List Using ASDM

To create a smart tunnel application list via ASDM, follow these steps:

Step 1. Navigate to **Configuration** > **Remote Access VPN** > **Clientless SSLVPN Access** > **Portal** > **Smart Tunnels**.

Step 2. In the Smart Tunnel Application List section, click **Add** bring up the Add Smart Tunnel List dialog box.

Step 3. Specify a list name for the new smart tunnel list.

Step 4. Click **Add** to bring up the Add Smart Tunnel Entry dialog box.

Step 5. Specify an application ID for the new smart tunnel entry.

Step 6. Select the operating system that the smart tunnel entry will apply to.

Step 7. Specify the name of the process that will be tunneled (for example, word.exe).

Step 8. Optionally, specify the hash of the process to further identify the correct process.

Step 9. Click **OK** to create the smart tunnel entry and close the Add Smart Tunnel Entry dialog box.

Step 10. Click **OK** to create the smart tunnel and close the Add Smart Tunnel List dialog box.

Figure 8-19 shows a new smart tunnel entry named PUTTY to tunnel traffic from the Windows process putty.exe. The smart tunnel entry is being added to the smart tunnel list named CONTRACTOR_SMARTTUNNEL.

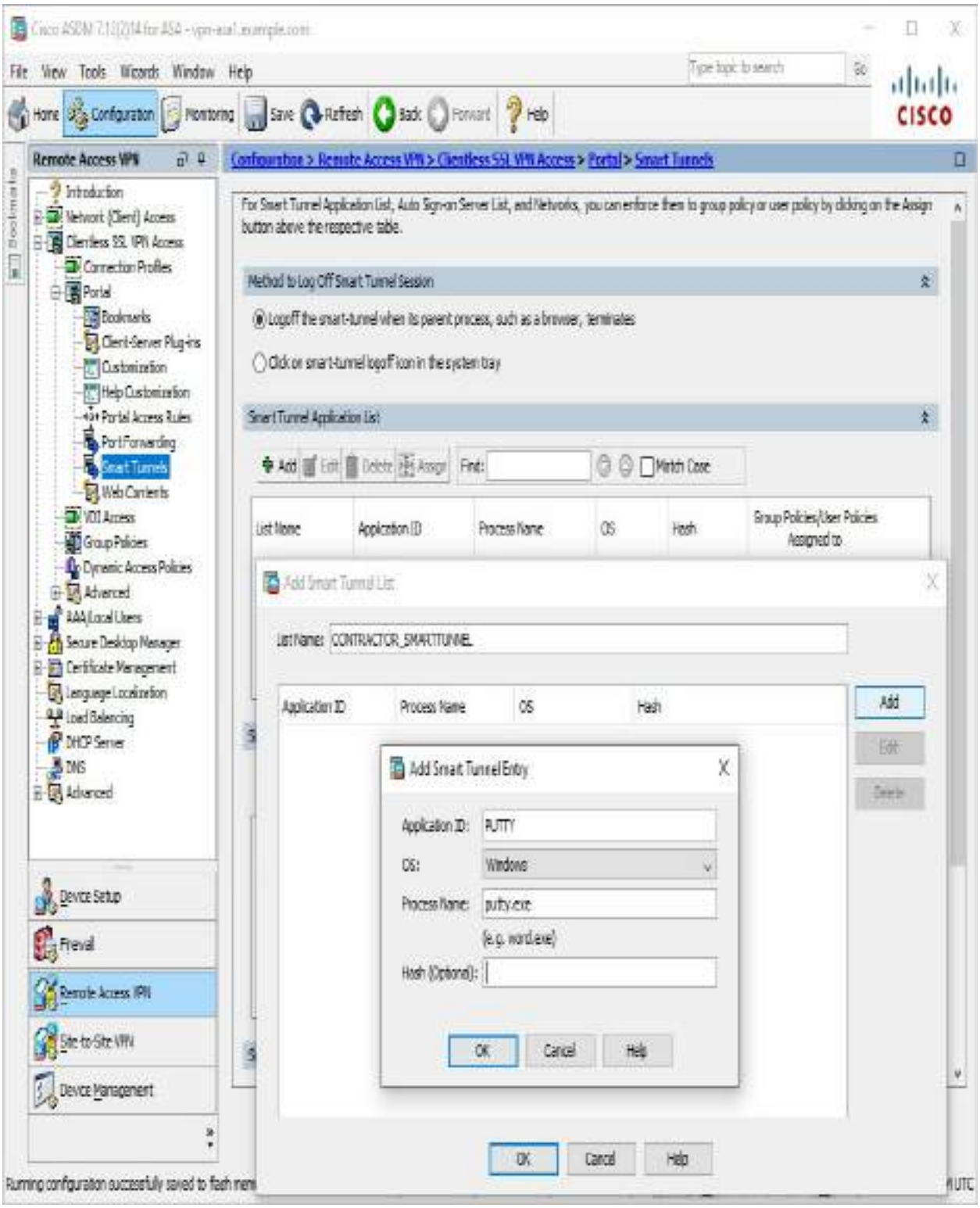


Figure 8-19 Creating a Smart Tunnel Application List via ASDM

Creating a Smart Tunnel List Using ASDM

To create a smart tunnel application list via the CLI, use the **smart-tunnel list** command. Example 8-15 shows an example of creating the smart tunnel application list CONTRACTOR_SMARTTUNNEL for the process putty.exe. It mirrors the configuration in Figure 8-19.

Example 8-15 Defining Smart Tunnel via the CLI

```
vpn-asa1(config)# webvpn
vpn-asa1(config-webvpn)# smart-tunnel list
CONTRACTOR_SMARTTUNNEL PUTTY putty.exe platform windows
```

Applying the Smart Tunnel List to a Group Policy Using ASDM

To apply the smart tunnel application list to a group policy via ASDM, follow these steps:

Step 1. Navigate to **Configuration** > **Remote Access VPN** > **Clientless SSLVPN Access** > **Group Policies** and select the desired group policy.

Step 2. Click **Edit** to bring up the Edit Internal Group Policy dialog box.

Step 3. Click **Portal**.

Step 4. Uncheck the **Inherit** check box next to Smart Tunnel Application and select the desired smart tunnel application list from the drop-down.

Step 5. Click **OK** to close the Edit Internal Group Policy dialog box.

Applying the Smart Tunnel List to a Group Policy Using CLI

To apply a smart tunnel list to a group policy via the CLI, use the **smart-tunnel** command in the group policy webvpn configuration mode. Example 8-16 shows an example of applying the smart tunnel application list CONTRACTOR_SMARTTUNNEL to the group policy CONTRACTOR_GROUP. It mirrors the configuration in Figure 8-20.

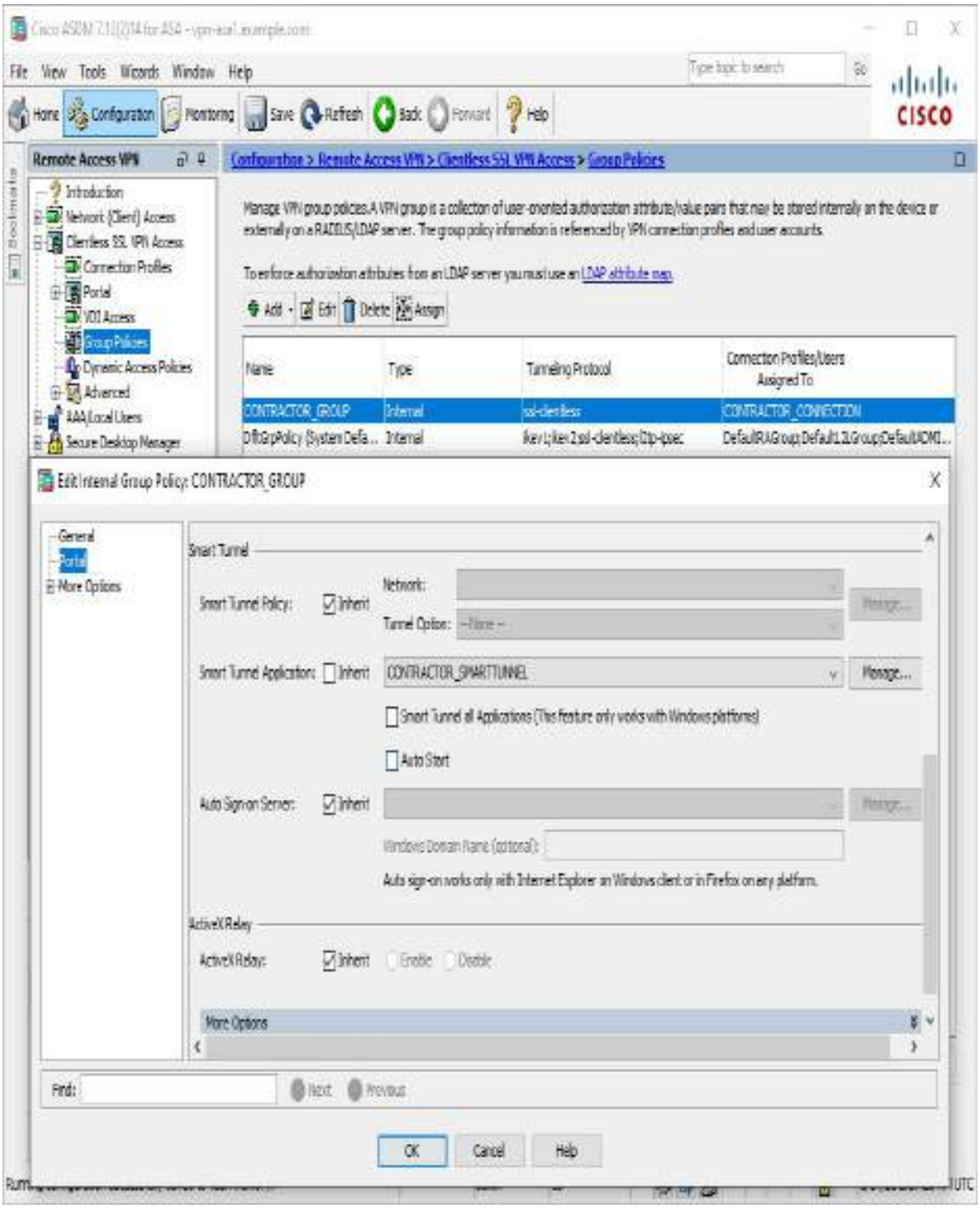


Figure 8-20 Applying a Smart Tunnel List to a Group Policy via ASDM

Example 8-16 Applying a Smart Tunnel List to a Group Policy via the CLI

```
vpn-asa1(config)# group-policy CONTRACTOR_GROUP attributes
vpn-asa1(config-group-policy)# webvpn
vpn-asa1(config-group-webvpn)# smart-tunnel enable
CONTRACTOR_SMARTTUNNEL
```

After the applet is loaded on the client, the user can launch an SSH client, such as putty.exe, to establish a connection to any server that offers SSH service as they would normally do.

Configuring Client/Server Plug-ins

Client/server plug-ins allow administrators to extend the applications supported by a clientless SSLVPN to includes applications such as RDP, VNC, Telnet, and SSH. Through the use of plug-ins, users can access resources that use these applications via the web browser without the use of port forwarding or smart tunnels. Administrators can also enable and control the use of these applications via native protocol support in bookmarks and web ACLs.

Obtaining Plug-ins

Plug-ins for RDP, VNC, Telnet, and SSH are available for download from the Cisco website and are packaged in the .jar file format. Once a plug-in has been imported, the ASA adds the appropriate protocol to the list of protocols available for browsing, bookmarks, and web ACLs. For example, installing the RDP plug-in adds rdp:// as selectable protocol, and installing the VNC plug-in adds vnc:// as a selectable protocol—similar to http:// or cifs://, which are supported without plug-ins.

To import a client/server plug-in via ASDM, follow these steps:

Step 1. Navigate to **Configuration** > **Remote Access VPN** > **Clientless SSLVPN Access** > **Portal** > **Client/server Plug-ins**.

Step 2. Click **Import** to bring up the Import Client-Server Plug-in dialog box.

Step 3. Select the appropriate plug-in name (protocol) from the drop-down

for the plug-in being imported.

Step 4. Click **Browse Local Files** to browse and select the plug-in file from the local computer and click **OK**.

Step 5. Click **Import Now** to import the plug-in and close the Import Client-Server Plug-in dialog box.

Figure 8-21 shows the SSH and Telnet plug-in file ssh-plugin.1.30918.jar being imported from the local computer.

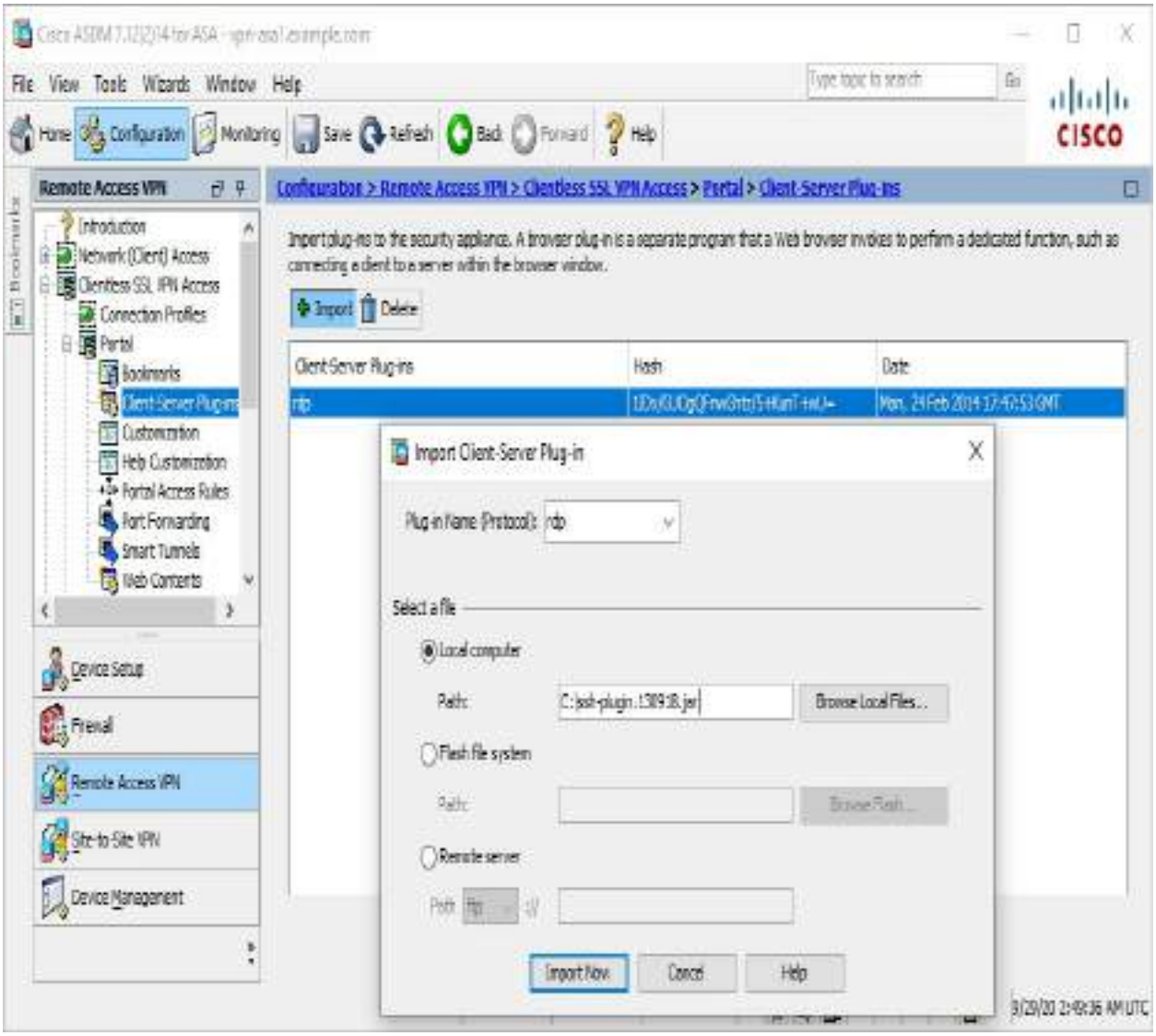


Figure 8-21 Importing Client/Server Plug-ins via ASDM

Note

You must use ASDM to import client/server plug-ins. Importing client/server plug-ins via the CLI is not currently supported.

Summary

This chapter reviewed the differences between clientless SSLVPN and client VPN technologies. It also reviewed the OS, browser, and software requirements for deploying clientless SSLVPN functionality as well as the licensing options available for AnyConnect and the ASA. This chapter presented the steps necessary to configure a basic SSLVPN, including certificate enrollment, group policy creation, connection profile creation, and user authentication. The chapter also explored different features that can be used to enable and control application access, including bookmarks, web ACLs, port forwarding, smart tunnels, and client/server plug-ins.

Now that we have covered clientless VPN, next up we dive into the Cisco flagship client-based VPN using Cisco AnyConnect.

References

ASDM Book 3: Cisco ASA Series VPN ASDM Configuration Guide, 7.14. Retrieved from https://www.cisco.com/c/en/us/td/docs/security/asa/asa914/asdm714/vpn/asdm-714-vpn-config.html

CLI Book 3: Cisco ASA Series VPN CLI Configuration Guide, 9.14. Retrieved from https://www.cisco.com/c/en/us/td/docs/security/asa/asa914/configuration/vpn/asa-914-vpn-config.html

Exam Preparation Tasks

As mentioned in the section “How to Use This Book” in the Introduction, you have a couple of choices for exam preparation: the exercises here,

Chapter 11, “Final Preparation,” and the exam simulation questions in the Pearson Test Prep software online.

Review All Key Topics

Review the most important topics in the chapter, noted with the key topics icon in the outer margin of the page. Table 8-9 lists these key topics and the page number on which each is found.

Table 8-9 Key Topics for Chapter 8

Key Topic Element	Description	Page
Table 8-2	Comparison Between a Clientless SSLVPN and an AnyConnect VPN	
Table 8-3	Supported Features by License Type	
List	SSLVPN support requirements	
List	Basic SSLVPN configuration summary	
Figure 8-7	Attribute Inheritance	
Table 8-5	Group Policy Attributes for Clientless SSLVPNs	
Table 8-6	WebVPN Group Policy Attributes for Clientless SSLVPNs	
Table 8-7	Connection Profile General Attributes for Clientless SSLVPNs	
Table 8-8	Connection Profile WebVPN Attributes for Clientless SSLVPNs	
List	Bookmark Support	
List	Web ACL Support	
List	Smart Tunnel Requirements	

Complete Tables and Lists from Memory

Print a copy of Appendix C, "Memory Tables" (found on the companion website), 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 companion website), includes completed tables and lists to check your work.

Define Key Terms

There are no key terms for this chapter.

Use the Command Reference to Check Your Memory

Table 8-10 lists the important commands from this chapter. To test your memory, cover the right side of the table with a piece of paper, read the description on the left side, and see how much of the command you can remember.

Table 8-10 Command Reference

Task	Command Syntax
Define a CA trustpoint	**crypto ca trustpoint** *<name>*
Request a certificate from a CA	**crypto ca enroll** *<name>* **[noconfirm]**
Import a certificate or pkcs-12 data	**crypto ca import** *<name>* **certificate [nointeractive]**
Configure the WebVPN feature	**webvpn**
Configure a group policy database	**group-policy** *<name>* **internal [from** *<name>***]** OR **group-policy** *<name>* **attributes**
Enter permitted tunneling protocols	**vpn-tunnel-protocol [l2tp-ipsec | ipsec | webvpn]**
Create and manage the database of connection-specific records for IPsec, L2TP/IPsec, and WebVPN connections	**tunnel-group** *<name>* **type** *<type>* OR **tunnel-group** *<name> <general-attributes | ipsec-attributes | ppp-attributes | webvpn-attributes>*
Name of the default group policy	**default-group-policy** *<name>*
Create and manage a group alias for tunnel groups	**group-alias** *<name>* **[enable|disable]**
Configure a list of URL entries for use with the WebVPN feature	**url-list** *<listname> <displayname> <url>*
Enable, disable, or view URL, FTP, and HTTPS filtering	**filter url** *<port>***[-***<port>***]|except** *<lcl_ip> <mask> <frgn_ip> <mask>* **[allow] [proxy-block] [longuri-truncate | longuri-deny] [cgi-truncate]** OR **filter ftp** *<port>***[-***<port>***]|except** *<lcl_ip> <mask> <frgn_ip> <mask>* **[allow] [interact-block]** OR **filter https** *<port>***[-***<port>***]|except** *<lcl_ip> <mask> <frgn_ip> <mask>* **[allow]** OR **filter activex|java** *<port>***[-***<port>***]|except** *<lcl_ip> <mask> <frgn_ip> <mask>*
Configure a list of port forwarding entries for use with the WebVPN feature	**port-forward** *<listname> <localport> <remoteserver> <remoteport> <description>*
Configures smart tunnel features	**smart-tunnel {list** *<program list name> <program display name> <program path>* **[platform** *<platform>***] [***<sha-1 hash>***] | auto-signon** *<host list name>* **[use-domain] [realm** *<realm string>***] [port** *<port num>***] {ip** *<ip address>* **[netmask] | host** *<host mask>***} | network** *<network name>* **{ip** *<ip address>* **[netmask] | host** *<host mask>***}}**
Enable a smart tunnel on a group policy	**smart-tunnel enable** *<program-list>*

Chapter 9. AnyConnect VPNs on the ASA and IOS

This chapter covers the following topics:

- **AnyConnect VPN Review:** This section provides a brief review of AnyConnect VPNs, including the different types of AnyConnect VPNs that are configured in this chapter.
- **AnyConnect VPN Prerequisites on ASA:** This section covers the OS, browsers, and licensing required to implement AnyConnect VPNs on ASA.
- **Basic AnyConnect SSLVPN Configuration on ASA:** This section describes the basics steps needed to configure an AnyConnect SSLVPN on ASA, including certificates, group policy, connection policy, and authentication.
- **Extended AnyConnect SSLVPN Configuration on ASA:** This section describes how to configure split tunneling, name resolution, and filters on ASA.
- **AnyConnect IKEv2 VPN on ASA:** This section covers how to configure IKEv2 AnyConnect on ASA, including the necessary AnyConnect profile.
- **AnyConnect IKEv2 VPN on Routers:** This section covers how to configure an IKEv2 AnyConnect on an IOS router, including certificates, authentication, and the necessary AnyConnect profile.

“I can’t work with idiots. That’s why I work from home and got rid of all of the mirrors.”

—Anthony T. Hincks

This chapter covers the following exam objectives:

- 2.0 Remote access VPNs

- 2.1 Implement AnyConnect IKEv2 VPNs on ASA and routers
- 2.2 Implement AnyConnect SSLVPN on ASA

- 4.0 Secure Communications Architectures
  - 4.2 Describe functional components of FlexVPN, IPsec, and Clientless SSL for remote access VPN solutions
  - 4.4 Recognize VPN technology based on configuration output for remote access VPN solutions
  - 4.5 Describe split tunneling requirements for remote access VPN solutions
  - 4.7 Design remote access VPN solutions
    - 4.7.c Clientless SSL browser and client considerations and requirements

With the clientless SSLVPN deployment complete, we now turn our attention to AnyConnect VPN deployments, which are by far the most common Cisco remote access deployment type today. There are many reasons why a client-based VPN is the preferred option, and we cover everything you need to know for the SVPN along with what is important to know for real-world deployments.

This chapter explores the basic steps to deploy both SSL and IKEv2 AnyConnect VPNs on the ASA as well as IKEv2 AnyConnect VPNs on IOS. It also explores optional, but extremely common, VPN features on the ASA, such as split tunneling, name resolution, and filters. Once you master the concepts in this chapter, you will be ready for the final chapter of this book, which covers troubleshooting remote access VPN technology.

Learning beyond the SVPN concepts:

- AnyConnect VPN Prerequisites on ASA

“Do I Know This Already?” Quiz

The "Do I Know This Already?" quiz enables you to assess whether you should read the entire chapter. If you miss no more than one of these self-assessment questions, you might want to move ahead to the "Exam Preparation Tasks" section of the chapter. Table 9-1 lists the major headings in this chapter and the "Do I Know This Already?" quiz questions related to the material in each of those sections to help you assess your knowledge of these specific areas. The answers to the "Do I Know This Already?" quiz appear in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes."

Table 9-1 "Do I Know This Already?" Foundation Topics Section-to-Question Mapping

Foundation Topics Section	Questions
AnyConnect VPN Review	1
AnyConnect VPN Prerequisites on ASA	2
Basic AnyConnect SSLVPN Configuration on ASA	3–7
Extended AnyConnect SSLVPN Configuration on ASA	8
AnyConnect IKEv2 VPN on ASA	9
AnyConnect IKEv2 VPN on Routers	10, 11

1. Which of the following types of AnyConnect VPNs typically provides better performance than TLS but does not rely on IPsec?

a. IKEv2

b. DTLS

c. L2TP

d. PPTP

2. Administrative privileges on the endpoint are required for which of the following actions?

a. Installation

b. Updates

c. Connecting

d. Disconnecting

3. On the ASA, which command must be configured before you can enable AnyConnect VPN access?

a. anyconnect image

b. vpn-tunnel-protocol

c. group-policy

d. tunnel-group

4. On the ASA, which configuration option automatically maps an AnyConnect connection to a connection profile based on the URL used?

a. Certificate Mapping

b. Connection Alias

c. Group URL

d. Group URL Alias

5. Which VPN protocol uses UDP 443 by default?

a. TLS

b. DTLS

c. IKEv2

d. IKEv2 with NAT-T

6. On the ASA, which of the following is *not* a supported protocol when configuring a AAA server group?

a. Kerberos

b. SAML

c. EAP

d. SDI

7. On the ASA, which of the following is *not* a method of assigning IP addresses to AnyConnect clients?

a. Using a DHCP server

b. Using a local address pool

c. Using a RADIUS server

d. Manually

8. On the ASA, which split tunneling option in ASDM selects traffic by IP address and sends the selected traffic over the tunnel?

a. Tunnel Network List Below

b. Exclude Network Below

c. Dynamic Split Tunneling

d. Manual Split Tunneling

9. On the ASA, when configuring a server list in the AnyConnect profile editor for an IKEv2 VPN, which of the following is not required to be configured?

a. FQDN or IP Address

b. IKE Identity

c. User Group

d. Primary Protocol

10. What is the default identity for AnyConnect?

a. *$AnyConnectClient$*

b. AnyConnectClient

c. *$AnyConnect$*

d. AnyConnect

11. On IOS, which of the following is not supported with self-signed

certificates?

a. AnyConnect IKEv2 VPN

b. Certificate authentication

c. Local user authentication with EAP

d. Third-party IKEv2 VPN

Foundation Topics

Traditional VPN technology leverages a client. The concept simply uses a software client that forces traffic through an encrypted tunnel to a trust resource. Older versions of client-based VPN technology have had huge challenges that modern client-based VPN technology has overcome. One challenge is the requirement of a fat client, meaning software that eats up a lot of processing power on the host system. Another challenge is that the VPN required an on-premises appliance that limited the number of users who could use it. Older VPN technology was limited to certain ports, which most firewall deployments would block by default. All of these challenges led to administrative problems.

The good news regarding modern client-based VPN technology is that many of the challenges encountered by older versions of VPN technology have been solved. The software clients have become much thinner or included with a larger security-related package that includes multiple capabilities beyond VPN. Common ports such as 443 can be used by modern VPN technology and are less likely to be blocked by a firewall. VPN concentrators can exist in different formats, including virtual software run from the cloud. To accommodate large user counts, different load balancing and clustering techniques can be used, allowing for much larger user support. To battle the increase in compute power, encryption can be enhanced, reducing the risk of an attacker compromising the VPN's encryption.

A lot of innovation has occurred, enabling modern VPN technology to offer a lot of value while not impacting normal work operations. VPN technology can support the demands of today's modern workforce, which needs access to specific resources from anywhere in the world. Cisco AnyConnect is the

largest deployed VPN client and a focus topic for the SVPN exam. Let's start off our deeper look at AnyConnect by reviewing what we have covered about AnyConnect in previous chapters.

AnyConnect VPN Review

As discussed in Chapters 7, "Remote Access VPNs," and 8, "Clientless Remote Access SSLVPNs on the ASA," AnyConnect VPNs create a secure, remote access VPN tunnel to an ASA security appliance or IOS router by using the AnyConnect software client. The use of a client enables full network connectivity to remote applications and allows for remote access of any TCP-, UDP-, or ICMP-based applications. As a Cisco VPN administrator, you will have to choose which VPN technology you want to use for each of your VPN projects. To keep things simple regarding preparing for the SVPN, we break down the decision of which version of AnyConnect you can deploy into two options: SSLVPN or IKEv2.

SSLVPN Versus IKEv2

For the purposes of the SVPN 300-730 exam, AnyConnect VPNs on ASA and IOS come in two flavors: SSLVPN and IKEv2. AnyConnect SSLVPNs use Transport Layer Security (TLS) over TCP and Datagram Transport Layer Security (DTLS) over UDP for negotiation and transport. DTLS typically provides better performance than TLS and is the preferred protocol, when allowed. As an alternative to TLS and DTLS, an AnyConnect VPN can also be configured to use IKEv2, which uses IKEv2 for negotiation and IPsec for transport. For the SVPN 300-730 exam, make sure you know what is supported by AnyConnect as well as what is the best option for different situations. For example, DTLS is a better choice than TLS when video and voice support is a requirement.

Note

SSLVPNs are only supported with the AnyConnect client. From ASA Release 9.3.2 and onward, Cisco added interoperability with standards-based, third-party, IKEv2 remote access clients (in addition to AnyConnect). Authentication support includes pre-shared keys, certificates, and user authentication via Extensible Authentication Protocol (EAP).

For the SVPN 300-730 exam, you need to know how to configure three different types of AnyConnect-based VPNs, as described in this chapter:

- AnyConnect SSLVPN terminating on an ASA
- AnyConnect IKEv2 VPN terminating on an ASA
- AnyConnect IKEv2 VPN terminating on an IOS router

Before we get into configuring these three options, we first must review all the prerequisites for running an AnyConnect-based VPN.

AnyConnect SSLVPN VPN Prerequisites on ASA

As with the clientless SSLVPNs covered in Chapter 8, you must meet a number of prerequisites before implementing AnyConnect SSL or IKEv2 VPN on the ASA. This includes having the required licensing, client operating system, and supported browsers. There is overlap between the prerequisites for clientless and client-based VPN technology. To avoid being repetitive, we will summarize the prerequisites in this section and reference Chapter 8 for more detail.

AnyConnect Licenses

Any Cisco VPN deployment must first consider license requirements. The license requirements for SSL and AnyConnect are similar, and the section "Software Licenses" in Chapter 8 covers the different licensing options available for the Cisco ASA and the specific VPN capabilities enabled with each license. For the purposes of the example in this chapter, an AnyConnect Plus, Apex, or VPN Only license will suffice. Review Chapter 8's "Software

Licenses” section to see details about license requirements for an AnyConnect deployment.

Supported Operating Systems

The next prerequisite to consider is whether the host operating system supports AnyConnect. You will not be tested on system support on the SVPN exam, but it is important to validate host system support for a real-world deployment. AnyConnect is supported on the following operating systems:

- Windows 7, 8, 8.1, and 10 (x86, x64, and ARM64)
- macOS 10.13, 10.14, and 10.15
- Linux Red Hat 6, 7, and 8.1
- Ubuntu 16.04 (LTS), 18.04 (LTS), and 20.04 (LTS)
- Android 4.0 and later
- Apple iOS 10.3 and later

Note

For the latest operating system and system requirements information, visit http://www.cisco.com/en/US/products/ps10884/prod_release_notes_list.html . The SVPN 300-730 exam will not test you on the versions of AnyConnect that are and are not supported on a host system, but you will need to know this for a real-world deployment.

Compatible Browsers

Another prerequisite to think about beyond the host operating system is the host’s Internet browser. There are different needs for the browser regarding SSL versus client-based VPN technology. For SSL, the host system browser must support the VPN technology for the VPN to work. For this chapter, we

look to the browser to provide the capability to download AnyConnect to the host. To download AnyConnect from the security appliance, you must use a TLS-enabled browser such as Google Chrome, Microsoft Edge, Firefox, or Safari.

Administrative Privileges

The final prerequisite to consider is whether AnyConnect can be installed and run on the host system. AnyConnect requires administrative rights for the initial installation. The client does not require administrative rights after installation. It is common for administrators to push AnyConnect to host systems or include it as part of a system template to enable it to be installed on systems that the users do not have administrative access rights.

That summarizes the prerequisites you need to consider for an AnyConnect VPN deployment. Prerequisites likely will not be on the SVPN exam, but they are critical for the success of a real-world deployment.

Basic SSLVPN AnyConnect Configuration on ASA

With the prerequisites in place, you are now ready to configure a basic AnyConnect-based remote access VPN. To do so, you need to perform the following steps, which are detailed in the following sections:

Step 1. Install an identity certificate.

Step 2. Load an AnyConnect package.

Step 3. Enable AnyConnect VPN client SSL access.

Step 4. Configure a group policy.

Step 5. Configure an AnyConnect connection profile.

Step 6. Configure user authentication.

Step 7. Configure an address pool.

The examples in this section use the lab environment shown in Figure 9-1, which uses the following software and hardware versions:

- Cisco Adaptive Security Virtual Appliance (ASAv) Release 9.12(4)
- Cisco Adaptive Security Device Manager (ASDM) Release 7.12(2)
- Cisco AnyConnect Security Mobility Client Release 4.8.03052 running on Windows 10

Figure 9-1 Client SSLVPN on ASA Lab Diagram

Step 1: Installing an Identity Certificate

For SSLVPN to function, the ASA must have a digital certificate to identify itself to connecting clients. This can be accomplished with a self-signed certificate as well as with a certificate from a certificate authority (CA). For production deployments, the use of a certificate from a publicly trusted CA is the preferred approach. Chapter 8 covers the steps necessary to obtain and install an identity certificate. To avoid being repetitive, we will skip walking through those steps.

Step 2: Loading an AnyConnect Package

Before enabling AnyConnect access on the interfaces of the security appliance, you must upload and install the AnyConnect package on the security appliance. It is important to know that there are different versions of AnyConnect based on the systems you plan to support. For example, if you plan to support both Windows and Mac, you will need to download two different AnyConnect packages. If a system connects that does not have a version of AnyConnect available, the host will not be offered a package they can install, leading to a failure in providing VPN services. We recommend you evaluate which host systems you plan to support as part of your prerequisite planning to avoid not including an AnyConnect package needed to support your end users.

Loading an AnyConnect Package Using ASDM

To upload and install the AnyConnect client package via ASDM, follow these steps:

Step 1. Navigate to **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **AnyConnect Client Software**.

Step 2. Click **Add** to open the Add AnyConnect Client Image dialog box.

Step 3. Click **Upload** to open the Upload Image dialog box.

Step 4. Click **Browse Local Files** to open the Select dialog box.

Step 5. Select the AnyConnect package file and click **Select**.

Step 6. Click **Upload File** to upload the AnyConnect package to flash.

Step 7. When the upload completes, click **OK** on each of the remaining dialog boxes to add the AnyConnect package to the ASA configuration.

Note

You can download the AnyConnect package from the Cisco website. Look for the product name AnyConnect Secure Mobility Client.

Note

You can upload multiple AnyConnect packages to a security appliance. If multiple files are uploaded, the order in which the files are listed within ASDM is the same order in which they will be presented to a user for download. It is common practice to offer multiple AnyConnect packages.

Caution

Do not rename the AnyConnect package files. The hash verification includes the filename. Changing the filename will cause the hash verification to fail.

Figure 9-2 shows an example of uploading the AnyConnect package anyconnect-win-4.8.03052-webdeploy-k9.pkg from the local C:\ drive to the local flash of the security appliance. When the upload completes, the path of the uploaded file is automatically populated in the Add AnyConnect Client Image dialog box.

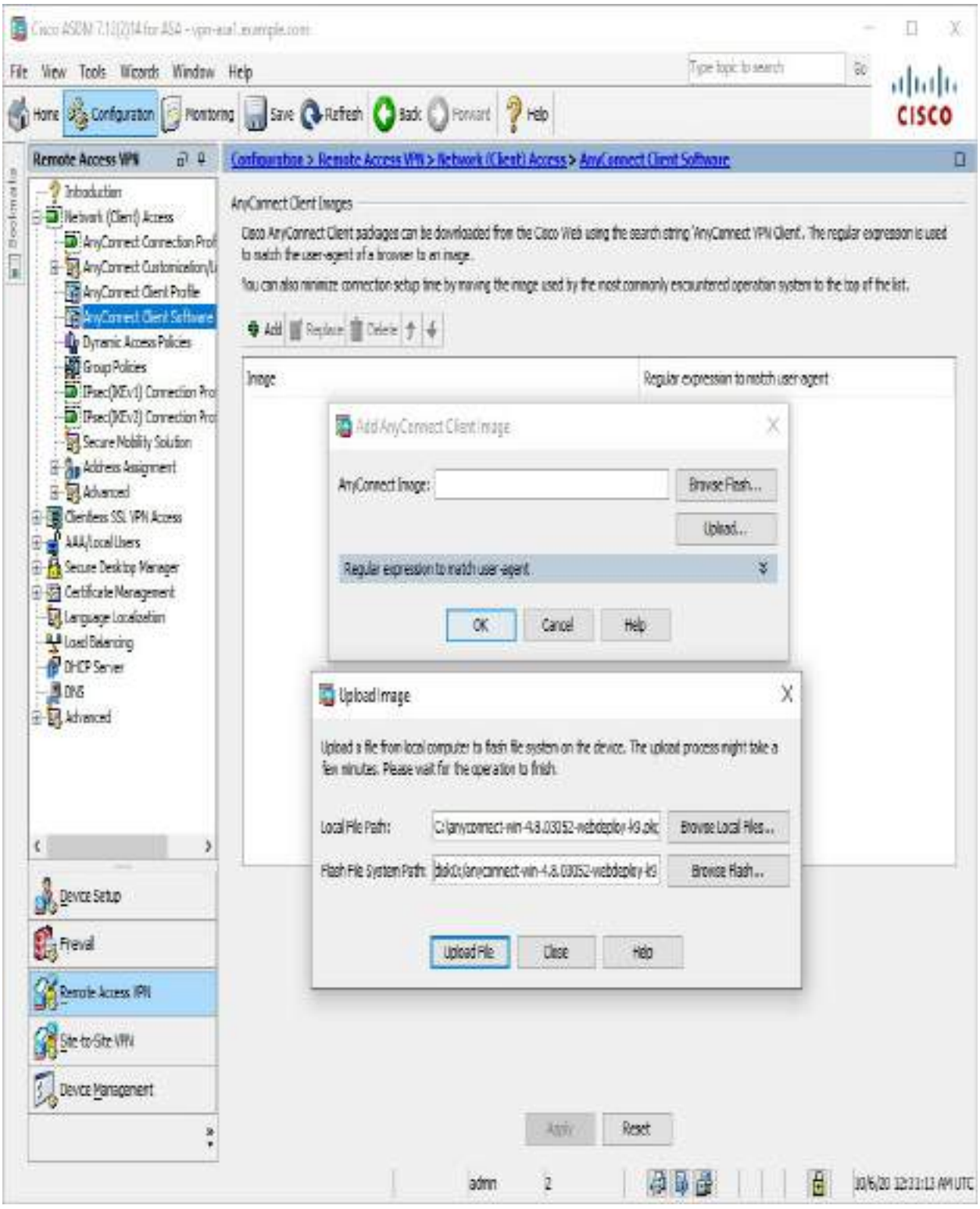


Figure 9-2 Uploading and Adding the AnyConnect Package via ASDM

Loading an AnyConnect Package Using CLI

To upload and install the AnyConnect package via the CLI, first use the **copy** command to upload the AnyConnect package to the security appliance. Then use the **anyconnect image** command from webvpn configuration mode to install the AnyConnect package. Example 9-1 shows an example of uploading the AnyConnect client package anyconnect-win-4.8.03052-webdeploy-k9.pkg via TFTP and then installing the same package on the security appliance. It mirrors the configuration shown in Figure 9-2.

Example 9-1 Uploading and Adding the AnyConnect Package via the CLI

```
vpn-asa1# copy tftp flash

Address or name of remote host [172.20.1.50]?

Source filename [anyconnect-win-4.8.03052-webdeploy-k9.pkg]?

Destination filename [anyconnect-win-4.8.03052-webdeploy-
k9.pkg]?

Accessing tftp://172.20.1.50/anyconnect-win-4.8.03052-
webdeploy-
k9.pkg…!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!
Writing file disk0:/anyconnect-win-4.8.03052-webdeploy-
k9.pkg...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!
72771616 bytes copied in 60.570 secs (1212860 bytes/sec)
vpn-asa1# configure terminal
vpn-asa1(config)# webvpn
vpn-asa1(config-webvpn)# anyconnect image disk0:/ anyconnect-
win-4.8.03052-webdeploy-k9.pkg
```

Step 3: Enabling AnyConnect VPN Client SSL Access

After the AnyConnect package is uploaded to flash, AnyConnect VPN client access must be enabled on the interface that terminates the connection. Keep this in mind as a potential troubleshooting issue if users are not able to connect to the VPN you manage. You might also find test questions that don’t have this interface enabled or errors appear and you must predict

potential problems.

Enabling AnyConnect VPN Using ASDM

To enable AnyConnect VPN client access, follow these steps:

Step 1. Navigate to **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **AnyConnect Connection Profiles**.

Step 2. Check **Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below**.

Step 3. Check **Allow Access** and **Enable DTLS** for the desired interfaces in the SSL Access section of the table.

Figure 9-3 shows an example of enabling AnyConnect connections via TLS and DTLS on the OUTSIDE interface. By default, TLS connections terminate on port 443, and DTLS connections terminate on UDP port 443.

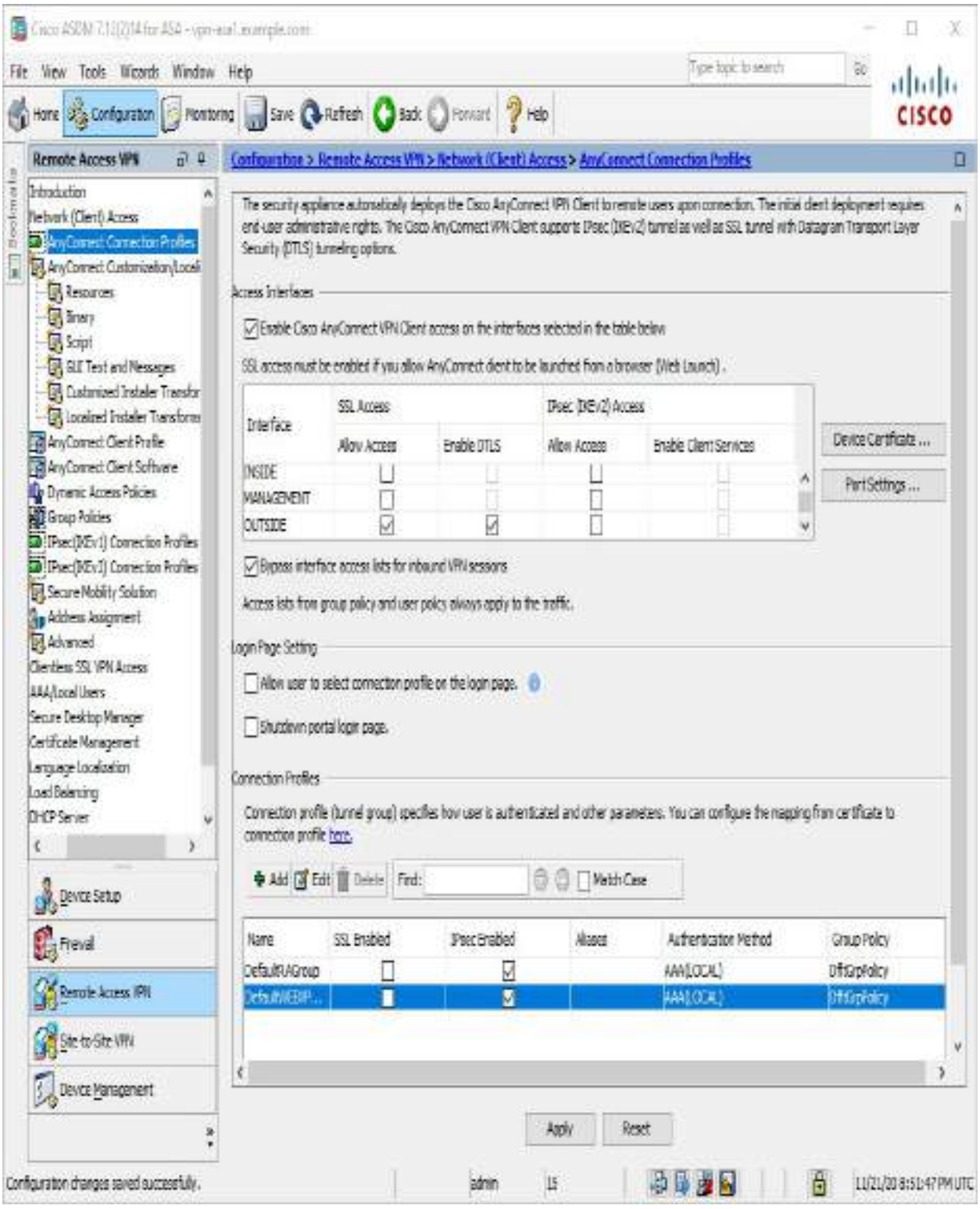


Figure 9-3 Enabling AnyConnect Client Access via ASDM

Enabling AnyConnect VPN Using CLI

To enable AnyConnect VPN client access via the CLI, use the **enable** command in webvpn configuration mode. Example 9-2 shows an example of enabling AnyConnect VPN client access on the OUTSIDE interface and mirrors the configuration shown in Figure 9-3.

Example 9-2 Enabling AnyConnect on an Interface via the CLI

```
vpn-asa1(config)# webvpn
vpn-asa1(config-webvpn)# enable OUTSIDE
INFO: WebVPN and DTLS are enabled on 'OUTSIDE'.
```

Step 4: Configuring a Group Policy

As with clientless SSLVPN, with a client VPN, group policies specify attributes that determine user access and use of the VPN. They can be defined at the user level, connection profile level, or appliance level (default group policy), with each level inheriting any undefined attributes from the parent level. Any attributes that are not defined in the user policy are inherited from the connection profile policy, and any attributes that are not defined in the connection profile policy are inherited from the default group policy.

Note

The default group policy is always named DfltGrpPolicy. It can’t be deleted, but it can be modified.

Note

For a more complete discussion of group policies, review Chapter 8. We recommend you are familiar with group policies as well as the default group policy for the SVPN exam.

Configure Group Policy Using ASDM

To create and modify a group policy via ASDM, follow these steps:

Step 1. Navigate to **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Group Policies**.

Step 2. Click **Add** to open the Add Internal Group Policy dialog box.

Step 3. Specify a name for the group policy.

Step 4. Uncheck **Inherit** next to the attributes you would like to modify and make the desired changes.

Step 5. Click **OK** to create the group policy.

Figure 9-4 shows the simple group policy EMPLOYEE_GROUP with the Tunneling Protocols attribute set to only allow SSLVPN client connections. For users or connections mapped to this group policy, all other connection types will be denied.

Note

The default group policy allows clientless SSLVPN, IPsec IKEv1, IPsec/IKEv2, and L2TP/IPsec connections. A newly created group policy also allows all these connection types unless inheritance is disabled for tunneling protocols and specific connection types are selected.

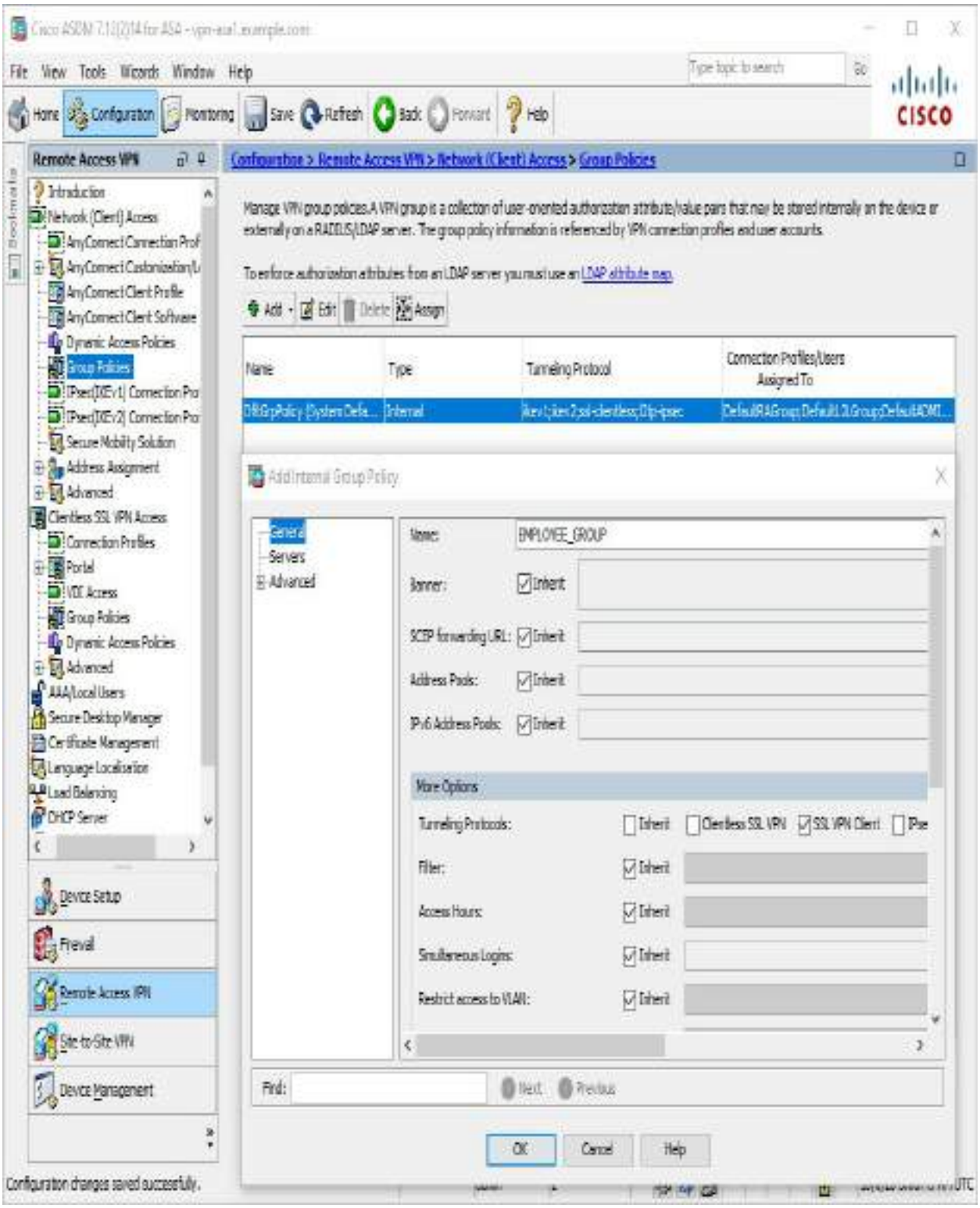


Figure 9-4 Creating and Modifying a Group Policy

Configure Group Policy Using CLI

To create and modify a group policy via the CLI, first use the **group-policy** *name* **internal** command to create the group policy. Then use the **group-policy** *name* **attributes** command to enter the group-policy configuration mode and use the commands from Table 9-2 to modify the desired attribute(s). Example 9-3 shows an example of creating the group policy EMPLOYEE_GROUP, which only allows AnyConnect connections. It is equivalent to the configuration shown in Figure 9-4.

Table 9-2 Group Policy Attributes for AnyConnect VPNs

Command	Description
	Specifies a list of up to six address pools from which to assign addresses
	Specifies a list of backup servers to be used by the remote client
	Indicates banner or welcome text to be displayed on the VPN remote client
	Specifies rules permitting/denying access to specific client types and versions
	Specifies client behavior for protocols for which the client has not received an address
	Specifies firewall requirements for users in this group policy
	Indicates the default domain name given to users of this group
	Specifies a range of IP addresses to indicate to the DHCP server for address assignment
	Specifies the primary and secondary DNS servers
	Specifies the gateway FQDN to be sent down to the client
	Specifies the name of an existing tunnel group that users are required to connect with
	Indicates to use group policy for clients requesting Microsoft DHCP
	Enables IP compression (LZS)
	Allows a client to operate through a NAT device using UDP encapsulation
	Specifies the UDP port to be used by the client for IPsec through NAT
	Specifies a list of up to six IPv6 address pools from which to assign addresses
	Indicates the split tunneling method to be used for IPv6 traffic by the remote client
	Specifies the MSIE Browser Proxy settings for a client system
	Enables/disables storage of the login password on the client system
	Configures periodic authentication
	Enables perfect forward secrecy
	Enables reauthentication of the user on IKE rekey
	Specifies the CA SCEP URL to forward the SCEP messages.
	Configures the CTS security group tag to be used for users in this group policy
	Specifies the client action for smart card removal
	Specifies a list of domains to be resolved through the split tunnel
	Indicates how the client should handle DNS queries when split tunneling is enabled
	Specifies the name of the access list for split tunnel configuration
	Specifies the split tunneling method to be used for IPv4 traffic by the remote client
	Indicates the VLAN onto which VPN traffic for this group will be forwarded
	Specifies the name of a configured time range policy
	Specifies the name of a configured ACL to apply to users
	Specifies the idle timeout period, in minutes
	Specifies the maximum user connection time in minutes, with none indicating unlimited time
	Deletes the old tunnel immediately in the event that simultaneous login connection is preempted
vpn-simultaneous-logins	Specifies the maximum number of simultaneous logins allowed
vpn-tunnel-protocol	Specifies the permitted tunneling protocols
wins-server	Specifies primary and secondary WINS servers

Command	Description
address-pools	Specifies a list of up to six address pools from which to assign addresses
backup-servers	Specifies a list of backup servers to be used by the remote client
banner	Indicates banner or welcome text to be displayed on the VPN remote client
client-access-rule	Specifies rules permitting/denying access to specific client types and versions
client-bypass-protocol	Specifies client behavior for protocols for which the client has not received an address
client-firewall	Specifies firewall requirements for users in this group policy
default-domain	Indicates the default domain name given to users of this group
dhcp-network-scope	Specifies a range of IP addresses to indicate to the DHCP server for address assignment
dns-server	Specifies the primary and secondary DNS servers
gateway-fqdn	Specifies the gateway FQDN to be sent down to the client
group-lock	Specifies the name of an existing tunnel group that users are required to connect with
intercept-dhcp	Indicates to use group policy for clients requesting Microsoft DHCP
ip-comp	Enables IP compression (LZS)
ipsec-udp	Allows a client to operate through a NAT device using UDP encapsulation
ipsec-udp-port	Specifies the UDP port to be used by the client for IPsec through NAT
ipv6-address-pools	Specifies a list of up to six IPv6 address pools from which to assign addresses
ipv6-split-tunnel-policy	Indicates the split tunneling method to be used for IPv6 traffic by the remote client
msie-proxy	Specifies the MSIE Browser Proxy settings for a client system
password-storage	Enables/disables storage of the login password on the client system
periodic-authentication	Configures periodic authentication
pfs	Enables perfect forward secrecy
re-xauth	Enables reauthentication of the user on IKE rekey
scep-forwarding-url	Specifies the CA SCEP URL to forward the SCEP messages.
security-group-tag	Configures the CTS security group tag to be used for users in this group policy
smartcard-removal-disconnect	Specifies the client action for smart card removal
split-dns	Specifies a list of domains to be resolved through the split tunnel
split-tunnel-all-dns	Indicates how the client should handle DNS queries when split tunneling is enabled
split-tunnel-network-list	Specifies the name of the access list for split tunnel configuration
split-tunnel-policy	Specifies the split tunneling method to be used for IPv4 traffic by the remote client
vlan	Indicates the VLAN onto which VPN traffic for this group will be forwarded
vpn-access-hours	Specifies the name of a configured time range policy
vpn-filter	Specifies the name of a configured ACL to apply to users
vpn-idle-timeout	Specifies the idle timeout period, in minutes
vpn-session-timeout	Specifies the maximum user connection time in minutes, with none indicating unlimited time
vpn-simultaneous-login-delete-no-delay	Deletes the old tunnel immediately in the event that simultaneous login connection is preempted
vpn-simultaneous-logins	Specifies the maximum number of simultaneous logins allowed
vpn-tunnel-protocol	Specifies the permitted tunneling protocols
wins-server	Specifies primary and secondary WINS servers

Foundation Topics Section	Questions
AnyConnect VPN Review	1
AnyConnect VPN Prerequisites on ASA	2
Basic AnyConnect SSLVPN Configuration on ASA	3–7
Extended AnyConnect SSLVPN Configuration on ASA	8
AnyConnect IKEv2 VPN on ASA	9
AnyConnect IKEv2 VPN on Routers	10, 11

Command	Description
address-pools	Specifies a list of up to six address pools from which to assign addresses
backup-servers	Specifies a list of backup servers to be used by the remote client
banner	Indicates banner or welcome text to be displayed on the VPN remote client
client-access-rule	Specifies rules permitting/denying access to specific client types and versions
client-bypass-protocol	Specifies client behavior for protocols for which the client has not received an address
client-firewall	Specifies firewall requirements for users in this group policy
default-domain	Indicates the default domain name given to users of this group
dhcp-network-scope	Specifies a range of IP addresses to indicate to the DHCP server for address assignment
dns-server	Specifies the primary and secondary DNS servers
gateway-fqdn	Specifies the gateway FQDN to be sent down to the client
group-lock	Specifies the name of an existing tunnel group that users are required to connect with
intercept-dhcp	Indicates to use group policy for clients requesting Microsoft DHCP
ip-comp	Enables IP compression (LZS)
ipsec-udp	Allows a client to operate through a NAT device using UDP encapsulation
ipsec-udp-port	Specifies the UDP port to be used by the client for IPsec through NAT
ipv6-address-pools	Specifies a list of up to six IPv6 address pools from which to assign addresses
ipv6-split-tunnel-policy	Indicates the split tunneling method to be used for IPv6 traffic by the remote client
msie-proxy	Specifies the MSIE Browser Proxy settings for a client system
password-storage	Enables/disables storage of the login password on the client system
periodic-authentication	Configures periodic authentication
pfs	Enables perfect forward secrecy
re-xauth	Enables reauthentication of the user on IKE rekey
scep-forwarding-url	Specifies the CA SCEP URL to forward the SCEP messages.
security-group-tag	Configures the CTS security group tag to be used for users in this group policy
smartcard-removal-disconnect	Specifies the client action for smart card removal
split-dns	Specifies a list of domains to be resolved through the split tunnel
split-tunnel-all-dns	Indicates how the client should handle DNS queries when split tunneling is enabled
split-tunnel-network-list	Specifies the name of the access list for split tunnel configuration
split-tunnel-policy	Specifies the split tunneling method to be used for IPv4 traffic by the remote client
vlan	Indicates the VLAN onto which VPN traffic for this group will be forwarded
vpn-access-hours	Specifies the name of a configured time range policy
vpn-filter	Specifies the name of a configured ACL to apply to users
vpn-idle-timeout	Specifies the idle timeout period, in minutes
vpn-session-timeout	Specifies the maximum user connection time in minutes, with none indicating unlimited time
vpn-simultaneous-login-delete-no-delay	Deletes the old tunnel immediately in the event that simultaneous login connection is preempted
vpn-simultaneous-logins	Specifies the maximum number of simultaneous logins allowed
vpn-tunnel-protocol	Specifies the permitted tunneling protocols
wins-server	Specifies primary and secondary WINS servers

Example 9-3 Creating an SSLVPN Client Only Group Policy via the CLI

```
vpn-asa1(config)# group-policy EMPLOYEE_GROUP internal
vpn-asa1(config)# group-policy EMPLOYEE_GROUP attributes
vpn-asa1(config-group-policy)# vpn-tunnel-protocol ssl-client
```

Step 5: Configuring an AnyConnect Connection Profile

After a group policy is defined, it must be bound to a connection profile to take effect. All connections made using that connection profile will then use the attributes defined in that group policy to determine user access.

Configuring an AnyConnect Connection Profile Using ASDM

To create an AnyConnect connection profile via ASDM, follow these steps:

Step 1. Navigate to **Configuration** > **Remote Access VPN** > **Network (Client)** > **AnyConnect Connection Profiles**.

Step 2. Click **Add** to open the Add AnyConnect Connection Profile dialog box.

Step 3. Specify the name for the connection policy.

Step 4. Select the desired group policy.

Step 5. Make any other desired changes.

Step 6. Click **OK** to save the group policy and close the Add AnyConnect Connection Profile dialog box.

Figure 9-5 shows the AnyConnect connection profile named EMPLOYEE_CONNECTION, which is configured to use the default group policy EMPLOYEE_GROUP. SSLVPN client connections are enabled via

the Enable SSL VPN Client Protocol check box.

Note

Later in this chapter, you will see how to configure DNS servers and client address assignment. At this point, you can safely ignore any warnings regarding these items.

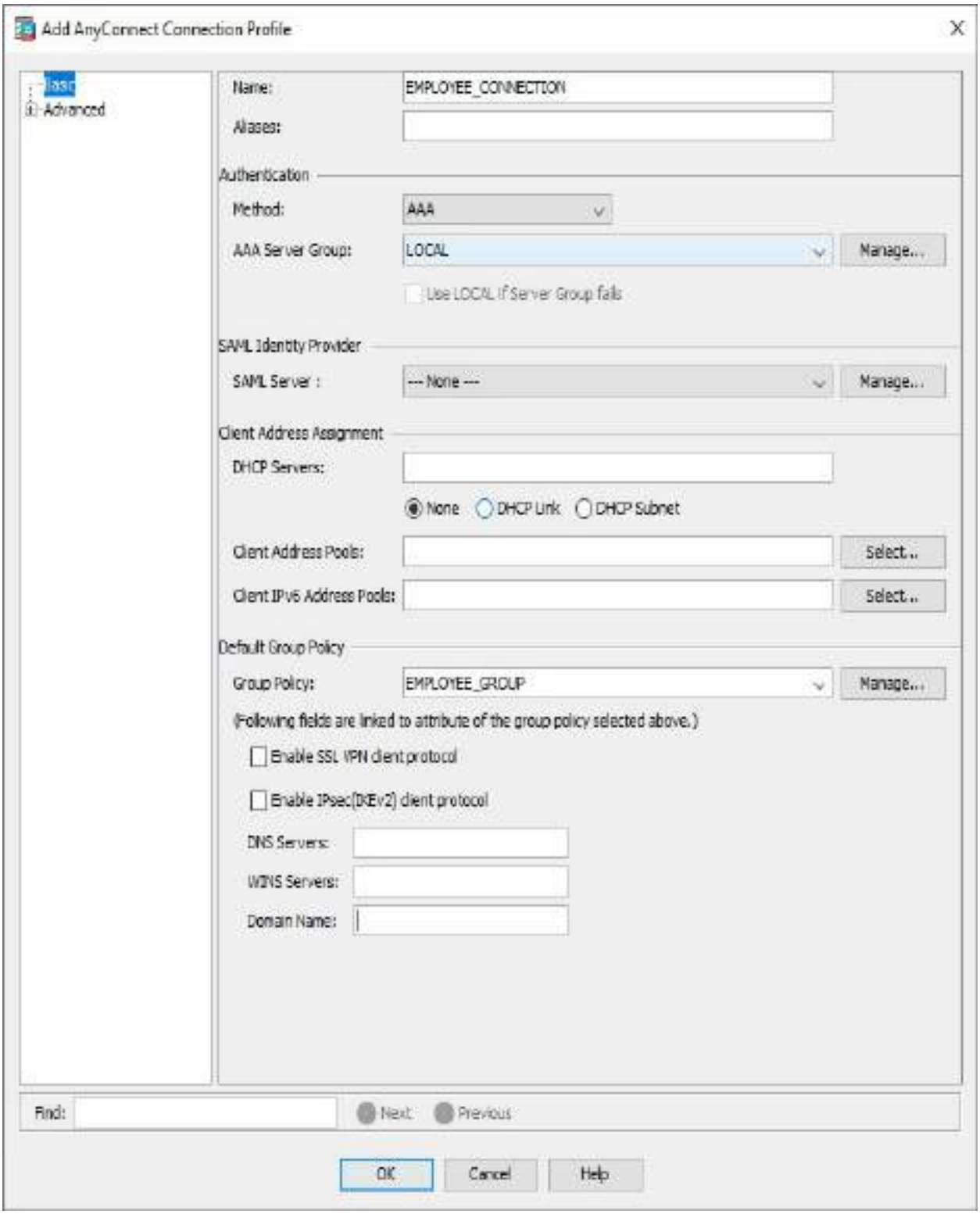


Figure 9-5 Configuring a Connection Profile

Configuring an AnyConnect Connection Profile Using CLI

To configure a connection profile via the CLI, use the **tunnel-group** *name* **type remote-access** command to create the tunnel group. Then use the **tunnel-group** *name* **general-attributes** command to enter the general-attributes configuration mode and configure attributes shown in Table 9-3 or use the **tunnel-group** *name* **webvpn-attributes** command to enter the webvpn-attributes configuration mode and configure attributes shown in Table 9-4. Example 9-4 shows the CLI commands to create a new connection profile and set the default group policy to EMPLOYEE_GROUP. It mirrors the configuration shown in Figure 9-5.

Table 9-3 Connection Profile General Attributes for AnyConnect VPNs

Command	Description
	Sets the authentication method (AAA or certificate).
	Identifies the name of a previously defined customization to apply. Customizations determine the appearance of the windows that the user sees upon login. You configure the customization parameters as part of configuring clientless SSLVPN.
	Identifies the name of the NetBIOS Name Service server (nbns-server) to use for CIFS name resolution.
	Specifies one or more alternative names by which the server can refer to a connection profile. At login, the user selects the group name from a drop-down menu.
	Identifies one or more group URLs. If you configure this attribute, users coming in on a specified URL need not select a group at login. A load balancing deployment that uses group URLs for AnyConnect client connectivity requires each ASA node in the cluster to configure a group URL for the virtual cluster address, as well as a group URL for the node's load balancing public address.
	Identifies the DNS server group that specifies the DNS server name, domain name, name server, number of retries, and timeout values for a DNS server to use for a connection profile.
	Specifies a VPN feature policy if you use the Cisco Secure Desktop Manager to set the Group-Based Policy attribute to Use Failure Group-Policy or Use Success Group-Policy, if Criteria Match.
	Overrides downloading the group policy or username attributes configured for downloading the AnyConnect VPN client to the remote user.
	Enables the display of the RADIUS reject message on the login screen when authentication is rejected.

Command	Description
authentication	Sets the authentication method (AAA or certificate).
customization	Identifies the name of a previously defined customization to apply. Customizations determine the appearance of the windows that the user sees upon login. You configure the customization parameters as part of configuring clientless SSLVPN.
nbns-server	Identifies the name of the NetBIOS Name Service server (nbns-server) to use for CIFS name resolution.
group-alias	Specifies one or more alternative names by which the server can refer to a connection profile. At login, the user selects the group name from a drop-down menu.
group-url	Identifies one or more group URLs. If you configure this attribute, users coming in on a specified URL need not select a group at login. A load balancing deployment that uses group URLs for AnyConnect client connectivity requires each ASA node in the cluster to configure a group URL for the virtual cluster address, as well as a group URL for the node's load balancing public address.
dns-group	Identifies the DNS server group that specifies the DNS server name, domain name, name server, number of retries, and timeout values for a DNS server to use for a connection profile.
hic-fail-group-policy	Specifies a VPN feature policy if you use the Cisco Secure Desktop Manager to set the Group-Based Policy attribute to Use Failure Group-Policy or Use Success Group-Policy, if Criteria Match.
override-svc-download	Overrides downloading the group policy or username attributes configured for downloading the AnyConnect VPN client to the remote user.
radius-reject-message	Enables the display of the RADIUS reject message on the login screen when authentication is rejected.

Command	Description
authentication	Sets the authentication method (AAA or certificate).
customization	Identifies the name of a previously defined customization to apply. Customizations determine the appearance of the windows that the user sees upon login. You configure the customization parameters as part of configuring clientless SSLVPN.
nbns-server	Identifies the name of the NetBIOS Name Service server (nbns-server) to use for CIFS name resolution.
group-alias	Specifies one or more alternative names by which the server can refer to a connection profile. At login, the user selects the group name from a drop-down menu.
group-url	Identifies one or more group URLs. If you configure this attribute, users coming in on a specified URL need not select a group at login. A load balancing deployment that uses group URLs for AnyConnect client connectivity requires each ASA node in the cluster to configure a group URL for the virtual cluster address, as well as a group URL for the node's load balancing public address.
dns-group	Identifies the DNS server group that specifies the DNS server name, domain name, name server, number of retries, and timeout values for a DNS server to use for a connection profile.
hic-fail-group-policy	Specifies a VPN feature policy if you use the Cisco Secure Desktop Manager to set the Group-Based Policy attribute to Use Failure Group-Policy or Use Success Group-Policy, if Criteria Match.
override-svc-download	Overrides downloading the group policy or username attributes configured for downloading the AnyConnect VPN client to the remote user.
radius-reject-message	Enables the display of the RADIUS reject message on the login screen when authentication is rejected.

Table 9-4 Connection Profile General Attributes for AnyConnect VPNs

Command	Description
	Specifies the name of the accounting server group
	Specifies a list of address pools from which to assign addresses
	Indicates the authenticated username that will be associated with the session
	Specifies the authentication server that provides authorization attributes for the session
	Specifies the name of the authentication server group
	Requires users to authorize successfully in order to connect
	Specifies the name of the authorization server group
	Specifies the name of the default group policy
	Specifies the IP address or name of the DHCP server
	Specifies a list of IPv6 address pools from which to assign addresses
	Maps the NAT-assigned IP address to a public IP address
	Enables password management
	Enables SCEP proxy enrollment
	Specifies the name of the secondary authentication server group
	Specifies the DN of the peer certificate used as secondary username for authorization
	Enables strip group processing
	Enables strip realm processing
	Specifies the DN of the peer certificate used as a username for authorization and/or authentication

Command	Description
accounting-server-group	Specifies the name of the accounting server group
address-pool	Specifies a list of address pools from which to assign addresses
authenticated-session-username	Indicates the authenticated username that will be associated with the session
authentication-attr-from-server	Specifies the authentication server that provides authorization attributes for the session
authentication-server-group	Specifies the name of the authentication server group
authorization-required	Requires users to authorize successfully in order to connect
authorization-server-group	Specifies the name of the authorization server group
default-group-policy	Specifies the name of the default group policy
dhcp-server	Specifies the IP address or name of the DHCP server
ipv6-address-pool	Specifies a list of IPv6 address pools from which to assign addresses
nat-assigned-to-public-ip	Maps the NAT-assigned IP address to a public IP address
password-management	Enables password management
scep-enrollment	Enables SCEP proxy enrollment
secondary-authentication-server-group	Specifies the name of the secondary authentication server group
secondary-username-from-certificate	Specifies the DN of the peer certificate used as secondary username for authorization
strip-group	Enables strip group processing
strip-realm	Enables strip realm processing
username-from-certificate	Specifies the DN of the peer certificate used as a username for authorization and/or authentication

Command	Description
accounting-server-group	Specifies the name of the accounting server group
address-pool	Specifies a list of address pools from which to assign addresses
authenticated-session-username	Indicates the authenticated username that will be associated with the session
authentication-attr-from-server	Specifies the authentication server that provides authorization attributes for the session
authentication-server-group	Specifies the name of the authentication server group
authorization-required	Requires users to authorize successfully in order to connect
authorization-server-group	Specifies the name of the authorization server group
default-group-policy	Specifies the name of the default group policy
dhcp-server	Specifies the IP address or name of the DHCP server
ipv6-address-pool	Specifies a list of IPv6 address pools from which to assign addresses
nat-assigned-to-public-ip	Maps the NAT-assigned IP address to a public IP address
password-management	Enables password management
scep-enrollment	Enables SCEP proxy enrollment
secondary-authentication-server-group	Specifies the name of the secondary authentication server group
secondary-username-from-certificate	Specifies the DN of the peer certificate used as secondary username for authorization
strip-group	Enables strip group processing
strip-realm	Enables strip realm processing
username-from-certificate	Specifies the DN of the peer certificate used as a username for authorization and/or authentication

Example 9-4 Configuring a Connection Profile via the CLI

```
vpn-asa1(config)# tunnel-group EMPLOYEE_CONNECTION type remote-
access
vpn-asa1(config)# tunnel-group EMPLOYEE_CONNECTION general-
attributes
vpn-asa1(config-tunnel-general)# default-group-policy
EMPLOYEE_GROUP
```

Configuring a Group URL for an AnyConnect Connection Profile Using ASDM

In Chapter 8, you saw how to configure an alias to allow users to select the proper connection profile. The downside of this approach is that a security appliance may have many connection profiles and require a user to make the proper selection, which can make connecting to the VPN overwhelming for users.

As an alternative, connection profiles support group URLs, which automatically select the associated connection profile without the need for user selection. By defining one or more group URLs and selectively distributing the URLs, administrators can eliminate the need for users to make the proper selection.

To specify a group URL for an AnyConnect connection profile via ASDM, follow these steps:

Step 1. Navigate to **Configuration** > **Remote Access VPN** > **Network (Client)** > **AnyConnect Connection Profiles**.

Step 2. Select the desired connection profile.

Step 3. Click **Edit** to open the Edit AnyConnect Connection Profile dialog box.

Step 4. Navigate to **Advanced** > **Group Alias/Group URL**.

Step 5. In the Group URLs section, click **Add** to open the Add Group URL dialog box.

Step 6. Specify the URL in the form https://<*ASA FQDN*>/<*PATH*>.

Step 7. Click **OK** to add the group URL to the connection profile.

Step 8. Click **OK** to close the Edit AnyConnect Connection Profile dialog box.

Figure 9-6 shows the group URL https://vpn-asa1.example.com/employees defined for the AnyConnect connection profile EMPLOYEE_CONNECTION.

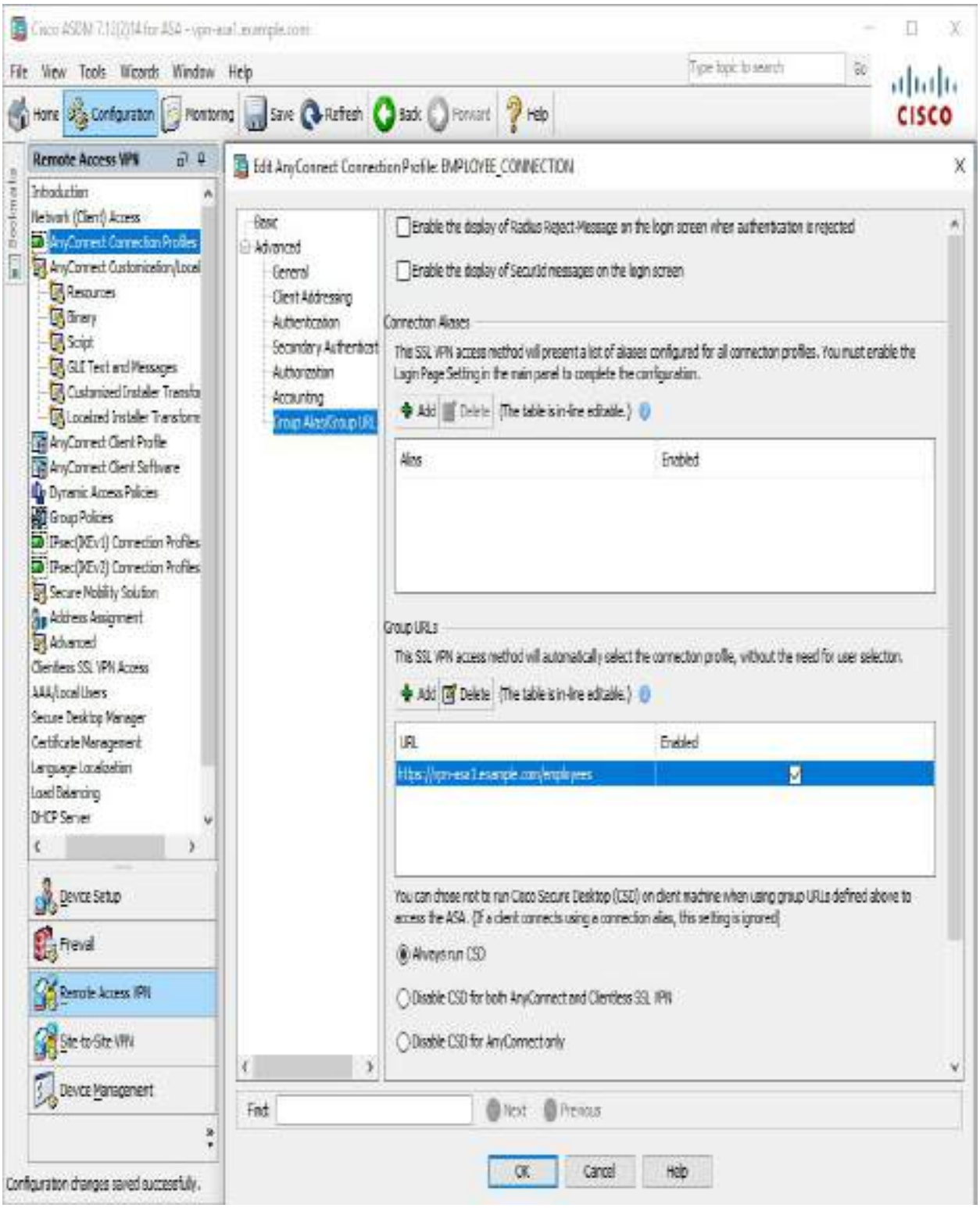


Figure 9-6 Defining an AnyConnect Connection Profile URL via ASDM

Configuring a Group URL for an AnyConnect Connection

Profile Using CLI

To specify a group URL via the CLI, use the **tunnel-group** *name* **webvpn-attributes** command to enter the webvpn configuration mode and then use the **group-url** command to define the desired URL for the connection profile. Example 9-5 shows an example of creating the group URL https://vpn-asa1.example.com/employees for the connection profile EMPLOYEE_CONNECTION. It is equivalent to the configuration shown in Figure 9-6.

Example 9-5 Defining a Connection Profile URL via the CLI

```
vpn-asa1(config)# tunnel-group EMPLOYEE_CONNECTION webvpn-
attributes
vpn-asa1(config-tunnel-webvpn)# group-url https://vpn-
asa1.example.com/employeesenable
```

Step 6: Configuring User Authentication

As discussed in Chapter 8, the Cisco ASA supports a number of differing authentication protocols and databases, including the following:

- RADIUS (Remote Authentication Dial-In User Service)
- NT domain
- Kerberos
- SDI (RSA SecureID)
- LDAP (Lightweight Directory Access Protocol)
- Digital certificates
- Smart cards

- Local database
- SAML 2.0 (Security Assertion Markup Language)

In Chapter 8, we walked you through how to use local user authentication for the VPN configuration example. For labs and small networks local user authentication works, however, real-world deployments will use an external, centralized authentication solution. You must know both so you can stand up labs and deploy in real environments, which is why in this section we cover how to leverage RADIUS for authentication. RADIUS is just one possible option, and the process of leveraging any external authentication solution will use similar steps.

Configuring RADIUS for authentication is a three-step process:

Step 1. Create a AAA server group.

Step 2. Add the RADIUS servers(s) to the AAA server group.

Step 3. Configure a connection profile to use the RADIUS server group.

Creating a AAA Server Group Using ASDM

To create a AAA server group via ASDM, follow these steps:

Step 1. Navigate to **Configuration** > **Remote Access VPN** > **AAA/Local User** > **AAA Server Groups**.

Step 2. Click **Add** in the AAA Server Groups section to open the Add AAA Server Group dialog box.

Step 3. Specify a name for the AAA server group.

Step 4. Select the desired protocol.

Step 5. Click **OK** to create the server group.

Figure 9-7 shows an example of creating the server group RADIUS_GROUP with the protocol RADIUS.

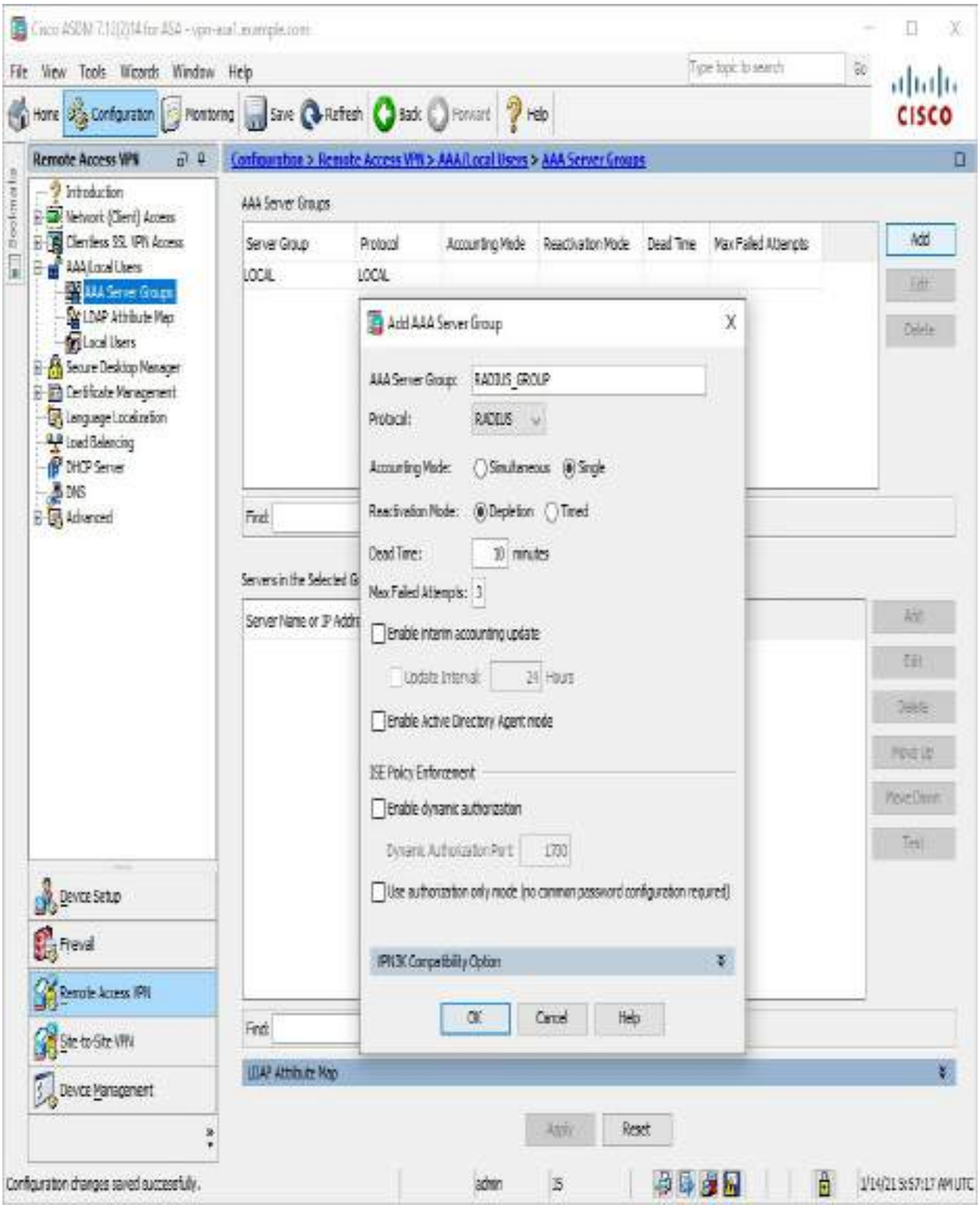


Figure 9-7 Creating a AAA Server Group via ASDM

Creating a AAA Server Group Using CL

To create a AAA server group via the CLI, use the **aaa-server** *name* **protocol** command. Example 9-6 shows an example of creating the AAA server-group RADIUS_GROUP with the protocol RADIUS. It mirrors the configuration shown in Figure 9-7.

Example 9-6 Creating a AAA Server Group via the CLI

```
vpn-asa1(config)# aaa-server RADIUS_GROUP protocol radius
```

Adding RADIUS Servers to a AAA Server Group Using ASDM

After the AAA server group is defined, it is possible to add one or more RADIUS servers to the AAA server group. If more than one RADIUS server is defined, the security appliance uses round-robin to the select the active RADIUS server. When the security appliance finds a RADIUS server that is reachable, it continues to use that RADIUS server for all requests until a failure occurs. Upon failure, the security appliance selects the next available RADIUS server.

To add a RADIUS server to a AAA server group via ASDM, follow these steps:

Step 1. Select the desired server group.

Step 2. In the Servers in the Selected Group section, click **Add** to open the Add AAA Server dialog box.

Step 3. Select the interface.

Step 4. Specify the server name or IP address.

Step 5. Specify the server secret key.

Step 6. Click **OK** to add the RADIUS server.

Figure 9-8 shows an example of adding the RADIUS server 171.20.1.50 to the server group RADIUS_GROUP. Traffic to the RADIUS server will be initiated through the INSIDE interface and will use the RADIUS secret key cisco123 (obfuscated).

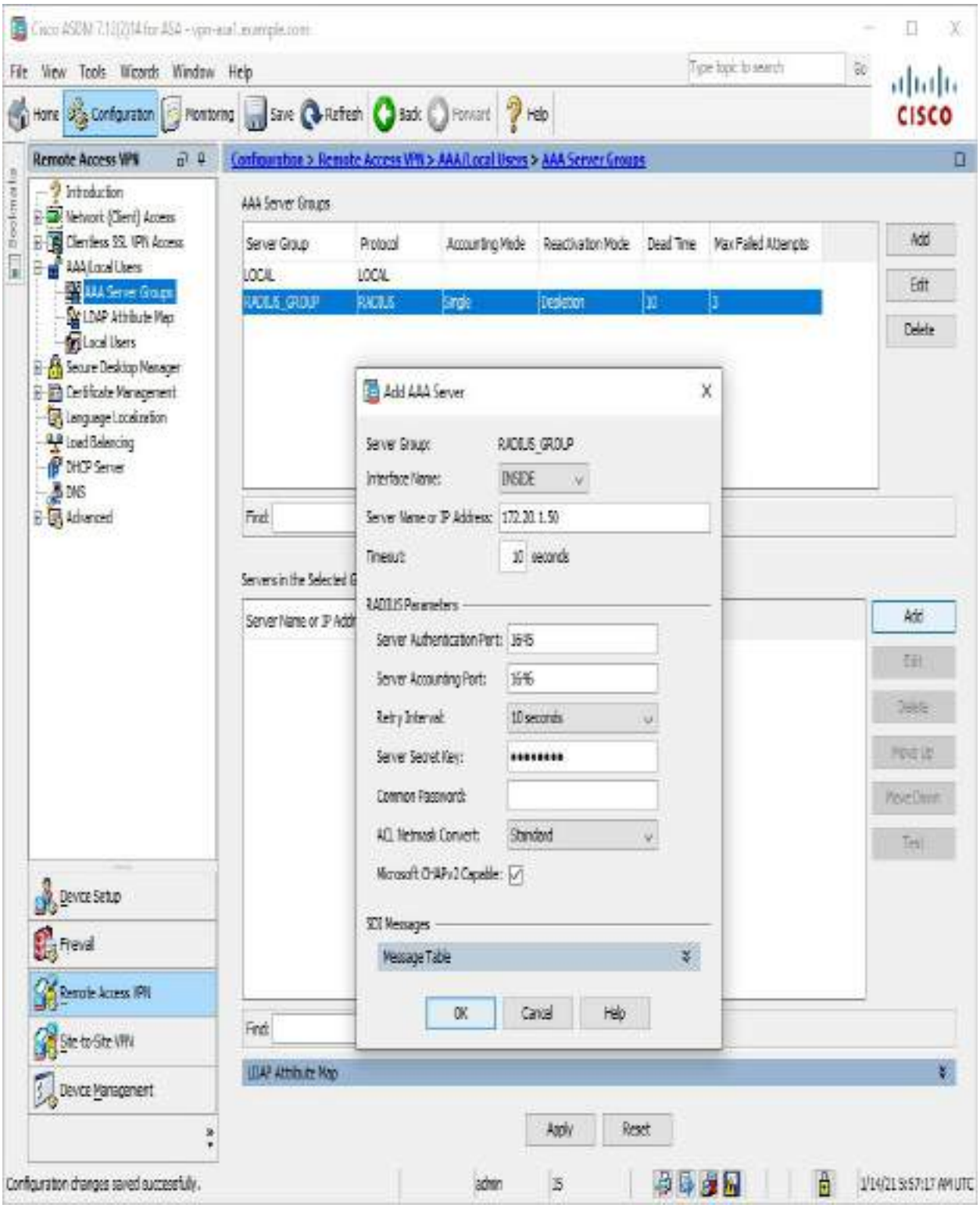


Figure 9-8 Adding a RADIUS Server to a Server Group via ASDM

Adding RADIUS Servers to a AAA Server Group Using CLI

To add a RADIUS server to a server via the CLI, use the **aaa-server** *name* **(***interface***) host** *x.x.x.x* command. Example 9-7 shows an example of adding the RADIUS server 172.20.1.50 on the INSIDE interface to the server group RADIUS_GROUP. It mirrors the configuration shown in Figure 9-8.

Example 9-7 Configuring RADIUS Authentication via the CLI

```
vpn-asa1(config-aaa-server-group)# aaa-server RADIUS_GROUP
(INSIDE) host 172.20.1.50
vpn-asa1(config-aaa-server-host)# key cisco123
```

Configuring a Connection Profile to Use the RADIUS Server Group Using ASDM

The final step after defining the authentication servers is to configure the connection profile to use the RADIUS group for authentication.

To configure a connection profile to use RADIUS for authentication via ASDM, follow these steps:

Step 1. Navigate to **Configuration** > **Network (Client) Access** > **AnyConnect Connection Profiles**.

Step 2. Select the desired connection profile.

Step 3. Click **Edit** to open the Edit AnyConnect Connection Profile dialog box.

Step 4. Select the desired AAA server group.

Step 5. Click **OK** to close the Edit AnyConnect Connection Profile dialog box.

Figure 9-9 shows an example of configuring the connection profile EMPLOYEE_CONNECTION to use the AAA server group RADIUS_GROUP for authentication.

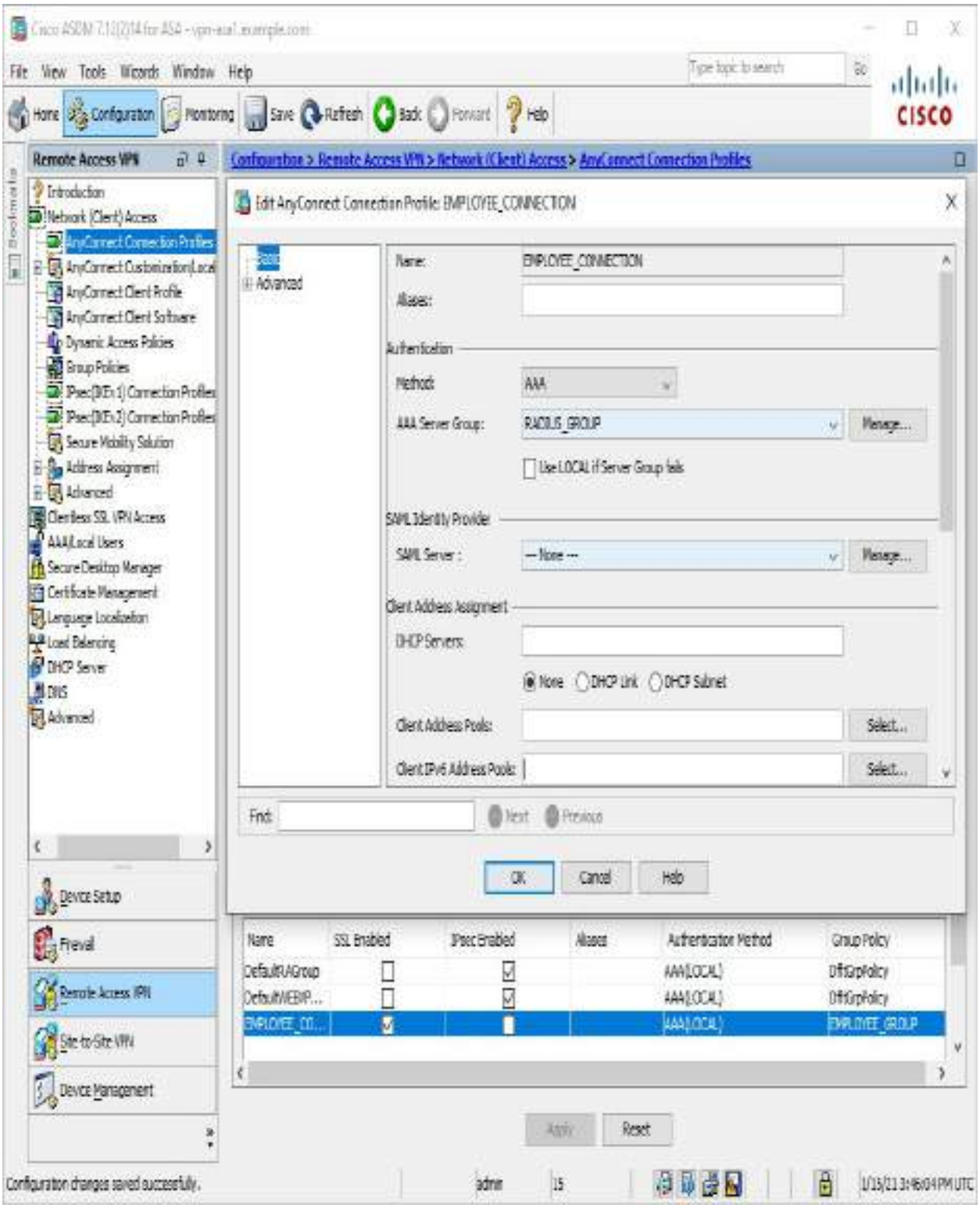


Figure 9-9 Configuring a Connection Profile to Use the AAA Server Group for Authentication via ASDM

Configuring a Connection Profile to Use the RADIUS Server Group Using CLI

To configure the connection profile to use the AAA server group via the CLI, use the **authentication-server-group** command in group policy configuration mode. Example 9-8 shows an example of configuring the connection profile EMPLOYEE_CONNECTION to use the server group RADIUS_GROUP for authentication. It mirrors the configuration shown in Figure 9-9.

Example 9-8 Configuring RADIUS Authentication via the CLI

```
vpn-asa1(config)# tunnel-group EMPLOYEE_CONNECTION general-
attributes
vpn-asa1(config-tunnel-general)# authentication-server-group
RADIUS_GROUP
```

Step 7: Defining an Address Pool

When a connection is made to the VPN, AnyConnect receives an IP address to assign to the VPN interface. This IP address is used as the source IP address when accessing protected resources on the other side of the VPN tunnel.

The Cisco ASA supports three methods of assigning IP addresses:

- Local address pools
- DHCP server
- RADIUS server

If multiple methods for IP address assignment are configured, the Cisco ASA uses the IP address obtained through RADIUS. If no IP address is obtained through RADIUS and DHCP is configured, the Cisco ASA attempts to obtain an IP address from the DHCP server. If IP assignment through DHCP fails or is not configured, the Cisco ASA attempts to obtain an IP address from the local address pool.

The method organizations most commonly use to assign IP addresses is through a local address pool. Assigning IP addresses through a local address pool is a two-step process:

Step 1. Create an address pool.

Step 2. Associate the address pool to a policy group (for example, a group policy).

Creating an Address Pool Using ASDM

To create an address pool via ASDM, follow these steps:

Step 1. Navigate to **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Address Assignment** > **Address Pools**.

Step 2. Click **Add** to open the Add IPv4 Pool dialog box.

Step 3. Specify a name for the address pool.

Step 4. Specify a starting IP address for the address pool.

Step 5. Specify an ending IP address for the address pool.

Step 6. Select a subnet mask for the address pool.

Step 7. Click **OK** to add the address pool.

Figure 9-10 shows an example of creating the new address pool EMPLOYEE_POOL. The first IP address assigned to clients will be 172.16.30.1, and the last IP address assigned to clients will be 172.16.30.254. All clients will receive the subnet mask 255.255.255.0.

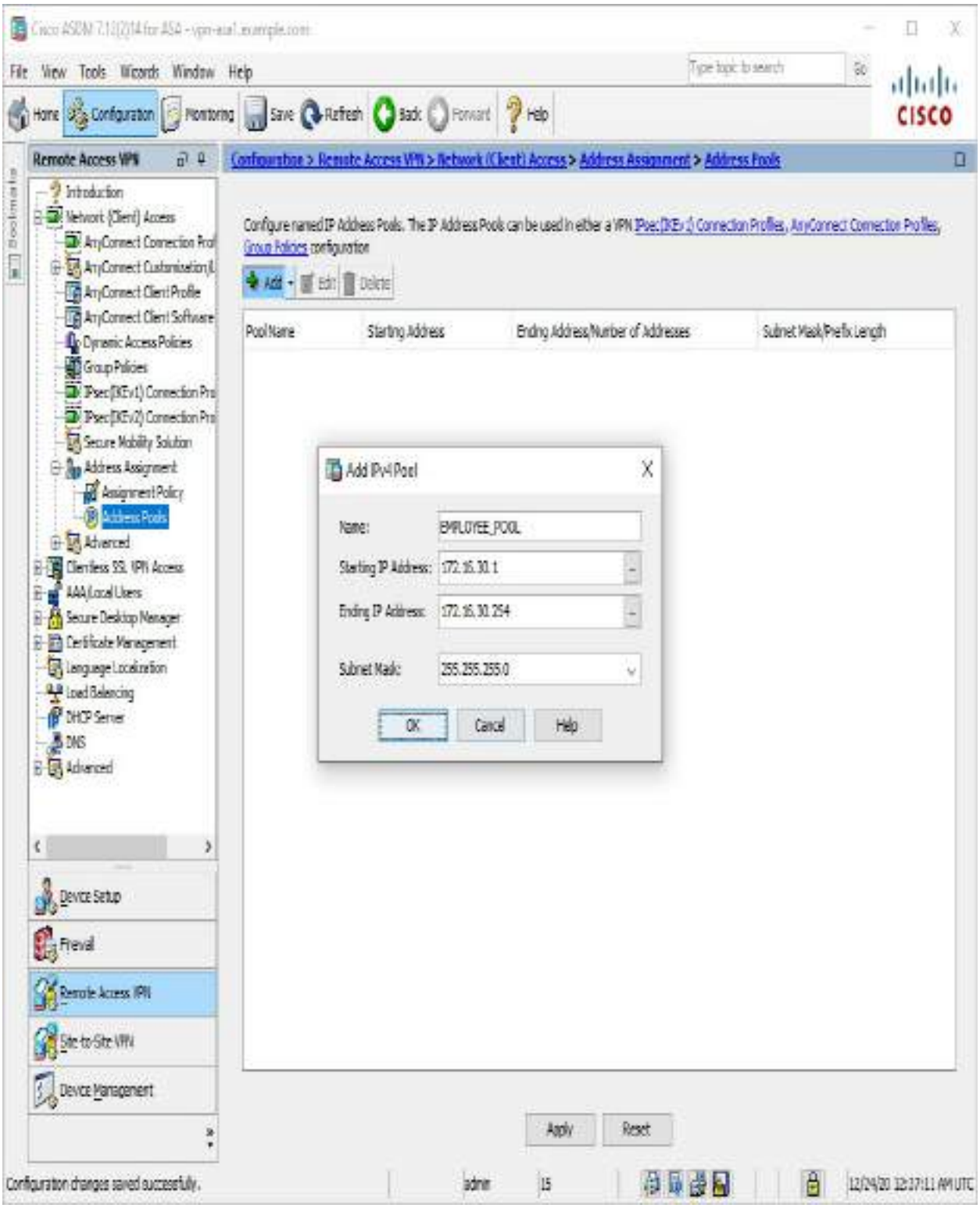


Figure 9-10 Creating an Address Pool via ASDM

Creating an Address Pool Using CLI

To create an address pool via the CLI, use the **ip local pool** command. Example 9-9 shows an example of creating the new address pool EMPLOYEE_POOL. The first IP address assigned to clients will be 172.16.30.1, and the last IP address assigned to clients will be 172.16.30.254. All clients will receive the subnet mask 255.255.255.0. It mirrors the configuration shown in Figure 9-10.

Example 9-9 Creating an Address Pool via the CLI

```
vpn-asa1(config)# ip local pool EMPLOYEE_POOL 172.16.30.1-
172.16.30.254 mask 255.255.255.0
```

Applying the Address Pool to a Group Policy Using ASDM

To apply an address pool to a group policy via ASDM, follow these steps:

Step 1. Navigate to **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Group Policies**.

Step 2. Select the desired group policy, and click **Edit** to open the Edit Internal Group Policy dialog box.

Step 3. Uncheck the **Inherit** check box for Address Pools.

Step 4. Click **Select** to open the Select Address Pools dialog box.

Step 5. Select the desired address pool(s) and click **Assign**.

Step 6. Click **OK** to add the address pools to the group policy.

Step 7. Click **OK** to close the Edit Internal Group Policy dialog box.

Figure 9-11 shows an example of associating the address pool EMPLOYEE_POOL with the group policy EMPLOYEE_GROUP.

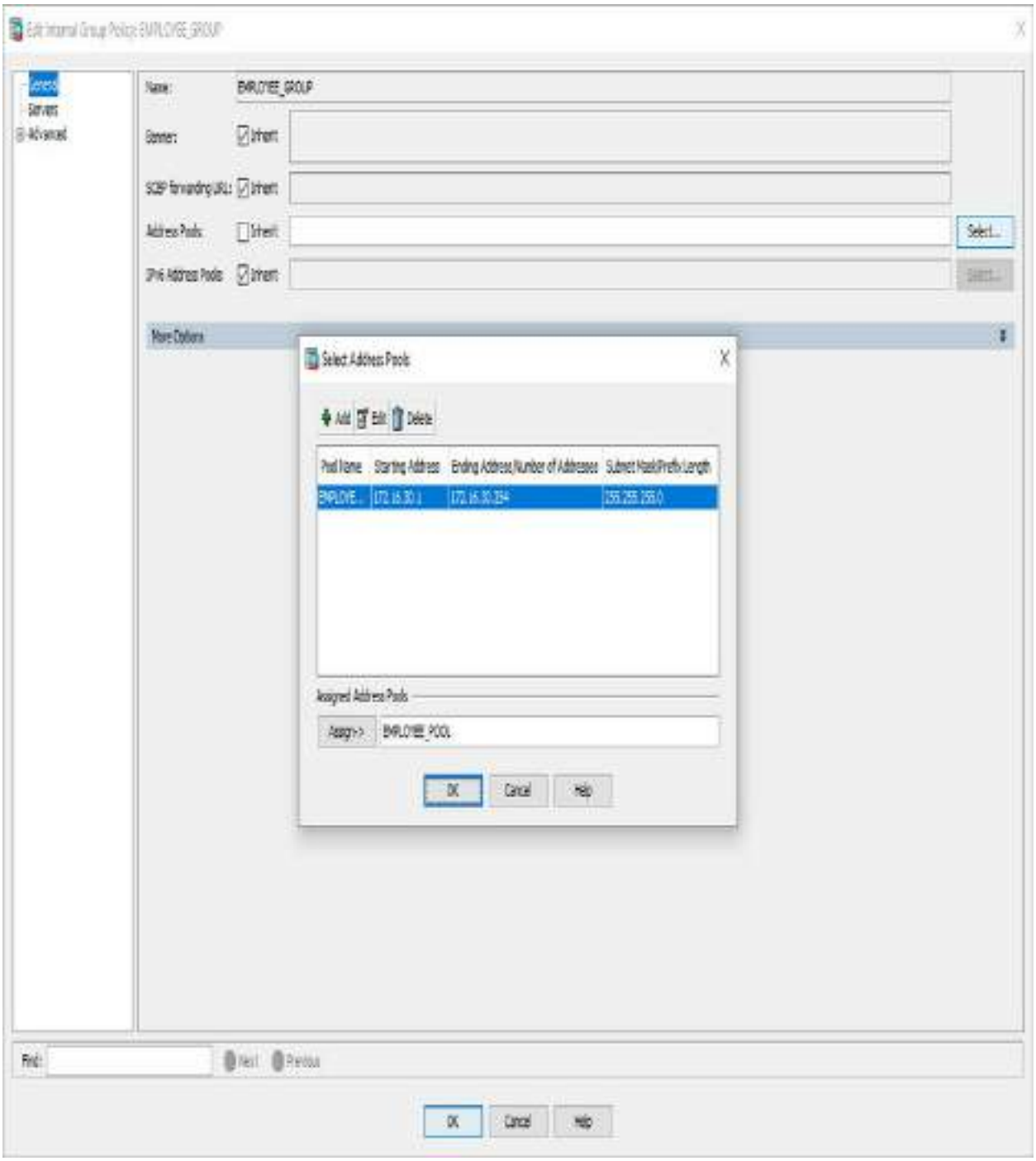


Figure 9-11 Associating an Address Pool to a Group Policy via ASDM

Applying the Address Pool to a Group Policy Using CLI

To associate an address pool to a group policy via the CLI, use the **address pools value** command in group-policy configuration mode. Example 9-10

shows an example of associating the address pool EMPLOYEE_POOL with the group policy EMPLOYEE_GROUP and mirrors the configuration shown in Figure 9-11.

Example 9-10 Associating an Address Pool to a Group Policy via the CLI

```
vpn-asa1(config)# group-policy EMPLOYEE_GROUP attributes
vpn-asa1(config-group-policy)# address-pools value
EMPLOYEE_POOL
```

AnyConnect Installation

Earlier in this chapter we covered prerequisites for deploying an AnyConnect VPN solution. One of those is having the ability to deploy AnyConnect, meaning host rights and support for the AnyConnect software. Another prerequisite is considering how to deliver the package to the end users. This includes considerations for the types of user systems. Remember that it is common practice to have multiple versions of AnyConnect available, such as one for Windows and another for Mac-based hosts. Know that if a host attempts to connect and a version of AnyConnect they can support is not available, it will cause a failure in delivering your VPN solution.

Once you meet these prerequisites, you must choose how to give the end users the AnyConnect software. There are two methods to install AnyConnect on a user's computer that is running a desktop operating system:

- **Predeployment:** New installations and upgrades are done either by the end user or by using an enterprise software management system (SMS).
- **Web deployment:** The user connects to the clientless portal on the Cisco ASA and selects the option to download AnyConnect. The browser downloads the AnyConnect Downloader. The AnyConnect Downloader downloads the client, installs the client, and starts a VPN connection. This option requires that the user have local administrative rights to the workstation.

A user using a mobile device (iPhone, iPad, or Android device) can download AnyConnect from the Apple App Store for iOS devices or Google

Play for Android devices.

It is important to know that users who download a generic version of AnyConnect might still need to download the version of AnyConnect that is pushed to their systems before the VPN can work. We highly recommend you test different user types similar to what you expect to support before going live with your VPN deployment.

Connecting from the AnyConnect Client

When the basic AnyConnect client configuration is complete, it is possible to establish a connection to the VPN headend. After installing the VPN client, either via a predeployment package or web deployment, the user can enter the URL to connect. For the earlier example, the user would browse to https://vpn-asa1.example.com/employees to authenticate and download the web deployment package. Once AnyConnect is installed, the user would enter the same URL in the AnyConnect connection bar.

That is a summary of how to deliver a generic AnyConnect SSL VPN deployment. Next, let’s look at other common features that are deployed along with an AnyConnect SSL VPN deployment.

Extended AnyConnect SSLVPN Configuration on ASA

After setting up basic full tunnel client parameters, you can configure some of the optional, but very common, features to enhance the SSLVPN implementation in your network. These important features are discussed in the following sections:

- DNS and WINS assignment
- Split tunneling
- Traffic filters

It is important to also know these features for the SVPN exam. You may find

questions regarding how to deploy and troubleshoot these key features.

Configuring DNS and WINS Using ASDM

While an AnyConnect VPN can be technically functional without DNS or WINS configured, it wouldn't be very user friendly. Users and applications are accustomed to name resolution via DNS and WINS being ubiquities, even in VPNs. For AnyConnect, you can assign internal DNS and WINS server IP addresses so that after their SSL tunnel is established, users can browse and access internal sites using the names they are already accustomed to using.

It is also common practice to use a security-based DNS tool such as Cisco Umbrella as the DNS provider, allowing for additional security capabilities to be enforced post VPN connection. This same concept is one possible option for delivering cloud-based security coined by the industry as Secure Access Service Edge (SASE), meaning forcing VPN traffic through a cloud delivery security structure. If you have never heard about SASE, we highly recommend researching this topic as many industry experts such as Gartner have stated that SASE is the future of cybersecurity architectures. Also know that SASE will not be on the SVPN exam today but could appear in future versions of the exam.

To configure DNS and WINS via ASDM, follow these steps:

Step 1. Navigate to **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Group Policies**.

Step 2. Select the desired group policy and click **Edit** to open the Edit Internal Group Policy dialog box.

Step 3. Navigate to **Servers**.

Step 4. Specify the DNS servers, separating entries with commas.

Step 5. If desired, specify the WINS servers, separating entries with commas.

Step 6. Expand **More Options**.

Step 7. If desired, specify the default domain to push to clients.

Step 8. Click **OK** to close the Edit Internal Group Policy dialog box.

Figure 9-12 shows the group policy EMPLOYEE_GROUP with the DNS servers 172.20.1.50 and 172.20.1.51 with a default domain example.com.

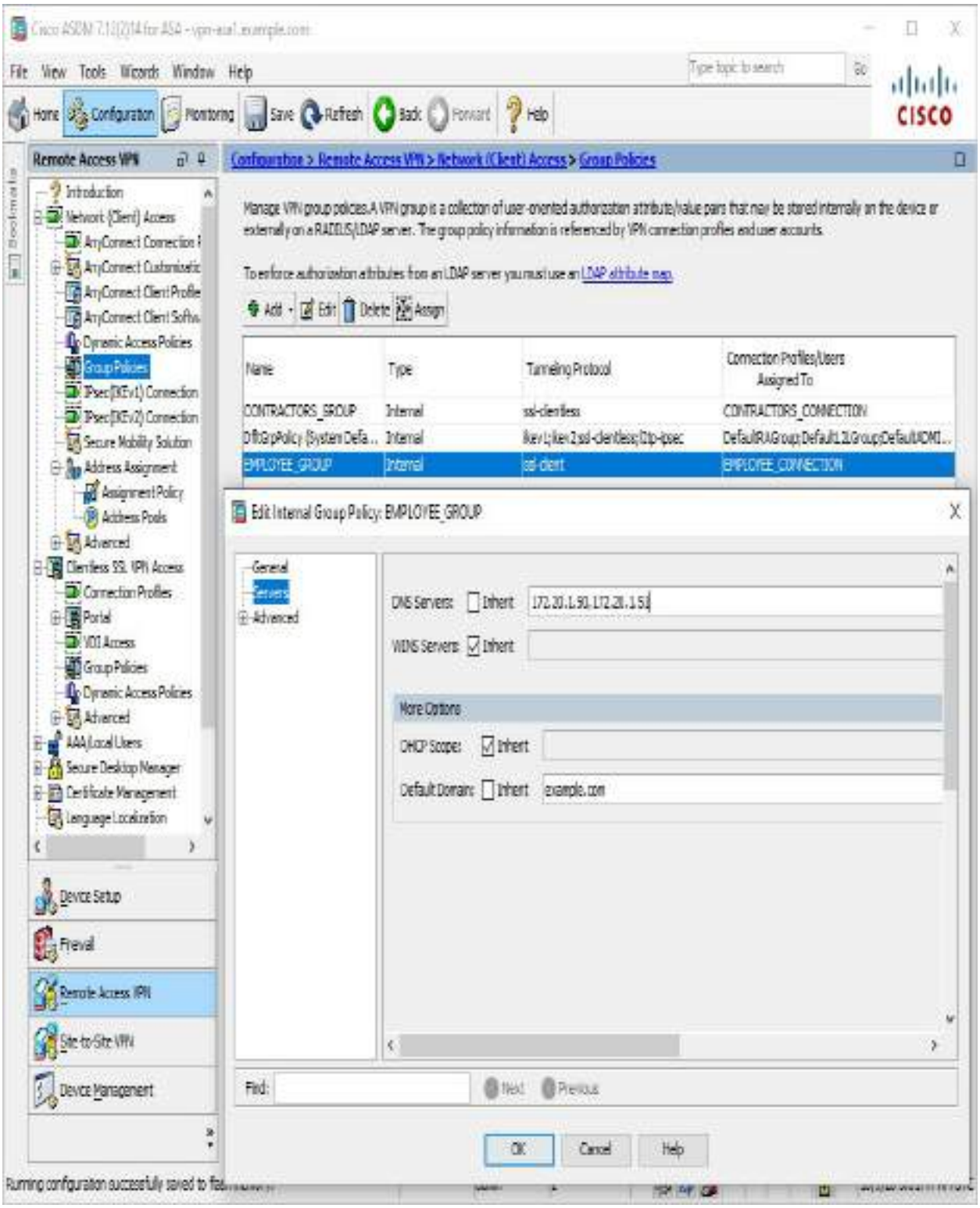


Figure 9-12 Configuring DNS via ASDM

Configuring DNS and WINS Using CLI

To configure DNS via the CLI, use the **dns-server value** command to specify the DNS servers for clients, the **win-server value** command to specify the WINS, and the **default-domain value** command to set the default domain. All commands are entered in group-policy configuration mode. Example 9-11 shows the CLI equivalent of Figure 9-12.

Example 9-11 Configuring Name Resolution via the CLI

```
vpn-asa1(config)# group-policy EMPLOYEE_GROUP attributes
vpn-asa1(config-group-policy)# dns-server value 172.20.1.50
172.20.1.51
vpn-asa1(config-group-policy)# default-domain value example.com
```

Configuring Split Tunneling Using ASDM

After a VPN tunnel is established, the default behavior of AnyConnect is to direct all traffic through the VPN tunnel (encrypted), including traffic destined for the Internet. For some organizations, this can be desirable as they have sophisticated Internet monitoring and filtering technology that they want all users to egress through, regardless of whether they are in the office or remote. Other organizations may prefer users only send specific traffic through the VPN.

Note

During the COVID-19 pandemic, some organizations ran into problems in which their VPN solution was slowing down the network for end users. This occurred when everybody started working from home and the VPN solution was stretched to its maximum level support. To reduce the throughput, organizations were forced to use split tunneling to remove nonbusiness-related traffic. However, this put those organizations at risk of attack because nonbusiness-related traffic was no longer protected by their security investments. Split tunneling can be a temporary fix to this problem, but industry best practice is to either properly size your VPN solution and network for expected throughput or include cloud-based security such as SASE to ensure that all traffic is protected.

To accomplish this, the Cisco ASA and AnyConnect support two types of split tunneling:

- **Split tunneling:** This type of tunneling uses an access list to define which subnets should or should not be sent across the tunnel. If the option Exclude Network Below is selected, subnets contained within the ACL are sent in plaintext and are not sent across the tunnel. If the option Tunnel Network List Below is selected, only the subnets contained within the ACL are sent across the tunnel.
- **Dynamic split tunneling:** This type of tunneling expands on split tunneling by allowing traffic to be included or excluded from the VPN tunnel, based on DNS names rather than IP addresses or subnets. For example, office.com can be configured for exclusion from the tunnel regardless of the many IP addresses office.com may resolve to.

Note

For more information on dynamic split tunneling, see the "About Dynamic Split Tunneling" section of the Cisco AnyConnect Secure Mobility Client Administrator Guide.

To configure split tunneling via ASDM, follow these steps:

Step 1. Navigate to **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Group Policies**.

Step 2. Select the desired group policy, and click **Edit** to open the Edit Internal Group Policy dialog box.

Step 3. Navigate to **Advanced** > **Split Tunneling**.

Step 4. Uncheck the **Inherit** check box for Policy.

Step 5. Select the desired policy.

Step 6. Uncheck the **Inherit** check box for Network List.

Step 7. Click **Manage** to open the ACL Manager dialog box.

Step 8. Navigate to **Add** > **Add ACL** to open the Add ACL dialog box.

Step 9. Specify an ACL name.

Step 10. Click **OK** to close the Add ACL dialog box.

Step 11. Select the ACL that you just created.

Step 12. Navigate to **Add** > **Add ACE** to open the Add ACE dialog box.

Step 13. Specify the subnet address.

Step 14. Click **OK** to close the Add ACE dialog box.

Figure 9-13 shows the split tunneling policy for EMPLOYEE_GROUP. This policy is set to only tunnel the subnets in SPLIT_TUNNEL_LIST, and the ACE 172.20.1.0/24 is in the process of being added to SPLIT_TUNNEL_LIST.

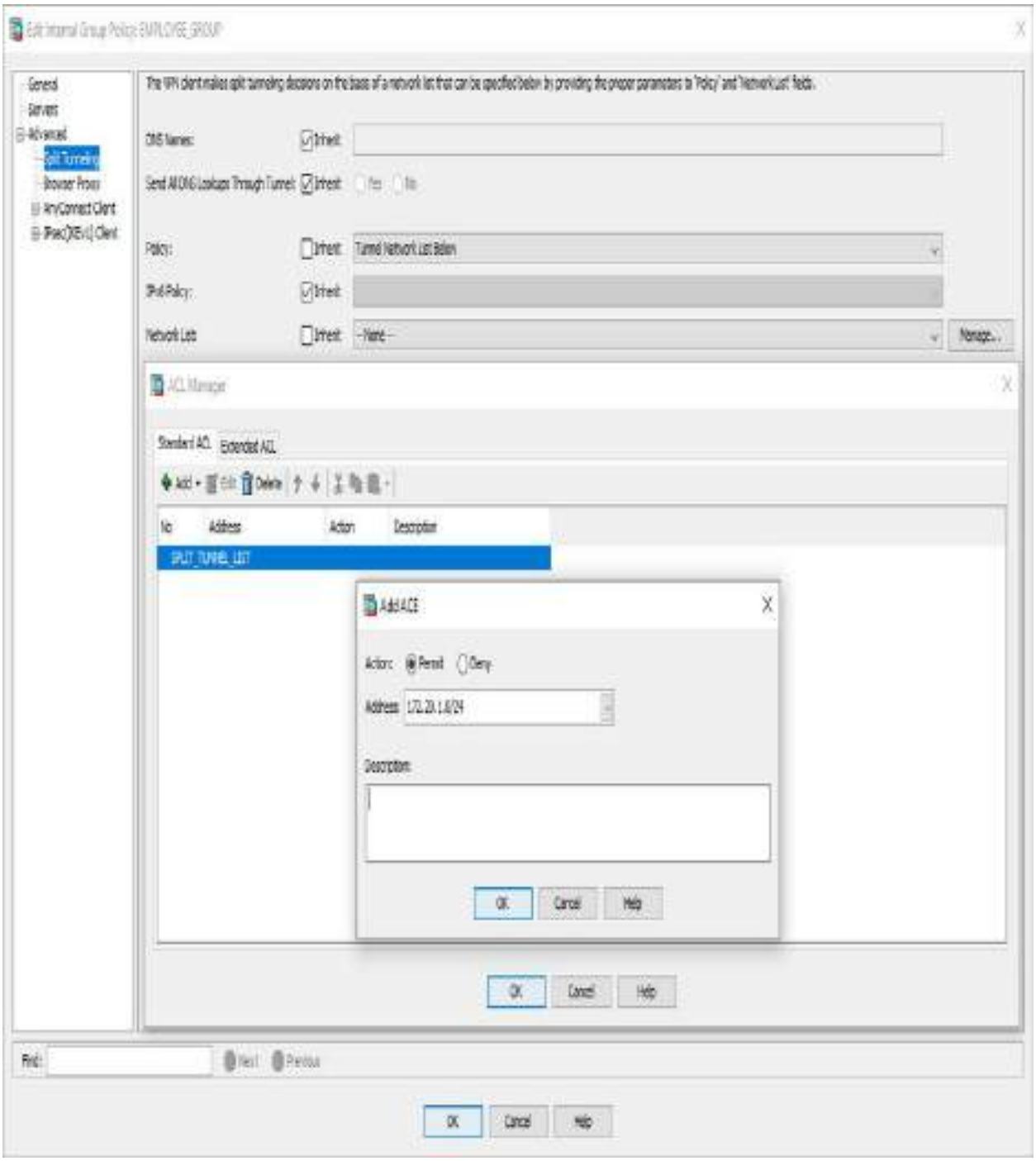


Figure 9-13 Configuring Split Tunneling via ASDM

Configuring Split Tunneling Using CLI

To configure split tunneling via the CLI, first use the **access-list** command to create the split-tunnel ACL. Then use the **split-tunnel-policy** command in

group-policy configuration mode to specify the split tunneling policy. Finally, use the **split-tunnel-network-list value** command in group-policy configuration mode to specify the split tunneling ACL. Example 9-12 mirrors the configuration shown in Figure 9-13.

Example 9-12 Configuring Split Tunneling via the CLI

```
vpn-asa1(config)# access-list SPLIT_TUNNEL_LIST standard permit
172.20.1.0 255.255.255.0
vpn-asa1(config)# group-policy EMPLOYEE_GROUP attributes
vpn-asa1(config-group-policy)# split-tunnel-policy
tunnelspecified
vpn-asa1(config-group-policy)# split-tunnel-network-list value
SPLIT_TUNNEL_LIST
```

Configuring a Traffic Filter Using ASDM

One of the most common group policy settings to configure is filters, which specify which access control list to use for an IPv4 or IPv6 connection. A filter consists of rules that determine whether to allow or reject tunneled data packets coming through the ASA, based on criteria such as source address, destination address, and protocol.

Note

You will need to understand traffic filters for the SVPN exam. There could be questions related to the wrong traffic being blocked, and you must recognize that a traffic filter is the root cause for the problem.

To create and configure a traffic filter via ASDM, follow these steps:

Step 1. Navigate to **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Group Policies**.

Step 2. Select the desired group policy and click **Edit** to open the Edit Internal Group Policy dialog box.

Step 3. Expand **More Options**.

Step 4. Uncheck the **Inherit** check box for Filter.

Step 5. Click **Manage** to open the ACL Manager dialog box.

Step 6. Click the **Extended ACL** tab.

Step 7. Navigate to **Add** > **Add ACL** to open the Add ACL dialog box.

Step 8. Specify an ACL name.

Step 9. Click **OK** to close the Add ACL dialog box.

Step 10. Select the ACL you just created.

Step 11. Navigate to **Add** > **Add ACE** to open the Add ACE dialog box.

Step 12. Specify the source criteria and/or destination criteria, and click **OK** to close the Add ACE dialog box.

Figure 9-14 shows the group policy EMPLOYEE-GROUP with a new filter list named FILTER_LIST. An ACE that will only allow traffic to the IP address 172.20.1.50 on port 80 (HTTP) is being added.

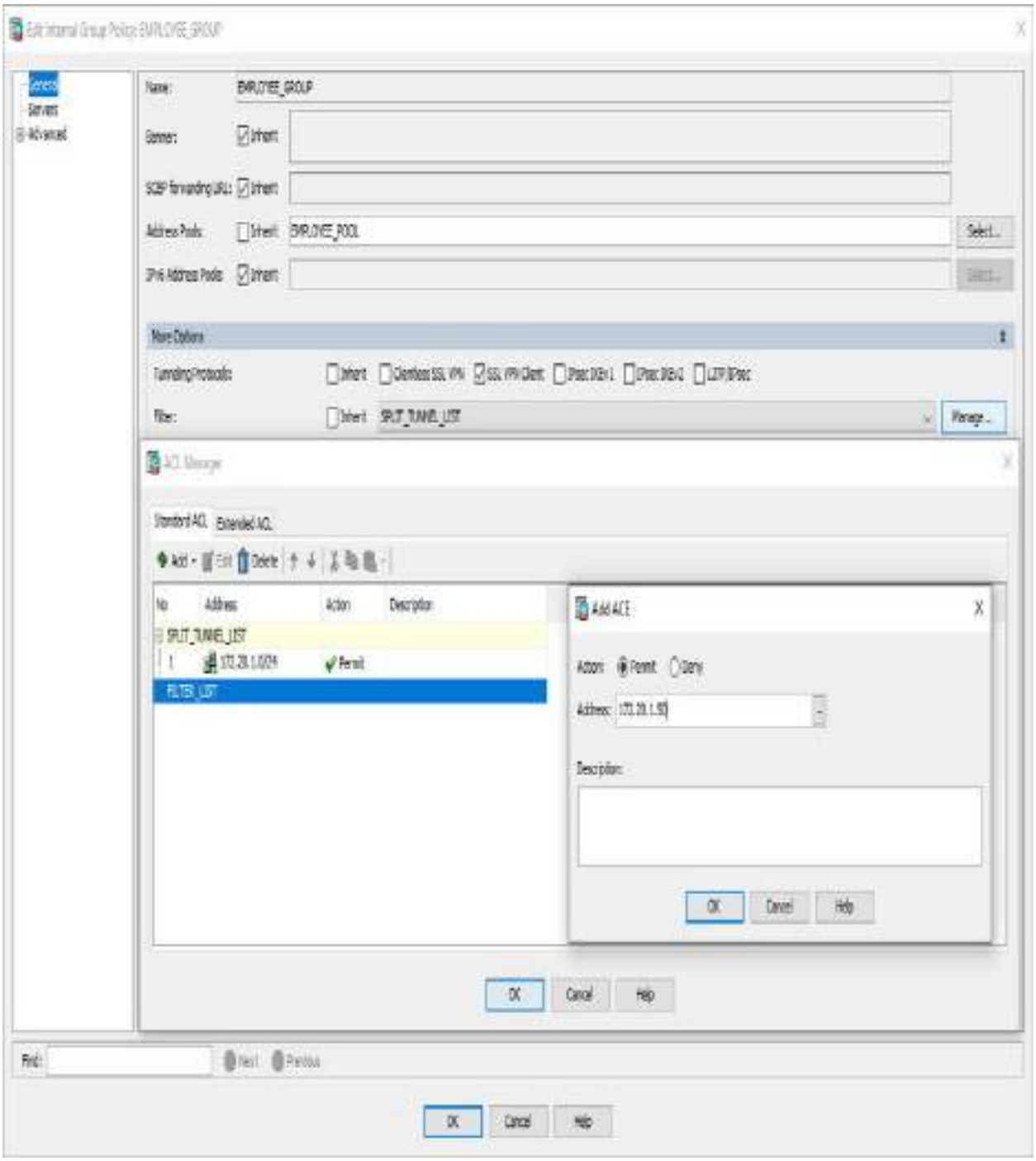


Figure 9-14 Adding a Filter List via ASDM

Configuring a Traffic Filter Using CLI

To create and configure a filter list via the CLI, first use the **access-list** command to create an access list of the traffic you want to allow and/or

block. Then use the **vpn-filter** command in group-policy configuration mode to apply the filter to the group policy. Example 9-13 shows the same configuration as Figure 9-14.

Example 9-13 Adding a Filter List via the CLI

```
vpn-asa1(config)# access-list FILTER_LIST extended permit tcp
any host 172.20.1.50 eq http
vpn-asa1(config)# group-policy EMPLOYEE_GROUP attributes
vpn-asa1(config-group-policy)# vpn-filter value FILTER_LIST
```

That wraps up three foundational features that are commonly deployed with an AnyConnect VPN offering. There are other options you can consider, and other options could appear on the SVPN exam. We focused on these three because we know you will run into them in real-world deployments, and we highly recommend that you know them because they can appear on the SVPN exam.

Next up, let's switch focus to AnyConnect IKEv2 VPN on a Cisco ASA.

AnyConnect IKEv2 VPN on ASA

IKEv2 is an alternative transport to SSL that supports both AnyConnect and standards-based (third-party) endpoint clients. You will need to know both IKEv2 and SSL for the SVPN exam. Both are also common options used for real-world deployments.

Configuration of an AnyConnect IKEv2 VPN on ASA consists of two steps in addition to the steps completed previously for the AnyConnect SSLVPN on ASA:

Step 1. Enable IPsec (IKEv2).

Step 2. Configure an AnyConnect client profile for IKEv2.

Step 1: Enabling IPsec (IKEv2)

The first step in deploying IKEv2 is to enable IPsec. Don’t forget to do this, and know you could find a troubleshooting question related to users being unable to connect to your VPN and one possible issue is that IPsec is not enabled.

Configuring IPsec (IKEv2) Using ASDM

To enable IPsec (IKEv2) via ASDM, follow these steps:

Step 1. Navigate to **Configuration** > **Network (Client) Access** > **AnyConnect Connection Profiles**.

Step 2. In the IPsec (IKEv2) Access section, check **Allow Access and Enable Client Services** for the desired interfaces.

Step 3. In the Connection Profiles section, check **IPsec Enabled** for the desired connection profiles.

Figure 9-15 shows an example of enabling IPsec (IKEv2) access on the OUTSIDE interface and enabling IPsec for the EMPLOYEE_CONNECTION connection profile.

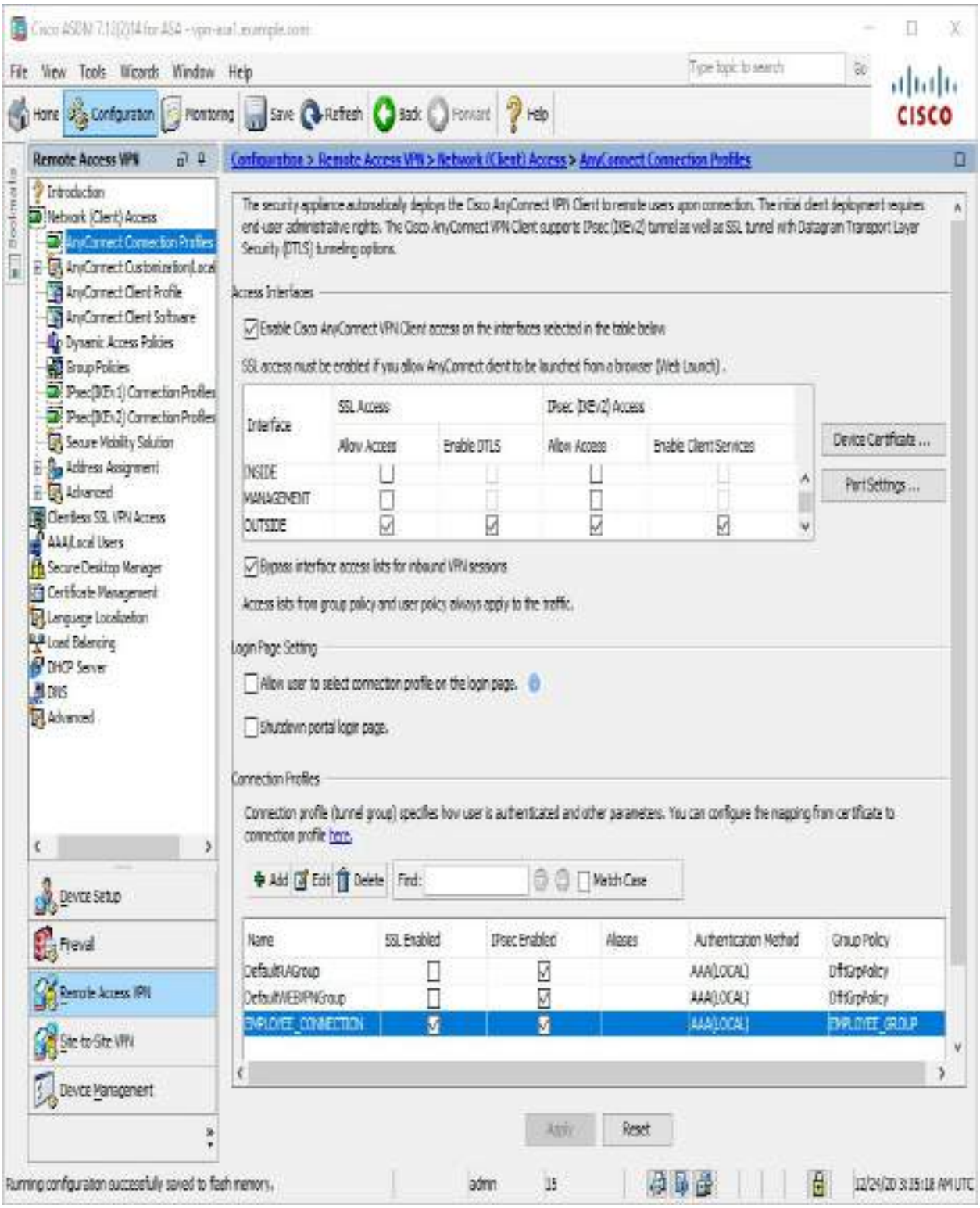


Figure 9-15 Enabling IPsec (IKEv2) via ASDM

Configuring IPsec (IKEv2) Using CLI

To enable IPsec (IKEv2) via the CLI, the configuration is slightly more involved than it appears in ASDM because ASDM automatically generates a lot of the basic IKEv2 configuration for you. Therefore, we split the configuration for IPsec (IKEv2) via the CLI into two sections for clarity. The first section covers only the specific configuration changes made in ASDM. The second section covers the configuration changes automatically generated by ASDM.

To make the specific configuration changes made in ASDM via the CLI, use the **crypto ikev2 enable** command to allow IKEv2 on the desired interfaces. Then use the **vpn-tunnel-protocol** command in group-policy configuration mode to enable IKEv2 for the desired group policies. The first section of Example 9-14 shows an example of enabling IKEv2 on the OUTSIDE interface and enabling IKEv2 for the EMPLOYEE_GROUP group policy. It mirrors the specific configuration changes shown in Figure 9-15.

To make the configuration changes automatically generated by ASDM, use the following commands via the CLI:

- Use the **crypto ikev2 policy** command to create one or more IKEv2 policies. Then use the **group** command and the **encryption** command in ikev2 policy configuration mode to set the acceptable Diffie–Hellman (DH) group(s) and encryption algorithm(s) for each IKEv2 policy. These transforms will be used for the IKE SAs and to secure the negotiation.

- Use the **crypto ikev2 remote-access trustpoint** command to select a trustpoint to use to identify the ASA during session setup.

- Use the **crypto ipsec ikev2 ipsec-proposal** command to create one or more IPsec proposals. Then use the **protocol esp encryption** command and the **protocol esp integrity** command in ipsec proposal configuration mode to set the acceptable encryption algorithm(s) and integrity algorithms for each IPsec proposal. These transforms will be used for the child SAs and to secure the tunnel data.

- Use the **crypto dynamic-map** command to create a dynamic crypto map and associate the IPsec proposals with the dynamic crypto map.
- Use the **crypto map** command to create a crypto map and add a dynamic map entry referencing the previously created dynamic crypto map. Then use the **crypto map** command again to associate the crypto map with the desired interface.

The second section of Example 9-14 shows the commands automatically generated by ASDM.

Example 9-14 Enabling IPsec (IKEv2) via the CLI

```
vpn-asa1(config)# crypto ikev2 enable OUTSIDE client-services
port 443
vpn-asa1(config)# group-policy EMPLOYEE_GROUP attributes
vpn-asa1(config-group-policy)# vpn-tunnel-protocol ssl-client
ikev2

!!!The commands below are automatically generated by ASDM!!!
vpn-asa1(config)# crypto ikev2 policy 1
vpn-asa1(config-ikev2-policy)# group 2 5
vpn-asa1(config-ikev2-policy)# encryption aes-256
vpn-asa1(config-ikev2-policy)# crypto ikev2 policy 10
vpn-asa1(config-ikev2-policy)# group 2 5
vpn-asa1(config-ikev2-policy)# encryption aes-192
vpn-asa1(config-ikev2-policy)# crypto ikev2 policy 20
vpn-asa1(config-ikev2-policy)# group 2 5
vpn-asa1(config-ikev2-policy)# encryption aes
vpn-asa1(config-ikev2-policy)# crypto ikev2 policy 30
vpn-asa1(config-ikev2-policy)# group 2 5
vpn-asa1(config-ikev2-policy)# crypto ikev2 policy 40
vpn-asa1(config-ikev2-policy)# group 2 5
vpn-asa1(config-ikev2-policy)# encryption des
vpn-asa1(config)# crypto ikev2 remote-access trustpoint
EXAMPLE_IDENTITY_CERT
vpn-asa1(config)# crypto ipsec ikev2 ipsec-proposal AES256
vpn-asa1(config-ipsec-proposal)# protocol esp encryption aes-
256
vpn-asa1(config-ipsec-proposal)# protocol esp integrity md5
sha-1
vpn-asa1(config-ipsec-proposal)# crypto ipsec ikev2 ipsec-
proposal AES192
vpn-asa1(config-ipsec-proposal)# protocol esp encryption aes-
192
```

```
vpn-asa1(config-ipsec-proposal)# protocol esp integrity md5
sha-1
vpn-asa1(config-ipsec-proposal)# crypto ipsec ikev2 ipsec-
proposal AES
vpn-asa1(config-ipsec-proposal)# protocol esp encryption aes
vpn-asa1(config-ipsec-proposal)# protocol esp integrity md5
sha-1
vpn-asa1(config-ipsec-proposal)# crypto ipsec ikev2 ipsec-
proposal 3DES
vpn-asa1(config-ipsec-proposal)# protocol esp encryption 3des
vpn-asa1(config-ipsec-proposal)# protocol esp integrity md5
sha-1
vpn-asa1(config-ipsec-proposal)# crypto ipsec ikev2 ipsec-
proposal DES
vpn-asa1(config-ipsec-proposal)# protocol esp encryption des
vpn-asa1(config-ipsec-proposal)# protocol esp integrity md5
sha-1
vpn-asa1(config-ipsec-proposal)# crypto dynamic-map
SYSTEM_DEFAULT_CRYPTO_MAP 65535 set ikev2
ipsec-proposal AES256 AES192 AES 3DES DES
vpn-asa1(config)# crypto map OUTSIDE_map 65535 ipsec-isakmp
dynamic SYSTEM_DEFAULT_CRYPTO_MAP
vpn-asa1(config)# crypto map OUTSIDE_map interface OUTSIDE
```

We recommend that you be familiar with how to enable IPsec using CLI as well as how the code that is generated by ASDM looks when you enable IPsec using ASDM. You could see questions regarding recognizing this code, identifying errors in the code, or other use cases requiring you to be familiar with the CLI involved with enabling IPsec.

Step 2: Configuring an AnyConnect Client Profile for IKEv2

Configuration of AnyConnect is accomplished via AnyConnect client profiles. These profiles contain configuration settings for the core client VPN functionality and for the optional client modules, such as Network Access Manager, ISE Posture, Customer Experience Feedback, and Web Security. The ASA deploys the profiles during AnyConnect installation and updates. Users cannot manage or modify profiles.

You can configure the ASA to deploy profiles globally for all AnyConnect

users or to users based on their group policy. Usually, a user has a single profile file for each AnyConnect module installed. In some cases, you might want to provide more than one VPN profile for a user. Someone who works from multiple locations might need more than one VPN profile.

Profile Storage

Some profile settings are stored locally on the user's computer in a user preferences file or a global preferences file. The user file has information the AnyConnect client needs to display user-controllable settings in the Preferences tab of the client GUI and information about the last connection, such as the user, the group, and the host.

The profiles are stored in the locations listed in Table 9-5.

Table 9-5 Storage Locations for AnyConnect Client Profiles

OS	Location
	%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile
	/opt/cisco/anyconnect/profile
	/opt/cisco/anyconnect/profile

OS	Location
Windows	%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile
macOS	/opt/cisco/anyconnect/profile
Linux	/opt/cisco/anyconnect/profile

OS	Location
Windows	%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile
macOS	/opt/cisco/anyconnect/profile
Linux	/opt/cisco/anyconnect/profile

While manually editing the XML file via a text editor is possible, ASDM includes a built-in profile editor, and using this editor is the preferred method for editing the AnyConnect client profiles.

Creating AnyConnect Client Profile for IKEv2 Using ASDM

To create an AnyConnect client profile for IKEv2 via ASDM, follow these steps:

Step 1. Navigate to **Configuration** > **Remote Access VPN** > **AnyConnect Client Profile**.

Step 2. Click **Add** to open the Add AnyConnect Client Profile dialog box.

Step 3. Specify a profile name.

Step 4. Select the desired group policy.

Step 5. Click **OK**.

Step 6. Click **Edit** to open the AnyConnect Client Profile Editor dialog box.

Step 7. Navigate to **VPN** > **Server List**.

Step 8. Click **Add** to open the Server List Entry dialog box.

Step 9. Specify a display name.

Step 10. Specify a FQDN.

Step 11. Specify a user group.

Step 12. Change the primary protocol from SSL to **IPsec**.

Step 13. Click **OK** to close the Server List Entry dialog box.

Step 14. Click **OK** to close the AnyConnect Client Profile Edit dialog box.

Figure 9-16 shows an example of creating the server list named EMPLOYEE IKEV2 CONNECTION, the FQDN of the ASA (which is vpn-asa1.example.com), and the user group EMPLOYEE_CONNECTION. The primary protocol has been set to IPsec, and the ASA Gateway check box is checked.

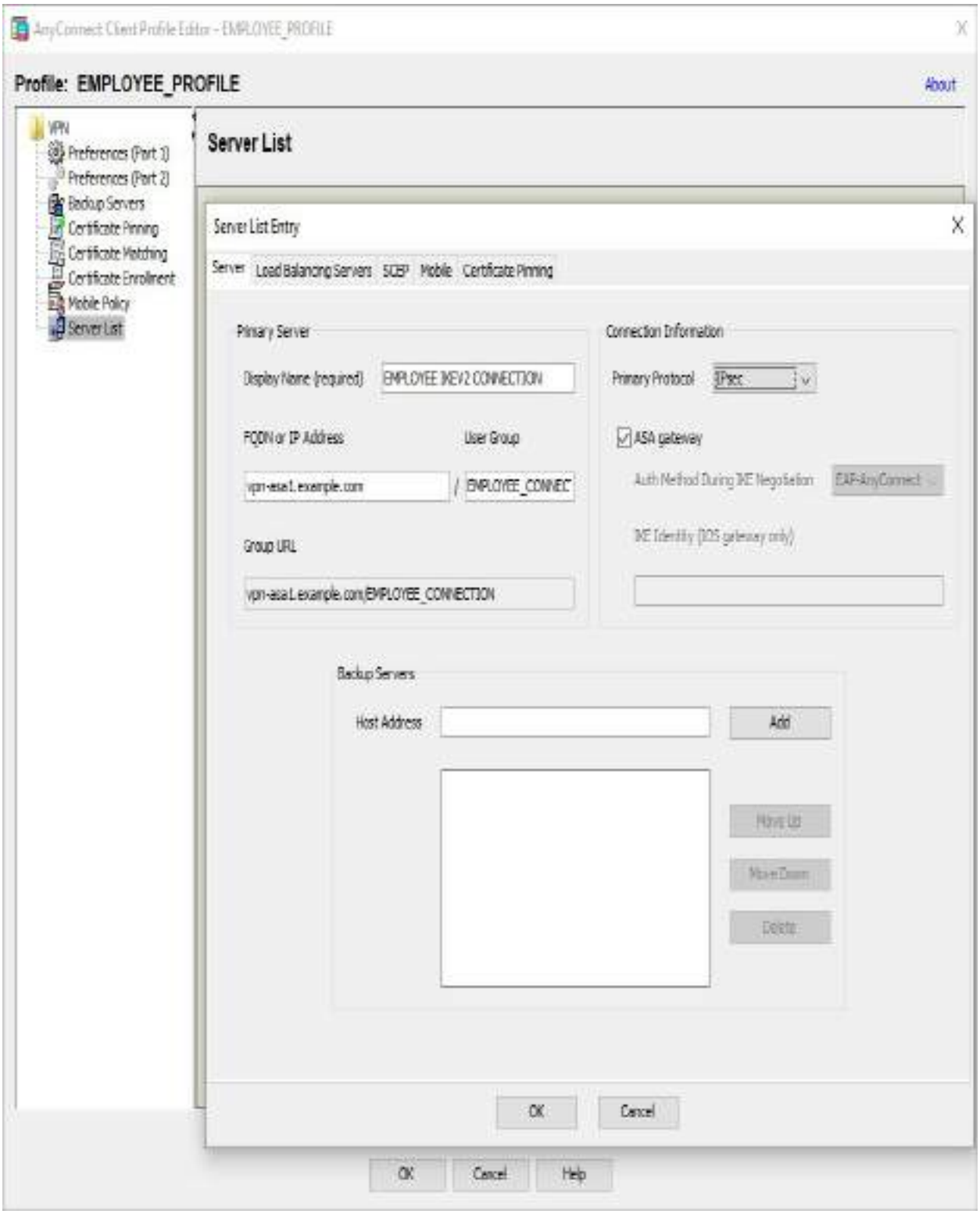


Figure 9-16 Creating an AnyConnect Client Profile for IKEv2 via ASDM

Note

The User Group name must be the same as the name of the connection profile on the ASA; otherwise, the error message “Invalid Host Entry. Please re-enter” appears in the AnyConnect client.

Note

There is no CLI interface for the profile editor.

That concludes how to deploy both IKEv2 and SSLVPN using a Cisco ASA. Next, we look at how to deliver an AnyConnect IKEv2 VPN on Cisco routers.

AnyConnect IKEv2 VPN on Routers

Like the Cisco ASA, Cisco routers running IOS or IOS XE can terminate IKEv2 VPN remote access connections. Terminating IKEv2 VPN remote access connections involves using the same FlexVPN framework discussed in earlier chapters, providing IP layer connectivity via IKEv2 and IPsec for both AnyConnect and third-party clients. Refer to the prerequisites section of this chapter to prepare for a router-based IKEv2 VPN deployment. The same license and host requirements apply.

This section discusses how to implement an AnyConnect IKEv2 VPN on a Cisco routers, specifically IOS XE. Figure 9-17 shows the lab environment used in this section, which includes the following software and hardware versions:

- Cisco Cloud Services Router (CSR) running IOS XE 17.03.01a
- AnyConnect client Version 4.8.03052 running on Windows 10

Figure 9-17 AnyConnect IKE VPN on Routers Lab Diagram

Configuring a Cisco router to terminate AnyConnect IKEv2 remote access connections is a six-step process:

Step 1. Configure PKI.

Step 2. Disable the HTTP and HTTPS servers on the router.

Step 3. Configure AAA.

Step 4. Create an IKEv2 authorization policy.

Step 5. Create an IKEv2 profile.

Step 6. Create a virtual template.

Step 1: Configuring PKI

While it is not uncommon to use self-signed certificates when testing technologies in the lab, it is highly recommended to avoid doing so when dealing with AnyConnect IKEv2 VPN configurations. Some AnyConnect IKEv2 VPN configurations do not work if a self-signed certificate is used. One example is local user authentication when EAP is used between the AnyConnect client and router. EAP requires a proper certificate chain

consisting of a server certificate signed by a separate CA certificate. If this is not in place, the EAP exchange fails.

This happens to be a common AnyConnect IKEv2 VPN configuration and the one that will be configured in the examples in this section. This example uses an external CA rather than a self-signed certificate.

To install a signed certificate from an external CA, perform the following steps:

Step 1. Generate a key pair with the **crypto key generate rsa** command.

Step 2. Create a trustpoint with the **crypto pki trustpoint** command.

Step 3. Import the root CA certificate with the **crypto pki authenticate** command.

Step 4. Generate a certificate signing request (CSR) with the **crypto pki enroll** command.

Step 5. Import the signed server certificate with the **crypto pki import** command.

Generating a Key Pair

An RSA key pair, also known as an *asymmetric key pair*, consists of a public key and a private key. When setting up a PKI trustpoint, you must include the public key of the key pair in the certificate enrollment request. After the certificate has been granted, the public key is included in the certificate so that peers can use it to securely exchange data with the router during session setup. The private key is kept on the router and can be used both to decrypt data sent by peers and to digitally sign transactions when negotiating with peers.

An RSA key pair contains a key modulus value. The modulus determines the size of the RSA key. The larger the modulus, the more secure the RSA key.

However, keys with large modulus values take longer to generate, and encryption and decryption operations take longer with larger keys.

To generate a key pair, use the **crypto key generate rsa** command. Example 9-15 shows an example of creating the key pair named RSA_KEY with a modulus of 2048 bits. A modulus of 2048 bits has been chosen as that is the minimum key length required by public CAs for signing certificates and is the generally accepted minimum key length as of the publication date of this book. On many versions of IOS and IOS XE code, the default modulus is less than 2048 bits. A certificate request using a key with a modulus less than 2048 bits would most likely be rejected by a public CA as keys less than 2048 bits are vulnerable to cryptographic attacks.

Example 9-15 Generating a Key Pair

```
VPN-ROUTER(config)# crypto key generate rsa label RSA_KEY
modulus 2048
The name for the keys will be: RSA_KEY

% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 2 seconds)
```

Creating a Trustpoint

A *trustpoint* is an abstract container used to hold a certificate in IOS. A single trustpoint is capable of storing two active certificates at any given time:

- **A CA certificate:** Loading a CA certificate into a given trustpoint is known as the trustpoint authentication process.
- **An ID certificate issued by the CA:** Loading or importing an ID certificate into a given trustpoint is known as the trustpoint enrollment process.

Trust Point Policy

A trustpoint configuration is known as a trust policy, and it defines the following:

- Which CA certificate is loaded in the trustpoint
- Which CA the trustpoint enrolls to
- How the IOS enrolls the trustpoint
- How a certificate issued by the given CA is validated

Configuring a Trustpoint

To create a trustpoint, use the **crypto pki trustpoint** command. Then use the **rsakeypair** command to specify the key pair the trustpoint should use. Example 9-16 shows an example of creating the trustpoint named RSA_CERT and configuring the trustpoint to use the previously generated RSA_KEY key pair.

Define Trust Policy

The next step in configuring the trustpoint is to define the trust policy. To output the CSR to the terminal, use the **enrollment terminal** command to instruct the router to display the CSR during the enrollment process.

Disable FQDN

To ensure the CSR is well formed and accepted by the CA, disable the insertion of the FQDN via the **fqdn none** command, which uses a nonstandard distinguished name field. Instead, provide the FQDN using the standard common name (CN) distinguished name (DN) field via the **subject-name** command and manually specify the distinguished name in the form *CN=<FQDN>* (see Example 9-16).

Example 9-16 Creating a Trustpoint

```
VPN-ROUTER(config)# crypto pki trustpoint RSA_CERT
VPN-ROUTER(ca-trustpoint)# rsakeypair RSA_KEY
VPN-ROUTER(ca-trustpoint)# enrollment terminal
VPN-ROUTER(ca-trustpoint)# fqdn none
VPN-ROUTER(ca-trustpoint)# subject-name CN=VPN-
ROUTER.EXAMPLE.COM
```

Importing the Root CA Certificate

With the trustpoint defined, the next step is to load the root certificate of the chosen CA. To load a CA certificate, use the **crypto pki authenticate** command. Example 9-17 shows an example of loading a root certificate into the RSA_CERT trustpoint.

When using terminal enrollment, the **crypto pki authenticate** command requires a base-64-encoded CA certificate. This can be obtained from the CA and is often referred to as Privacy-Enhanced Mail (PEM) format. After you paste the certificate, the router displays the MD5 and SHA-1 hashes of the certificate. This allows you as the administrator to confirm whether the right certificate has been loaded and choose whether to accept or reject the certificate.

Example 9-17 Importing the Root CA Certificate

```
VPN-ROUTER(ca-trustpoint)# crypto pki authenticate RSA_CERT

Enter the base 64 encoded CA certificate.
End with a blank line or the word “quit” on a line by itself

-----BEGIN CERTIFICATE-----
MIIDLjCCAhagAwIBAgIGAXTMiaEAMA0GCSqGSIb3DQEBCwUAMCcxCzAJBgNVBAY
T
AlVTMRgwFgYDVQQDDA9FeGFtcGxlIFJvb3QgQ0EwHhcNMjAwOTI2MjIzMDA1Whc
N
MzAwOTI3MjIzMDE5WjAnMQswCQYDVQQGEwJVUzEYMBYGA1UEAwwPRXhhbXBsZSB
S
b290IENBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvw4xs1LPKfj
Y
tubLGZZNU5vttMqXzK5HbnN4H9bl66QZuSPwc9/3sFlRgUlOWXnZXp1oj8C7/mD
F
BD87SdMAgGhWlR43m3FAVghwtd/kVcMhPj19wgxh95l0FxfMC3ryqM232Ts27V+
4
a/M572C6lsL7rCAKZVP5UHkwKlvXVGdGTOE1bBLMMmy6wW+ReMILHFOJ3StxHEg
t
MKlsHrBrYKKHrUFk89y7w9bCau1oBNEWFaptvtprv2/MoFUbCM/1iDjk5i2FJIY
W
VYbLEspkCqx43I24cIEBX6obIOvMMdi2dcl9cFHZNZLvWlP+Eboj0skeEanXBLk
8
5zNH1c+vlQIDAQABo2AwXjAfBgNVHSMEGDAWgBSDErDZDe+D8biDHBnc2v7cmwn
L
```

```
GTAMBgNVHRMEBTADAQH/MA4GA1UdDwEB/wQEAwIBhjAdBgNVHQ4EFgQUgxKw2Q3
v
g/G4gxwZ3Nr+3JsJyxkwDQYJKoZIhvcNAQELBQADggEBAGU6l464oU225qNSq6o
F
I2m5n39L9V6g3L/QzhMzAQEDnG3NzbPtp0/GrXQdoA4QS+JgzKClgeVPn9D726x
Z
nflVF/WWilX//9wIY5W8PyIoAny1/8m6ej+WbcwdJHRNDyf8Dtw4OMdYG23ZNT/
1
UmCZH376JxkagkCKCKLO2yOVvvnETiaD+g5zI7wuMP+zL1ofdGhzThLMbuykyOM
K
cdxA93wZmkXki9Uqq9QTAWqUdDS1xXxGdECfJSPxRgNqGFsCLQ58sumBMXGdFwc
2
VeV0eJ2+H+RjMJbnBK0KiOsvk2YIZhlmaqLQsilZm92WkDH/TvbYPD6lWjRsqNE
v
iY4=
-----END CERTIFICATE-----

Certificate has the following attributes:
       Fingerprint MD5: 9546B887 B143A4D7 FAB3AACA BA69281D
      Fingerprint SHA1: C615CF85 9441B99E 5E217B68 4D7E3983
467B9425

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

Generating a Certificate Signing Request (CSR)

With the root CA certificate successfully loaded, the next step is to obtain a certificate for the router itself. To generate a CSR, use the **crypto pki enroll** command. To display the CSR to the terminal, answer yes to the appropriate question. Example 9-18 shows an example of generating a CSR for the RSA_CERT trustpoint. In this example, the router serial number or IP address is not needed in the CSR.

Example 9-18 Generating a Certificate Signing Request (CSR)

```
VPN-ROUTER(config)# crypto pki enroll RSA_CERT
% Start certificate enrollment ..

% The subject name in the certificate will include: CN=VPN-
ROUTER.EXAMPLE.COM
% The fully-qualified domain name will not be included in the
certificate
```

```
% Include the router serial number in the subject name?
[yes/no]: no
% Include an IP address in the subject name? [no]: no
Display Certificate Request to terminal? [yes/no]: yes
Certificate Request follows:

MIIChzCCAW8CAQAwITEfMB0GA1UEAxMWVlBOLVJPVVRFUi5FWEFNUExFLkNPTTC
C
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALZ1y4VzbbfyzmBuyPVsRs4
d
0aqpB1eEj7t5fGTnqVP3jPjdD56fKEQToW26xgAwhWpUnJnMjjrXR/LBv5poc2o
U
9Vdi/mNAZhaAj61JkWS3frozoQVPBR+3U5Vq1YXpQrA75/P6zcz7hvk4X67b2rR
l
s7psoN/LPGOdPPe9T8w277BvOD2uX9fNWk1KyOnidFdSe1OoLea9MQ6DCN6EMj/
i
PzdXdgX1LLchrVtaS2eSe3kEs6//GZFkd8fLn4OUyMm4jqqOcL6Ufu31s1q3xJC
1
sRO7HajBucsB97F5T6FcoUttzZpCbwtNqCk4hjxVt5FUvF94WEypPjg7MRldaFU
C
AwEAAaAhMB8GCSqGSIb3DQEJDjESMBAwDgYDVR0PAQH/BAQDAgWgMA0GCSqGSIb
3
DQEBBQUAA4IBAQBMu9341alZSUeoCFdRE4Qhk4zHqA6DEFvSgSIoblLjhUdRh6z
r
v7Hra8spqvy7WaA93vvLhCZkHJhrQk9CNwAYP6MyBrs8LmehBSEi8eTCoCKqPMN
C
fTC0kgyq5VZ0myn7G/aY0dEIXfMo3J1DrFth0JOWiYcoUIf0FACWBJ8vKqTkOUn
g
8qxstPOsZaDcErcFCl8WuvkCUqhzS19JcVW2Ljnb8mc/1/RL6QHx94jDGnpkBMo
Y
GB58gXLrTFDML++2KfFUsJK3NtsN2yuVYIAT2MfQmPHq08cBJj6cvdI2+4jCBoL
v
zMkyhgQpCBFwJQYSDfPIeVFjjyECxYOdFPfa

---End - This line not part of the certificate request---

Redisplay enrollment request? [yes/no]: no
```

This example does not show the submission of the CSR (labeled Certificate Request in Example 9-18) to the chosen CA. The process for this varies by CA, but it typically involves copying/pasting the text displayed into a web form or submitting the text in a plaintext file. When the request is completed and approved, the CA returns a signed certificate.

Importing the Signed Server Certificate

To import the signed certificate into the router, use the **crypto pki import** command. To import the certificate via the CLI (by copying and pasting), the certificate must be obtained from the CA in PEM format or must be converted to PEM format by using a tool such as OpenSSL. Example 9-19 shows an example of importing the signed certificate using the trustpoint RSA_CERT created previously.

Example 9-19 Importing the Signed Server Certificate

```
VPN-ROUTER(config)# crypto pki import RSA_CERT certificate
% The fully-qualified domain name will not be included in the
certificate

Enter the base 64 encoded certificate.
End with a blank line or the word “quit” on a line by itself

-----BEGIN CERTIFICATE-----
MIIDJTCCAg2gAwIBAgIGAXbwIYOtMA0GCSqGSIb3DQEBCwUAMCcxCzAJBgNVBAY
T
AlVTMRgwFgYDVQQDDA9FeGFtcGxlIFJvb3QgQ0EwHhcNMjEwMTExMDYyODE2Whc
N
MjIwMTExMDYyODE3WjAhMR8wHQYDVQQDExZWUE4tUk9VVEVSLkVYQU1QTEUuQ09
N
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtnXLhXNtt/LOYG7I9Wx
G
zh3RqqkHV4SPu3l8ZOepU/eM+N0Pnp8oRBOhbbrGADCFalScmcyOOtdH8sG/mmh
z
ahT1V2L+Y0BmFoCPrUmRZLd+ujOhBU8FH7dTlWrVhelCsDvn8/rNzPuG+Thfrtv
a
tGWzumyg38s8Y508971PzDbvsG84Pa5f181aTUrI6eJ0V1J7U6gt5r0xDoMI3oQ
y
P+I/N1d2BfUstyGtW1pLZ5J7eQSzr/8ZkWR3x8ufg5TIybiOqo5wvpR+7fWzWrf
E
kLWxE7sdqMG5ywH3sXlPoVyhS23NmkJvC02oKTiGPFW3kVS8X3hYTKk+ODsxGV1
o
VQIDAQABo10wWzAfBgNVHSMEGDAWgBSDErDZDe+D8biDHBnc2v7cmwnLGTAJBgN
V
HRMEAjAAMA4GA1UdDwEB/wQEAwIFoDAdBgNVHQ4EFgQUgnWNDpF3SSxC9hoqAWj
k
/2jUujIwDQYJKoZIhvcNAQELBQADggEBAI/2iivi4rD9De06ep/LkhuzDWxFIBc
m
kaaCUfZFU60iAXNKuvFi1rxR3ZlfbyFhJ1L5jskZr523C3OeKWvNNwHgBUMUyd0
d
DPO1VdIEX8cmD2CkBVwwKR6WnLWIWcGneI5aPmj0KyllOd9fjuV20Od/3zxkZfh
R
```

```
MxA9hefdwp7ZnLiXq+pSVIAxMdmxmzjZcNCzHthS4wB3FBxSVqZYDHM8rltc/v8
6
CctneOXA3BZk7ICtvAEZ5FtO1FRfjV+m8hmWyc9ga1NKnjFpcRUmxQSrxjgLh+m
5
WycYh508gn2sNBZor9C4HuNQ5UYRFE8ccmMrY1OKCrXmU0JDgAu9Jxk=
-----END CERTIFICATE-----

% Router Certificate successfully imported
```

To verify that the root CA and identity certificate have been installed correctly, use the **show crypto pki trustpoints** command. Example 9-20 shows the output of this command when both the root CA and identity certificate have been successfully installed.

Example 9-20 Verifying the Root CA and Identity Certificate Installation

```
VPN-ROUTER# show crypto pki trustpoints RSA_CERT status
*Jan 11 06:29:45.480: %SYS-5-CONFIG_I: Configured from console
by admin on vty0 (100.100.1.254)
Trustpoint RSA_CERT:
  Issuing CA certificate configured:
    Subject Name:
     cn=Example Root CA,c=US
    Fingerprint MD5: 9546B887 B143A4D7 FAB3AACA BA69281D
    Fingerprint SHA1: C615CF85 9441B99E 5E217B68 4D7E3983
467B9425
  Router General Purpose certificate configured:
    Subject Name:
     cn=VPN-ROUTER.EXAMPLE.COM
    Fingerprint MD5: 219DFA6B 420C2F94 7F994E18 C850B935
    Fingerprint SHA1: 4B857419 BBA20413 931FF128 565BC70E
2C87EBAE
  State:
    Keys generated ..... Yes (General Purpose, non-
exportable)
    Issuing CA authenticated ..... Yes
    Certificate request(s) ..... Yes
```

With the trustpoint on the router configured properly, the next step is to disable the HTTP server on the router.

Step 2: Disabling the HTTP and HTTPS Servers on

the Router

When a user attempts an IKEv2 connection to a Cisco router with the HTTP or HTTPS server enabled, the AnyConnect client receives a reply that is not expected, triggering the detection of a captive portal and preventing connections to the headend. To avoid this issue, there are two options:

- Disable AnyConnect captive portal detection via an AnyConnect client profile
- Disable the HTTP and HTTPS servers on the Cisco router

Because AnyConnect captive portal detection is a generally useful feature, the preferred option is to disable the HTTP and HTTPS server on the Cisco router via the **no http server** and **no http server-server** commands, as shown in Example 9-21.

Example 9-21 Disabling the HTTP and HTTPS Servers on the Router

```
VPN-ROUTER(config)# no ip http server
VPN-ROUTER(config)# no ip http secure-server
```

Step 3: Configuring AAA

Next, you need to enable AAA with the **aaa new-model** command and configure the necessary authentication and authorization for our users. For users connecting remotely, this is broken into two components. The first components is the **aaa authentication login** command with the list named LOCAL_USER_AUTHC, which directs user authentication to use the local database. The second components is the **aaa authorization network** command with the list named LOCAL_GROUP_AUTHZ, which directs group authorization to also use the local database. Example 9-22 shows all of these commands.

Example 9-22 Configuring AAA

```
VPN-ROUTER(config)# aaa new-model
VPN-ROUTER(config)# aaa authentication login LOCAL_USER_AUTHC
local
VPN-ROUTER(config)# aaa authorization network LOCAL_GROUP_AUTHZ
local
```

With the authentication and authorization lists defined, you now need to populate the local database with users and groups. To define a user, use the **username** command. Example 9-23 shows an example of creating the user vpnuser.

Example 9-23 Creating a User

```
VPN-ROUTER(config)# username vpnuser password cisco123
WARNING: Command has been added to the configuration using a
type 0 password. However, type 0
passwords will soon be deprecated. Migrate to a supported
password type
```

Step 4: Creating an IKEv2 Authorization Policy

The next step is to create a group for authorization via an IKEv2 authorization policy. This group, which will be used for local group authorization, defines various configuration attributes that will be pushed to the AnyConnect client upon connection. To create an IKEv2 authorization policy, use the **crypto ikev2 authorization policy** command. Example 9-24 shows an example of creating an IKEv2 authorization policy. EMPLOYEES is both the name of the policy and the group name that will be used during authorization.

To ensure that the connecting user has connectivity, you also define various attributes that will be returned to the AnyConnect client, which determines how the client connects to the network (see Example 9-24):

- **pool** defines the IP addresses that are assigned to the client. This example uses a dedicated subnet pool of IP addresses named EMPLOYEE_POOL

with the range 172.16.2.1 to 172.16.2.254, using the **ip local pool** command.

- **netmask** defines the IP subnet mask used by the AnyConnect client.
- **dns** defines the DNS servers used by the AnyConnect client.

Example 9-24 Creating an IKEv2 Authorization Policy

```
VPN-ROUTER(config)# ip local pool EMPLOYEE_POOL 172.16.2.1
172.16.2.254
VPN-ROUTER(config)# crypto ikev2 authorization policy EMPLOYEES
VPN-ROUTER(config-ikev2-author-policy)# pool EMPLOYEE_POOL
VPN-ROUTER(config-ikev2-author-policy)# netmask 255.255.255.0
VPN-ROUTER(config-ikev2-author-policy)# dns 172.20.1.50
```

Note

Although it is not shown, the DMZ-ROUTER must also have a route for 172.16.2.0/24 pointing to the internal interface of the VPN-ROUTER.

Step 5: Creating an IKEv2 Profile

An IKEv2 profile is a repository of nonnegotiable parameters of the IKE SA, such as local or remote identities and authentication methods and services that are available to authenticated peers that match the profile. For a remote access VPN, an IKEv2 profile contains the bulk of the configuration.

Create New IKEv2 Profile

To create a new IKEv2 profile, use the **crypto ikev2 profile** command. Example 9-25 shows an example of creating a new profile named LOCAL_USER_IKEV2_PROFILE.

Identifying Match Criteria

In Example 9-25, the **match identity remote key-id *$AnyConnectClient$*** command identifies the match criteria to select the profile LOCAL_USER_IKEV2_PROFILE. Put another way, the IKE identity of type key-id sent by the client is used as the selection criteria to select this IKEv2 profile. The string *$AnyConnectClient$* is the default key ID provided by the AnyConnect client. With this match criteria, any AnyConnect client that is using the default key ID will be matched to this profile.

RSA Certificate Authentication

The next command in Example 9-25, **authentication local rsa-sig**, tells the router to use an RSA certificate to authenticate itself to the remote client, and the **pki trustpoint** *RSA_CERT* command identifies the RSA_CERT trustpoint certificate as the certificate that should be used for this authentication.

Authenticating Remote Users

To authenticate remote users, the **authentication remote anyconnect-eap aggregate** command identifies that the proprietary method AnyConnect-EAP (also known as aggregate authentication) will be used to perform authentication of the remote users. It is important to note that the **authentication remote** command only identifies the method used for authentication. It does not specify what database will be used to authenticate users. You will define that in the next step.

Authentication List

To specify the authentication list used for authenticating users, use the **aaa authentication anyconnect-eap** command. In Example 9-25, the **aaa authentication anyconnect-eap** LOCAL_USER_AUTHC command points authentication to the LOCAL_USER_AUTHC list previously configured.

To specify the authorization list used for authorizing groups, use the **aaa authorization group anyconnect-eap** command. In Example 9-25, the **authorization group anyconnect-eap list** LOCAL_GROUP_AUTHZ

EMPLOYEES tells the router to use the authorization list LOCAL_GROUP_AUTHZ and the group name EMPLOYEES for authorization. LOCAL_GROUP_AUTHZ is the authorization list previously configured with the **aaa authorization network** command and points to the local database on the router. EMPLOYEES references the IKEv2 authorization policy previously configured with the **crypto ikev2 authorization policy** command.

Virtual Template

As the second-to-last step, specify a virtual template that will be used by the profile via the **virtual-template** command. The virtual template will be defined later.

AnyConnect Client Profile

Finally, specify an AnyConnect client profile that will be pushed to connecting clients via the **anyconnect profile** command. The AnyConnect client profile will be defined later as well.

Configuration Summary

Putting all of these pieces together, we end up with the complete configuration for the IKEv2 profile shown in Example 9-25.

Example 9-25 Creating an IKEv2 Profile

```
VPN-ROUTER(config)# crypto ikev2 profile
LOCAL_USER_IKEV2_PROFILE
IKEv2 profile MUST have:
   1. A local and a remote authentication method.
   2. A match identity or a match certificate or match any
statement.
VPN-ROUTER(config-ikev2-profile)# match identity remote key-id
*$AnyConnectClient$*
VPN-ROUTER(config-ikev2-profile)# authentication local rsa-sig
VPN-ROUTER(config-ikev2-profile)# pki trustpoint RSA_CERT
VPN-ROUTER(config-ikev2-profile)# authentication remote
anyconnect-eap aggregate
VPN-ROUTER(config-ikev2-profile)# aaa authentication
```

```
anyconnect-eap LOCAL_USER_AUTHC
VPN-ROUTER(config-ikev2-profile)# aaa authorization group
anyconnect-eap list LOCAL_GROUP_AUTHZ
EMPLOYEES
VPN-ROUTER(config-ikev2-profile)# virtual-template 1
VPN-ROUTER(config-ikev2-profile)# anyconnect profile acvpn
```

Step 6: Creating a Virtual Template

Example 9-26 shows how to create the virtual template via the **interface virtual-template** command with interface number 1, a type of tunnel, and the following commands:

- **ip unnumbered gigabitEthernet 2** enables IP on the interfaces without assigning a specific IP address on the interface. In this case, you are piggybacking on the interface gigabitEthernet 2, but this could be any interface with an IP address, such as a loopback.
- **ip mtu 1400** configures the largest packet size/maximum transmission unit (MTU) for the tunnel interface. It is customary to set this to a conservative 1400 bytes to prevent fragmentation and performance degradation.
- **tunnel mode ipsec ipv4** configures the virtual template to use IPsec tunnel encapsulation over IPv4.
- **tunnel protection ipsec profile default** configures the virtual template to use the smart defaults IPsec profile named default. Alternatively, a custom IPsec profile could be referenced that was previously created with the **crypto ipsec profile** command.

Example 9-26 Creating the Virtual Template

```
VPN-ROUTER(config)# interface Virtual-Template1 type tunnel
VPN-ROUTER(config-if)# ip unnumbered gigabitEthernet 2
VPN-ROUTER(config-if)# ip mtu 1400
VPN-ROUTER(config-if)# tunnel mode ipsec ipv4
VPN-ROUTER(config-if)# tunnel protection ipsec profile default
```

With the virtual template configured, you now have a working configuration that provides full tunnel connectivity via AnyConnect. The configuration you have built so far is shown in Example 9-27.

Example 9-27 Full AnyConnect IKEv2 Configuration

```
aaa new-model
aaa authentication login LOCAL_USER_AUTHC local
aaa authorization network LOCAL_GROUP_AUTHZ local

username vpnuser password cisco123

ip local pool EMPLOYEE_POOL 172.16.2.1 172.16.2.254

crypto ikev2 authorization policy EMPLOYEES
 pool EMPLOYEE_POOL
 netmask 255.255.255.0
 dns 172.20.1.50

crypto ikev2 profile LOCAL_USER_IKEV2_PROFILE
 match identity remote key-id *$AnyConnectClient$*
 authentication local rsa-sig
 pki trustpoint RSA_CERT
 authentication remote anyconnect-eap aggregate
 aaa authentication anyconnect-eap LOCAL_USER_AUTHC
 aaa authorization group anyconnect-eap list LOCAL_GROUP_AUTHZ
EMPLOYEES
 virtual-template 1
 anyconnect profile acvpn

interface virtual-template 1 type tunnel
 ip unnumbered vlan 3
 ip mtu 1400
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile default
```

Creating the AnyConnect Client Profile

To complete the configuration, you need to build an AnyConnect client profile to allow the clients to connect. The reason for this is threefold:

- By default, AnyConnect uses SSL/TLS as the primary protocol for connections. Because the FlexVPN server in this case only supports

IKEv2, AnyConnect will fail to connect if there is no profile configured to use IPsec as the primary protocol.

- By default, AnyConnect assumes that it is connecting to an ASA gateway. The FlexVPN server in this case is running IOS XE.
- By default, the AnyConnect client tries to download the AnyConnect profile after successful login. If the profile is not available, the connection fails. Only newer versions of IOS XE (16.9.1 or higher) support the downloading of the AnyConnect profile after successful login.

AnyConnect Profile Editor

To configure the AnyConnect client profile, you can use the AnyConnect profile editor running on Windows. As Figure 9-18 shows, the Windows AnyConnect profile editor looks identical to the AnyConnect profile editor in ASDM.

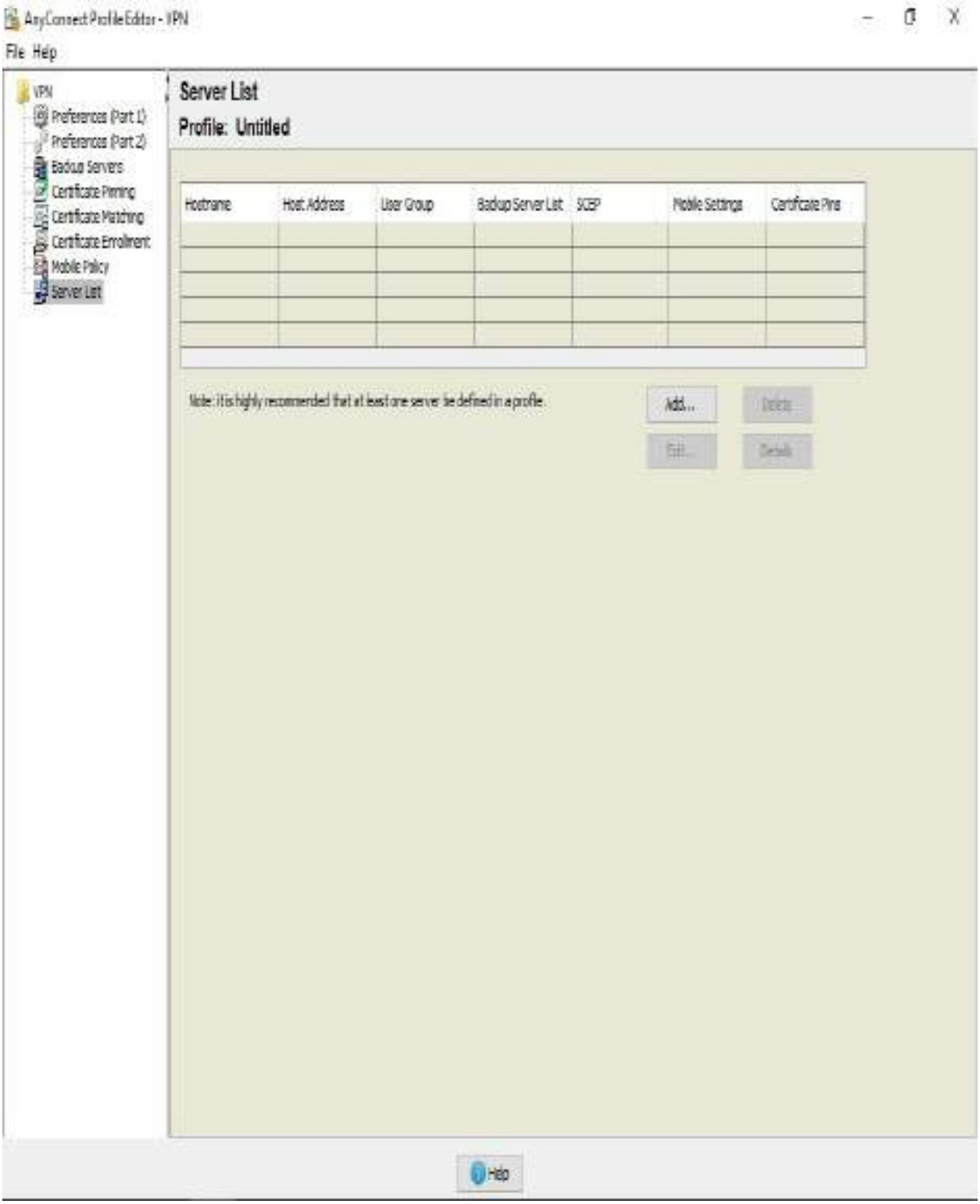


Figure 9-18 AnyConnect Profile Editor Server List

To create an AnyConnect client profile for IKEv2 terminating on a Cisco

router via the Windows AnyConnect Profile Editor, follow these steps:

Step 1. Navigate to **VPN** > **Server List**.

Step 2. Click **Add** to open the Server List Entry dialog box.

Step 3. Specify a display name.

Step 4. Specify a FQDN.

Step 5. Specify a user group.

Step 6. Change Primary Protocol from SSL to **IPsec**.

Step 7. Uncheck **ASA Gateway**.

Step 8. Click **OK** to close the Server List Entry dialog box.

Step 9. Navigate to **File** > **Save As**.

Step 10. Specify a location to save the profile.

Step 11. Click **Save**.

Figure 9-19 shows an example of creating the server list named IOS IKEV2 LOCAL. Connections using this server list entry will be made to the FQDN vpn-router.example.com. The primary protocol has been changed from SSL to IPsec because the connection uses IKEv2. Finally, the ASA gateway has been unselected because the VPN will terminate on a Cisco router.

Note

The display name is a friendly name shown to users in the AnyConnect client and does not have to match any portion of the configuration.

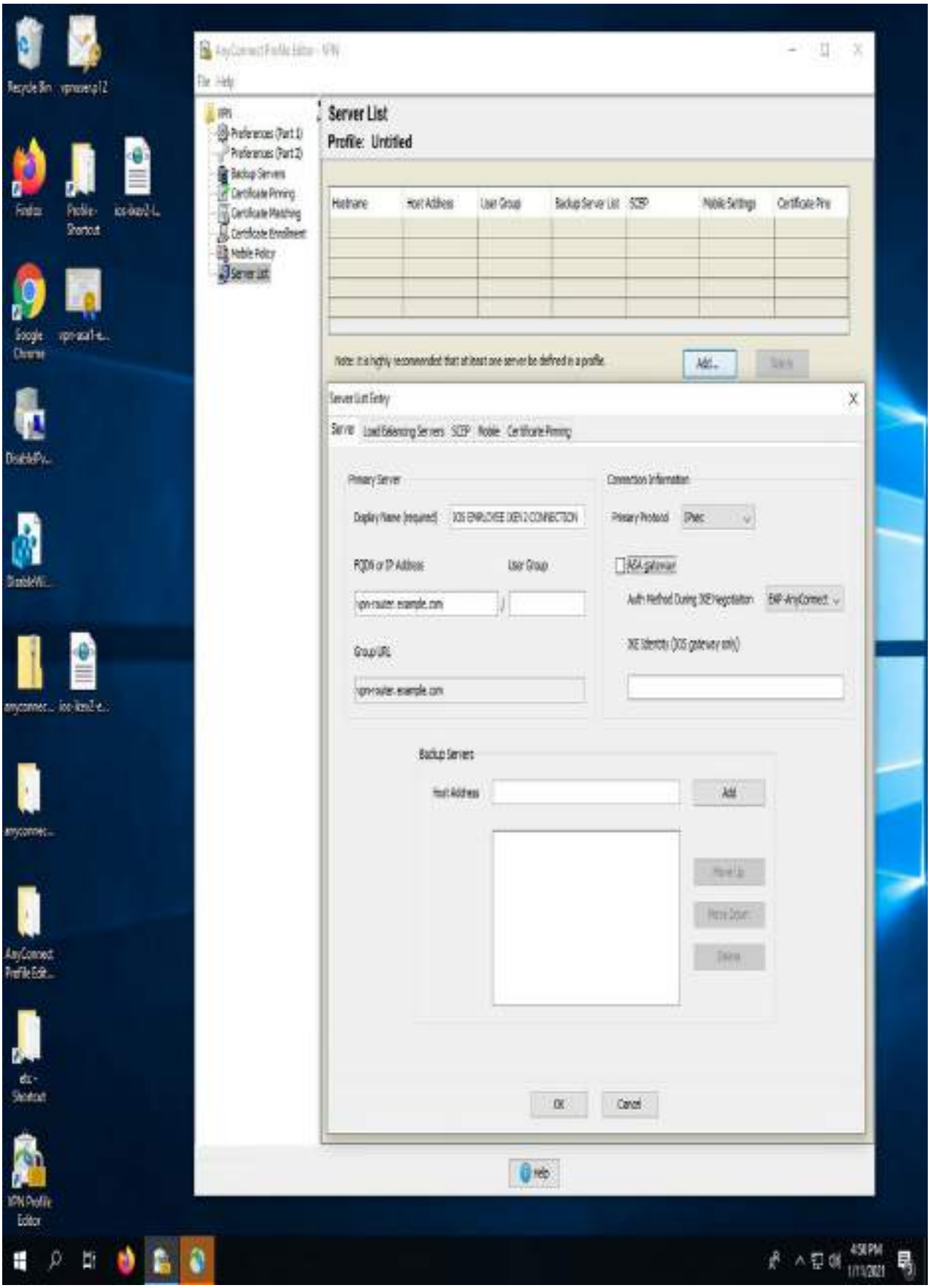

Server List
Profile: Untitled
Server List Entry
Primary Server
Backup Servers
OK
Cancel

Figure 9-19 Creating an AnyConnect Client Profile for IKEv2 VPN to a Router

Copying to the Router

You can now copy the file to the router and use the **crypto vpn anyconnect profile** command to define the profile to push down to clients upon connection. The name of the profile on the Cisco router must be acvpn.xml.

> ### Note
>
> Cisco routers running IOS XE releases older than 16.9.1 do not have the capability to push down a profile to AnyConnect. With those routers, you must disable the profile download capability by changing the text <*BypassDownloader*>**true**</*BypassDownloader*> to <*BypassDownloader*>**false**</*BypassDownloader*> in the AnyConnectLocalPolicy.xml. On Windows, this file is stored in the %ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile folder, and on macOS and Linux, it is stored in the /opt/cisco/anyconnect/profile folder.

Example 9-28 shows an example of uploading the profile via TFTP and defining the profile in the configuration.

Example 9-28 Defining an AnyConnect Client Profile on a Cisco Router

```
VPN-ROUTER(config)# crypto vpn anyconnect profile acvpn
bootflash:/acvpn.xml
```

The final step is to install and load the AnyConnect client profile on the endpoint in the appropriate folder. Assuming that AnyConnect is already installed, you can transfer the file to the profile location for the operating system being used, as shown in Table 9-6.

Table 9-6 Storage Locations for AnyConnect Client Profiles

Operating System	Location
Windows	%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile
macOS	/opt/cisco/anyconnect/profile
Linux	/opt/cisco/anyconnect/profile

Reboot

To load the new profiles, the AnyConnect client needs to be restarted. You can restart the client by right-clicking the AnyConnect icon in the Windows tray and selecting the Quit option. One restarted, AnyConnect should show the profile IOS IKEV2 LOCAL USER in the drop-down. After you click Connect, enter the username vpnuser and the password cisco123, the VPN connection should be successful, as shown in Figure 9-20.

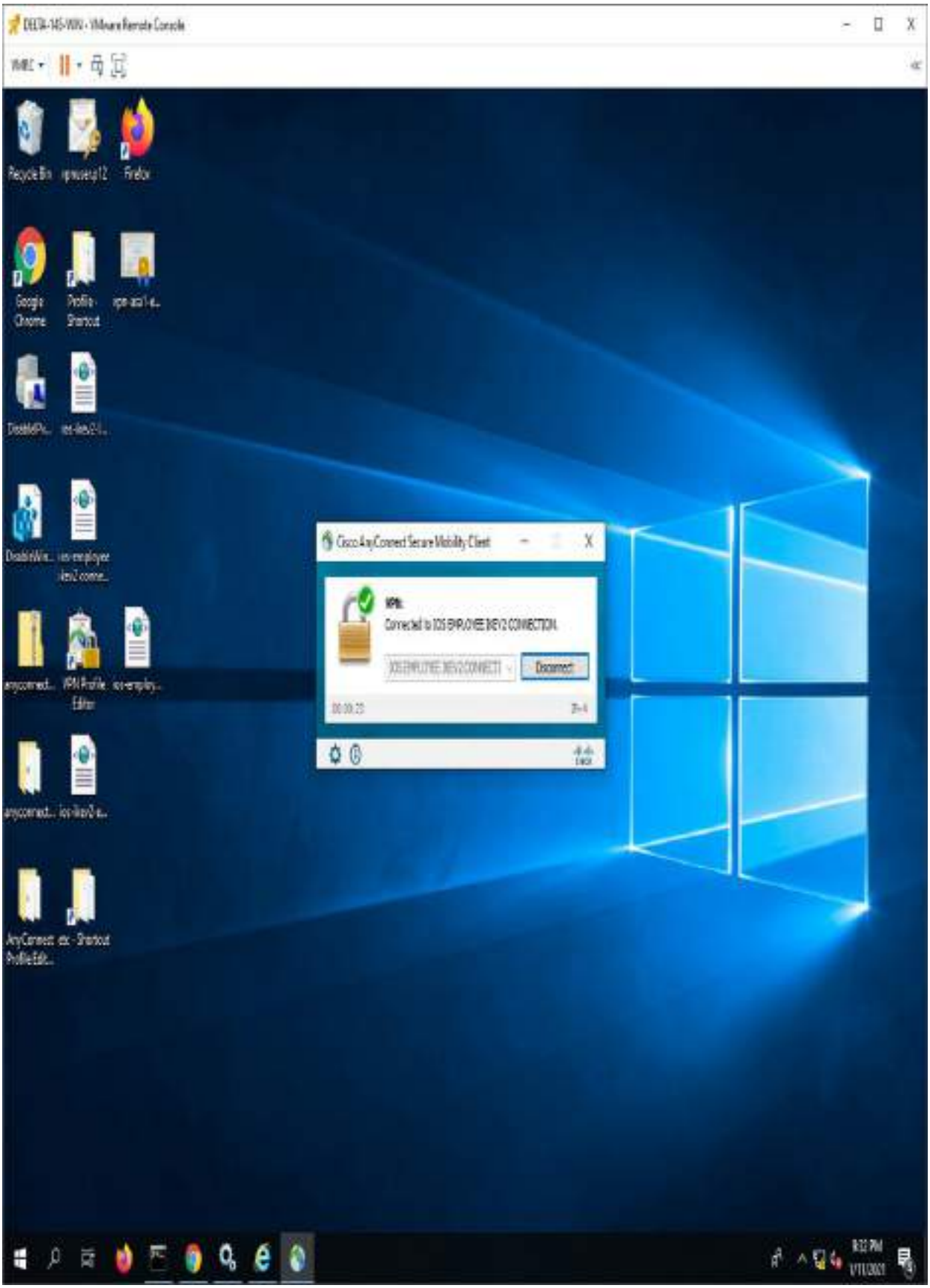

DELTA-145-WIN - VMware Remote Console
Recycle Bin
Firefox
Google Chrome
Cisco AnyConnect Secure Mobility Client
VPN:
Disconnect
Firefox
Google Chrome

Figure 9-20 Successful AnyConnect IKEv2 Connection to a Cisco Router

Configuring Split Tunneling

By default, AnyConnect provides a full tunnel connection; all traffic, regardless of destination, is sent across the tunnel. You can modify this behavior by configuring a split tunnel list to only tunnel specific traffic across the tunnel. An example of this is shown in Example 9-29, which involves the configuration of two items:

- A standard access list named SPLIT_TUNNEL_ACL is created via the **ip access-list standard** command. You add a permit access control entry (ACE) for the subnet 172.20.1.0/24 via the **permit** command. Note the wildcard mask.
- Within the EMPLOYEES IKEv2 authorization policy you previously configured, you add SPLIT_TUNNEL_ACL via the **route set access-list** command.

Example 9-29 Configuring Split Tunneling

```
VPN-ROUTER(config)# ip access-list extended SPLIT_TUNNEL_ACL
VPN-ROUTER(config-std-nacl)# permit 172.20.1.0 0.0.0.255
VPN-ROUTER(config-std-nacl)#
VPN-ROUTER(config-std-nacl)# crypto ikev2 authorization policy
EMPLOYEES
VPN-ROUTER(config-ikev2-author-policy)# route set access-list
SPLIT_TUNNEL_ACL
```

With this configuration, future connections to the VPN headend will only tunnel traffic destined to the subnet 172.20.1.0/24, and all other traffic will use the default gateway of the local PC.

That wraps up our last configuration example. Make sure you understand all three versions of AnyConnect VPN technology deployments covered in this chapter. Once you master this and the previous clientless VPN concepts you are ready to move into the last chapter, which is troubleshooting all remote access VPN concepts.

Summary

This chapter provides an overview of the AnyConnect SSLVPN functionality on the ASA, including both basic configuration and more advanced configuration. This chapter also covers AnyConnect IKEv2-based VPNs on ASA and introduces the AnyConnect profile editor. Finally, this chapter also discusses how to deploy AnyConnect IKEv2-based VPNs on IOS. You will need to know all three of these versions of AnyConnect deployments for the SVPN exam. All are also widely used by organizations around the world.

AnyConnect is one of the most widely deployed software applications and is a critical topic to know for the SVPN 300-730 exam. Make sure you know how to configure AnyConnect both from the command line and using ASDM as both methods are sure to come up on the exam. This includes understanding what could go wrong with a deployment, because troubleshooting is a large part of the SVPN exam. The next chapter brings together concepts from both this and the last chapter with a focus on troubleshooting. You must first understand how things work before you can learn how to fix them. We highly recommend you master the concepts of both Chapter 8 and Chapter 9 before moving into Chapter 10.

We want to remind you that although this book focuses on the VPN benefits of AnyConnect, AnyConnect is more than a VPN client. You will get a taste of some of these additional benefits in Chapter 10, "Troubleshooting Remote Access VPNs." You can also learn more about the full power of AnyConnect by visiting the Cisco AnyConnect Mobility Client web page. VPN is also a huge part of the industry movement toward cloud-based security commonly called Secure Access Service Edge or SASE (pronounced *sassy*). SASE will not be on the current version of the SVPN but it is a topic we highly recommend you become familiar with because it is the future of cybersecurity.

References

ASDM Book 3: Cisco ASA Series VPN ASDM Configuration Guide, 7.14. Retrieved from https://www.cisco.com/c/en/us/td/docs/security/asa/asa

914/asdm714/vpn/asdm-714-vpn-config.html

CLI Book 3: Cisco ASA Series VPN CLI Configuration Guide, 9.14. Retrieved from https://www.cisco.com/c/en/us/td/docs/security/asa/asa914/configuration/vpn/asa-914-vpn-config.html

FlexVPN: AnyConnect IKEv2 Remote Access with Local User Database. Retrieved from https://www.cisco.com/c/en/us/support/docs/security/flexvpn/200555-FlexVPN-AnyConnect-IKEv2-Remote-Access.html

Exam Preparation Tasks

As mentioned in the section "How to Use This Book" in the Introduction, you have a couple of choices for exam preparation: the exercises here, Chapter 11, "Final Preparation," and the exam simulation questions in the Pearson Test Prep software online.

Review All Key Topics

Review the most important topics in the chapter, noted with the key topics icon in the outer margin of the page. Table 9-7 lists these key topics and the page number on which each is found.

Table 9-7 Key Topics for Chapter 9

Key Topic Element	Description	Page
Paragraph	SSLVPN verse IKEv2	
List	Basic SSLVPN AnyConnect Configuration Summary	
Table 9-2	Group Policy Attributes for AnyConnect VPNs	
List	Configuring An AnyConnect Connection Profile Summary	
Table 9-3	Connection Profile General Attributes for AnyConnect VPNs	
Table 9-4	Connection Profile General Attributes for AnyConnect VPNs	
List	User Authentication Options	
List	Configure DNS and WINS via ASDM	
List	Two types of Split tunneling	
List	Steps to create a traffic filter using ASDM	
List	Steps to configure IPsec IKEv2 using CLI	
Table 9-5	Storage Locations for AnyConnect Client Profiles	
List	Steps to configure AnyConnect IKEv2 remote access on a	
	Cisco Router	
List	Steps to install a certificate from an external CA	
List	Disabling HTTP and HTTPS servers on a router	

Complete Tables and Lists from Memory

Print a copy of Appendix C, "Memory Tables" (found on the companion website), 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 companion website), includes completed tables and lists to check your work.

Define Key Terms

There are no key terms for this chapter

Use the Command References to Check Your Memory

Tables 9-8 and 9-9 list the important commands from this chapter. To test your memory, cover the right side of the table with a piece of paper, read the description on the left side, then see how much of the command you can remember.

Table 9-8 Command Reference on ASA

Task	Command Syntax
Create and manage group URLs for tunnel groups. When configured, the appropriate tunnel group is automatically selected for the user.	**group-url** *<name>* **[enable|disable]**
Define AAA server group.	**aaa-server** *<group tag>* **protocol** *<protocol>* and **aaa-server** *<group tag>* **<(if_name)> host** *<ip_address>*
Specify the name of the authentication server group.	**authentication-server-group [(interface id)]** *<server group>* **[LOCAL]**
Define a local address pool.	**ip local pool** *<poolname>* *<ip1>* **[-***<ip2>***] [mask** *<netmask>***]**
Specify a space-separated list of up to six local address pools from which to request addresses.	**address-pools** *<pool1>* **[***<pool2>...<pool6>***]**
Configure the primary and secondary DNS servers.	**dns-server value** *<ip_address>* **[***<ip_address>***]**
Configure the default domain name given to users of this group.	**default-domain value** *<domain name>*
Select the split tunneling method to be used by the remote client.	**split-tunnel-policy** *<policy>*
Configure a standard or extended access list for split tunnel configuration.	**split-tunnel-network-list value** *<access-list>*
Enter the name of a user-specific ACL to filter VPN traffic.	**vpn-filter value** *<ACL name>*
Enable IKEv2 on the specified interface.	**crypto ikev2 enable** *<(if_name)>* **[client-services] [port** *<port>***]**

Table 9-9 Command Reference on IOS

Set authentication, authorization, and accounting (AAA) authentication at login.	**aaa authentication login {default |** *<list-name>* **| method1 [method2 . . .]**
Set the parameters that restrict user access to a network.	**aaa authorization {auth-proxy | cache | commands level | config-commands | configuration | console | exec | ipmobile | multicast | network | policy-if | prepaid | radius-proxy | reverse-access | subscriber-service | template} {default |** *<list-name>***} [method1 [method2 . . .]]**
Configure a group of local IP address pools, give this group a name, and specify a cache size.	**ip local pool {default |** *<poolname>* **} {low-ip-address [high-ip-address] [group** *<group-name>* **] [cache-size** *size* **]]**
Configure an IKEv2 authorization policy.	**crypto ikev2 authorization policy** *policy-name*
Define a local pool address.	**[ipv6]** *pool name*
Specify the subnet mask to be used by the client for local connectivity.	**netmask** *mask*
Specify the primary and secondary Domain Name Service (DNS) servers.	**dns primary-server [***secondary-server***]**
Configure an IKEv2 profile.	**crypto ikev2 profile** *profile-name*
Match a profile on frontdoor VPN routing and forwarding (FVRF) or local parameters, such as the IP address, the peer identity, or the peer certificate.	**match { address local {** *<ipv4-address>* **|** *<ipv6-address>* **|** *<interface name>* **} | certificate certificate-map | fvrf {** *<fvrf-name>* **| any } | identity remote address {** *<ipv4-address>* **[***<mask>***] | ipv6-address-prefix } | email [***domain***] string | fqdn [***domain***] string | key-id opaque-string | any }**
Specify the local and remote authentication methods in an IKEv2 profile.	**authentication {local {rsa-sig | pre-share [key** *<password>***] | ecdsa-sig | eap | [gtc | md5 | mschapv2 | [username** *<username>***] | [password** *<password>***]]] | remote [eap [query-identity | timeout seconds] | rsa-sig | pre-share [key** *<password>***] | ecdsa-sig]}**
Specify the trustpoints that are used with the RSA signature authentication method.	**pki trust-point trustpoint-name [sign | verify]**
Enable AAA accounting method lists when the IKEv2 remote authentication method is AnyConnect EAP.	**aaa accounting anyconnect-eap** *<list-name>*
Specify the AAA authorization for a local or external group policy.	**aaa authorization {group [override] {cert | eap | psk} | user {cert list | eap {cached | list} | psk {cached | list}} {aaa-listname | [aaa-username | [local] | name-mangler** *<mangler-name>***] | [password** *password***]}]**
Configure an IKEv2 profile with a virtual template to be used for cloning the virtual access interfaces.	**virtual-template** *<template-number>* **mode auto**
Enable a profile for AnyConnect profile download.	**anyconnect profile** *<name>*
Create a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces.	**interface virtual-template** *<number>*
Enable IP processing on an interface without assigning an explicit IP address to the interface.	**ip unnumbered type number [poll]**
Set the encapsulation mode for the tunnel interface.	**tunnel mode { aurp | auto | cayman | dvmrp | eon | gre | gre multipoint | gre ip | gre ipv6 | ipip [decapsulate-any] | ipsec ipv4 | iptalk | ipv6 | ipsec ipv6 | mpls | nos | rbscp]**
Associate a tunnel interface with an IPsec profile.	**tunnel protection ipsec profile** *<name>* **[shared | { isakmp-profile | ikev2-profile }** *<name>***]**
Install a Cisco Secure Desktop (CSD) or Cisco AnyConnect VPN client package file on an SSLVPN gateway for distribution to end users.	**crypto vpn { anyconnect file** *<name>* **sequence** *<sequence-number>* **| profile** *<profile-name>* **device ifile** *<name>* **| csd file** *<name>* **}**

Chapter 10. Troubleshooting Remote Access VPNs

This chapter covers the following topics:

- **Troubleshooting Clientless SSLVPNs on the ASA:** This section explores the key steps involved in troubleshooting a Cisco clientless SSLVPN deployment on the ASA, including SSL errors and conditional debugging techniques.
- **Troubleshooting AnyConnect SSLVPNs on the ASA:** This section steps through various Cisco commands for troubleshooting an AnyConnect SSL deployment on an ASA.
- **Troubleshooting AnyConnect IKEv2 VPNs on the ASA:** This section examines the unique issues related to an IKEv2 VPN deployment and how the troubleshooting process occurs.
- **Troubleshooting AnyConnect IKEv2 VPNs on Routers:** This section discusses how to troubleshoot an IKEv2 configuration on a router platform.

"Giving up is the only sure way to fail."

—Gena Showalter

This chapter covers the following exam objectives:

- 3.0 Troubleshooting using ASDM and CLI
  - 3.4 Troubleshooting AnyConnect IKEv2 on ASA and routers
  - 3.5 Troubleshooting SSLVPN and Clientless SSLVPN on ASA
- 4.0 Secure Communications Architectures
  - 4.4 Recognize VPN technology based on configuration output for remote access VPN solutions

Mastering troubleshooting of clientless and AnyConnect VPNs takes practice. Practice means making mistakes, learning from mistakes, and being able to recognize when a mistake is being made. We believe you don't truly understand a topic until you not only can make it work but also know why it won't work. Troubleshooting is a very powerful way to validate that you know a topic such as VPNs, and troubleshooting will come up many times on the SVPN 300-730 exam. Do not overlook this chapter and do not be afraid to fail.

This chapter examines how to troubleshoot the features and critical configuration components used for different VPN solutions covered in previous chapters of this book. It uses a strategy that works across different aspects of a VPN to help you narrow down problems to a specific area of troubleshooting. It is a quick and streamlined troubleshooting strategy. Our goal for this troubleshooting strategy is to help you quickly eliminate obvious wrong answers on the SVPN 300-730 exam by isolating potential correct answers to specific troubleshooting focus domains.

Keep in mind that troubleshooting VPN technology requires knowledge of how the technology works. If you lack knowledge from previous chapters and don't understand what you are trying to fix, you will most likely find troubleshooting very difficult. For this reason, we highly recommend you first mastering all previous chapters before taking on this last chapter. We see this chapter as a good resource for validating what you have learned by reading this book. The focus will be on troubleshooting remote access VPN technology however most concepts can apply to troubleshooting any form of VPN technology as well.

The SVPN 300-730 exam will challenge you on your ability to recognize common issues. In some cases, the exam will provide a handful of options to choose from. In other cases, it will ask you which packet contains specific information, such as negotiation traffic, that you can use for troubleshooting. The exam might also ask you which command generates particular output or what output results from particular commands. The exam might present a scenario where something isn't working along with code output that you need to use to determine why the VPN isn't working.

We highly recommend studying troubleshooting by getting hands-on

experience. You must become familiar with what commands, protocols, and technologies do what when used. Do not attempt to memorize a few troubleshooting steps and assume that you have troubleshooting covered. Doing so will likely lead to lost points on the exam and will also not be helpful when you're troubleshooting real VPN deployments.

"Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz enables you to assess whether you should read the entire chapter. If you miss no more than one of these self-assessment questions, you might want to move ahead to the "Exam Preparation Tasks" section of the chapter. Table 10-1 lists the major headings in this chapter and the "Do I Know This Already?" quiz questions related to the material in each of those sections to help you assess your knowledge of these specific areas. The answers to the "Do I Know This Already?" quiz appear in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes."

Table 10-1 "Do I Know This Already?" Foundation Topics Section-to-Question Mapping

Foundation Topics Section	Questions
Troubleshooting Clientless SSLVPNs on the ASA	2, 3, 7
Troubleshooting AnyConnect SSLVPNs on the ASA	1, 4, 5, 8
Troubleshooting AnyConnect IKEv2 VPNs on the ASA	6, 10
Troubleshooting AnyConnect IKEv2 VPNs on Routers	9

1. You are the administrator for a VPN deployment. You have received a ticket saying that a user can't connect to the VPN. You find that the VPN is working fine, but no more users are able to connect. You verify this by using the **show vpn-sessiondb** command and see that there is room for more users. Which of the following could be causing this problem?

a. The group profile has been misconfigured and is limiting the number of VPN users.

b. The local address pool has been exhausted.

c. There isn't a version of AnyConnect available for the version of the operating system that is trying to connect to the VPN.

d. The ASA is out of memory and can't support the load of another VPN session.

2. Which feature needs to be enabled to support smart tunnel functionality?

a. Java or ActiveX browser support must be enabled.

b. The client must have a proxy configured.

c. Applications can only be UDP based.

d. A smart tunnel hash is mandatory.

3. If clientless VPN bookmarks are grayed out and not working, what is the most likely issue?

a. WebACL is denying access.

b. There is a DNS resolution problem.

c. AAA authorization is not working.

d. The bookmark is missing URL information.

4. When using an XML profile on an ASA, what must match the connection profile?

a. UserGroup

b. HostName

c. HostAddress

d. All of the above

5. What ASA configuration sends all DNS through the SSLVPN tunnel?

a. split-tunnel-dns enable

b. dns tunnel enable

c. dns tunnel full enable

d. split-tunnel-all-dns enabled

6. Which command includes details about data counts, SPI details, and child and parent SA status?

a. show vpn-sessiondb detail anyconnect

b. show run

c. show crypto ikev2 sa

d. show crypto ikev2 sa detail

7. Which method will *not* help you determine whether the ASA WebVPN service is running?

a. Run the **show vpn sessiondb** command.

b. Run the **show ipsec crypto sa** command.

c. View the client TLS event under **Monitoring** > **Logging** > **Real-time Log Viewer** > **View**.

d. Use the **show logging** command with logging buffered enabled.

8. Which statement about DfltGrpPolicy is correct?

a. DfltGrpPolicy does not allow any policies by default.

b. DfltGrpPolicy allows administrator SSLVPN client connections by default.

c. DfltGrpPolicy allows all SSLVPN client connections by default.

d. DfltGrpPolicy does not allow SSLVPN client connections by default

9. Which command does not work on a Cisco router for viewing VPN details?

a. debug crypto ikev2

b. show crypto session detail

c. show webvpn anyconnect

d. debug aaa authentication

10. Which ASA VPN **show** command shows the most details regarding a live VPN session?

a. show vpn-sessiondb detail anyconnect

b. show vpn-sessiondb

c. debug vpn-sessiondb

d. show running-configuration

Foundation Topics

Welcome to the final chapter, which focuses on troubleshooting remote access based VPN deployments. As you read through this chapter, we highly recommend keeping a notepad available. Any time you run into a concept you do not recognize, add it to that notepad as something you will need to master before you attempt to troubleshoot it. Troubleshooting is about making things work properly. If you don't understand how things work, you will have trouble fixing them.

The SVPN 300-730 exam will challenge you on all aspects of troubleshooting. You will have to validate your understanding of how components work, including what could cause something to break. For example, the exam will show you ASA **debug** output and ask you to determine what is not working or why something is not working. Any type of troubleshooting topic—from reviewing code to being told about a user experience that is not working—is fair game for the SVPN 300-730 exam. The exam will even expect you to understand how to perform end-to-end troubleshooting of real-world VPN deployments. Know that version 1.1 has 35% of the exam dedicated to troubleshooting questions!

It's hard to give a firm answer but having hands-on experience is extremely helpful in confirming your understanding of troubleshooting concepts. This chapter works through some of the most common troubleshooting situations we find with our customers as well as situations that are likely to come up on

the SVPN 300-730 exam. Consider your ability to troubleshoot as a way to validate that you understand everything you have learned in this book. If you don't understand any troubleshooting topics covered in this chapter, you should go back to the appropriate earlier chapter and review how things should function before proceeding.

Troubleshooting Clientless SSLVPNs on the ASA

This section takes a step-by-step approach to troubleshooting SSLVPNs. Some of these steps apply to troubleshooting any type of VPN, and other steps are specific to SSLVPNs. The good news about troubleshooting clientless SSLVPNs is that it will likely seem easier than troubleshooting other types of remote connectivity solutions. Clientless SSLVPN technology doesn't require as many deployment and troubleshooting steps as client VPN deployments. Pay attention to all of the steps and topics in this section; the following sections do not repeat steps that are identical for troubleshooting other topics within this chapter.

Troubleshooting Categories

When troubleshooting SSLVPNs on an ASA, we recommend breaking down the troubleshooting into the following areas:

Step 1. Connectivity: Validate that the client system can reach the ASA.

- Enabled interfaces
- Certificate configuration
- Group URL/alias

Step 2. Login: Troubleshoot any login issues, including validating that the proper connection profile is selected and that the user is able to pass all authentication and authorization steps.

- Connection profile selection
- Authentication
- Authorization
- Group policy selection

Step 3. Web page services: Troubleshoot problems associated with the clientless web page services. The focus in this section is on DNS, plug-ins, and bookmarks.

- DNS configuration on the ASA
- ASA plug-ins
- Bookmarks

Step 4. Application access: Troubleshoot issues related to accessing the application.

- ASA-to-application connectivity
- URL rewrite failures
- Application for port forwarding (needs to point to 127.0.0.1:<*port*>)
- Application for smart tunneling (wrong SHA-256 or application in the configuration)

During the clientless SSLVPN troubleshooting process, you should step through these four areas to identify where you need to focus your attention. This is a similar approach to troubleshooting the creation of software in the sense that you need to isolate any issue into focus areas so that you can validate and eliminate possible problems as you perform troubleshooting. For example, if a user is unable to log in to a clientless VPN solution, you know your problem falls into the login area, which can be either an authentication, authorization, or group selection problem. Login challenges have three technology components that could be the source of the issue, and you would test each component to further narrow down the problem. Similar logic can be applied as you evaluate sample code or provided troubleshooting

situations on the SVPN 300-730 exam; narrowing down the issue can help you quickly eliminate wrong answers. If one answer speaks about URL rewrite failures, that would fall under application access, which has nothing to do with authentication, authorization, or group selection, so it would be easy to drop that as a possible answer for a login failure question. Keep this strategy in mind as you work through this chapter.

These four troubleshooting areas just listed cover most issues related to resolving problems with clientless VPNs on a Cisco ASA, but other issues can exist as well. The Cisco SVPN 300-730 exam blueprint calls out "the need to be able to troubleshoot clientless SSL VPNs on an ASA" and does not specify further details about what is in and out of scope for this topic. Therefore, any configuration related to clientless VPNs could potentially appear on the exam. We highly recommend that you configure your own ASA clientless VPNs solution and work with it until you understand the how the configuration works.

Step 0: SSLVPN Components

Before beginning any troubleshooting, you need to perform *step zero*, which involves validating the architecture and components. You must understand what you are working with before you take any actions. For clientless VPN technology, there is no VPN client. Hence, the components involve some system attempting to connect to a private network by accessing the ASA. The ASA will authenticate and authorize access, leading to a secure tunnel being established between the ASA and the client. Most organizations use a third-party authentication solution, such as an Active Directory server. The ASA may also host different services, such as, bookmarks or plug-ins. Figure 10-1 shows a basic diagram of the core components you will be troubleshooting in this section.

Figure 10-1 Basic Clientless ASA VPN Design

It's a great idea to place a simplified version of the architecture in your mind before thinking about how to fix it. Using this approach can help in an exam by enabling you to quickly eliminate any answer involving technology components that are not part of the design spoken about in the question. You can use a similar approach with protocols. Mapping how the technology works in your mind using a simple architecture can help you weed out the obviously wrong answers.

Step 1: Connectivity Troubleshooting

Any troubleshooting action must start with connectivity. Please remember this when dealing with any technology troubleshooting you encounter throughout your time on this planet. Seriously, anything from why your TV is not working to why some security product is not working must have its general connectivity evaluated first when things are not working. People spend countless hours troubleshooting something that is not working and eventually realize that the failure is due to the system not being powered on or a cable being unplugged. We know of a case in which administrators and service providers spent hours troubleshooting a customer's VPN, only to later find out the headend was unplugged by accident by the local cleaning crew during a late-night cleaning service. You can also think about this in technical terms: Validate Layer 1 before troubleshooting anything else.

Troubleshooting Questions

When troubleshooting connectivity, we recommend starting with basic questions such as these:

- Are the devices powered on?
- Are the cables plugged in?
- Have any security tools been put in place or changed that could prevent connectivity?
- Has anything in the environment changed that could impact connectivity?
- Have there been any recent thunderstorms or reported network outages?
- Has the service provider acknowledged that services are running normally?
- Has anything else occurred that could impact the system?

The most common troubleshooting technique for connectivity is sending a ping between systems that are supposed to be connected. If the ping fails and things worked in the past, the answer to any of the previous questions could identify the reason for the failure. The SVPN 300-730 exam will likely not test you on cables failing or systems being powered off, but real-world deployments will have these issues, and overlooking troubleshooting related to these basic connectivity problems can to countless hours wasted on more advanced troubleshooting techniques. We don’t cover basic connectivity troubleshooting details again in this chapter, but you should keep in mind that this is always the first step, regardless of the VPN—or other technology—being tested.

Exam-Focused Connectivity Troubleshooting

The connectivity troubleshooting you will encounter on the SVPN 300-730 exam will likely include failures in protocols or things that can be configured within the client or ASA rather than a cable being unplugged. For the exam, you can typically assume that power and cable issues are not the problem; the

exam is more likely to test you on configuration problems. For example, the VPN user might be able to reach the ASA, but the ASA does not have a certificate or group configured correctly, and thus the user has basic connectivity issues. In this case, as with basic connectivity testing, you would start by sending a ping to the outside IP address interface. Additional steps for connectivity troubleshooting include validating that the interfaces of all used connections are up, pinging from the client side, interviewing the client for details regarding the issue they are seeing, and validating that the Cisco ASA can ping the next hop router or an IP address hosted on the Internet. Finally, you should also check licensing as it is possible that you have run into a situation where the permitted user count is oversubscribed.

Note

If more than two users attempt to access an ASA without the necessary additional licenses, users receive error messages and are unable to log in. This may occur if either AnyConnect or clientless users have used up the licenses. To troubleshoot licenses, you can use the command **show vpn-sessiondb license-summary**, which provides the information needed to validate whether you have enough licenses to support your VPN environment. Figure 10-2 shows an example of using this command to view the available licenses on a Cisco ASAv.

```
ASAv# show vpn-sessiondb license-summary
----------------------------------------------------------------------------
VPN Licenses and Configured Limits Summary
----------------------------------------------------------------------------
                                  Status : Capacity : Installed :  Limit
                                 ----------------------------------------
AnyConnect Premium               :  ENABLED :      250 :       250 :   NONE
AnyConnect Essentials            : DISABLED :      250 :         0 :   NONE
Other VPN (Available by Default) :  ENABLED :      250 :       250 :   NONE
Shared License Server            : DISABLED
Shared License Participant       : DISABLED
AnyConnect for Mobile            :  ENABLED(Requires Premium or Essentials)
Advanced Endpoint Assessment     :  ENABLED(Requires Premium)
AnyConnect for Cisco VPN Phone   :  ENABLED
VPN-3DES-AES                     :  ENABLED
VPN-DES                          :  ENABLED
----------------------------------------------------------------------------


----------------------------------------------------------------------------
VPN Licenses Usage Summary
----------------------------------------------------------------------------
                       Local : Shared :   All   :   Peak :  Eff.   :
                      In Use : In Use : In Use : In Use :  Limit  : Usage
                     ---------------------------------------------------
AnyConnect Premium   :      0 :      0 :      0 :      1 :    250 :    0%
  AnyConnect Client  :                :      0 :      0           :    0%
    AnyConnect Mobile:                :      0 :      0           :    0%
  Clientless VPN     :                :      0 :      1           :    0%
  Generic IKEv2 Client :             :      0 :      0           :    0%
Other VPN            :                :      0 :      0 :    250 :    0%
  Cisco VPN Client   :                :      0 :      0           :    0%
  L2TP Clients
  Site-to-Site VPN   :                :      0 :      0           :    0%
----------------------------------------------------------------------------

ASAv#
```

Figure 10-2 show vpn-sessiondb license-summary Example

Note

You will see many versions of the **show vpn-sessiondb** command in this chapter. We highly recommend that you become familiar with how this command and its options work because it is one of the most common command-line troubleshooting commands used for evaluating VPNs.

ASA WebVPN Service

After you validate connectivity by using **ping** and preforming other basic connectivity testing, you should determine whether the ASA *WebVPN* service is running. Because the ASA is listening on the outside interface for the inbound 443 request, you must determine whether that service is functioning. If it is not functioning, users will not be able to connect to the ASA and will receive a connection failure error. We recommend checking whether a service such as WebVPN is running after performing basic connectivity for all VPN troubleshooting.

You need to check the ASA configuration to ensure that the WebVPN service is up and that it is not configured for another port. An easy way to do this is by using the ASDM monitor page or from the CLI, using the **show run webvpn** command, as shown in Figure 10-3. Two other options are the commands **show vpn-sessiondb** and **show asp table socket**. When a client connects to the ASA, in ASDM, you can see client TLS events under **Monitoring** > **Logging** > **Real-time Log Viewer** > **View**. With logging to the internal buffer enabled (via the command **logging buffered** *severity_level*), you can also see the same output when using the command **show logging**. Be sure to be familiar with all of these options for the SVPN 300-730 exam.

```
ASAv# show run webvpn
webvpn
 enable outside
 hostscan image disk0:/hostscan_3.1.07021-k9.pkg
 hostscan enable
 anyconnect image disk0:/anyconnect-win-4.5.04029-webdeploy-k9.pkg 1
 anyconnect profiles DCLOUD-AMP-PROFILE disk0:/dcloud-amp-profile.asp
 anyconnect profiles DCLOUD-ANYCONNECT-PROFILE disk0:/dcloud-anyconnect-profile.xml
 anyconnect profiles DCLOUD-ISE-POSTURE-PROFILE disk0:/dcloud-ise-posture-profile.isp
 anyconnect enable
 smart-tunnel list CONTRACTOR-SMART-TUNNEL RDP_Client mstsc.exe platform windows
 smart-tunnel list CONTRACTOR-SMART-TUNNEL PuTTY putty.exe platform windows
 smart-tunnel list DCLOUD-SMART-TUNNEL RDP_Client mstsc.exe platform windows
 smart-tunnel list DCLOUD-SMART-TUNNEL PuTTY putty.exe platform windows
 cache
  disable
 error-recovery disable
ASAv#
```

Figure 10-3 show run webvpn Example

Troubleshooting Certificates

One reason users may have connectivity issues could be the certificate configuration. A common issue is that a certificate has expired or been revoked. Besides these obvious certificate issues, the certificate problem could be related to how the certificate was configured. You need to make sure that a certificate is signed and that the certificate's common name is the fully qualified domain name (FQDN) used by users to connect to the ASA. You need to validate that the signed certificate is imported into the ASA. Chapter 9, "AnyConnect VPNs on the ASA and IOS," provides an example of using the **crypto ca import** command to import a base-64-encoded certificate. During installation of the signed certificate, the ASA provides output informing you of the FQDN used by the certificate. A mismatch between the FQDN and what users use to connect to the ASA can cause connectivity issues. Be sure to verify that the ASA FQDN is the same as on the certificate. We have run into this issue a handful of times when new VPNs are being set up in customer environments.

Applied Certificates

Another issue to check is whether the certificate is applied to the interface used to terminate the SSLVPN. Using the command **ssl trust-point** from the command line applies the certificate to the correct interface. If this is not done, the proper certificate won't be used when a VPN is established, and this can lead to connectivity issues. This same issue can lead to inbound VPN user connections receiving a certificate warning. This warning could mean that either a self-signed certificate was applied to the interface or, during the installation, something failed; for example, the proper certificate might not have been applied to the interface.

Full Certificate Chain

One final certificate validation is verifying that the full certificate chain is loaded on the ASA. A certificate can be installed on an ASA using either the command line or ASDM. The command for installing a certificate is **crypto ca authenticate ssl-trustpoint**, and you can install an SSL certificate in ASDM by going to **Configuration** > **Remote Access VPN** > **Advanced** > **SSL Settings**. A PKCS12 certificate can also be used. Regardless of what certificate is used, the entire certificate chain must be copied, or you will run into problems. You can verify the installed certificates in ASDM by going to **Configuration** > **Remote Access VPN** > **Certificate Management**, or you can use the command line to run the command **show crypto ca certificate**.

Correct Certificate

The next step in troubleshooting certificates is to verify that the proper certificate is being used by the hosts attempting to connect to the VPN. To do this, first connect to the WebVPN through a web browser using https:// followed by the FQDN. After you request the certificate, double-click the lock icon that appears in the lower-right corner of the WebVPN login page to bring up the installed certificate information.

Certificate Debug Commands

If you believe you have a potential certificate failure, you can run either

debug crypto ca 255, **debug crypto ca message 255**, or **debug crypto ca transaction 255** to view details about the potential failure. One example of a common problem is the error message “Untrusted certificate warning when using a valid third-party SSL certificate on the external interface.” This error can occur when an RSA key pair is used with the certificate. By default, ASA software version 4(1) and onward have all ECDSA and RSA ciphers enabled by default, and the strongest cipher (usually an ECDSA cipher) is used for negotiation. This could cause the ASA to present a self-signed certificate instead of the currently configured RSA-based certificate, and you would see this in the debug output. A fix for this specific problem is to disable ECDSA ciphers and test.

Note

Make sure to review the certificate configuration before moving on to other troubleshooting tasks. We have run into many live deployments that have tickets due to expired certificates.

The capture Command

The last suggestion for troubleshooting connectivity is to use the **capture** command on the ASA. The **capture** command creates a .zip file encrypted with the password koleso that includes HTML contents of clientless web pages that the client accesses. This is useful for troubleshooting websites that do not display properly without having to access the user’s host system. The syntax for this command is **capture** *webvpn-issue* **type webvpn user** *user*. For this example, the output name of the **capture** command is *webvpn-issue*, and it is located in the default capture directory on the ASA by name.

Note

Many engineers start with a **capture** command, but keep in mind our recommendation regarding the troubleshooting flow. Don’t waste time diving right into evaluating performance when a Layer 1 problem may exist.

Connectivity Troubleshooting Summary

The following are the key concepts for troubleshooting connectivity problems:

- Always start by troubleshooting basic connectivity possibilities, including power and cabling.
- The simplest way to validate connectivity is by using **ping**.
- Validate VPN licenses by using the **show vpn-sessiondb license-summary** command.
- Validate that the ASA WebVPN service is running on the ASA by using the command **show run webvpn** or using the ASA GUI.
- Validate that the entire certificate chain is imported into the ASA, and ensure that it has a FQDN and the certificate is properly applied to the correct interface.
- To get a general view of connectivity, use the **capture webvpn-issue type webvpn user user1** command.

Step 2: Login Troubleshooting

If the user is able to reach the HTML landing page for the ASA, you know that connectivity works. The next area of troubleshooting focuses on the user logging in to the VPN. A user who can’t log in to the VPN will likely see an error or failure message indicating that there is an issue with group selection, authentication, or authorization. In such a case, you must determine why the user is unable to log in after successfully connecting to the landing page. Troubleshooting the login process for an SSLVPN can be broken down into a few areas: connection profile selection, group URL, authentication, and authorization.

Note

The login troubleshooting steps described here can be applied to any form of VPN. For this reason, we do not repeat many of these steps for troubleshooting other topics in this chapter.

Connection Profile Group URL

A group URL can be defined under a connection profile. Using a group URL enables the remote client to automatically select a connection profile, simplifying the process of remote users connecting to the VPN. This is different from the alias concept, but URLs and aliases can use the same names. An example of a group URL would be https://ciscoasa.example.com/clientless. This would take the user directly to a WebVPN login page for that specific connection profile. The use of a connection profile URL with an FQDN requires the appropriate name to be defined in DNS for users to reach it. You need to look at this first when troubleshooting a group URL. You must validate that the URL is a FQDN that users can reach by using **ping** or **nslookup**. You also must validate that users are going to the correct URL by asking them for the specific URL they are attempting to access. Any of these issues would lead to a URL not working.

Say that you configured your ASA to support a URL address for a group of contractors, and you provide those contractors a customized URL for their web VPN access needs. You inform the contractors to log in to their customized web portal by using the URL https://vpn-asa1.example.com/contractor. (We cover how to build this type of setup in Chapter 9, and you need to understand this configuration because the SVPN 300-730 exam might question you on both building and troubleshooting an SSLVPN leveraging a customized group URL.) If the wrong URL is provided to the VPN user, or if the user isn't authorized to use that connection profile, the user might be unable to access the VPN. As part of troubleshooting, you would need to ask for the URL that was used and where the contractor was connecting from. You need to test the URL and might also need to access the network used by the contractor to validate that you can access the URL from the user's point of view. (If you need to test connectivity from the user side, see the connectivity steps described earlier in

this chapter.)

Viewing Group URLs

To view the group URLs configured for a particular connection profile, open the connection profile and navigate to **Advanced** > **Group Alias/Group URL**. Figure 10-4 shows an example of group URLs configurated for the EMPLOYEE_CONNECTION connection profile. Notice the three different capitalizations of employees: EMPLOYEES, Employees, and employees. The URL is case sensitive, and so the three most common capitalizations of employees were used to ensure a more consistent user experience if users enter the URL manually.

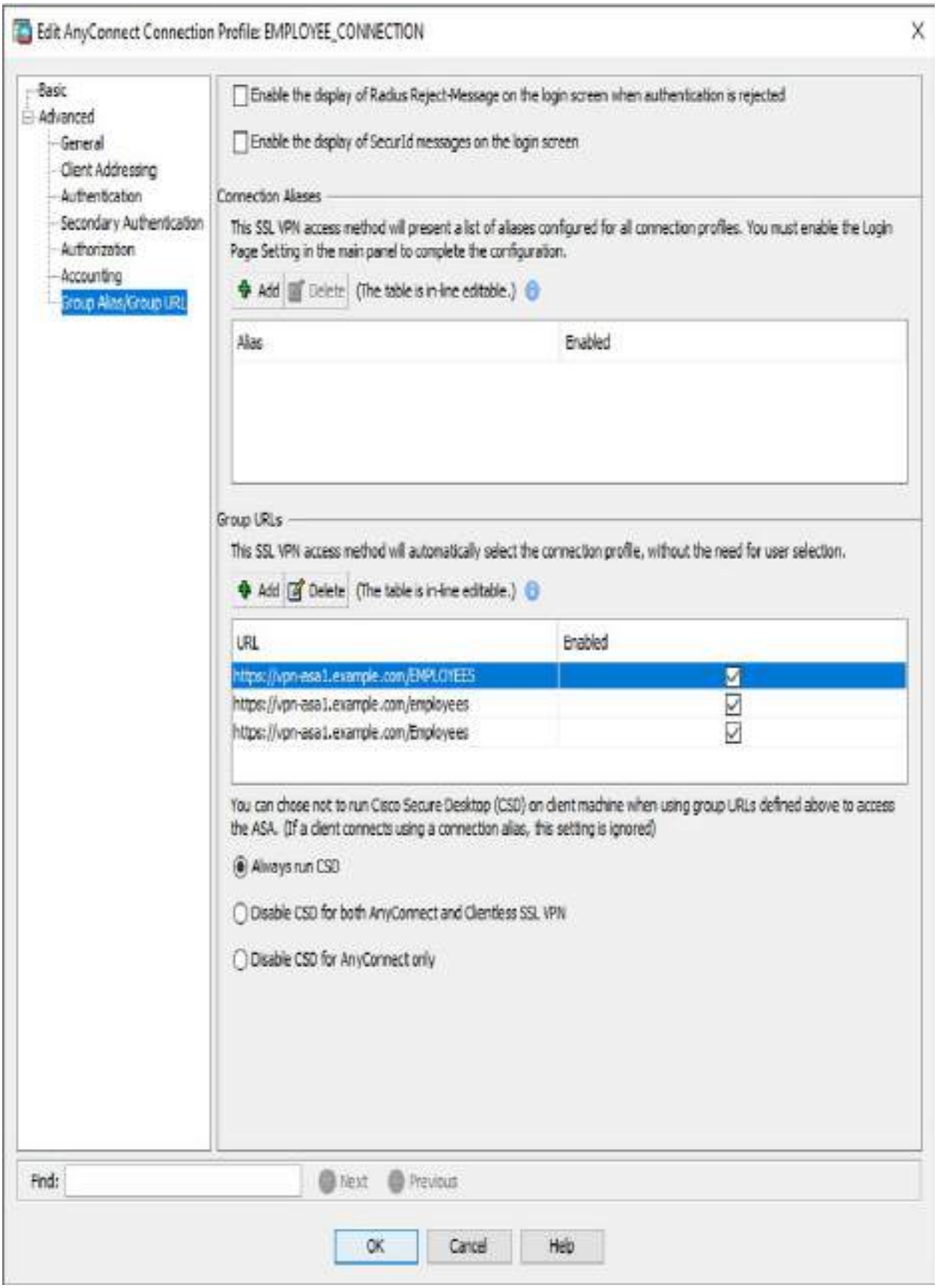

Edit AnyConnect Connection Profile: EMPLOYEE_CONNECTION
Basic
Advanced
General
Client Addressing
Authentication
Secondary Authentication
Authorization
Accounting
Group Alias/Group URL
Enable the display of Radius Reject-Message on the login screen when authentication is rejected
Enable the display of SecurId messages on the login screen
Connection Aliases
This SSL VPN access method will present a list of aliases configured for all connection profiles. You must enable the Login Page Setting in the main panel to complete the configuration.
Add
Delete
(The table is in-line editable.)
Alias
Enabled
Group URLs
This SSL VPN access method will automatically select the connection profile, without the need for user selection.
Add
Delete
(The table is in-line editable.)
URL
Enabled
https://vpn-asa1.example.com/EMPLOYEES
https://vpn-asa1.example.com/employees
https://vpn-asa1.example.com/Employees
You can chose not to run Cisco Secure Desktop (CSD) on client machine when using group URLs defined above to access the ASA. (If a client connects using a connection alias, this setting is ignored)
Always run CSD
Disable CSD for both AnyConnect and Clientless SSL VPN
Disable CSD for AnyConnect only
Find:
Next
Previous
OK
Cancel
Help

Figure 10-4 Connection Profile Configuration Example

Profile Selection

A user who gets to the SSLVPN login window in a browser might be given the option to select a group at the login prompt. Whether a user is presented with the option to select a group depends on two configuration options. First, the option Allow Users to Select Connection, Identified by Alias in the Table Above, at Login Page must be enabled within ASDM. Second, a connection alias must be configured in the connection profile. Without either of these being enabled/present, the user will not have the option to select the specific connection profile at login. Why is this so important? A user who selects the incorrect connection profile might not be able to authenticate or may be denied access, in which case you, as the VPN administrator, will receive a troubleshooting ticket.

For example, let's say that a test user is configured as a local user on the ASA and is instructed to use the LOCAL_USER_PROFILE connection profile to log in. Instead, the user chooses the RADIUS_USER_PROFILE connection profile and tries to log in, but their username and password are rejected. Why might that be? The RADIUS_USER_PROFILE, as the name implies, is configured to use RADIUS to authenticate users, but the user is not set up on the RADIUS server. This user is configured as a local user on the ASA and hence must use a connection profile that uses the local user database for authentication to an SSLVPN group that does not support clientless SSLVPN access. When the test user attempts to log in to WebVPN, that user cannot log in using any group policy via the web interface and fails due to using the default group policy, which, by default, does not support SSLVPN clients.

Authentication

If connectivity and the connection profile look correct, the next step is to validate authentication. *Authentication* means showing that something is true, genuine, or valid. When troubleshooting authentication, you essentially need to validate that the users can prove who they are. You could use a local database for managing users, but organizations typically use external authentication solutions, such as Microsoft Active Directory (LDAP),

RADIUS, or TACACS+. Troubleshooting these types of login authentication issues may involve simply determining whether AAA server groups are working properly and whether the user ID is in the remote authentication system.

Note

Multifactor authentication could be used, including facial recognition technology or a solution such as Cisco Duo that confirms one factor by leveraging the user's phone. Troubleshooting multifactor authentication is very relevant for real-world deployments but out of scope for the SVPN 300-730 exam.

ASA Authentication Testing

A Cisco ASA includes features to test authentication with a user ID and password. You enter a user ID and submit it to the ASA to test the authentication process. For example, a system administrator could first test their own ID to determine if LDAP is configured properly and communicating with the Microsoft AD server. If that works, the next step would be to perform a similar test for the user account that is having problems. We recommend using this process as a way to validate whether a username ID would work if used for connecting to your VPN setup.

Debug ASA to Authentication System

If you perform an initial login validation test and basic authentication is not working, the next step would be to test/debug the process from the ASA to the authentication system. You can enable LDAP debugging by using the command **debug LDAP 255** on the ASA. For testing and troubleshooting RADIUS, you can start troubleshooting by using the command-line test command **test aaa-server authentication** *Radius-Server-Group* **host** *1.2.3.4* **username** *johndoe* **password** *cisco123*. If this test fails, you can next try the **debug radius aaa-request** command. Each authentication protocol supported on the ASA includes a test and debug process, and the output

shows any potential issues.

Figure 10-5 shows an example of output from the **debug LDAP 255** command after a user attempts to log in to the VPN. Notice some key points that are highlighted, including debugging being enabled, the authentication of the user “doctor” being successful, and details about the doctor’s profile. The command **debug RADIUS 255** is another command you might use. (Keep in mind that these commands provide more output than is shown in Figure 10-5.)


ASAv# debug LDAP 255
debug ldap enabled at level 255
ASAv#
[27] Session Start
[27] New request Session, context 0x00007ffa71b9a180, reqType = Authentication
[27] Fiber started
[27] Creating LDAP context with uri=ldap://198.19.10.1:389
[27] Connect to LDAP server: ldap://198.19.10.1:389, status = Successful
[27] supportedLDAPVersion: value = 3
[27] supportedLDAPVersion: value = 2
[27] Binding as asa
[27] Performing Simple authentication for asa to 198.19.10.1
[27] LDAP Search:
Base DN = [dc=dcloud, dc=cisco, dc=com]
Filter = [sAMAccountName=doctor]
Scope = [SUBTREE]
[27] User DN = [CN=Doctor,OU=Demo Users,DC=dcloud,DC=cisco,DC=com]
[27] Talking to Active Directory server 198.19.10.1
[27] Reading password policy for doctor, dn:CN=Doctor,OU=Demo Users,DC=dcloud,DC=cisco,DC=com
[27] Read bad password count 0
[27] Binding as doctor
[27] Performing Simple authentication for doctor to 198.19.10.1
[27] Processing LDAP response for user doctor
[27] Message (doctor):
[27] Authentication successful for doctor to 198.19.10.1
[27] Retrieved User Attributes:
[27] objectClass: value = top
[27] objectClass: value = person
[27] objectClass: value = organizationalPerson
[27] objectClass: value = user
[27] cn: value = Doctor
[27] sn: value = Doctor
[27] telephoneNumber: value = +1 408 555 6028
[27] givenName: value = Doctor
[27] distinguishedName: value = CN=Doctor,OU=Demo Users,DC=dcloud,DC=cisco,DC=com
[27] instanceType: value = 4
[27] whenCreated: value = 20120904194525.0Z
[27] whenChanged: value = 20210708164606.0Z
[27] displayName: value = Doctor
[27] uSNCreated: value = 90972
[27] memberOf: value = CN=Healthcare,CN=Builtin,DC=dcloud,DC=cisco,DC=com
[27] mapped to Group-Policy: value = CN=Healthcare,CN=Builtin,DC=dcloud,DC=cisco,DC=com
[27] mapped to LDAP-Class: value = CN=Healthcare,CN=Builtin,DC=dcloud,DC=cisco,DC=com
[27] memberOf: value = CN=TIER1_USERS,CN=Builtin,DC=dcloud,DC=cisco,DC=com
[27] mapped to Group-Policy: value = DCLOUD-CLIENTLESS-ANYCONNECT
[27] mapped to LDAP-Class: value = DCLOUD-CLIENTLESS-ANYCONNECT
[27] uSNChanged: value = 639432
[27] proxyAddresses: value = SMTP:doctor@dcloud.cisco.com
[27] name: value = Doctor
[27] objectGUID: value = ..d.5.LM.'(....:
[27] userAccountControl: value = 66048
[27] badPwdCount: value = 0
[27] codePage: value = 0
[27] countryCode: value = 0
[27] badPasswordTime: value = 130753324287675732
[27] lastLogoff: value = 0
[27] lastLogon: value = 131451215217355534
[27] pwdLastSet: value = 130541663379796523
Debug enabled
Connecting to LDAP successful
User "doctor" authenticated successfully

Figure 10-5 debug LDAP 255 Output

Authorization

Troubleshooting the authorization process is like troubleshooting the authentication process, but the focus is on validating what authenticated users are permitted to access. The troubleshooting process depends on what protocol you are using for external authorization. This chapter focuses on one protocol, but Cisco provides several technical guides on troubleshooting each of the authorization methods supported by the ASA. The process is basically the same, regardless of the authorization protocol used, but the commands required for troubleshooting are slightly different.

Authorization Debugging

The Cisco ASA supports several methods for applying user authorization attributes to clientless VPN connections. For example, you can configure the Cisco ASA to use the group name supplied by LDAP (Microsoft AD) attributes. As mentioned earlier, if the group attributes are incorrect, the user cannot log in. An easy way to debug the credentials is by using the **debug LDAP 255** command to determine whether the group attribute is mapping correctly. You can simply enable debugging and attempt to log in to the VPN to view any error messages. Figure 10-5 shows an example of using the **debug LDAP 255** command and viewing output after a user attempts to connect to the VPN solution.

Note

We once again encourage you not to start troubleshooting login problems by running **debug** commands. First, consider the issue and see if you can isolate the problem to a focus area and troubleshoot that focus area rather than performing a configurationwide **debug** command. This will save you time, and it is also a valuable way to break up troubleshooting concepts in much the same way as the SVPN 300-730 exam. Remember that the SVPN 300-730 exam will not give you access to an active Cisco ASA, so you won’t be able to run **debug** commands as you would on a real deployment.

Group Policy

Closely related to authorization is the group policy configured for a connection profile and/or user and the access permissions it grants to a user. Examples of group policy settings include access hours, simultaneous logins, and maximum connection time, just to name a few. Each of these settings could cause a user to either fail to log in or lock out a user who falls outside of what is permitted by the group policy configuration. Troubleshooting group policies must include validating the group configuration and matching it against the user's expectations, which can be done by simply accessing the policy and noting what features are enforced. You need to collect information on the situation, including when the user logged in, what user account is being used, and other data points that you validate against the group configuration. Figure 10-6 shows an example of the group selection configuration options.

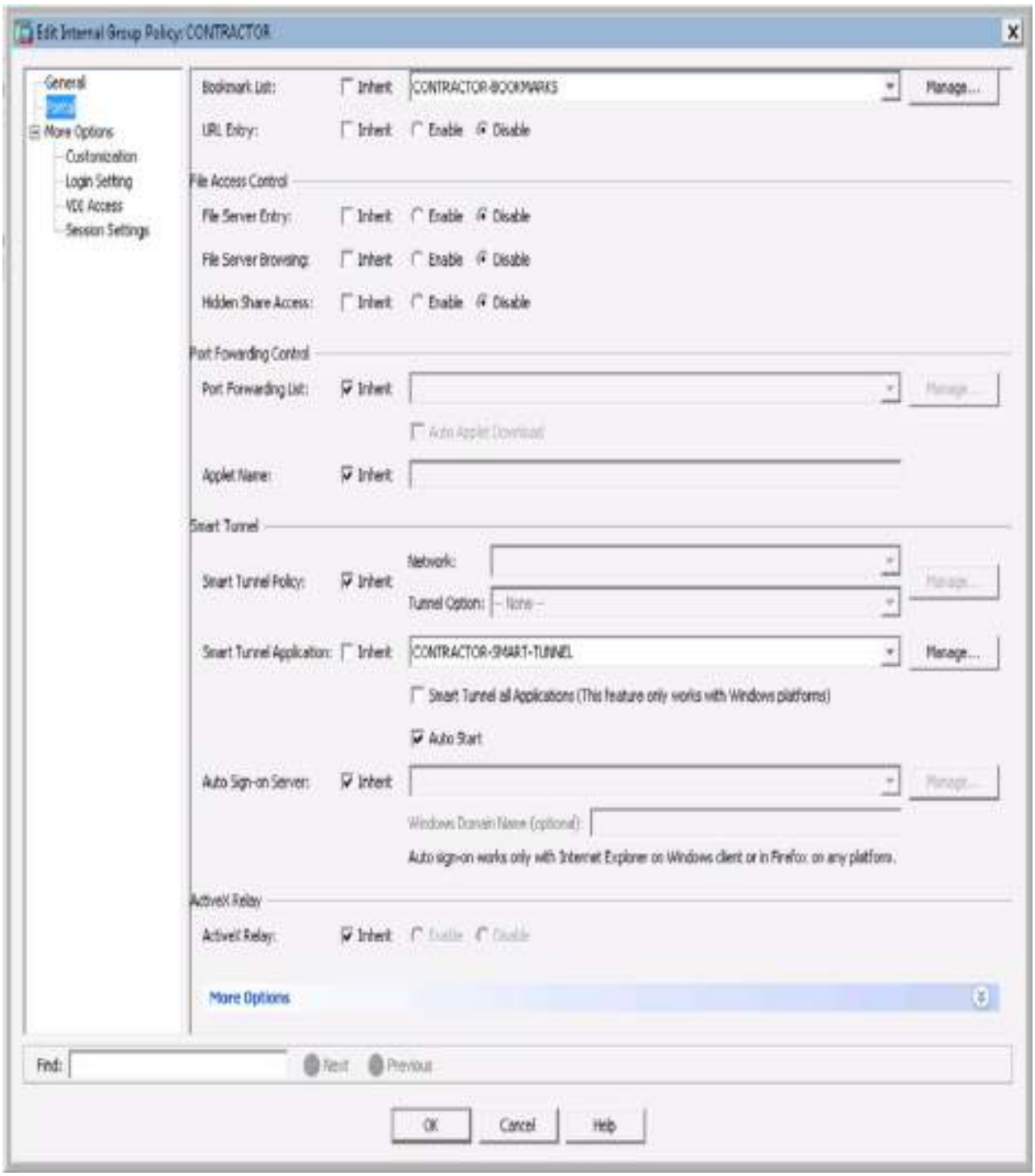


Figure 10-6 Group Selection Configuration Example

Group Policy Validation Using CLI

You can view the same information by using the Cisco ASA command line. To focus on group policy information, you can run the **show running-**

configuration all group-policy command to see how any group policy has been configured. You can also add the group policy of interest to the end of the command. For example, Figure 10-7 displays the DfltGrpPolicy settings.

```
ASAv# show running-config all group-policy DfltGrpPolicy
group-policy DfltGrpPolicy internal
group-policy DfltGrpPolicy attributes
 banner value Welcome to dCloud!
 wins-server none
 dns-server value 198.18.133.1
 dhcp-network-scope none
 vpn-access-hours none
 vpn-simultaneous-logins 3
 vpn-idle-timeout 30
 vpn-idle-timeout alert-interval 1
 vpn-session-timeout none
 vpn-session-timeout alert-interval 1
 vpn-filter none
 ipv6-vpn-filter none
 vpn-tunnel-protocol l2tp-ipsec
 password-storage disable
 ip-comp disable
 re-xauth disable
 group-lock none
 pfs disable
 ipsec-udp disable
 ipsec-udp-port 10000
 split-tunnel-policy tunnelspecified
 ipv6-split-tunnel-policy tunnelall
 split-tunnel-network-list value DCLOUD-SPLIT-TUNNEL
 default-domain value dcloud.cisco.com
 split-dns none
 split-tunnel-all-dns disable
 intercept-dhcp 255.255.255.255 disable
 secure-unit-authentication disable
 user-authentication disable
 user-authentication-idle-timeout 30
 ip-phone-bypass disable
```

Figure 10-7 show running-configuration all group-policy DfltGrpPolicy

Example

Login Troubleshooting Summary

The following are the key concepts for troubleshooting login problems:

- DfltGrpPolicy does not allow SSLVPN client connections.
- Testing a group URL involves validating that the URL is correct, ensuring that it has a FQDN, and making sure the user is permitted to log in with the associated connection profile.
- For Activate Directory authentication testing, use the Cisco ASA to test authentication such as the user ID and password.
- At the Cisco ASA CLI, use the command **debug LDAP 255** or **debug RADIUS 255** to debug LDAP problems. Enable debugging and attempt to log in to the VPN.
- For RADIUS, use the command **test aaa-server authentication** *Radius-Server-Group* **host** *x.x.x.x* **username** *johndoe* **password** *cisco123* to validate a login and password.
- If RADIUS validation fails to work, run the **debug radius 255** command and view the error logs.
- Troubleshooting group policies must include validating the group configuration and matching it against the user's expectations.

Step 3: Clientless WebVPN Service Issues

Earlier in this section, you saw an example of validating whether the ASA WebVPN services are running. That example does not look at how those services are functioning. Remember that you first want to ensure that connectivity works and that login issues have been resolved before you dive into how the VPN works.

WebVPN services problems are related to the browser on the client machine. One problem a user could complain about is not being able to see the WebVPN page, even though they can successfully connect to it. One possible problem that could cause this issue is the user's browser not trusting the web page provided by the ASA due to a corporate policy restriction or another limitation on the user's system. Troubleshooting this particular problem will most often have to be done from the user system. However, you could use another system to verify that the service is functioning correctly before moving to performing similar tests on the impacted user's system. If you can access the user's system, you will want to validate that the ASA's provided web page is included in the browser's trusted zone as well as that cookies are enabled. You will also want to try clearing the browser cache and Java cache before trying to connect to the ASA WebVPN page again. In short, you want to focus troubleshooting on the user's browser that is experiencing problems first before proceeding with troubleshooting the ASA side of the service. Figure 10-8 shows the browser configuration options on a Chrome browser.

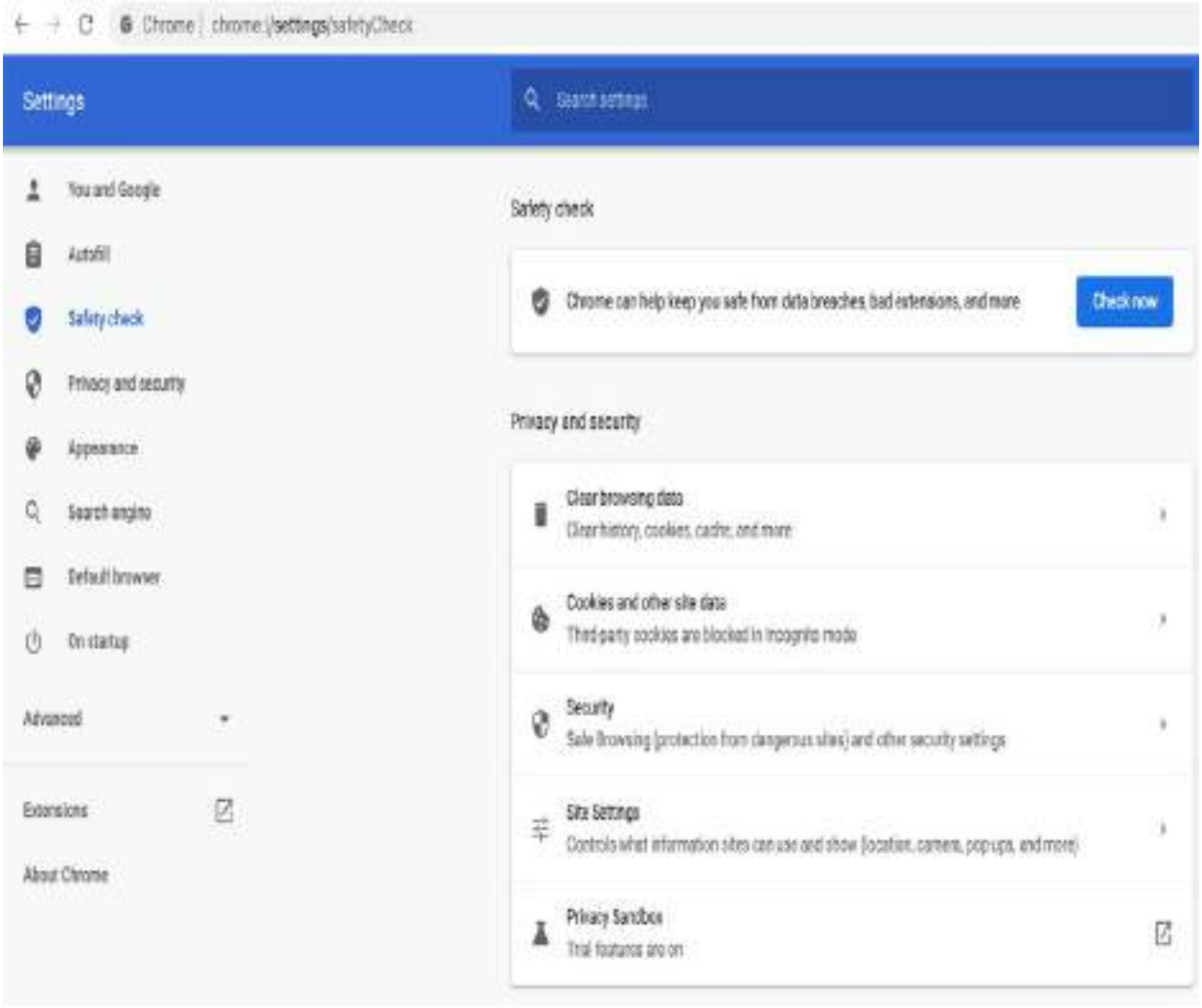


Figure 10-8 Web Browser Configuration Example

Validating WebVPN Service Details

If you believe the WebVPN service should be working and have tested the VPN user's web browser, but there are still problems associated with the service, you need to look more closely at how the service is configured and running on the ASA side. One place to start is by using the **show vpn-sessiondb detail webvpn** command. Figure 10-9 provides an example of using this command and demonstrates that the user vpnuser is connected to the ASA. Notice that the other fields in this output also provide useful troubleshooting information. For example, the browser type is included, which might help determine if the user is using a version that is known to have problems.

```
ASAv# show vpn-sessiondb detail webvpn

Session Type: WebVPN Detailed

Username     : doctor                 Index        : 10
Public IP    : 198.18.133.36
Protocol     : Clientless
License      : AnyConnect Premium
Encryption   : Clientless: (1)AES-GCM-128
Hashing      : Clientless: (1)SHA256
Bytes Tx     : 570819                 Bytes Rx     : 154357
Pkts Tx      : 6                      Pkts Rx      : 2
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : DCLOUD-CLIENTLESS-ANYCONNECT
Tunnel Group : DCLOUD-CLIENTLESS-ANYCONNECT
Login Time   : 18:29:38 UTC Thu Jul 8 2021
Duration     : 0h:09m:06s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : c6130a640000a00060e74412
Security Grp : none

Clientless Tunnels: 1

Clientless:
  Tunnel ID    : 10.1
  Public IP    : 198.18.133.36
  Encryption   : AES-GCM-128           Hashing      : SHA256
  Ciphersuite  : ECDHE-RSA-AES128-GCM-SHA256
  Encapsulation: TLSv1.2               TCP Dst Port : 443
  Auth Mode    : Certificate and userPassword
  Idle Time Out: 30 Minutes            Idle TO Left : 20 Minutes
  Client Type  : Web Browser
  Client Ver   : Mozilla/5.0 (Windows NT 6.1; WOW64; rv:47.0) Gecko/20100101 Firefox/47.0
  Bytes Tx     : 572513                Bytes Rx     : 160377

ASAv#
```

Figure 10-9 show vpn-sessiondb detail webvpn Command Output

In addition, the authentication mode (Auth Mode) and group policy might provide helpful information if a user is able to log in to the VPN but cannot access required services. We highly recommend being familiar with the **show**

vpn-sessionsdb detail webvpn output.

WebVPN Debugging

If you need to take a deeper look at troubleshooting the WebVPN service, you can use the **debug** command. The command **debug webvpn condition user** *user* can help you see specifics related to a user or group. If an ASA has hundreds of inbound WebVPN connections but a single user is having a problem, then this might be the option to employ to look for error messages. You could run this command and ask the user to attempt to connect to the VPN. The output should include error messages that might lead you back to the ASA or user side for further troubleshooting.

Validating DNS Configuration

Another possible problem with WebVPN services could involve the DNS configuration on the Cisco ASA. DNS is a good starting point if connectivity to the Cisco ASA works but the user can't access a protected application. Remember that, technically, the user's application requests initiate from the ASA, so you need to make sure that the ASA can resolve names. To validate that the ASA can resolve names, you need to check the ASA configuration for the critical command **dns domain-lookup** *inside*. In addition, you need to make sure that the IP address associated with the DNS server is correct by looking at the **dns name-server** *x.x.x.x* setting. You might want to add a second DNS name server to provide a level of fault tolerance if you suspect DNS issues. If the WebVPN client application is accessing applications through a DMZ interface, you should make sure DNS lookup is also enabled in the ASA. You can see all of these settings by using the **show run** or **show run dns** command to view the ASA configuration. Figure 10-10 shows output of the **show run dns** command.

Figure 10-10 Critical DNS Command Example

ASA Plug-ins

The Cisco ASA supports multiple plug-ins related to specific applications. These plug-ins support RDP, VNC, Citrix, SSH, and Telnet. Keep in mind that each of these plug-ins presents a potential unique issue to troubleshoot. Best practice regarding plug-in maintenance is keeping all plug-ins updated and understanding the pieces that they are dependent on for their functionality. An example of a dependency is that some plug-ins require Java and must have the correct Java feature set for the plug-in to function properly. If a VPN user's Java client is out of date or the VPN user is using an old version of Java, they could experience problems unrelated to how the ASA is configured; this would be a host problem. If you run into a dependency problem such as one with Java, we recommend removing Java and reinstalling the latest version on the VPN user's system.

Troubleshooting ASA plug-ins involves isolating the problem to the plug-in and validating dependencies for the plug-in. Then you can troubleshoot from the user's side as the issue is likely related to the user being unable to support the plug-in. Figure 10-11 shows plug-in options.

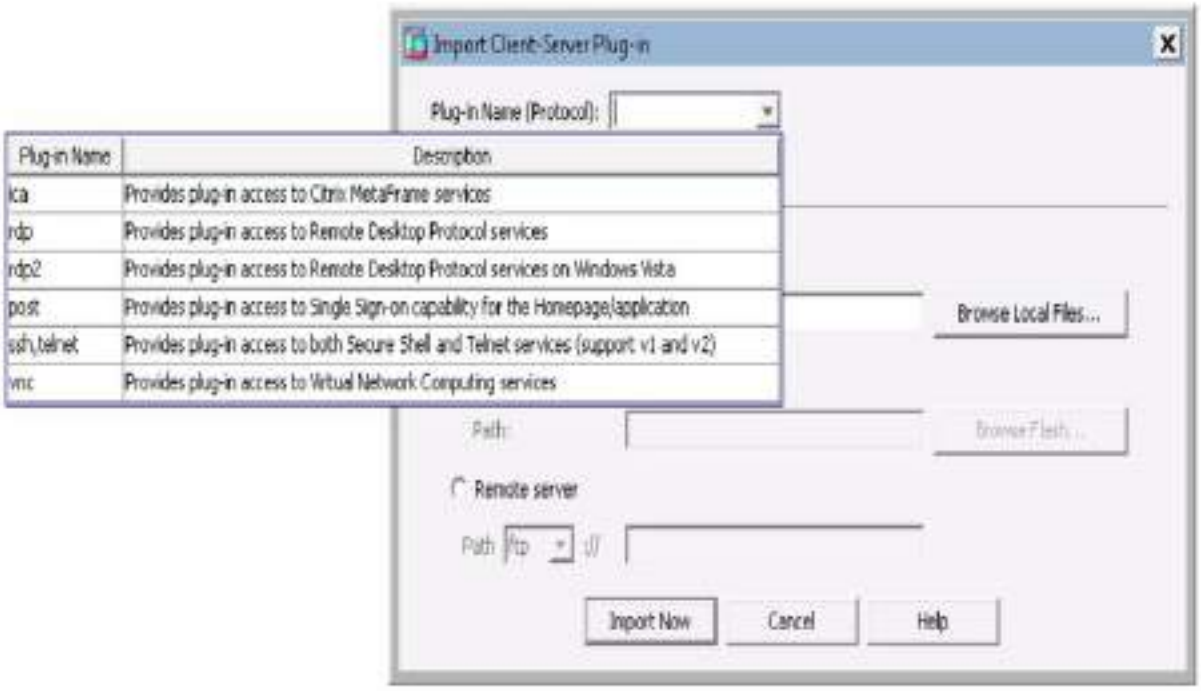


Figure 10-11 ASA SSLVPN Plug-ins

You can also view what WebVPN plug-ins are being used by leveraging the ASA command line. Run the command **show import webvpn plug-in** and look to see what plug-ins are listed.

Bookmarks

You saw how to configure bookmarks on an ASA in Chapter 9. Bookmarks are designed to help enable easy setup of applications for VPN clients. If a user complains that a bookmark isn't working, you should check the group policy associated with the user. It is possible that the user does not have the correct rights to see the bookmarks list. Next, you need to make sure the bookmarks list is not empty since that would cause the bookmark to not work. You can validate a bookmarks list by using the command **export webvpn url-list** *url-list-name* **stdout**. We recommend starting with these two items as they are the most common reasons for bookmark access problems.

Figure 10-12 shows an example of exporting bookmarks in a file named CONTRACTOR-BOOKMARKS.

```
ASAv# export webvpn url-list conTRACTOR-BOOKMARKS stdout
<url-list>
<bookmark>
<title><![CDATA[Healthcare Portal]]></title>
<method><![CDATA[get]]></method>
<favorite><![CDATA[yes]]></favorite>
<url><![CDATA[http://health.dcloud.cisco.com]]></url>
<subtitle><![CDATA[]]></subtitle>
<thumbnail><![CDATA[/+CSCOU+/dcloud-healthcare-logo.png]]></thumbnail>
<smart-tunnel><![CDATA[no]]></smart-tunnel>
</bookmark>

<bookmark>
<title><![CDATA[Education Portal]]></title>
<method><![CDATA[get]]></method>
<favorite><![CDATA[yes]]></favorite>
<url><![CDATA[http://edu.dcloud.cisco.com]]></url>
<subtitle><![CDATA[]]></subtitle>
<thumbnail><![CDATA[/+CSCOU+/dcloud-education-logo.png]]></thumbnail>
<smart-tunnel><![CDATA[no]]></smart-tunnel>
</bookmark>
```

Figure 10-12 export webvpn url-list Example

DAP and Bookmarks

If the bookmarks list still does not appear on the VPN user's system but looks to be available for them to use, try checking the dynamic access policy (DAP) settings. A DAP rule could be removing the bookmarks list from the user or group, leading to the bookmarks not being available. To validate whether DAP is the culprit behind the bookmark issue, you can execute the command **debug dap trace**.

Note

One key point about bookmarks is that not all applications are compatible with the clientless VPN server. Cisco provides workarounds for this, such as using smart tunnels.

DNS and Bookmarks

If users complain that a bookmarks list is available but grayed out, you need to ensure that the DNS server is reachable from the ASA. You need to validate that the ASA can ping the website by name to rule out this possible issue. If a ping does not work, you need to verify that the ASA has the correct DNS configuration.

WebVPN Services Troubleshooting Summary

The following are the key concepts for troubleshooting WebVPN services problems:

- WebVPN services problems are typically related to the browser on the client machine. You should start by troubleshooting the user's side before moving to validating that the ASA is configured properly.
- The **show vpn-sessiondb detail webvpn** command can be used to view the WebVPN service status details.
- You should validate that the DNS configuration exists on the ASA by using **dns domain-lookup** *inside* and **dns name-server** *x.x.x.x* with the **show run** command.
- ASA plug-in problems can be isolated to the plug-in and its dependencies. For example, a browser might not support a plug-in dependency such as Java.
- When troubleshooting bookmarks, make sure a bookmark exists and ensure that the user has privileges to view the bookmark. You also need

to ensure that a DAP rule isn't causing the problem by using the **debug dap trace** command.

Step 4: Application Access

The final area of focus for clientless VPN troubleshooting is application access problems. Issues associated with applications launching through a clientless VPN can be challenging to solve because the ASA is proxying the connectivity, and the ASA HTTP server interacts with the authentication subsystem to authenticate the user for the specific application. When troubleshooting application access, Cisco recommends that you review the limitations for clientless SSLVPN to determine whether the application and its associated security model will function properly. This way, you can avoid wasting time troubleshooting something that Cisco has already identified as not working. In short, you should start by researching the application's support through the clientless SSLVPN before taking any other troubleshooting actions.

ASA-to-Application Connectivity

We started off troubleshooting problems with a focus on connectivity. If you find that a VPN is working but the application is not, you should test the connectivity between the ASA and the application. The key for troubleshooting connectivity is to determine where the error is coming from. First, validate that the ASA and the application server have connectivity by using **ping**. Next, determine if the local web client browser can access the application by using the tactics covered earlier in this chapter regarding user browser troubleshooting. If the browser settings are correct, try to clear the browser cache and the Java cache. You can also disable the ASA's cache at the CLI. The commands to use are **webvpn** followed by **cache**, as shown in Figure 10-13. Figure 10-13 shows the configuration options, including disabling cache.

```
ASAv# config t
ASAv(config)# webvpn
ASAv(config-webvpn)# cache
ASAv(config-webvpn-cache)# ?

cache command:
  cache-static-content  Configure WebVPN static content caching
  disable               Disable cache
  exit                  Exit from cache mode
  expiry-time           Configure WebVPN cache expiry time
  help                  Help for cache commands
  lmfactor              Configure WebVPN cache last modified factor
  max-object-size       Configure cache max object size
  min-object-size       Configure cache min object size
  no                    Remove a command or set to its default
ASAv(config-webvpn-cache)#
```

Figure 10-13 Working with the **webvpn** and **cache** Commands

Application-to-ASA Connectivity with Port Forwarding

Recall from Chapter 8, "Clientless Remote-Access SSLVPNs on the ASA," that port forwarding requires a change in how users connect to applications. For example, instead of connecting to hr.example.com on port 3389, the user instead might need to connect to 127.0.0.1:<*port forwarding port*>. You can see port forwarding in the window shown in Figure 10-14.

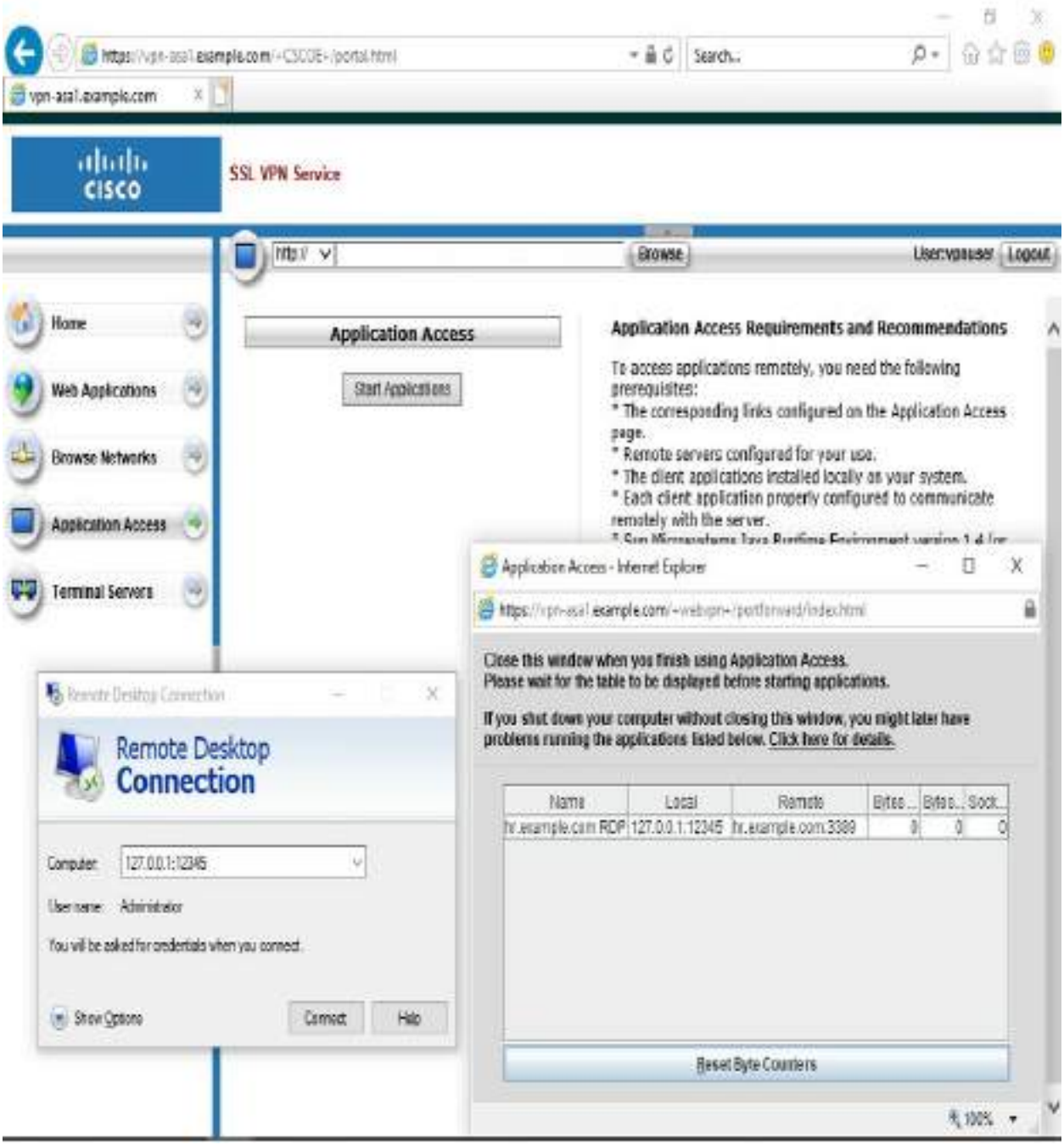


Figure 10-14 Port Forwarding of RDP Traffic

From a troubleshooting perspective, if port forwarding is in use, you need to ensure that the user is connecting to the proper local IP address and port. Otherwise, connectivity will fail.

Application Troubleshooting Summary

The following are the key concepts for troubleshooting application problems:

- Application troubleshooting starts with researching the application and validating that it is supported by Cisco.
- You need to validate connectivity between the ASA and the application as well as between the user's browser and the application.
- You should attempt to troubleshoot the user's browser problems by using steps previously covered as well as by clearing the browser cache.

Troubleshooting AnyConnect SSLVPNs on the ASA

This section focuses on troubleshooting an AnyConnect SSLVPN deployed using a Cisco ASA. As in the first section of the chapter, on troubleshooting clientless VPNs, we use a step-by-step approach in this section. The major difference for this section and the remaining sections is that now we are shifting to client-based VPN architecture; in this case, the client is Cisco AnyConnect. Adding a VPN client opens up new areas to troubleshoot, including how the customer obtains the client, ensuring that the client is supported by the host system, validating that the client is functioning properly, and using the client to obtain data for troubleshooting. Figure 10-15 shows a basic AnyConnect SSL deployment that includes a VPN client, a Cisco ASA acting as the VPN concentrator, and an external identity database. Once again, try to keep a simple diagram like this in your mind as you approach any SVPN 300-730 exam troubleshooting questions as doing so will help you eliminate obviously wrong answers.

Figure 10-15 Basic AnyConnect SSLVPN Design

Some of the troubleshooting concepts covered in the first section of this chapter apply to all VPN deployments. To avoid being repetitive, in this section we summarize those concepts and focus on what is either new or specific to AnyConnect SSLVPN deployments. You will also find some of these repeating concepts in our recommended summary for troubleshooting AnyConnect SSLVPN deployments since we want to keep our troubleshooting process intact.

Troubleshooting AnyConnect SSLVPNs involves the following steps:

Step 1. Connectivity: Confirm all aspects of connectivity between the user and the VPN provider (in this case, the Cisco ASA).

Step 2. Login: Troubleshoot any login issues, including validating that the proper user group is selected and that the user is able to pass all authentication and authorization steps.

Step 3. Network access: Review all aspects of how network access is provided by the VPN. Many of these topics are different than with the clientless VPN troubleshooting process:

- Address pool
- Routing problems
- DNS

- Browser proxy
- AnyConnect client
- NAT
- Traffic filters

Step 4. Diagnostic and Report Tool (DART): Leverage the Cisco diagnostic tool for AnyConnect.

Step 5. VPN diagnostic commands: If the VPN is working but certain configurations are possibly not correct, run diagnostic commands to view details about how the VPN is running.

Step 6. Application access: Troubleshoot issues related to accessing the application.

- ASA-to-Application connectivity

Let's start from the top of the list with troubleshooting connectivity.

Step 1: Connectivity Troubleshooting

As you have already seen in this chapter, the first step for any troubleshooting process is to examine connectivity. The first section of this chapter covers key points to validate, including communication between systems, the status of interfaces involved with the connectivity, possible certificate issues, license problems, and anything else that prevents connectivity from occurring. We recommend working up the OSI model from Layer 1 (the physical layer) to ensure that you can reach the VPN application.

If you find connectivity problems by using commands like **ping** but are unsure of the cause, you can use the command **debug webvpn anyconnect**. Debugging enables you to view error messages as you perform connectivity testing.

Step 2: Login Troubleshooting

As with clientless, when troubleshooting a client-based VPN, you focus on

ensuring that accounts are created and authorized to access the VPN. You can test this by using an administration account or using the client's account and verifying that services are functioning. Debugging can also be used to view login problems such as the wrong password being used or a reference to the wrong access group. You should follow the same troubleshooting steps presented earlier in this chapter, starting with basic authentication verification and moving to group member problems. Do not proceed with further troubleshooting until you have ruled out connectivity and login issues as possible causes of an SSLVPN problem.

Step 3: Network Access Troubleshooting

After you validate that connectivity and login aspects of the VPN are functioning as expected, you should move on to troubleshooting network access. Unlike with a clientless VPN, the AnyConnect VPN has potential complexity around routing IP packets to the correct destination. This means you need to take different steps for troubleshooting, including looking at how AnyConnect establishes the VPN service and potential NAT or DNS issues.

This section starts by troubleshooting using ASDM but also shows the same steps using the ASA command line. The SVPN 300-730 exam will likely have the command line version of steps; however, real-world troubleshooting can be accomplished using both the command line and the GUI, so we cover both approaches here.

AnyConnect Enabled

With ASDM, navigate to **Configuration** > **Remote Access VPN** > **Network (Client) Access**. Verify that AnyConnect is enabled via the appropriate check boxes. You might also want to validate that DTLS is enabled, as it typically provides better performance, especially for jitter-sensitive applications such as voice. If the VPN action check boxes under the SSL Access section for Interfaces are not checked, you are not allowing network access and so will block users. Make sure the connection profile you are using also has SSL enabled. Figure 10-16 shows an example of some of the check boxes you need to examine.

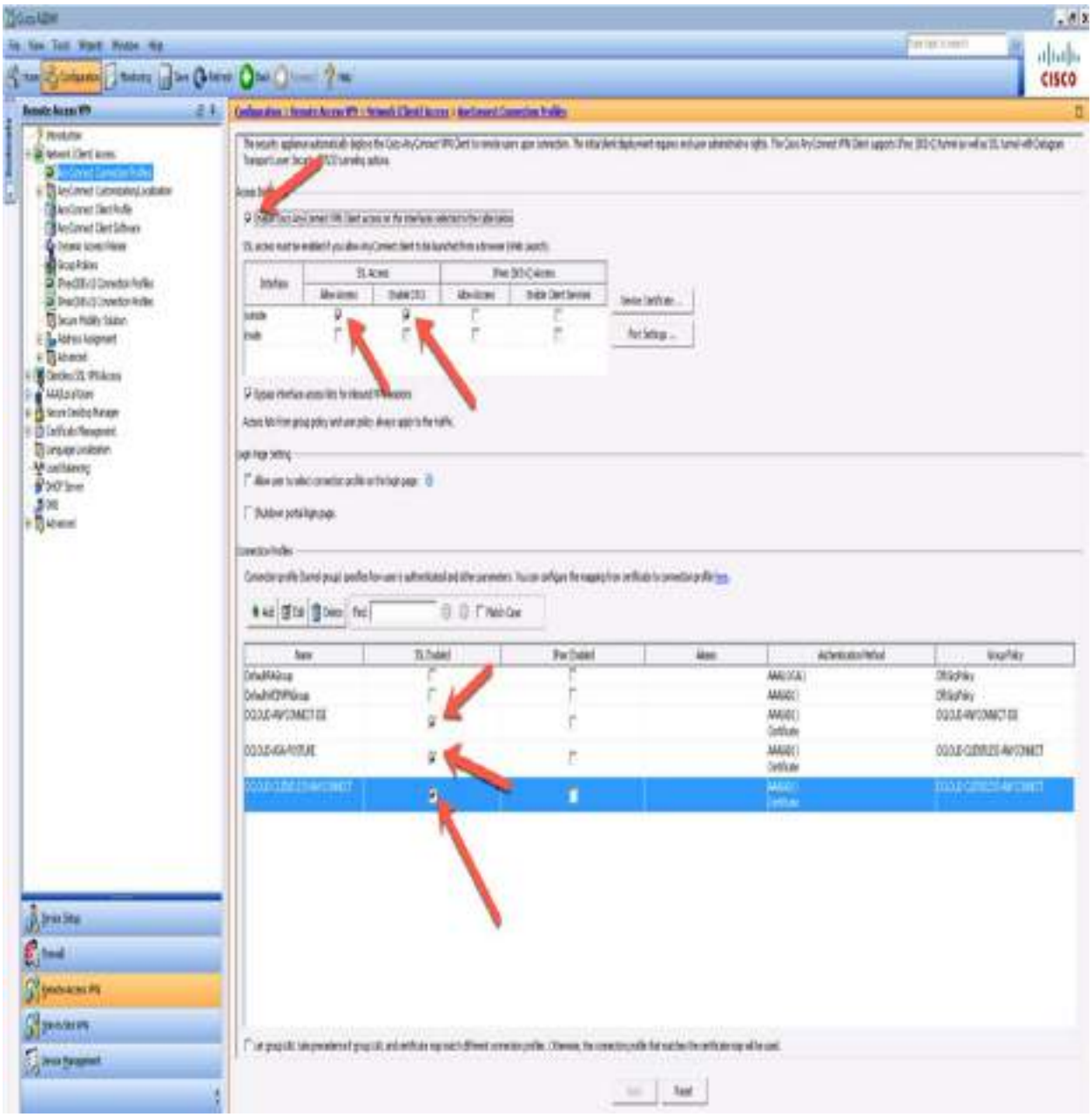


Figure 10-16 Troubleshooting SSLVPN with ASDM

You can validate the same information by using the ASA command line and running the command **show running-configuration webvpn**. The output enables you to verify whether the outside interface has been enabled for WebVPN, what profiles have been set up, whether AnyConnect is enabled, and details on the smart tunnels being used (see Figure 10-17).

```
ASAv# show running-config webvpn
webvpn
 enable outside
 hostscan image disk0:/hostscan_3.1.07021-k9.pkg
 hostscan enable
 anyconnect image disk0:/anyconnect-win-4.5.04029-webdeploy-k9.pkg 1
 anyconnect profiles DCLOUD-AMP-PROFILE disk0:/dcloud-amp-profile.asp
 anyconnect profiles DCLOUD-ANYCONNECT-PROFILE disk0:/dcloud-anyconnect-profile.xml
 anyconnect profiles DCLOUD-ISE-POSTURE-PROFILE disk0:/dcloud-ise-posture-profile.isp
 anyconnect enable
 smart-tunnel list CONTRACTOR-SMART-TUNNEL RDP_Client mstsc.exe platform windows
 smart-tunnel list CONTRACTOR-SMART-TUNNEL PuTTY putty.exe platform windows
 smart-tunnel list DCLOUD-SMART-TUNNEL RDP_Client mstsc.exe platform windows
 smart-tunnel list DCLOUD-SMART-TUNNEL PuTTY putty.exe platform windows
 cache
  disable
 error-recovery disable
ASAv#
```

Figure 10-17 show running-configuration webvpn Example

Group Policy Configuration

After you make sure all the correct options are enabled, you need to look at the group policy configuration. Think about what the VPN concentrator (ASA) needs to provide a client. When you create a VPN, you are essentially providing a new network configuration, which means a unique IP address that is separate from the client. To validate this, you go to **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Group Policies**. The examples in this section focus on the default group policy DfltGrpPolicy (the system default). You can also view group policies by using the command line and running the **show running-configuration group-policy** command.

While in ASDM, double-clicking a policy brings up a separate window related to the AnyConnect client configuration.

The following are some of the areas where you need to focus your troubleshooting:

- Address pool
- Routing problems
- DNS
- Browser proxy
- AnyConnect client
- NAT problem
- Traffic filters

Let’s work through each of these focus areas more closely to see they relate to potential problems you might need to troubleshoot.

Address Pool

When you open a policy and begin troubleshooting, you should validate the address pool. Make sure you click the Select button and verify what IP address range is being used. If the range being used is too small to support the VPN deployment, a client might not be able to get an IP address, and thus communication will fail due to lack of available IP addresses. You also must ensure that the IP subnet mask and the address block used by the address pool are in the headend routing table and that the routing table indicates the correct location for the client. We have been at organizations troubleshooting VPN deployment issues and found the organizations using one-way routing. When viewing traffic in this situation, you see that the VPN client is transmitting traffic, but nothing is returning. This behavior would be a good indication

that the headend (the terminating side of the VPN tunnel) does not know how to return packets to the client. Figure 10-18 shows an address pool configuration example for DfltGrpPolicy.

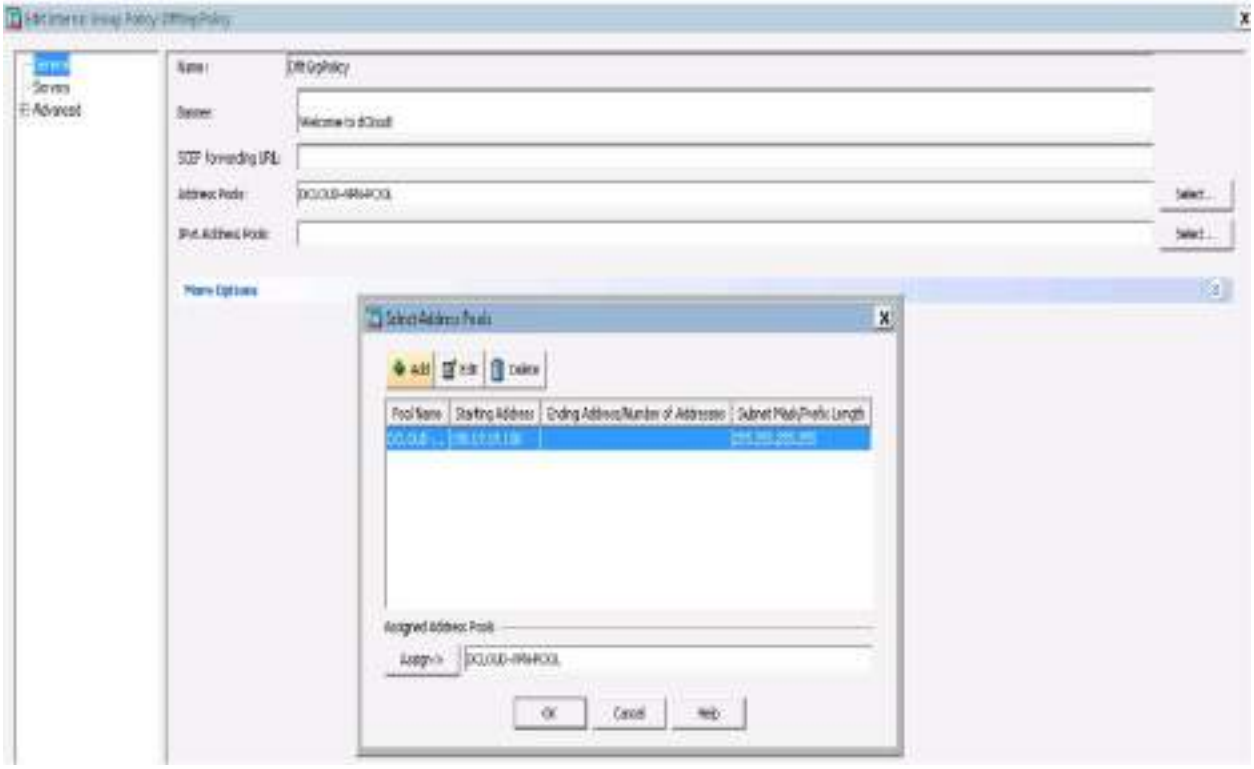


Figure 10-18 Address Pool Example with DfltGrpPolicy

Validating the Address Pool

You can quickly find any address pool from the ASA command line by issuing the command **show running-config tunnel group**. This command shows details for any connection profile, including associated address pools. Alternatively, you can simply filter on address pools by using the command **show running-configuration | include address-pool** followed by **show running-configuration | include** *THE_VPN_POOL_Name* to see details regarding the IP address range within the VPN pool. For example, the following output could come from our small lab (although a real-world deployment would have a range of IP addresses):

```
ASAv# show running-configuration | include address-pool
 address-pool value DCLOUD-VPN-POOL
 address-pool value DCLOUD-VPN-POOL
```

```
 address-pool value DCLOUD-VPN-POOL
 address-pool value DCLOUD-VPN-POOL
```

You would validate this address pool by using a **show** command and **ip local pool** or using the command **DCLOUD-VPN-POOL**, as in this example:

```
ASAv# show running-configuration | include DCLOUD-VPN-POOL
ip local pool DCLOUD-VPN-POOL 198.19.19.100 mask 255.255.255.255
 address-pools value DCLOUD-VPN-POOL
 address-pool value DCLOUD-VPN-POOL
 address-pool value DCLOUD-VPN-POOL
 address-pool value DCLOUD-VPN-POOL
```

Routing Problems

After you confirm that the address pool is correct, your next area of focus should be how traffic is routed. Routing table problems can take many forms, as you have already begun to see. Another common issue is that the client may be receiving a split tunneling policy, but the policy does not include the correct address range. You should validate what IP range is provided by going under the connection profile default group policy found under the Advanced settings within the group policy. Here, you need to verify what type of tunnel is being configured and view details about the network list, which shows what networks are passing through the tunnel. If you click the Managed button next to the network list that is being used, you can see what access control list the client will receive when this group policy is applied. You need to verify that the tunnel policy isn't applying an access list policy that blocks traffic. Figure 10-19 shows an example of validating the access list for a tunnel policy.

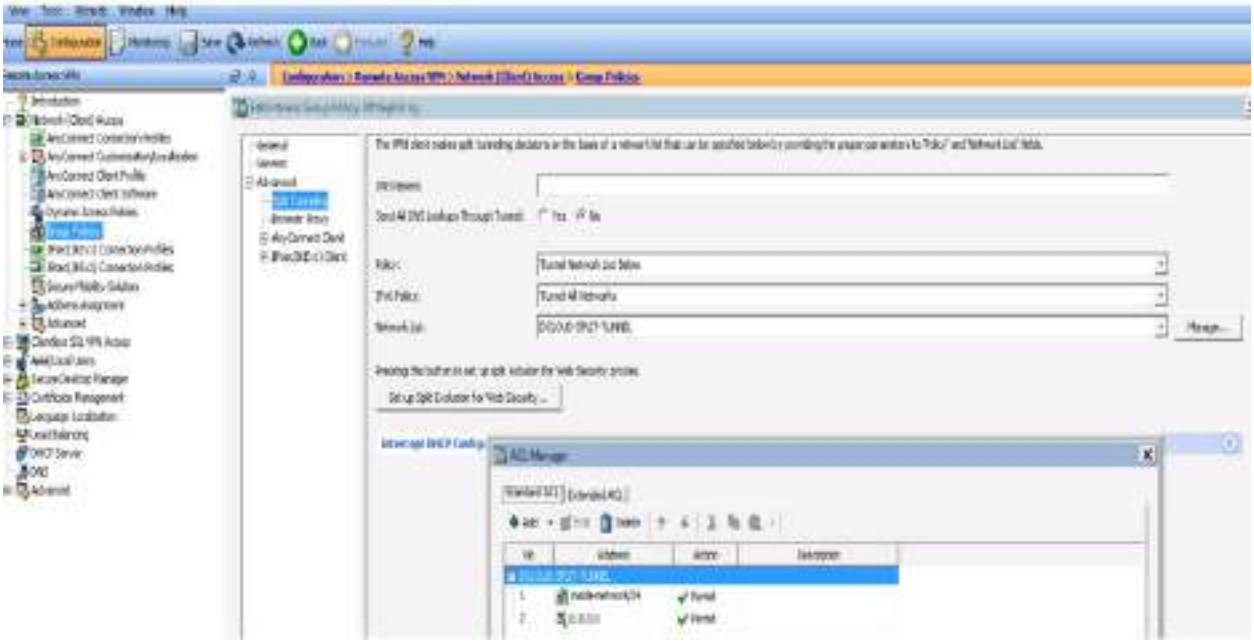


Figure 10-19 Validating an Access List in a Tunnel Policy

Use the **show running-configuration tunnel-group** command to view the connection profile configuration details using the ASA command line and use the **show running-configuration group-policy** command to view details. To view access list details, you can use the command **show running-configuration access-list**, which lists all the access lists configured. You could also use the **tunnel-group** command to see details about the connection profile you are interested in including and to identify any configured tunnel policies. Next, you run the **show** command for the specific group policy to get an idea of any associated access lists. Finally, you run the **show access-list** command to view details for the related access lists.

DNS Troubleshooting

The DNS configuration of the AnyConnect client permits clients to resolve internal IP addresses by using the tunnel connection. This is obviously important and needs to be validated. There are also situations, such as when using split tunneling, in which you do not want all DNS lookup traffic to come through the VPN tunnel. You need to validate which approach is being used and match it to your desired DNS results. Validating the DNS being used could be as simple as using the client **ping** command from the CLI and viewing the results.

To view how DNS is being configured, you need to view whether split DNS is being used or whether all DNS lookups are being sent through a tunnel. Split DNS enables a client to send specific DNS queries across the tunnel, and all others uses an outside DNS server. When all DNS lookups are being sent through a tunnel, all DNS queries are sent to the organization's DNS server. Figure 10-20 shows where this is configured under the **Group Policy** > **Advanced** > **Split Tunneling**.

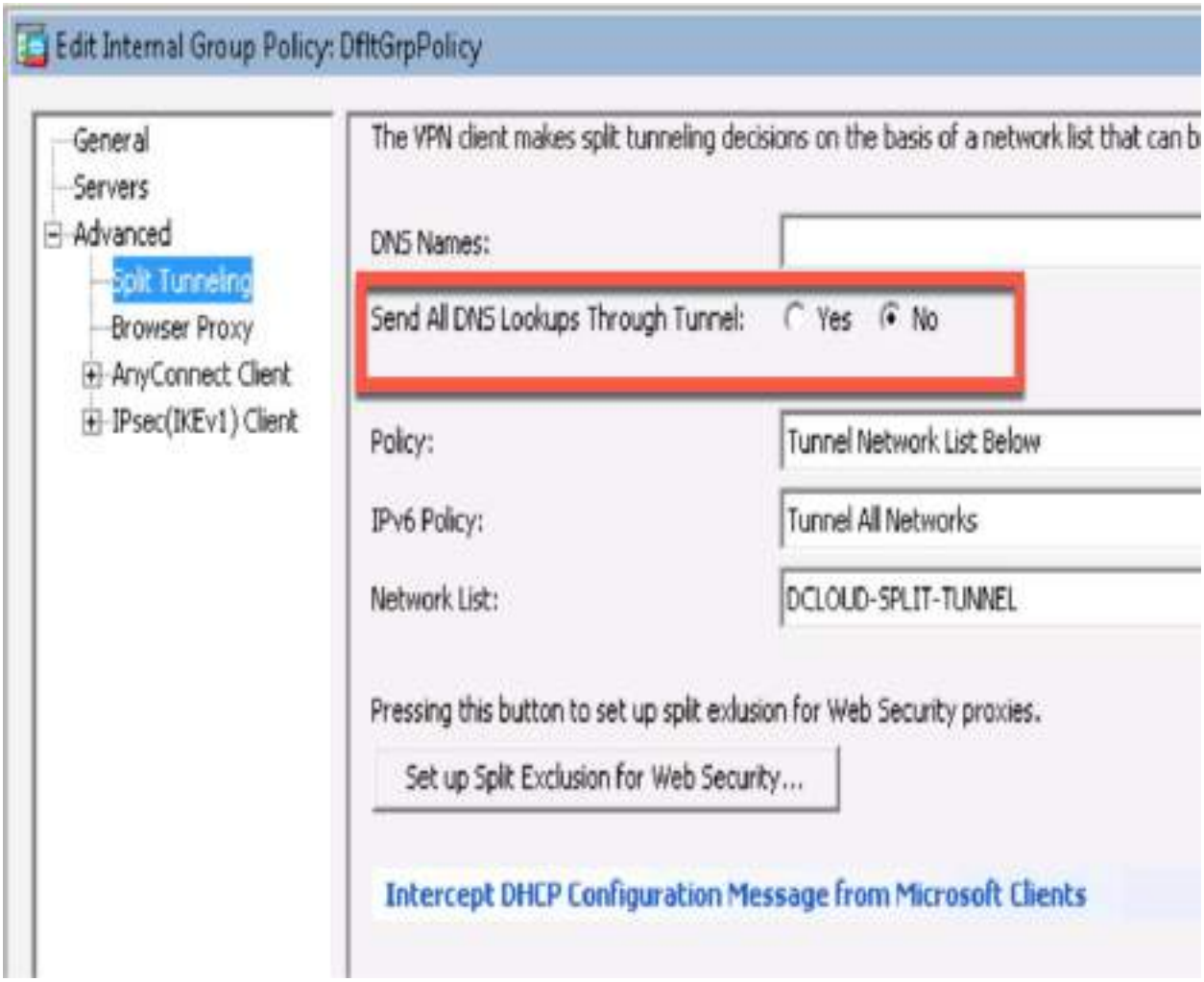


Figure 10-20 Configuration Example for DNS Tunneling

You can view the same information by using the **show running-configuration group-policy** command, as shown in Figure 10-21. You need to look for the line **split-tunnel-all-dns** and see if it is enabled or disabled.

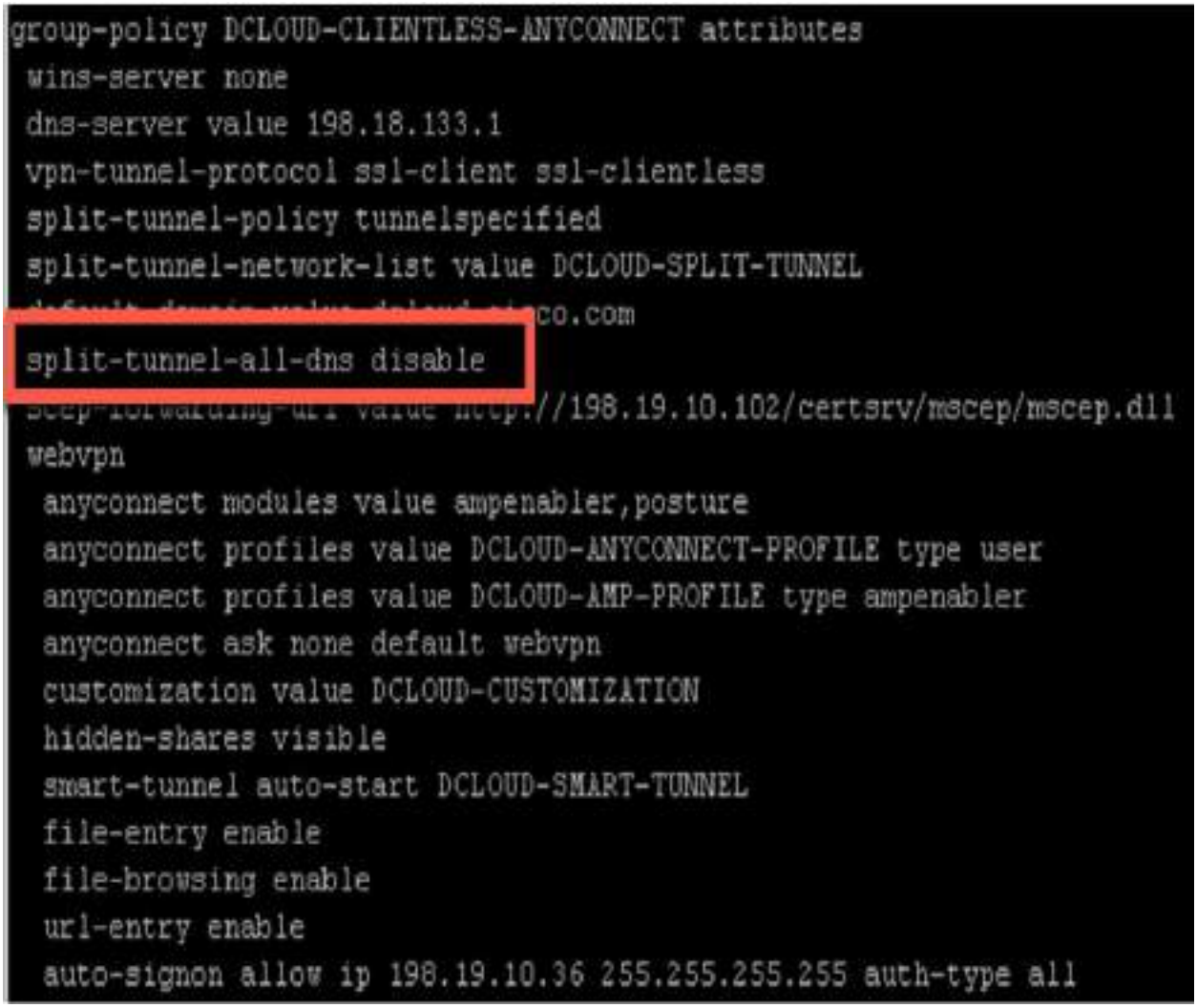


Figure 10-21 show running-configuration group-policy Example

DNS Split Tunnel Range

You also need to make sure the DNS server at the headend of the VPN architecture is within the split tunnel range. If it is not, DNS resolution will fail. Verify this by viewing the address pool range along with the network list used by the split tunnel policy, as already discussed. In addition, the DNS server could block DNS requests from the client because of corporate or other existing policies. This issue would relate back to validating connectivity, including whether security tools are preventing the connection.

Browser Proxy

The browser proxy settings of the AnyConnect client are designed to push web browser proxy settings and force the client to use specific proxy server settings. There are a variety of options for this attribute, and troubleshooting this should be considered when a user is unable to browse websites. You can validate this under the group policy by viewing the browser proxy settings and reviewing whether a browser proxy is being used as well as what the address is for that proxy. Figure 10-22 shows the configuration page with a dummy proxy placed as the proxy server address.

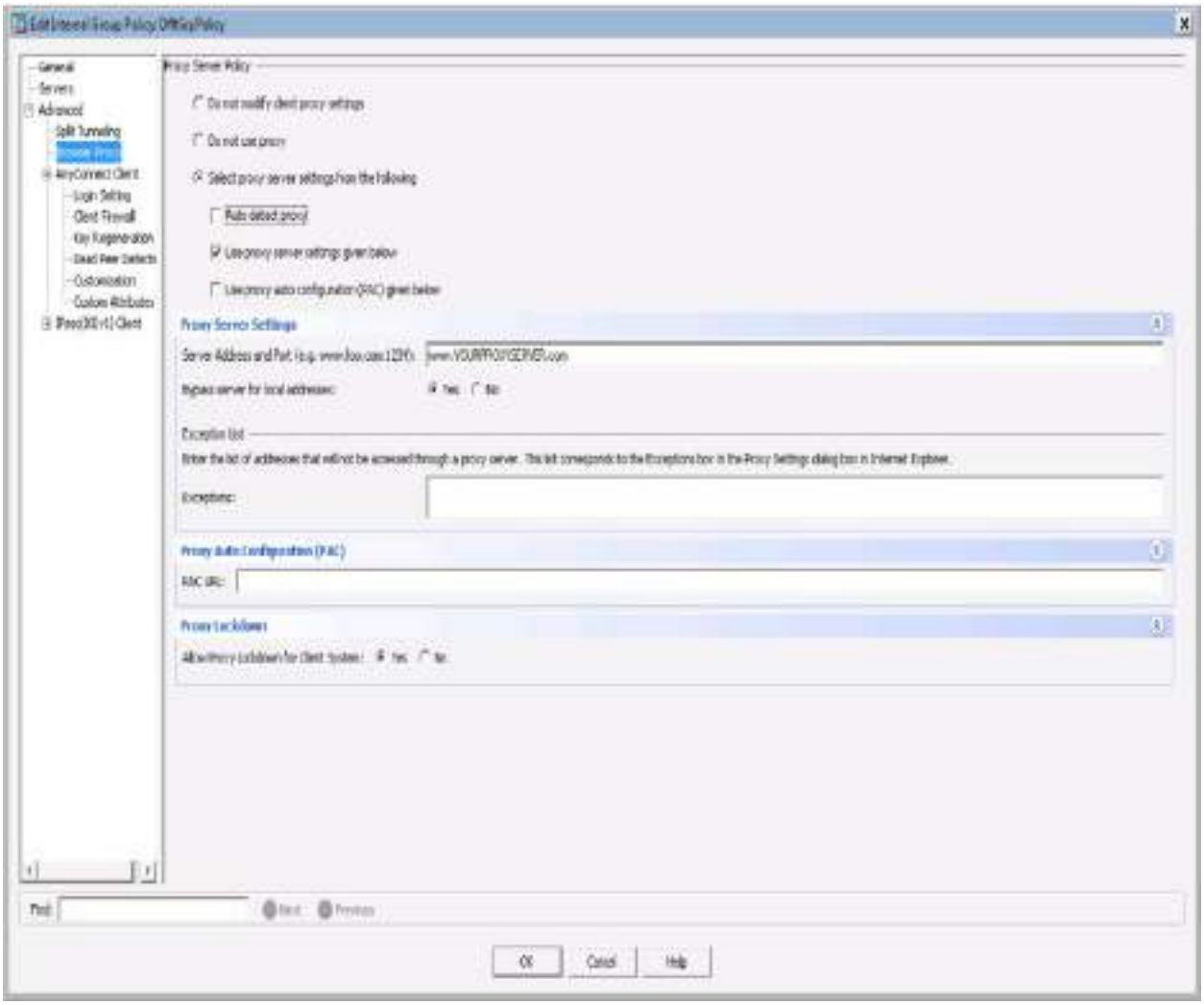


Figure 10-22 Browser Proxy Configuration in a Group Policy

You can also view this information by running the **show running-configuration group-policy** command. Figure 10-23 shows an example for the DfltGrpPolicy and viewing the same proxy server as shown in Figure 10-

22 by using the ASA command line.

Figure 10-23 Browser Proxy Configuration in a Group Policy Using the CLI

NAT Problem

If NAT is not done correctly, it will quickly lead to trouble. Remember that with NAT, the client is sending traffic, and the NAT policy is changing the packet on the way to the network or out from the network. To validate NAT, you can use a tool provided by Cisco, known as Packet Tracer, to view the NAT logic. You can use this tool from the ASA command line, and it is also embedded in ASDM. You can find the tool in ASDM under the Tools menu or by going to **Configuration** > **Firewall** > **Access Rules** and right-clicking an IP address range. You then choose Packet Tracer, as shown in Figure 10-24.

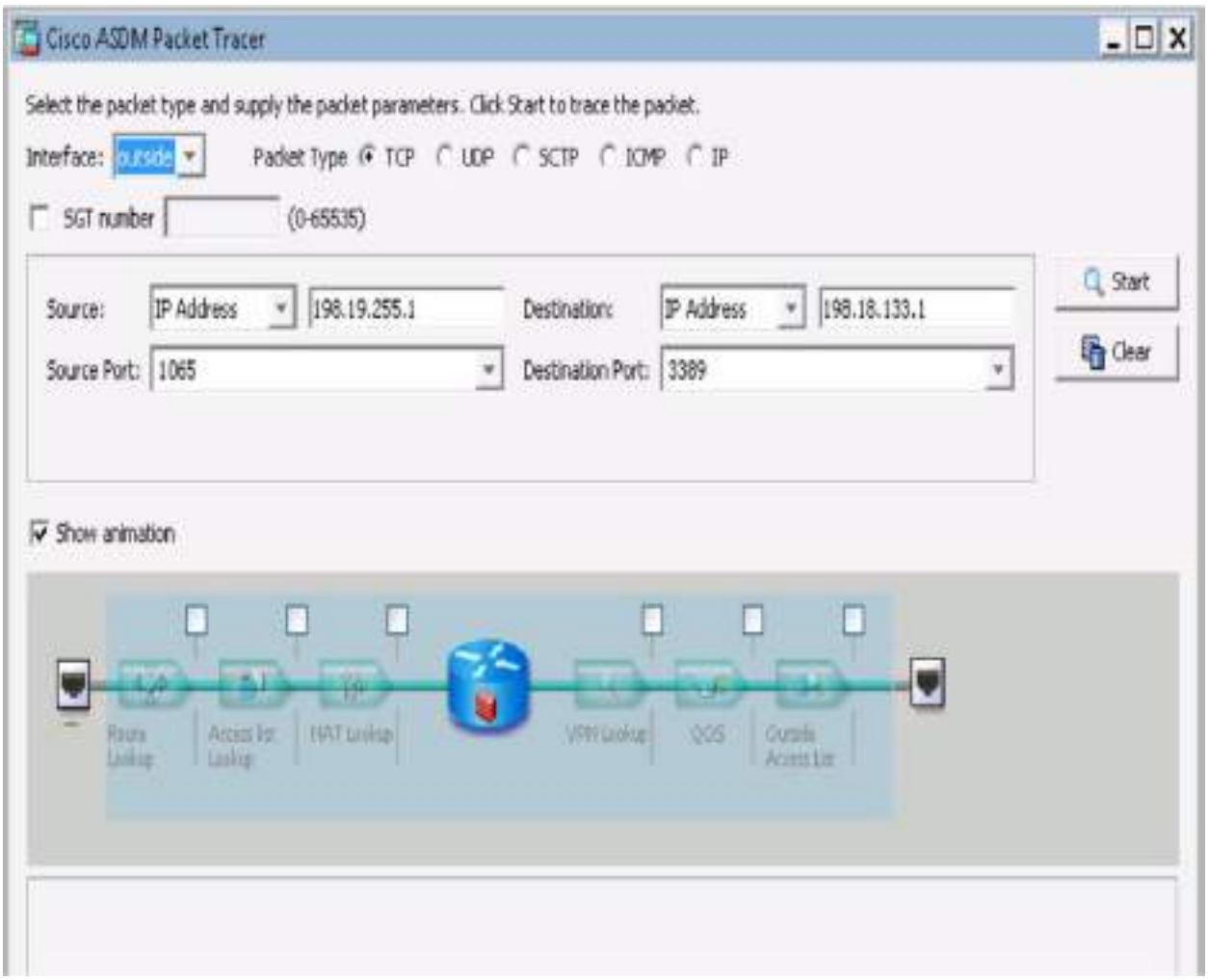


Figure 10-24 Packet Tracer in ASDM

capture Command

You can also use the ASA command line to capture packets for troubleshooting. You run the command **capture** *capture_name* **interface** *interface_name*, where *capture_name* is the name of the capture, and *interface_name* is the name of interface used to perform the capture. You end the command with the IP address range you want to collect.

For example, you could collect traffic to a capture named capin, via the inside interface, matching the source IP address 198.19.255.1, the mask 255.255.255.255, the match destination IP address 198.18.133.1, and the mask 255.255.255.255 as follows:

```
ASA# capture capin interface inside match ip 198.19.255.1
255.255.255.255 198.18.133.1
255.255.255.255
```

Another example for collecting traffic from the outside interface would be as follows:

```
ASA# capture capout interface outside match ip 198.19.255.1
255.255.255.255 198.18.133.1
255.255.255.255
```

When you run a **capture** command, the ASA begins collecting traffic flow until you stop it. To stop the ASA from collecting packets, you run the command **no capture** *capture_name* **interface** *interface_name*. To view the details of what was captured, run the **show capture** *capture_name* command.

capture Command Options

The following are some of the options available with the **capture** command that you need to be familiar with for the SVPN 300-730 exam:

- **asa_dataplane:** Captures packets on the ASA backplane that pass between the ASA and a module that uses the backplane, such as the ASA CX or IPS module.
- **asp-drop** *drop-code***:** Captures packets that are dropped by the accelerated security path. *drop-code* specifies the type of traffic that is dropped by the accelerated security path.
- **ethernet-type** *type***:** Selects an Ethernet type to capture. Supported Ethernet types include 8021Q, ARP, IP, IP6, IPX, LACP, PPPOED, PPPOES, RARP, and VLAN.
- **real-time:** Displays the captured packets continuously in real time. To terminate a real-time packet capture, press Ctrl+C. To permanently remove the capture, use the **no** form of this command. This option is not supported when you use the **cluster exec capture** command.
- **trace:** Traces the captured packets in a manner similar to the ASA Packet Tracer feature.

- **ikev1/ikev2:** Captures only IKEv1 or IKEv2 protocol information.
- **isakmp:** Captures Internet Security Association and Key Management Protocol (ISAKMP) traffic for VPN connections. The ISAKMP subsystem does not have access to the upper-layer protocols. The capture is a pseudo capture, with the physical, IP, and UDP layers combined together in order to satisfy a PCAP parser. The peer addresses are obtained from the SA exchange and are stored in the IP layer.
- **lacp:** Captures Link Aggregation Control Protocol (LACP) traffic. If configured, the interface name is the physical interface name. This might be useful when you work with EtherChannel in order to identify the present behavior of LACP.
- **tls-proxy:** Captures decrypted inbound and outbound data from the Transport Layer Security (TLS) proxy on one or more interfaces.
- **webvpn:** Captures WebVPN data for a specific WebVPN connection.

Note

The Packet Tracer tool may not be able to see VPN traffic.

For the SVPN 300-730 exam, you will likely not have to know how to run Packet Tracer. However, you could see the output of one of these versions of the command-line Packet Tracer command and asked to interpret it. The goal when viewing the output of a packet trace in regard to NAT is to validate how NAT is occurring to ensure traffic is being routed properly. We recommend keeping this skill in mind as packet tracing can also be used for troubleshooting many other network-related issues.

Traffic Filters

The ASA provides a way of filtering traffic that traverses the VPN tunnel, which is a good thing but can also cause some problems if this feature is not properly configured. Traffic filters are configured on the group policy and consist of rules that determine whether to permit or deny tunneled data as it

transverses the ASA. You can filter on source IP address, destination IP address, or even protocol. Administrators use traffic filters as essentially ACLs in order to block or permit various types of traffic but from the VPN policy level. It is important to validate what traffic filter policies are in place if a user complains they are unable to access a specific resource, such as an application.

You configure a traffic filter by first building an ACL and assigning the ACL to a group policy. Next, you assign the group policy to the connection profile used by the VPN and that will force VPN traffic through your filter. An example of a configuration would involve creating an ACL such as one called VPN-FILTER and a group policy called VPN-FILTERPOLICY and then assigning default traffic through the group policy, as shown in the following configuration example:

```
access-list VPN-FILTER permit ip 192.168.1.0 255.255.255.0
10.1.1.0 255.255.255.0
group-policy VPN-FILTERPOLICY internal
group-policy VPN-FILTERPOLICY attribute
 vpn-filter value VPN-FILTER
```

Troubleshooting Traffic Filters

Troubleshooting involves validating the ACLs used in the policy. Essentially, an ACL has an option to permit or deny any resources that are part of what is being permitted or denied. The following is a general ACL skeleton representing what you would need to view as you verify what should be permitted or denied by any traffic filters:

access-list VPN-FILTER permit <*remote-IP*> **[***remote-Port***]** <*local-IP*> [*local-Port*]

Note

The SVPN 300-730 exam may show you an output screen with a ping failing while a VPN is established and ask you to view an output snippet that includes ACLs and filter policies. You will need to be able to identify whether an ACL is the cause of a connection problem. We therefore highly

recommend that you know how to read and build ACLs on a Cisco ASA using the command line.

Network Access Troubleshooting Summary

The following are the key concepts for troubleshooting network access problems:

- Start network access troubleshooting by validating that AnyConnect is enabled, DTLS is enabled, SSL is allowed out of the ASA, and the connection profile being used has SSL enabled.
- Next move to the group policy configuration and verify that the address pool(s) and routing are set up correctly, including whether and how split tunneling is being used.
- Validate whether split DNS or whether all DNS lookups are being sent through a tunnel, and make sure configuration settings are correct.
- Verify whether a browser proxy is enabled and review the AnyConnect client settings that are associated with the VPN policy being used.
- Check for NAT and traffic filtering problems by running Packet Tracker and validating any ACLs that are being used by the VPN policy.

Step 4: Diagnostic and Report Tool (DART)

Cisco provides a tool for troubleshooting AnyConnect connections: Diagnostics and Reporting Tool (DART). DART is a tool built in to AnyConnect that provides troubleshooting information regarding installation, configuration, and environmental problems. DART collects logs, diagnostics, and status information from AnyConnect and outputs them into a .zip file. DART is an AnyConnect module that must be deployed on a client workstation. The SVPN 300-730 exam does not cover detailed DART

troubleshooting, but we mention DART because it can be useful for real-world deployments, and we encourage you to use it at this point of the troubleshooting process. You can use DART instead of running a long list of general diagnostic commands, and its results provide a general diagnostic view of AnyConnect.

Step 5: Diagnostic Commands

It is very possible a VPN will seem to be working correctly, but issues will come up such as packets being dropped, resources being blocked, or other problems that we have covered in this section. If you work through the previous steps and find that everything looks okay, but a problem still exists, you should try running a few diagnostic commands and reviewing the details. The SVPN 300-730 exam may show you output of a general diagnostic command and expect you to identify the problem in the output.

A very important general diagnostic command is the **show vpn-sessiondb detail anyconnect** command. This command shows you what resources are being used by AnyConnect, who the user is, counters for successful packets, and details about the VPN tunnel being used. Example 10-1 shows an example of running this diagnostic command.

Example 10-1 show vpn-sessiondb detail anyconnect Example

```
vpn-asa1# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username     : vpnuser                Index        : 9
Assigned IP  : 172.16.30.1            Public IP    :
198.18.100.10
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-
GCM-256  DTLS-Tunnel: (1)AES-GCM-256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel:
(1)SHA384  DTLS-Tunnel: (1)SHA384
```

```
Bytes Tx     : 15498                  Bytes Rx     : 12934
Pkts Tx      : 12                     Pkts Rx      : 48
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : EMPLOYEE_GROUP         Tunnel Group :
EMPLOYEE_CONNECTION
Login Time   : 04:31:57 UTC Mon Feb 22 2021
Duration     : 0h:01m:07s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 6464018f00009000603333bd
Security Grp : none

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:
  Tunnel ID    : 9.1
  Public IP    : 198.18.100.10
  Encryption   : none                   Hashing      : none
  TCP Src Port : 49870                  TCP Dst Port : 443
  Auth Mode    : userPassword
  Idle Time Out: 30 Minutes             Idle TO Left : 28
Minutes
  Client OS    : win
  Client OS Ver: 10.0.17763
  Client Type  : AnyConnect
  Client Ver   : Cisco AnyConnect VPN Agent for Windows
4.8.03052
  Bytes Tx     : 7749                   Bytes Rx     : 0
  Pkts Tx      : 6                      Pkts Rx      : 0
  Pkts Tx Drop : 0                      Pkts Rx Drop : 0

SSL-Tunnel:
  Tunnel ID    : 9.2
  Assigned IP  : 172.16.30.1            Public IP    :
198.18.100.10
  Encryption   : AES-GCM-256            Hashing      : SHA384
  Ciphersuite  : ECDHE-RSA-AES256-GCM-SHA384
  Encapsulation: TLSv1.2                TCP Src Port : 49874
  TCP Dst Port : 443                    Auth Mode    :
userPassword
  Idle Time Out: 30 Minutes             Idle TO Left : 28
Minutes
  Client OS    : Windows
  Client Type  : SSL VPN Client
  Client Ver   : Cisco AnyConnect VPN Agent for Windows
```

```
4.8.03052
  Bytes Tx     : 7749                    Bytes Rx     : 10112
  Pkts Tx      : 6                       Pkts Rx      : 36
  Pkts Tx Drop : 0                       Pkts Rx Drop : 0

DTLS-Tunnel:
  Tunnel ID    : 9.3
  Assigned IP  : 172.16.30.1             Public IP    :
198.18.100.10
  Encryption   : AES-GCM-256             Hashing      : SHA384
  Ciphersuite  : ECDHE-ECDSA-AES256-GCM-SHA384
  Encapsulation: DTLSv1.2                UDP Src Port : 49771
  UDP Dst Port : 443                     Auth Mode    :
userPassword
  Idle Time Out: 30 Minutes              Idle TO Left : 29
Minutes
  Client OS    : Windows
  Client Type  : DTLS VPN Client
  Client Ver   : Cisco AnyConnect VPN Agent for Windows
4.8.03052
  Bytes Tx     : 0                       Bytes Rx     : 2822
  Pkts Tx      : 0                       Pkts Rx      : 12
  Pkts Tx Drop : 0                       Pkts Rx Drop : 0
```

A more generic and less detailed version of the previous diagnostic command is the **show vpn-sessiondb** command. It is useful for verifying whether a VPN is running, how many clients are using the VPN, and load numbers. You don't get as much detail from this command, but it is useful for getting a quick look at the VPN status. Example 10-2 shows an example of running the **show vpn-sessiondb** command.

Example 10-2 show vpn-sessiondb Example

```
vpn-asa1# show vpn-sessiondb
-------------------------------------------------------------------
------------
VPN Session Summary
-------------------------------------------------------------------
------------
                                Active : Cumulative : Peak
Concur : Inactive
                              ------------------------------------
------------
AnyConnect Client             :      1 :          2
```

```
:           1 :        0
  SSL/TLS/DTLS                :      1 :          2
:           1 :        0
Clientless VPN                :      0 :          3
:           1
  Browser                     :      0 :          3
:           1
-------------------------------------------------------------------
------------
Total Active and Inactive     :      1             Total
Cumulative :      5
Device Total VPN Capacity     :    750
Device Load                   :     0%
-------------------------------------------------------------------
------------


-------------------------------------------------------------------
------------
Tunnels Summary
-------------------------------------------------------------------
------------
                                 Active : Cumulative : Peak
Concurrent
                               ---------------------------------
------------
Clientless                    :      0 :          3
:               1
AnyConnect-Parent             :      1 :          2
:               1
SSL-Tunnel                    :      1 :          2
:               1
DTLS-Tunnel                   :      1 :          2
:               1
-------------------------------------------------------------------
------------
Totals                        :      3 :          9
-------------------------------------------------------------------
------------
```

Additional diagnostic commands to consider include the following:

- **show version:** Checks what type of code is running and shows the system status
- **show cpu usage:** Validates how the system is performing

- **debug webvpn:** Starts running general debugging for the VPN traffic

Step 6: Application

The final troubleshooting topic is verifying whether an issue is related to a specific application, such as an ASA plug-in or the user's browser. Application troubleshooting mirrors client and clientless VPN deployment troubleshooting, and you use the same troubleshooting steps as described earlier in this chapter. As a brief reminder, you first research the application that is causing the problem and validate that it is supported by Cisco. Next, you validate connectivity between the ASA and the application as well as between the user's browser and the application. Finally, you attempt to access the application from the user's site and troubleshoot the user's browser, including clearing the browser cache. Application troubleshooting is not likely to be on the SVPN 300-730 exam, but you might have to deal with it while supporting real-world ASA VPN deployments.

Troubleshooting AnyConnect IKEv2 VPNs on the ASA

The next troubleshooting focus area you must be familiar with to properly prepare for the Cisco SVPN 300-730 exam is troubleshooting AnyConnect IKEv2 VPNs on an ASA. As in the previous sections, in this section we provide a process you can step through to narrow down the possible issues. In this section and the next, we focus on AnyConnect IKEv2 VPNs both when using a Cisco ASA and when leveraging a Cisco router as the VPN headend. The focus is on the VPN tunnel and a few common host-side error messages; other troubleshooting steps, including testing connectivity and login problems, are covered earlier in this chapter. We mention those steps to keep the troubleshooting process complete, but we leave out the details to avoid repetition.

Step 0: Prepare

As with the other troubleshooting sections, the first part of troubleshooting

any technology deployment is understanding what components are involved —what we call *step zero*. Troubleshooting AnyConnect IKEv2 VPNs means looking at an ASA that is acting as the VPN concentrator with AnyConnect playing the role of VPN client and the IKEv2 protocol being used for the VPN, as shown in Figure 10-25. It is highly recommended that you keep this simple architecture in your mind as you approach AnyConnect IKEv2 questions on the exam so you can quickly weed out any wrong answers referencing technology or configurations that aren't being used.

Figure 10-25 AnyConnect IKEv2 VPN on a Cisco ASA Example

In this section, as in the earlier sections of this chapter, we look at troubleshooting in different section. First, we look at connectivity to the ASA. Steps for troubleshooting connectivity are covered earlier in this chapter and are not repeated here. If the ASA can't be reached, you know the issue is likely network or certificate related, and the focus can be on fixing these types of problems. If connectivity works but you can't log in to the VPN after making a connection, troubleshooting should focus on login challenges, which is also covered earlier in this chapter.

Once you have validated that connectivity and login issues do not exist, you focus on the VPN connection status, which is the focus of this section and the next. Our focus on troubleshooting the VPN connection will be limited to a handful of specific commands you can use to validate the VPN status for a IKEv2 VPN deployment. The details provided from using these commands should give you enough information to troubleshoot the VPN connection

status. You need to be familiar with all aspects of using these commands for the SVPN 300-730 exam, including understand what each command does, what type of output it shows, and how the output relates to troubleshooting.

Finally, troubleshooting shifts to the client side if you do not have access to the ASA command line, if you want to test VPN problems from the client side, or if the exam asks questions regarding host-based troubleshooting. We touched on general host troubleshooting, including host browser settings and potential browser problems, earlier in this chapter, and this section covers just a few common host errors found specifically in AnyConnect IKEv2 deployments.

Troubleshooting AnyConnect IKEv2 VPNs involves the following steps:

Step 1. Connectivity: Confirm that the system looking to connect to the VPN tunnel can reach the ASA or router.

- Can you ping between systems?
- Validate certificate configuration.

Step 2. Login: Troubleshoot any login issues, including ensuring that the proper user group is selected and that the user is able to pass all authentication and authorization steps.

- Tunnel group selection
- Authentication
- Authorization
- Group policy selection

Step 3. IKEv2 status validation: Run commands to validate the status of the VPN.

- Run the command **show vpn-sessiondb detail anyconnect**
- Run the command **show crypto ikev2 sa**
- Run the command **show crypto ikev2 sa detail**
- Run the command **debug crypto ikev2**

Step 4. Host: Troubleshoot issues related to accessing the application.

- Check for an invalid host entry.
- View the AnyConnect agent by using the DART tool or general agent logs to confirm that there isn't a host side issue.

Let's walk through these steps in more detail, starting with troubleshooting connectivity and login issues.

Steps 1 and 2: Connectivity and Login to the VPN Concentrator

All troubleshooting steps start off by validating connectivity to the VPN concentrator (ASA or router). This is the most common place for an issue to occur. Issues could occur during the initial deployment but more commonly come up later, while the VPN solution is in operation. Network changes, such as a firewall rule change that disables Internet access to the ASA, commonly break working VPN deployments. Therefore, troubleshooting should focus on performing all standard network validation efforts, such as pinging each device involved to validate that the devices are reachable (device-to-ASA and vice versa) and confirming that a firewall or other technology along the path of the connection hasn't been changed. We cover how to troubleshoot connectivity earlier in this chapter, and the troubleshooting steps are the same for any type of VPN setup.

Once connectivity is validated, you need to confirm that users can log in. This includes ensuring that the connection/group is properly configured, the user is properly authenticated, and the user is authorized for the privileges associated with the assigned group. We cover troubleshooting ASA login issues earlier in this chapter, and the troubleshooting steps are the same, regardless of the type of ASA VPN being deployed.

If connectivity and login testing confirm that there are no issues, the next step for troubleshooting an IKEv2 VPN is to troubleshoot the VPN connection. This brings us to the third step in troubleshooting a IKEv2 VPN.

Step 3: VPN Status Validation

If the connectivity and login is confirmed to be working, the next step for troubleshooting an IKEv2 VPN is validating that the VPN is working from the VPN concentrator viewpoint. SVPN 300-730 exam troubleshooting questions will mostly provide snippets of either debugging code or **show** commands as your only view into troubleshooting a connectivity problem. You will be expected to review the output of a command and determine the most likely cause of the issue. It is very unlikely that the exam will test you on something as simple as a ping showing that something is unavailable, so make sure to be familiar with all steps that occur during an IKEv2 VPN connection, as explained in Chapter 8. You might, however, find that a ping is successful but the VPN does not works due to the UDP and TCP ports for the VPN being filtered. For SSLVPN, TCP and UDP port 443 must be available. For IKE, UDP port 500 and UDP port 4500 are used. Questions around required ports are fair game on the SVPN 300-730 exam.

This troubleshooting section focuses on validating different aspects of an IKEv2-based VPN tunnel using the ASA command line. For the exam and real-world deployments, the most common ASA commands that you need to be familiar with for IKEv2 troubleshooting with AnyConnect are as follows:

- **show vpn-sessiondb detail anyconnect:** The **show vpn-sessiondb** command is used to view summary information about the VPN session. Adding **detail anyconnect** provides even more details about AnyConnect sessions.
- **show crypto ikev2 sa:** This command displays the state of the Phase 1 tunnel
- **show crypto ikev2 sa detail:** This command displays more details about the state of the Phase 1 tunnel
- **show crypto ipsec sa:** This command displays details about the state of the Phase 2 tunnel

- **debug crypto ikev2 255:** This command enables debugging, which provides details on current crypto IKEv2 activity

---

Note

We can't stress enough the need to be familiar with the output expected from each of these commands. The SVPN 300-730 exam may ask you to both interpret command output and identify which command would display certain output. Knowing these commands is also essential for real-world troubleshooting.

Each of these commands can be used to validate the status of a VPN session. The following sections look at them in more detail.

Command 1: show vpn-sessiondb detail anyconnect

When you run the command **show vpn-sessiondb detail anyconnect** on the ASA command line, you need to look for an established VPN connection, validate the user and network information, validate the protocol used, check the group policy and connection profile information, check the authentication method used, and check NAT information. Example 10-3 shows a healthy VPN connection.

For the SVPN 300-730 exam and in the real world, you need to know how to validate proper operation of any of the details seen in this output. The exam will expect you to be able to interpretate this output. Notice that you can validate the username, IP address information, protocol, license being used, type of encryption (in this example, AES-256), hashing (in this example, SHA-1), group policy, connection profile, login time, and many other details. (We cover how to set up an ASA VPN using IKEv2 in Chapter 9.) Be familiar with all data points shown in Example 10-3 and know how to flag errors in configuration compared to expected VPN configurations as you are troubleshooting.

Example 10-3 show vpn-sessiondb detail anyconnect Example

```
vpn-asa1# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username     : vpnuser                Index        : 11
Assigned IP  : 172.16.30.1            Public IP    :
198.18.100.10
Protocol     : IKEv2 IPsecOverNatT AnyConnect-Parent
License      : AnyConnect Premium
Encryption   : IKEv2: (1)AES256  IPsecOverNatT:
(1)AES256  AnyConnect-Parent: (1)none
Hashing      : IKEv2: (1)SHA1  IPsecOverNatT:
(1)SHA1  AnyConnect-Parent: (1)none
Bytes Tx     : 0                      Bytes Rx     : 12251
Pkts Tx      : 0                      Pkts Rx      : 45
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : EMPLOYEE_GROUP         Tunnel Group :
EMPLOYEE_CONNECTION
Login Time   : 04:46:27 UTC Mon Feb 22 2021
Duration     : 0h:00m:11s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 6464018f0000b00060333723
Security Grp : none

IKEv2 Tunnels: 1
IPsecOverNatT Tunnels: 1
AnyConnect-Parent Tunnels: 1

AnyConnect-Parent:
  Tunnel ID    : 11.1
  Public IP    : 198.18.100.10
  Encryption   : none                   Hashing      : none
  Auth Mode    : userPassword
  Idle Time Out: 30 Minutes             Idle TO Left : 29
Minutes
  Client OS    : win
  Client OS Ver: 10.0.17763
  Client Type  : AnyConnect
  Client Ver   : 4.8.03052

IKEv2:
  Tunnel ID    : 11.2
  UDP Src Port : 59697                  UDP Dst Port : 4500
  Rem Auth Mode: userPassword
  Loc Auth Mode: rsaCertificate
  Encryption   : AES256                 Hashing      : SHA1
```

```
  Rekey Int (T): 86400 Seconds          Rekey Left(T): 86387
Seconds
  PRF          : SHA1                   D/H Group    : 2
  Filter Name  :
  Client OS    : Windows                Client Type  :
AnyConnect

IPsecOverNatT:
  Tunnel ID    : 11.3
  Local Addr   : 0.0.0.0/0.0.0.0/0/0
  Remote Addr  : 172.16.30.1/255.255.255.255/0/0
  Encryption   : AES256                 Hashing      : SHA1
  Encapsulation: Tunnel
  Rekey Int (T): 28800 Seconds          Rekey Left(T): 28787
Seconds
  Idle Time Out: 30 Minutes             Idle TO Left : 29
Minutes
  Bytes Tx     : 0                      Bytes Rx     : 12416
  Pkts Tx      : 0                      Pkts Rx      : 46
```

Command 2: show crypto ikev2 sa

The next command on our list is the **show crypto ikev2 sa** command. When you execute this command, your goal is to validate the status of Phase 1 by looking for the *UP-ACTIVE* status. You can also validate the IP address ranges being used and details regarding the session. In a real-world deployment, you will likely use the detailed version of this command. However, the exam may only provide the standard **show** version, as shown in Example 10-4.

Example 10-4 show crypto ikev2 sa Example

```
vpn-asa1# show crypto ikev2 sa

IKEv2 SAs:

Session-id:1, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id
Local                                                   Remote
Status         Role
222048265
203.0.113.30/4500                                       198.18.100.
```

```
10/59697
READY    RESPONDER
      Encr: AES-CBC, keysize: 256, Hash: SHA96, DH Grp:2, Auth
sign: RSA, Auth verify: EAP
      Life/Active Time: 86400/101 sec
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 172.16.30.1/0 - 172.16.30.1/65535
          ESP spi in/out: 0x873fc6b5/0xaa72493d
```

Command 3: show crypto ikev2 sa detail

The **show crypto ikev2 sa detail** command adds detail to the previous command, allowing for more details to be included with the **show** output. In practice, you should use the **detail** version of this command, which gives you data counts, SPI details, child and parent SA status, and other details. Example 10-5 shows sample output of using the **show crypto ikev2 sa detail** command. We highly recommend being familiar with both versions of this command for the SVPN 300-730 exam.

Example 10-5 show crypto ikev2 sa detail Example

```
vpn-asa1# show crypto ikev2 sa detail

IKEv2 SAs:

Session-id:1, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id
Local                                                   Remote
Status         Role
222048265
203.0.113.30/4500                                       198.18.100.
10/59697
READY    RESPONDER
      Encr: AES-CBC, keysize: 256, Hash: SHA96, DH Grp:2, Auth
sign: RSA, Auth verify: EAP
      Life/Active Time: 86400/147 sec
      Session-id: 1
      Status Description: Negotiation done
      Local spi: 61C61EC6967F5ABF       Remote spi:
D7B7EBC81348D7D1
      Local id: cn=vpn-asa1.example.com
      Remote id: *$AnyConnectClient$*
```

```
      Local req mess id: 0             Remote req mess id: 10
      Local next mess id: 0            Remote next mess id: 10
      Local req queued: 0              Remote req queued: 10
      Local window: 1                  Remote window: 1
      DPD configured for 30 seconds, retry 2
      NAT-T is detected  outside
      Assigned host addr: 172.16.30.1
      IKEv2 Fragmentation Configured MTU: 576 bytes, Overhead:
28 bytes, Effective MTU: 548 bytes
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 172.16.30.1/0 - 172.16.30.1/65535
          ESP spi in/out: 0x873fc6b5/0xaa72493d
          AH spi in/out: 0x0/0x0
          CPI in/out: 0x0/0x0
          Encr: AES-CBC, keysize: 256, esp_hmac: SHA96
          ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
Parent SA Extended Status:
      Delete in progress: FALSE
      Marked for delete: FALSE
```

Command 4: show crypto ipsec sa

The **show crypto ipsec sa** command is important for troubleshooting Phase 2 and provides important details regarding the status of the VPN connection. The SVPN 300-730 exam may give you parts of this **show** output and ask you why an issue is occurring. This command includes various counters, including counters that are triggered when a failure occurs. The exam might ask you why a problem is occurring when it shows output with #pre-frag failures increasing in count. It might also ask you to confirm details in the output of this command, such as specifics in the *outbound esp sas* section.

A very common issue that can be identified with this command is traffic being blocked in one direction. In Example 10-6, #pkts encaps is 47, and #pkts decaps is 0. Such output can occur for two reasons: Either no traffic is being sent by the other side of the connection or traffic is being sent by the other side of the connection but is blocked along the path.

Example 10-6 show crypto ipsec sa Example

```
vpn-asa1# show crypto ipsec sa
interface: OUTSIDE
    Crypto map tag: SYSTEM_DEFAULT_CRYPTO_MAP, seq num: 65535,
```

```
local addr: 203.0.113.30

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port):
(172.16.30.1/255.255.255.255/0/0)
      current_peer: 198.18.100.10, username: vpnuser
      dynamic allocated peer ip: 172.16.30.1
      dynamic allocated peer ip(ipv6): 0.0.0.0

      #pkts encaps: 47, #pkts encrypt: 47, #pkts digest: 47
      #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts
decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments
created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs
needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 203.0.113.30/4500, remote crypto
endpt.: 198.18.100.10/59697
      path mtu 1472, ipsec overhead 66(52), override mtu 1406,
media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: AA72493D
      current inbound spi : 873FC6B5

    inbound esp sas:
      spi: 0x873FC6B5 (2269103797)
         SA State: active
         transform: esp-aes-256 esp-sha-hmac no compression
         in use settings ={RA, Tunnel,  NAT-T-Encaps, IKEv2, }
         slot: 0, conn_id: 11, crypto-map:
SYSTEM_DEFAULT_CRYPTO_MAP
         sa timing: remaining key lifetime (sec): 28611
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x0000FFFF 0xFFFFFFFF
    outbound esp sas:
      spi: 0xAA72493D (2859616573)
         SA State: active
         transform: esp-aes-256 esp-sha-hmac no compression
         in use settings ={RA, Tunnel,  NAT-T-Encaps, IKEv2, }
```

```
          slot: 0, conn_id: 11, crypto-map:
SYSTEM_DEFAULT_CRYPTO_MAP
          sa timing: remaining key lifetime (sec): 28611
          IV size: 16 bytes
          replay detection support: Y
          Anti replay bitmap:
           0x00000000 0x00000001
```

Command 5: debug crypto ikev2 255

The **debug crypto ikev2 255** command enables debugging. Logging messages start to appear when you attempt the VPN connection and often include log messages both before and after failure occurs. To disable debugging, you use the command **no debug all**. Unlike with routers, though, the ASA stops debugging when you log off.

Note

Questions on the SVPN 300-730 exam typically state that debugging was enabled and provide the debug output that was seen as the VPN connection was attempted.

Note

The five commands described here enables you to properly validate the status of an IKEv2 VPN. If everything looks functional from the VPN tunnel viewpoint or if you don’t have access to the command line of the ASA, you can troubleshoot the VPN from the host attempting to connect to the VPN concentrator (the ASA). The SVPN 300-730 exam might also test you on host troubleshooting, which is our next topic.

Step 4: Host Troubleshooting

Another focus area for troubleshooting is the host running AnyConnect

representing the system attempting to connect to the VPN concentrator (the ASA). It is likely that issues will first be discovered on hosts. That is, end users may experience problems and escalate the issue for administrators to troubleshoot. The focus of this section is on evaluating a few common error messages that can come up when you run an IKEv2 VPN deployment.

Chapter 9 describes how to view details about remote access VPN status using tools available in AnyConnect. Earlier in this chapter, you learned about common general host problems that occur due to browser problems, which would be identical for troubleshooting any type of VPN from the host viewpoint. Make sure you are familiar with validating VPN status from the host level as the SVPN 300-730 exam could include screenshots of output from AnyConnect and ask you to validate what is being shown.

The following sections look at two error messages your end users may experience when things are not working with an IKEv2 VPN set up on a Cisco ASA.

Invalid Host Entry

One possible error message a user may experience is the AnyConnect message “Invalid host entry. Please re-enter.” This error occurs when the user group name in the XML client profile does not match the name of the connection profile on the ASA. The user group name and connection profile name must be the same. Otherwise, the “Invalid host entry. Please re-enter.” error message appears on the AnyConnect client, as shown in Figure 10-26.


Recycle Bin
vpnuser.p12
Example Root CA_cert.cer
Google Chrome
Profile - Shortcut
Firefox
DisableIPv...
iss-ikev2-t...
vpn-ecdsa-e...
DisableIPv...
iss-employee ikev2 conne...
anyconnect...
VPN Profile Editor
iss-employ...
anyconnect...
iss-ikev2-c...
AnyConnect Profile Edit...
ikev - Shortcut
Cisco AnyConnect Secure Mobility Client
Cisco AnyConnect
Invalid host entry. Please re-enter.
OK
9:01 PM

Figure 10-26 “Invalid Host Entry. Please Re-enter” Error Example

Chapter 9 uses the user group EMPLOYEES for a configuration example. The user group EMPLOYEES in Figure 10-26 is the reason for the error that is being displayed. Chapter 9 calls the connection profile EMPLOYEE_CONNECTION, which is different from EMPLOYEES. Unlike with SSLVPN connections, where the user group does not have to match the connection profile name, the user group for IKEv2 connections must match the connection profile name exactly. You can validate this configuration in the AnyConnect client profiler editor by going to the Server List screen, as shown in Figure 10-27.

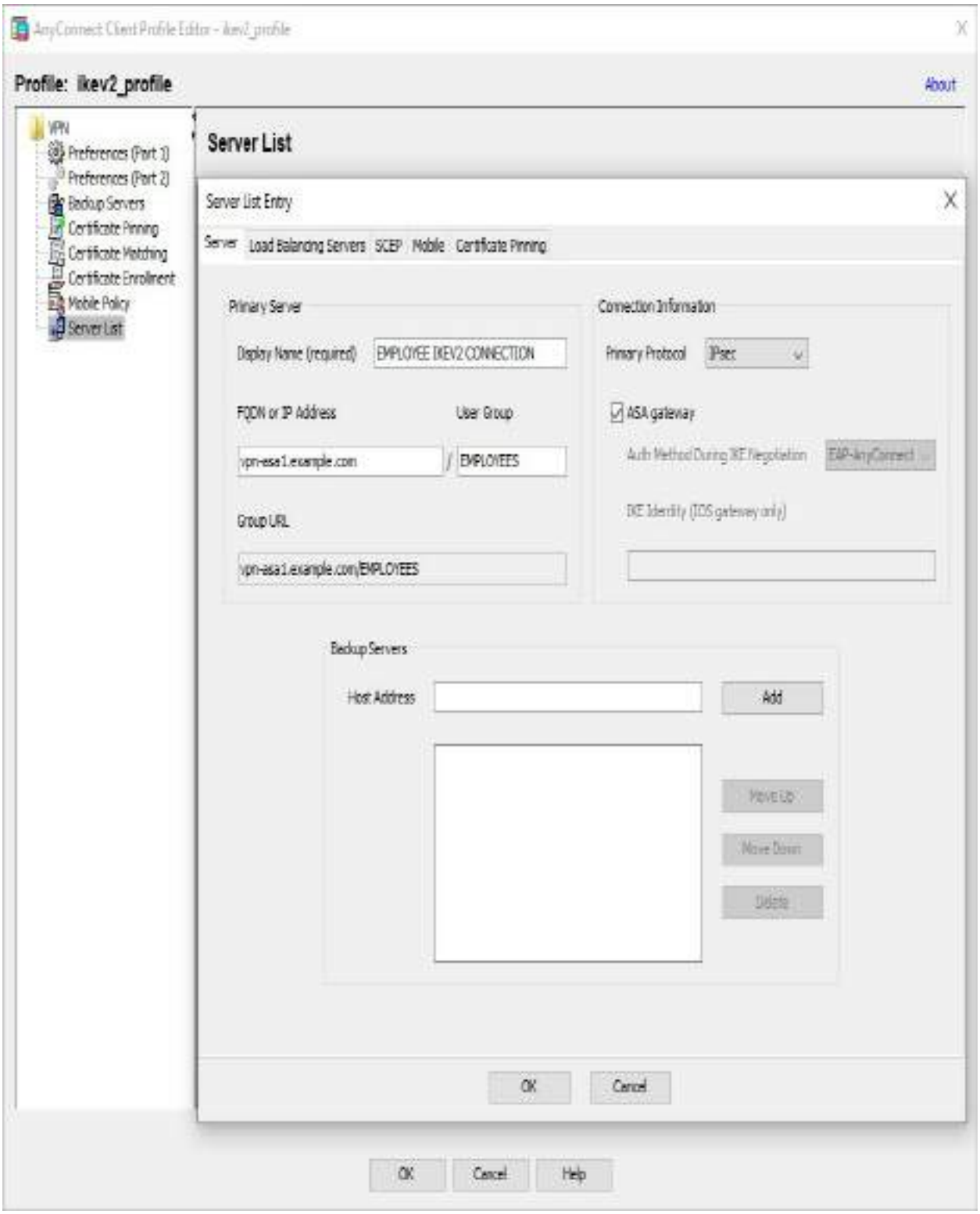


Figure 10-27 AnyConnect Client Profiler Editor Example

There are other issues that could come up, and we recommend leveraging

DART to view the log details. The SVPN 300-730 exam will likely use DART output od to test you on troubleshooting AnyConnect-related issues.

Troubleshooting AnyConnect IKEv2 VPNs on Routers

The final troubleshooting topic to cover is AnyConnect IKEv2 VPNs on routers. Up until this point in the chapter, we have focused on IKEv2 troubleshooting commands from the ASA command line. The Cisco SVPN 300-730 exam also expects you know router-based VPN troubleshooting, which is the focus of this section. The basic components involved with an AnyConnect IKEv2-based VPN on a router are the AnyConnect client and a router acting as the VPN concentrator. Figure 10-28 shows an example of the configuration used for this section's troubleshooting examples.

Figure 10-28 AnyConnect IKEv2 VPN Router Setup Example

Many of the steps for troubleshooting a router-based VPN are identical to the steps described for using an ASA. You should test connectivity to each device, validate the certificates, confirm that the login process works, test the IKEv2 status by using the router command line, and check the status of AnyConnect on the host.

Troubleshooting router-based AnyConnect IKEv2 VPNs involves the following steps:

Step 1. Connectivity: Confirm that the system looking to connect to the VPN tunnel can reach the router.

- Can you ping between systems?
- Validate certificate configuration.

Step 2. Login: Troubleshoot any login issues, including confirming that the proper user group is selected and the user is able to pass all authentication and authorization steps.

- Group selection
- Authentication
- Authorization

Step 3. IKEv2 status validation: Run commands to validate the status of the VPN.

- Run the command **show crypto ipsec sa detail**
- Run the command **show crypto session detail**
- Run the command **debug aaa commands**
- Run the command **debug crypto ikev2**

Step 4. Hosts: Troubleshoot issues related to accessing the application.

- Check for invalid host entry.
- View the AnyConnect agent by using DART or general agent logs to confirm that there isn't a host side issue.

Many of these steps are exactly the same as the ones covered earlier in this chapter.

Steps 1 and 2: Connectivity and Login to the Router

By now you know that any troubleshooting starts with testing connectivity. You must first confirm that everything is reachable by using **ping** to ensure that a security tool is not preventing communication or something else is not

causing a disruption in connection. Next, you need to make sure the certificates are valid. After testing connectivity, you need to confirm that the login process functions properly. If connectivity testing confirms that there are no issues and the login process works, the next step for troubleshooting an IKEv2 VPN is to troubleshoot the VPN connection. Let's look at how this works on a Cisco router.

Step 3: VPN Status Validation

If connectivity and login troubleshooting show that things are working, the next step you should take is validating the status of the VPN. This section focuses on validating different aspects of an IKEv2-based VPN tunnel on a Cisco router.

For the SVPN 300-730 exam, you should be familiar with the following router commands:

- **show crypto ipsec sa detail:** This command displays details about the state of the Phase 2 tunnel.
- **show crypto session detail:** This command provides details on the current status of the crypto session.
- **debug aaa commands:** These commands are used to validate the authentication and authorization lists that are used as well as troubleshooting any AAA-related issues.
- **debug crypto ikev2:** This command enables debugging for crypto IKEv2 to provide live details about the IKEv2 status.

Notice that a few of these commands are similar or identical to the ones just covered for troubleshooting an ASA IKEv2 VPN. The output will be different on a router, but the general details displayed will provide similar data points that you will need in order to validate the status of the VPN.

Let’s look more closely at these commands.

Command 1: show crypto ipsec sa detail

The **show crypto ipsec sa detail** command that you have already seen for troubleshooting IKEv2-based VPNs using an ASA is also used with routers. You use it to validate the status of the connection, determine which devices are involved, learn what is enabled or disabled, and get SPI info and other details. Example 10-7 shows an example of issuing the **show crypto ipsec sa detail** command on a router; as you can see, this is very similar to running this command at the CLI of a Cisco ASA.

Example 10-7 show crypto ikev2 sa detailed Example

```
VPN-ROUTER# show crypto ikev2 sa detailed
 IPv4 Crypto IKEv2  SA

Tunnel-id
Local                  Remote                fvrf/ivrf
  Status
1         203.0.113.20/4500     198.18.100.10/63454   none/none
            READY
      Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512,
DH Grp:21, Auth sign: RSA, Auth
verify: AnyConnect-EAP
      Life/Active Time: 86400/48 sec
      CE id: 1016, Session-id: 8
      Status Description: Negotiation done
      Local spi: 24C27AD8AF48D3E9       Remote spi:
49A438F8575181B2
      Local id: 203.0.113.20
      Remote id: *$AnyConnectClient$*
      Remote EAP id: vpnuser
      Local req msg id:  0              Remote req msg id:  7
      Local next msg id: 0              Remote next msg id: 7
      Local req queued:  0              Remote req queued:  7
      Local window:      5              Remote window:      1
      DPD configured for 0 seconds, retry 0
      Fragmentation not  configured.
      Dynamic Route Update: disabled
      Extended Authentication not configured.
      NAT-T is detected  outside
      Cisco Trust Security SGT is disabled
      Assigned host addr: 172.16.2.8
```

```
      Initiator of SA : No

 IPv6 Crypto IKEv2  SA
```

Command 2: show crypto session detail

As you have already seen for troubleshooting on an ASA, the **crypto session detail** command is used to validate the details of the crypto session on a router. The SVPN 300-730 exam may use the abbreviated version of this command, but real-world troubleshooting typically requires the **detail** version. Details include the profile being used, uptime, status, IP addresses for each side, and other details, as shown in Example 10-8.

Example 10-8 show crypto session detail Example

```
VPN-ROUTER# show crypto session detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation
R - IKE Auto Reconnect, U - IKE Dynamic Route Update
S - SIP VPN

Interface: Virtual-Access1
Profile: LOCAL_USER_IKEV2_PROFILE
Uptime: 00:00:11
Session status: UP-ACTIVE
Peer: 198.18.100.10 port 63454 fvrf: (none) ivrf: (none)
      Phase1_id: *$AnyConnectClient$*
      Desc: (none)
  Session ID: 32
  IKEv2 SA: local 203.0.113.20/4500 remote 198.18.100.10/63454
Active
          Capabilities:N connid:1 lifetime:23:59:49
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 host 172.16.2.8
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 48 drop 0 life (KB/Sec)
4607985/3589
        Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec)
4608000/3589
```

Command 3: debug aaa

You use general AAA **debug** commands to determine whether authentication and authorization are functioning properly. As with any other **debug** command, you must first enable debugging before you attempt to perform an activity or wait for the activity to occur before data will show. Example 10-9 shows an example of enabling debugging for authorization and authentication on a router. The same commands can be used on an ASA, and with either an ASA or a router, the goal is to validate the correct authentication and authorization groups. In Example 10-9, LOCAL_USER_AUTHC is the authentication list being used, and LOCAL_GROUP-AUTHZ is the authorization list being used. The SVPN 300-730 exam may show you **debug aaa** output and ask you to validate which list is being used. Understanding **debug aaa** output can help you easily select the correct response.

Example 10-9 debug aaa Example

```
VPN-ROUTER# debug aaa authentication
AAA Authentication debugging is on
VPN-ROUTER# debug aaa authorization
AAA Authorization debugging is on
*Feb 23 03:44:58.203: AAA/BIND(0000001C): Bind i/f
*Feb 23 03:44:58.204: AAA/AUTHEN/LOGIN (0000001C): Pick method
list 'LOCAL_USER_AUTHC'
*Feb 23 03:44:58.211: AAA/BIND(0000001D): Bind i/f
*Feb 23 03:44:58.211: AAA/AUTHOR (0x1D): Pick method list
'LOCAL_GROUP_AUTHZ'
*Feb 23 03:44:58.213: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Virtual-Access1, changed
state to down
*Feb 23 03:44:58.246: %SYS-5-CONFIG_P: Configured
programmatically by process Crypto INT from
console as console
*Feb 23 03:44:58.286: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Virtual-Access1, changed
state to up
```

Summary

Troubleshooting a VPN requires a strong understanding of how VPN

technology works. If you don’t feel confident in the deployment of any of the four VPN designs covered in this chapter, you need to go back to the chapter that covers how the technology works and master how to build the VPN before you invest time understanding associated troubleshooting concepts. Consider studying troubleshooting as a way to validate what you already know about a particular VPN technology.

The general steps for troubleshooting VPN technology covered in this chapter can be broken into a number of focus areas. Before taking any action, we recommended a taking a step zero to understand the technology you are working with. After you have researched what you will be working with, you can begin troubleshooting connectivity concepts to ensure that communication is functioning. This includes troubleshooting certificate and DNS problems as well as using **ping** to confirm connectivity. Next, you can look at how users log in to the VPN. When you have eliminated connectivity and login problems as the cause of a VPN issue, you can move to troubleshooting VPN services. For SSL, this includes focusing on the WebVPN service, bookmarks, and applications; with IKEv2, troubleshooting includes running a handful of commands to view different aspects of the VPN status. Finally, troubleshooting should focus on the host, looking at problems specific to the user’s system. Problems could include the user’s browser or system not supporting different aspects of the VPN, and you would need to work with the user to address such problems.

Even though you have finished reading the topical chapters of this book, you need to do more to prepare for the SVPN 300-730 exam and master configuring, running, and troubleshooting VPN networks. Security is a journey, not a destination, and you cannot master it just by reading a book. Mastering a skill requires practice. We have included a bunch of sample questions you should work through not with the focus of memorizing, but with a focus on understanding why each question is being asked so you can challenge your knowledge of the topic being addressed. We also highly recommend working with VPN technology in a lab environment so you can better understand when to use the steps covered here as well as what the output of certain commands looks like. You could also use a search engine to find videos and screenshots of commands or walkthroughs of topics covered in this book.

This book provides coverage of the SVPN 300-730 exam topics, and you will be expected to know everything covered here, including different viewpoints, such as command-line code snippets, error messages, host VPN or administration viewpoints, and everything in between. In short, you should study the concepts in this book and leverage different resources to further review what you believe you need to master before you can feel confident going into the SVPN 300-730 exam.

We appreciate your investment in this resource and wish you the best of luck with the SVPN 300-730 exam as well as future work with VPN technology. Thank you from the writing team!

Reference

ASA Clientless VPN Troubleshooting. Retrieved from https://www.cisco.com/c/en/us/td/docs/security/asa/asa96/configuration/vpn/asa-96-vpn-config/webvpn-troubleshooting.html#ID-2276-00000005

Exam Preparation Tasks

As mentioned in the section "How to Use This Book" in the Introduction, you have a couple of choices for exam preparation: the exercises here, Chapter 11, "Final Preparation," and the exam simulation questions in the Pearson Test Prep software online.

Review All Key Topics

Review the most important topics in the chapter, noted with the key topics icon in the outer margin of the page. Table 10-2 lists these key topics and the page number on which each is found.

Table 10-2 Key Topics for Chapter 10

Key Topic Element	Description	Page Number
List	Understand four troubleshooting categories	
Paragraph	Understand troubleshooting ASA WebVPN service	
Paragraph	Troubleshooting certificates	
Section	Group Policy	
Section	Step 3: Clientless WebVPN Service Issues	
Paragraph	Bookmarks	
List	Group Policy Troubleshooting	
List	Network Access Troubleshooting Summary	
Paragraph	Diagnostic Commands	
List	IKEv2 Based VPN commands	
List	VPN Status Router commands	

Complete Tables and Lists from Memory

This chapter does not have any memory tables.

Define Key Term

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

WebVPN

Use the Command Reference to Check Your Memory

Table 10-3 lists the important commands from this chapter. To test your memory, cover the right side of the table with a piece of paper, read the description on the left side, and see how much of the command you can remember.

Table 10-3 ASA CLI Commands

Task	Command Syntax
Troubleshoot or validate ASA licenses	ciscoasa# **show vpn-sessiondb license-summary**
Validate that the ASA VPN service is up	ciscoasa# **show vpn-sessiondb**
Create a PCAP file on the ASA	ciscoasa# **capture webvpn-issue type webvpn user user1**
Enable LDAP debugging on ASA	ciscoasa# **debug LDAP 255**
Validate details about WebVPN service	ciscoasa# **show vpn-sessiondb detail webvpn**
Validate a VPN bookmarks list	ciscoasa# **export webvpn url-list stdout**
View summary information about the VPN session	ciscoasa# **show vpn-sessiondb detail anyconnect**
Displays details about the state of the phase 1 tunnel	ciscoasa# **show crypto ikev2 sa detail**
Displays details about the state of the phase 2 tunnel	ciscoasa# **show crypto ipsec sa**
Enables debugging, which provides details on current crypto IKEv2 activity	ciscoasa# **debug crypto ikev2**

Part IV: SVPN Preparation

Chapter 11. Final Preparation

The first 10 chapters of this book cover the technologies, protocols, design concepts, and considerations required to be prepared to pass the Implementing Secure Solutions with Virtual Private Networks (SVPN 300-730) exam. While these chapters supply the detailed information, most people need more preparation than simply reading the first 10 chapters of this book and going right into the exam. A large part of the exam will have you identify problems with configurations as well as interpret output from commands. The best way to learn these concepts is to practice with the technology using a lab environment. An alternative approach is watching videos of configuration so you can link the concepts we covered with examples of how they are used during a real deployment. To be clear, the SVPN is not memorization-based exam. It is an applied concept exam meaning you need to understand the content covered and apply that knowledge against situations you will encounter on the exam.

This chapter details a set of tools and a study plan to help you complete your preparation for the exam. We highly encourage you to also include spending time practicing the configuration concepts with Cisco VPN technology as part of your study plan if such technology is available to you. Alternatively, you can leverage technology simulators such as Cisco Modeling Labs or watch others configure VPN technologies by searching YouTube. For example, searching YouTube for “configure DMVPN on cisco router” will bring up multiple videos that can help you better understand the DMVPN concepts covered in this book.

This short chapter has three main sections. The first section helps you get ready to take the exam, and the second section lists the exam preparation tools useful at this point in the study process. The third section provides a suggested study plan you can use now that you have completed all the earlier chapters in this book.

Getting Ready

The first thing to focus on when preparing for any exam, including the SVPN exam, is developing a study plan. Your study plan should also include developing a strategy regarding how to approach the type of questions seen on the exam. We covered the format of the SVPN exam in Chapter 1, including the possible question types. Be familiar with how the exam will look, and make sure to check the official SVPN website to see if any changes have occurred before going into the exam.

Here are some important tips and best practices we use that you should keep in mind to ensure that you are ready for the SVPN 300-730 exam:

- **Build and use a study tracker:** Consider using the exam objectives to build a study tracker for yourself. Such a tracker can help ensure that you have not missed anything and that you are confident for your exam. As a matter of fact, this book offers a sample study planner as a website supplement.

- **Think about your time budget for questions on the exam:** When you do the math, you will see that, on average, you have one minute per question. While this does not sound like a lot of time, keep in mind that many of the questions will be very straightforward, and you will take 15 to 30 seconds on those. This leaves you extra time for other questions on the exam.

- **Watch the clock:** Check in on the time remaining periodically as you are taking the exam. You might even find that you can slow down pretty dramatically if you have built up a nice block of extra time.

- **Get some earplugs:** The testing center might provide earplugs, but get some just in case and bring them along. There might be other test takers in the center with you, and you do not want to be distracted by their screams. I personally have no issue blocking out the sounds around me, so I never worry about this, but I know it is an issue for some. You will also want to check if earplugs are permitted at the testing center if you plan to use them.

- **Plan your travel time:** Give yourself extra time to find the center and get checked in. Be sure to arrive early. As you test more at a particular center, you can certainly start cutting it closer time-wise.

- **Get rest:** Most students report that getting plenty of rest the night before the exam boosts their success. All-night cram sessions are not typically successful.

- **Bring in valuables but get ready to lock them up:** The testing center will take your phone, your smartwatch, your wallet, and other such items and will provide a secure place for them.

- **Take notes:** You will be given note-taking implements and should not be afraid to use them. I always jot down any questions I struggle with on the exam. I then memorize them at the end of the test by reading my notes over and over again. I always make sure I have a pen and paper in the car, and I write down the issues in my car just after the exam. When I get home—with a pass or fail—I research those items!

- **Mix up your review:** Hearing the same concept a different way will help ensure you fully understand it. We recommend using a blend of reading, lab and online research on all key learning objectives. If you want to master DMVPN, use the YouTube suggestion previously provided, read about it in this book and perform a configuration or review a sample configuration to see the topic different ways.

- **Practice testing stamina:** One factor we find that is hard to judge is the impact the exam will have on you while you are taking the test. The best way to prepare for exam stress is to simulate what you will have to endure. This can be done by blocking out the same time you are expected to take the exam and working through practice questions. We recommend considering working twice as long as the exam to properly prepare your mind and body for the stress this exam may require of you.

- **Read lots of practice questions:** Part of passing any exam is being able to comprehend what is being asked of you. Different certification programs will have their own approach to asking questions.

Tools for Final Preparation

This section lists some information about the available tools and how to access them. We can’t stress enough how important it is for you to know the

concepts we have covered, including how they apply to VPN technology versus purely memorizing statements. Take advantage of these tools and pay attention to the practice questions offered at the end of each chapter.

Pearson Cert Practice Test Engine and Questions on the Website

Register this book to get access to the Pearson IT Certification test engine (software that displays and grades a set of exam-realistic, multiple-choice questions). Using the Pearson Cert Practice Test Engine, you can either study by going through the questions in Study mode or take a simulated (timed) SVPN 300-730 exam.

The Pearson Test Prep practice test software comes with two full practice exams. These practice tests are available to you either online or as an offline Windows application. To access the practice exams that were developed with this book, please see the instructions in the card inserted in the sleeve in the back of the book. This card includes a unique access code that enables you to activate your exams in the Pearson Test Prep software.

Accessing the Pearson Test Prep Software Online

The online version of this software can be used on any device with a browser and connectivity to the Internet, including desktop machines, tablets, and smartphones. To start using your practice exams online, simply follow these steps:

Step 1. Go to http://www.PearsonTestPrep.com.

Step 2. Select **Pearson IT Certification** as your product group.

Step 3. Enter your email and password for your account. If you don’t have an account on PearsonITCertification.com or CiscoPress.com, you need to establish one by going to PearsonITCertification.com/join.

Step 4. In the **My Products** tab, click the **Activate New Product** button.

Step 5. Enter the access code printed on the insert card in the back of your

book to activate your product. The product is then listed in your My Products page.

Step 6. Click the Exams button to launch the exam settings screen and start the exam.

Accessing the Pearson Test Prep Software Offline

If you wish to study offline, you can download and install the Windows version of the Pearson Test Prep software. You can find a download link for this software on the book's companion website, or you can just enter this link in your browser:

http://www.pearsonitcertification.com/content/downloads/pcpt/engine.zip

To access the book's companion website and the software, simply follow these steps:

Step 1. Register your book by going to PearsonITCertification.com/register and entering the ISBN **9780136660606**.

Step 2. Respond to the challenge questions.

Step 3. Go to your account page and select the **Registered Products** tab.

Step 4. Click on the **Access Bonus Content** link under the product listing.

Step 5. Click the **Install Pearson Test Prep Desktop Version** link in the Practice Exams section of the page to download the software.

Step 6. When the software finishes downloading, unzip all the files onto your computer.

Step 7. Double-click the application file to start the installation and follow the onscreen instructions to complete the registration.

Step 8. When the installation is complete, launch the application and click the **Activate Exam** button on the My Products tab.

Step 9. Click the **Activate a Product** button in the Activate Product Wizard.

Step 10. Enter the unique access code from the card in the sleeve in the back of your book, and click the **Activate** button.

Step 11. Click **Next**, and then click the **Finish** button to download the exam data to your application.

Step 12. You can now start using the practice exams by selecting the product and clicking the **Open Exam** button to open the exam settings screen.

Note that the offline and online versions sync together, so saved exams and grade results recorded on one version will be available to you in the other version as well.

Customizing Your Exams

When you are in the exam settings screen, you can choose to take exams in one of three modes:

- Study mode
- Practice Exam mode
- Flash Card mode

Study mode enables you to fully customize an exam and review answers as you are taking the exam. This is typically the mode you use first to assess your knowledge and identify information gaps. Practice Exam mode locks certain customization options in order to present a realistic exam experience. Use this mode when you are preparing to test your exam readiness. Flash Card mode strips out the answers and presents you with only the question stem. This mode is great for late-stage preparation, when you really want to challenge yourself to provide answers without the benefit of seeing multiple-choice options. This mode does not provide the detailed score reports that the other two modes provide, so it is not the best mode for helping you identify knowledge gaps.

In addition to these three modes, you will be able to select the source of your questions. You can choose to take exams that cover all of the chapters, or you

can narrow your selection to just a single chapter or the chapters that make up specific parts in the book. All chapters are selected by default. If you want to narrow your focus to individual chapters, simply deselect all the chapters and then select only those on which you wish to focus in the Objectives area.

You can also select the exam banks on which to focus. Each exam bank comes complete with a full exam of questions that cover topics in every chapter. You can have the test engine serve up exams from all four banks or just from one individual bank by selecting the desired banks in the exam bank area.

There are several other customizations you can make to your exam from the exam settings screen, such as the time allowed for taking the exam, the number of questions served up, whether to randomize questions and answers, whether to show the number of correct answers for multiple-answer questions, and whether to serve up only specific types of questions. You can also create custom test banks by selecting only questions that you have marked or questions on which you have added notes.

Updating Your Exams

If you are using the online version of the Pearson Test Prep software, you should always have access to the latest version of the software as well as the exam data. If you are using the Windows desktop version, every time you launch the software, it will check to see if there are any updates to your exam data and automatically download any changes made since the last time you used the software. This requires that you be connected to the Internet at the time you launch the software.

Sometimes, due to a number of factors, the exam data might not fully download when you activate your exam. If you find that figures or exhibits are missing, you might need to manually update your exams.

To update a particular exam you have already activated and downloaded, simply select the Tools tab and click the Update Products button. Again, this is only an issue with the desktop Windows application.

If you wish to check for updates to the Windows desktop version of the Pearson Test Prep exam engine software, simply select the Tools tab and click the Update Application button. Doing so allows you to ensure that you are running the latest version of the software engine.

Premium Edition

In addition to the free practice exams provided on the website, you can purchase additional exams with expanded functionality directly from Pearson IT Certification. The Premium Edition of this title contains an additional two full practice exams and an eBook (in both PDF and ePub format). In addition, the Premium Edition title has remediation for each question to the specific part of the eBook that relates to that question.

Because you have purchased the print version of this title, you can purchase the Premium Edition at a deep discount. There is a coupon code in the book sleeve that contains a one-time-use code and instructions for where you can purchase the Premium Edition.

To view the premium edition product page, go to www.informit.com/title/9780136660606.

Chapter-Ending Review Tools

Chapters 1 through 10 each have several features in the "Exam Preparation Tasks" section at the end of the chapter. You might have already worked through these in each chapter. It can also be useful to use these tools again as you make your final preparations for the exam.

Suggested Plan for Final Review/Study

This section lists a suggested study plan from the point at which you finish reading through Chapter 10, until you take the SVPN 300-730 exam. You can ignore this plan, use it as is, or take suggestions from it. We have built these questions based on the requirements found with the SVPN exam. If you struggle with answering our test questions, you will likely struggle taking the

real SVPN exam.

Our recommended study plan regarding a final review before taking the SVPN exam involves two steps:

Step 1. Review key topics and "Do I Know This Already?" (DIKTA?) questions: You can use the table that lists the key topics in each chapter or just flip the pages, looking for key topics. Also, reviewing the DIKTA? questions from the beginning of the chapter can be helpful for review.

Step 2. Use the Pearson Cert Practice Test engine to practice: The Pearson Cert Practice Test engine allows you to study using a bank of unique exam-realistic questions available only with this book.

Summary

The tools and suggestions listed in this chapter have been designed with one goal in mind: to help you develop the skills required to pass the SVPN 300-730 exam. This book has been developed from the beginning to not just tell you the facts but to also help you learn how to apply the facts. We also included additional content based on what we felt is important to know about VPN technology. No matter what your experience level leading up to when you take the exam, it is our hope that the broad range of preparation tools, and even the structure of the book, will help you pass the exam with ease. We hope you do well on the exam.

Part V: Appendixes

Appendix A. Answers to the “Do I Know This Already?” Quizzes

Chapter 2

1. C. Mesh-to-spoke doesn’t make sense and isn’t an official architecture. Full mesh, hub-and-spoke, and spoke-to-spoke networks are all deployment models for a site-to-site VPN architecture.

2. C. A Cisco Integrated Services Router device can offer both site-to-site VPN capabilities and remote access VPN capabilities, depending on the model, licenses, and how it is configured.

3. A. VAM is not a VPN protocol. In the Cisco VPN world, VAM is short for the VPN Acceleration Module.

4. B. IKEv2 is a VPN encryption protocol, not a VPN option.

5. A and D. EasyVPN and IPsec VPN are tunnel-based VPN options.

6. A. Cisco SecureX is a centralized place for investigating event data, performing case management, and launching orchestration. Cisco SecureX does not provide VPN configuration management.

7. A. DART is a wizard that bundles all client logs and configuration and diagnostic information for analyzing and troubleshooting the AnyConnect client connection.

8. B and D. DMVPN, GETVPN, and Static IPsec don’t have software clients because they don’t apply to these VPN types.

9. B. L2TP is a tunneling protocol that doesn’t have any encryption. It is typically paired with IPsec for security.

10. C and D. With a client-based VPN, many host-based security capabilities are needed. Clients allow for additional features such as posture. Answer B is incorrect because the level of security is irrelevant; instead, the type of encryption used is important. SSL runs over standard HTTPs ports and

uses a web browser.

Chapter 3

1. B, C. Authentication Header (AH) provides authentication, and ESP provides data encryption and authentication.
2. A. The correct configuration command is **crypto ikev1 policy 1**.
3. B. IPsec SA exchange occurs during phase 2 of an IKE key exchange.
4. C. IKEv2 supports NAT by default. Answer A is not correct because that is a characteristic of IKEv2. IKEv2 authenticates with pre-shared keys or digital signatures. Answer B is not correct because IKEv2 can have peers using different authentication. Multi-hosting is supported using multiple IDs on a single IP address or port pair.
5. A, B, C. Public and private keys have nothing to do with authentication. They are used for encryption.
6. A, C, D. There isn't an initiation protocol.
7. B. False. With IKEv1, both peers use the same authentication. IKEv2 can have both peers use the same authentication option or different authentication options.
8. A, B. Answer C is incorrect because digital certificates are for authentication, not for authorization. Answer D is somewhat correct, but a digital certificate can be used for more than just authenticating systems.
9. B. Option B is the least important question. Best of breed is an objective statement and doesn't consider your organization's specific requirements.
10. A. A hot standby is essentially another system that is live in a standby mode, making it an active/standby option.

Chapter 4

1. A and C. GETVPN provides instant IP communication with IPsec

encryption between routers, and any group member can communicate with any other member without additional configuration.

2. A and D. Because the IP header on the original packet is not changed, GETVPN cannot be used in a NAT solution such as the public Internet.

3. D. Internet Security Association and Key Management Protocol (ISAKMP) provides protection for control plan communication in GETVPN.

4. A, C, and D. The three key components of GETVPN are the GDOI protocol, the key server, and the group member.

5. C. The key server is responsible for registering group members and sending out the keys to them so they are all synchronized.

6. D. The key encryption key (KEK) is responsible for sending out new keys, whereas the traffic encryption key (TEK) is responsible for payload encryption between group members.

7. C. The key server is the most critical component, and if it fails, the SA rekey process could also fail.

8. B. Only the key server would require the generation of an RSA private key.

9. B. The key server pushes the transform set parameters to the group members. The transform set dictates the SA encryption policy.

10. D. The group identity configuration is done in the crypto map statement.

Chapter 5

1. A, C, and D. DMVPN technology enables support for multicast traffic, dynamic routing protocols, and QoS for bandwidth optimization.

2. B. Remote sites can have DHCP addresses and participate in a DMVPN solution; legacy site-to-site VPN solutions cannot.

3. A and C. DMVPN can scale better than a crypto map–based VPN, and the

configuration overhead on the hub site is much lower.

4. A, C, E, and F. Four components of a DMVPN solution are IPsec, mGRE, NHRP, and routing protocols.

5. B. Next Hop Resolution Protocol (NHRP) is responsible for mapping hub-and-spoke routers' internal and external IP addresses for address resolution.

6. D. Generic Routing Encapsulation in an IPsec tunnel enables the use of dynamic routing protocols.

7. B and D. EIGRP and RIP are routing protocols that face a split-horizon issue that needs to be addressed.

8. A. A VPN link is not a traditional broadcast link, and, as a link-state routing protocol, OSPF needs to be configured to solve this issue.

9. B and D. You need to consider the number of remote sites as well as the need for QoS in applications.

10. D. Phase 3 has smaller routing tables because it can summarize routes.

11. B. The **dynamic** keyword in the NHRP command **ip nhrp map multicast dynamic** enables spokes to attach.

12. D. The command **no ip next-hop-self** prevents the hub router from rewriting the next hop IP address on the route advertisement.

13. C. The command to see whether a spoke was registered with the NHS is **show ip nhrp nhs detail**.

Chapter 6

1. B. FlexVPN includes predefined defaults for multiple components of the FlexVPN configuration, such as IKEv2 proposal and IKEv2 policy.

2. A, B. FlexVPN supports multiple types of VPNs: site-to-site, hub-and-spoke, and remote access. In addition, it offers backward compatibility.

3. B, D. FlexVPN supports the IKEv2 enhancements NSA Suite B and EAP support.

4. B, C. FlexVPN provides a default IPsec profile and IKEv2 policy.

5. A, B, C. FlexVPN provides support for configuration push, per-peer configuration, and full AAA management.

6. C. The IKEv2 authorization block provides the AAA, IP pool, and ACL information download.

7. D. The transform set is one of the smart defaults included to speed up configuration.

8. D. The **aaa authorization** command is responsible for connecting the IKEv2 authorization policy with the local **aaa authentication** information.

9. B. Spoke-to-spoke communication requires NHRP as well as a virtual template interface to copy the tunnel interface configuration to the virtual template. This makes it possible to establish a shortcut switching tunnel with another spoke.

10. A, D. On the spoke routers, a new entry in the keyring is required for authorization, and NHRP is needed for mapping the tunnel address to the remote public addresses.

11. C. The **show crypto ikev2 sa** command shows whether the IKEv2 process has completed.

12. A. The command **show ip route nhrp** shows what routes were installed in the table as a result of the NHRP resolution process.

13. D. FlexVPN does not support IKEv1. A design consideration would be making sure IKEv2 is supported.

Chapter 7

1. C. A network access server is needed to provide the VPN, and client-side software is needed to connect to the NAS.

2. A. ASDM is a centralized configuration management tool. By itself, it does not provide VPN services.

3. E. SHA256 is a hash function, not a VPN protocol.

4. B. Although you can download AnyConnect, if you do, it won't have any profile information regarding your specific VPN setup.

5. A. Both clientless mode and thin client mode provide secure access. However, clientless mode does not enable remote access TCP-based applications. You need thin client mode for that. Neither mode provides a full tunnel.

6. C. If an outage occurs, users do not disconnect because the ASAs are standalone and running. With a cluster, one ASA would be in standby mode and would not be active until the failure. This would force users to have to reconnect.

7. D. There isn't a specific step for selecting the encryption type.

8. A. BGP is a routing protocol that doesn't require a SEC-K9 bundle.

9. D. With a SEC-K9 bundled installed, nothing else is needed to enable SSLVPN.

10. B. Some Cisco routers do not support FlexVPN.

11. D. Meraki uses the L2TP tunneling protocol.

12. A. Cisco Firepower Threat Defense can support multiple AAA servers beyond three.

13. A. Answer a shows the correct way to create a tunnel group.

Chapter 8

1. B. A clientless SSLVPN uses TLS. SSL has been deprecated. Both IKEv2 and IPsec are used with AnyConnect VPNs.

2. B. AnyConnect Plus does not support clientless SSLVPNs. AnyConnect

Base is not an AnyConnect license type. Both AnyConnect Apex and AnyConnect VPN support only clientless SSLVPNs.

3. C. The industry standard set by the Certification Authority/Browser (CA/B) Forum requires that certificates that expire after December 31, 2013, must have a key length of at least 2048 bits. Key lengths shorter than 2048 are considered insecure.

4. D. By default, DfltGrpPolicy allows clientless SSLVPN, IPsec/IKEv2, and L2TP/IPsec connections. DfltGrpPolicy does not allow SSLVPN client connections by default.

5. B. When configuring a connection profile, a domain name must be configured for the configuration to be accepted. Tunnel group is another name for connection profile. DNS server and aliases can optionally be configured in a connection profile but are not required.

6. A. Attributes applied via a dynamic access policy (DAP) always override attributes from any other source, including user attributes, group policy attributes, and connection profile default group policy attributes.

7. B. Only port forwarding requires Java to function. Clientless SSLVPN, smart tunnel, and AnyConnect SSLVPN can all function in the absence of Java.

8. B. When configuring bookmarks, CIFS and HTTP bookmarks are supported by Cisco ASA by default. You can enable RDP bookmarks by installing the appropriate client/server plug-in. DNS is not a supported type of bookmark.

9. D. When configuring a smart tunnel, the application ID, operating system, and process name are all required. Only the hash is an optional configuration parameter.

10. C. Client/server plug-ins are available for RDP, VNC, and SSH. CIFS is supported without a client/server plug-in.

Chapter 9

1. B. DTLS typically provides better performance than TLS. IKEv2 is incorrect as it uses IPsec for transport. L2TP and PPTP are also incorrect as AnyConnect does not support these protocols.

2. A. Installing AnyConnect initially requires administrative privileges. To upgrade AnyConnect or install additional modules using web deploy (from ASA/ISE/Umbrella cloud with Downloader), you do not need administrative privileges. Connecting and disconnecting do not require administrative privileges.

3. A. Before configuring AnyConnect VPN access, an AnyConnect image must be loaded onto the ASA using the command **anyconnect image**.

4. C. Only Group URL maps an AnyConnect connection to a connection profile based on the URL. Connection Alias allows a user to select the connection profile during login, and Certificate Mapping allows for the automatic selection of the connection profile, based on the certificate. Group URL Alias does not exist.

5. B. DTLS uses UDP 443 by default. TLS uses TCP 443, IKEv2 uses UDP 500, and IKEv2 with NAT-T uses UDP 4500 by default.

6. C. The ASA supports the RADIUS, TACACS+, SDI (RSA), NT, Kerberos, and LDAP protocols when configuring a AAA server group.

7. D. AnyConnect clients may not be assigned IP addresses manually. IP addresses must be assigned via a local address pool, RADIUS server, or DHCP server.

8. A. The option Tunnel Network List Below in ASDM splits tunnel traffic by IP address and only tunnels the traffic specified by the ACL. In contrast, the option Exclude Network Below tunnels all traffic by the traffic specified by the ACL, and the option Dynamic Split Tunneling is used to split tunnel traffic by domain. The option Manual Split Tunneling does not exist.

9. B. When configuring a server list in the AnyConnect profile editor, only IKE Identity is optional. FQDN or IP address, User Group, and Primary Protocol are all required.

10. A. The default identity sent by AnyConnect is ***$AnyConnectClient$***.

11. C. On IOS, local user authentication with EAP is not supported with self-signed certificates. EAP requires a proper certificate chain consisting of a server certificate signed by a separate CA certificate. If that is not in place, the EAP exchange fails.

Chapter 10

1. B. If the local address pool is exhausted, no more IP addresses will be available, and hence no more VPN users can be added. You can verify whether this is the issue by using the command **show ip local pool [***pool-name***]**.

2. A. Java or ActiveX must be supported by the browser for smart tunnel functionality to work.

3. B. If a bookmark is grayed out, the ASA can no longer reach it, which likely points to a DNS resolution problem.

4. A. When using an XML profile, the connection profile must match the user group.

5. D. Using **split-tunnel-all-dns enable** sends all DNS traffic through the SSLVPN tunnel.

6. D. The **show crypto ikev2 sa detail** command contains all this information.

7. B. The **show ipsec crypto sa** command does not show details about the status of the WebVPN service.

8. D. DfltGropPolicy does not allow SSLVPN client connections by default.

9. C. The command **show webvpn anyconnect** is not available on a Cisco router.

10. A. The **show vpn-sessiondb detail anyconnect** command provides the most detail about the VPN session.

Appendix B. Implementing Secure Solutions with Virtual Private Networks (SVPN 300-730) Exam Updates

Over time, reader feedback enables Pearson to gauge which topics give our readers the most problems when taking the exams. To assist readers with those topics, the authors create new materials clarifying and expanding on those troublesome exam topics. As mentioned in the Introduction, the additional content about the exam is contained in a PDF on this book's companion website, at http://www.ciscopress.com/title/9780136660606.

This appendix is intended to provide you with updated information if Cisco makes minor modifications to the exam upon which this book is based. When Cisco releases an entirely new exam, the changes are usually too extensive to provide in a simple update appendix. In those cases, you might need to consult the new edition of the book for the updated content. This appendix attempts to fill the void that occurs with any print book. In particular, this appendix does the following:

- Mentions technical items that might not have been mentioned elsewhere in the book
- Covers new topics if Cisco adds new content to the exam over time
- Provides a way to get up-to-the-minute current information about content for the exam

Always Get the Latest at the Book's Product Page

You are reading the version of this appendix that was available when your book was printed. However, given that the main purpose of this appendix is to be a living, changing document, it is important that you look for the latest version online at the book's companion website. To do so, follow these steps:

Step 1. Browse to www.ciscopress.com/title/9780136660606.

Step 2. Click the **Updates** tab.

Step 3. If there is a new Appendix B document on the page, download it.

Note

The downloaded document has a version number. Comparing the version of the print Appendix B (Version 1.0) with the latest online version of this appendix, you should do the following:

- **Same version:** Ignore the PDF that you downloaded from the companion website.
- **Website has a later version:** Ignore this Appendix B in your book and read only the latest version that you downloaded from the companion website.

Technical Content

The current Version 1.0 of this appendix does not contain additional technical coverage.

Appendix C. Memory Tables

Chapter 2

Table 2-3 Comparing VPN Options

Network Design	DMVPN (mGRE)	GETVPN (tunnel-less)	SSLVPN (TLS)	FlexVPN (DVTI, IKEv2)	EasyVPN (dynamic Crypto Map/DVTI, IKEv1)	Static IPsec (Crypto Map, SVTI, IPsec/GRE)
Remote access (software client)	N/A	N/A	Supported	Supported	Not supported	N/A
Hub-and-spoke only (hardware client)	Supported	N/A	N/A	Supported	Not supported	Not supported
Hub-and-spoke with spoke-and-spoke	Dynamic mesh supported	Any to any (full-mesh) supported	N/A	Not supported	N/A	Not supported

Chapter 3

Table 3-2 Comparison of IKEv1 and IKEv2

Parameter	IKEv1	IKEv2
		One
Exchange messages	Nine for main mode; six for aggressive mode	
Authentication methods		
Authentication	Both peers use the same authentication	Each peer can use different authentication (for example, one using PSK and the other using RSA-Sig)
Number of combinations of a source IP range, a destination IP range, a source port, and a destination port allowed per IPsec SA	One	Multiple (IPv4 and IPv6 addresses can be configured for the same child SA)
Multi-hosting	Not supported	
Rekeying	Not defined	Defined
NAT traversal and dead peer detection	Can be defined as an extension	Supported by default
Remote access VPN	Not defined but supported by vender-specific implementations such as Mode config and Xauth	Supported by default; options including the following:
Multi-homing, mobile clients, and DoS protection	Not supported	Supported, as described in RFC 4555 (DoS protection includes anti-replay function, cookies for mitigating flooding attacks, and vulnerabilities found with IKEv1)

Chapter 5

Table 5-3 DMVPN Troubleshooting Commands

Troubleshooting Part	Commands
Crypto configuration (ISAKMP/IPSEC)	
Tunnel configuration	
NHRP configuration	
Routing configuration	

Chapter 6

Table 6-6 Key FlexVPN Troubleshooting Commands

Troubleshooting FlexVPN Building Block	Commands
Step 1: IKEv2 proposal and IKEv2 policy troubleshooting	
Step 2: IKEv2 authorization policy troubleshooting	
Step 3: Keyring and IKEv2 profile troubleshooting	
Step 4: IPsec profile troubleshooting	
NHRP troubleshooting	
Routing troubleshooting	

Chapter 8

Table 8-2 Comparison Between a Clientless SSLVPN and an AnyConnect VPN

Feature	Clientless SSLVPN	Client VPN
Common use cases		
Client		
Installation		
Protocols used		
Connectivity to resources		
IP address seen on internal servers		
Applications supported		

Table 8-5 Group Policy Attributes for Clientless SSLVPNs

Command	Description
	Creates a banner or welcome text to be displayed on the VPN remote client
	Specifies the name of an existing tunnel group that users are required to connect with
	Configures periodic authentication
	Specifies the VLAN onto which VPN traffic for this group will be forwarded.
	Specifies the name of a configured time-range policy
	Specifies the idle timeout period, in minutes
	Specifies the maximum user connection time, in minutes, or none for unlimited time
	Specifies the maximum number of simultaneous logins allowed
	Specifies the permitted tunneling protocols
	Configures additional group policy attributes for the WebVPN

Table 8-6 WebVPN Group Policy Attributes for Clientless SSLVPNs

Command	Description
	Lets a user who has established a clientless SSLVPN session use a browser to launch Microsoft Office applications. The applications use the session to download and upload ActiveX. The ActiveX relay remains in force until the clientless SSLVPN session closes.
	Sets values for auto sign-on, which requires that the user enter username and password credentials only once for a clientless SSLVPN connection.
	Assigns a customization object to a group policy or user.
	Specifies the message delivered to a remote user who logs in to clientless SSLVPN successfully but has no VPN privileges.
	Enables CIFS file browsing for file servers and shares. Browsing requires NBNS (Master Browser or WINS).
	Allows users to enter names of file servers to access.
	Sets the name of the web type access list.
	Controls the visibility of hidden shares for CIFS files.
	Sets the URL of the web page that displays upon login.
	Configures the content and objects to filter from the HTML for this group policy.
	Configures compression.
	Configures the ASA to use an external proxy server to handle HTTP requests.
	Sets the maximum object size to ignore for updating the session timer.
	Applies a list of clientless SSLVPN TCP ports to forward. The user interface displays the applications in this list.
	Sets the maximum object size to post.
	Configures a list of programs and several smart tunnel parameters to use a smart tunnel.
	Configures storage objects for the data stored between sessions.
	Configures SSLVPN client attributes.
	Sets the UNIX group ID.
	Sets the UNIX user ID.
	Controls the ability of the user to enter any HTTP/HTTPS URL.
	Applies a list of servers and URLs that the clientless SSLVPN portal page displays for end-user access.
	Configures a location for storing user data between sessions.

Table 8-7 Connection Profile General Attributes for Clientless SSLVPNs

Command	Description
	Specifies the name of the accounting server group
	Indicates that the authenticated username will be associated with the session
	Specifies the authentication server that provides an authorization attribute for the session
	Specifies the name of the authentication server group
	Requires users to authorize successfully in order to connect
	Specifies the name of the authorization server group
	Specifies the name of the default group policy
	Enables password management
	Enables SCEP proxy enrollment
	Specifies the name of the secondary authentication server group
	Specifies the DN of the peer certificate used as the secondary username for authorization
	Enables strip-group processing
	Enables strip-realm processing
	Specifies the DN of the peer certificate used as the username for authorization and/or authentication

Table 8-8 Connection Profile WebVPN Attributes for Clientless SSLVPNs

Command	Description
	Specifies the authentication method (either AAA or certificate).
	Specifies the name of a previously defined customization to apply. Customizations determine the appearance of the windows that the user sees upon login. You configure the customization parameters as part of configuring a clientless SSLVPN.
	Specifies the DNS server group, which indicates the DNS server name, domain name, name server, number of retries, and timeout values for a DNS server to use for a connection profile.
	Specifies the name of the NetBIOS name service server (nbns-server) to use for CIFS name resolution.
	Specifies the one or more alternate names by which the server can refer to a connection profile. At login, the user selects the group name from a drop-down menu.
	Specifies the one or more group URLs. If you configure this attribute, users coming in on a specified URL need not select a group at login.
	Specifies the VPN feature policy if you use the Cisco Secure Desktop Manager to set the Group-Based Policy attribute to Use Failure Group-Policy or Use Success Group-Policy, if Criteria Match.
	Specifies the username-to-certificate binding on this tunnel group.
	Flags this tunnel group as a specific proxy authentication tunnel group.
	Overrides download of the group policy or username attributes configured for downloading the AnyConnect VPN client to the remote user.
	Enables the display of the RADIUS reject message on the login screen when authentication is rejected.
	Configures SAML service.
	Configures a secondary username-to-certificate binding on this tunnel group.
	Disables CSD for a tunnel group.

Chapter 9

Table 9-2 Group Policy Attributes for AnyConnect VPNs

Command	Description
	Specifies a list of up to six address pools from which to assign addresses
	Specifies a list of backup servers to be used by the remote client
	Indicates banner or welcome text to be displayed on the VPN remote client
	Specifies rules permitting/denying access to specific client types and versions
	Specifies client behavior for protocols for which the client has not received an address
	Specifies firewall requirements for users in this group policy
	Indicates the default domain name given to users of this group
	Specifies a range of IP addresses to indicate to the DHCP server for address assignment
	Specifies the primary and secondary DNS servers
	Specifies the gateway FQDN to be sent down to the client
	Specifies the name of an existing tunnel group that users are required to connect with
	Indicates to use group policy for clients requesting Microsoft DHCP
	Enables IP compression (LZS)
	Allows a client to operate through a NAT device using UDP encapsulation
	Specifies the UDP port to be used by the client for IPsec through NAT
	Specifies a list of up to six IPv6 address pools from which to assign addresses
	Indicates the split tunneling method to be used for IPv6 traffic by the remote client
	Specifies the MSIE Browser Proxy settings for a client system
	Enables/disables storage of the login password on the client system
	Configures periodic authentication
	Enables perfect forward secrecy
	Enables reauthentication of the user on IKE rekey
	Specifies the CA SCEP URL to forward the SCEP messages.
	Configures the CTS security group tag to be used for users in this group policy
	Specifies the client action for smart card removal
	Specifies a list of domains to be resolved through the split tunnel
	Indicates how the client should handle DNS queries when split tunneling is enabled
	Specifies the name of the access list for split tunnel configuration
	Specifies the split tunneling method to be used for IPv4 traffic by the remote client
	Indicates the VLAN onto which VPN traffic for this group will be forwarded
	Specifies the name of a configured time range policy
	Specifies the name of a configured ACL to apply to users
	Specifies the idle timeout period, in minutes
	Specifies the maximum user connection time in minutes, with none indicating unlimited time
	Deletes the old tunnel immediately in the event that simultaneous login connection is preempted
vpn-simultaneous-logins	Specifies the maximum number of simultaneous logins allowed
vpn-tunnel-protocol	Specifies the permitted tunneling protocols
wins-server	Specifies primary and secondary WINS servers

Table 9-3 Connection Profile General Attributes for AnyConnect VPNs

Command	Description
	Sets the authentication method (AAA or certificate).
	Identifies the name of a previously defined customization to apply. Customizations determine the appearance of the windows that the user sees upon login. You configure the customization parameters as part of configuring clientless SSLVPN.
	Identifies the name of the NetBIOS Name Service server (nbns-server) to use for CIFS name resolution.
	Specifies one or more alternative names by which the server can refer to a connection profile. At login, the user selects the group name from a drop-down menu.
	Identifies one or more group URLs. If you configure this attribute, users coming in on a specified URL need not select a group at login. A load balancing deployment that uses group URLs for AnyConnect client connectivity requires each ASA node in the cluster to configure a group URL for the virtual cluster address, as well as a group URL for the node's load balancing public address.
	Identifies the DNS server group that specifies the DNS server name, domain name, name server, number of retries, and timeout values for a DNS server to use for a connection profile.
	Specifies a VPN feature policy if you use the Cisco Secure Desktop Manager to set the Group-Based Policy attribute to Use Failure Group-Policy or Use Success Group-Policy, if Criteria Match.
	Overrides downloading the group policy or username attributes configured for downloading the AnyConnect VPN client to the remote user.
	Enables the display of the RADIUS reject message on the login screen when authentication is rejected.

Table 9-4 Connection Profile General Attributes for AnyConnect VPNs

Command	Description
	Specifies the name of the accounting server group
	Specifies a list of address pools from which to assign addresses
	Indicates the authenticated username that will be associated with the session
	Specifies the authentication server that provides authorization attributes for the session
	Specifies the name of the authentication server group
	Requires users to authorize successfully in order to connect
	Specifies the name of the authorization server group
	Specifies the name of the default group policy
	Specifies the IP address or name of the DHCP server
	Specifies a list of IPv6 address pools from which to assign addresses
	Maps the NAT-assigned IP address to a public IP address
	Enables password management
	Enables SCEP proxy enrollment
	Specifies the name of the secondary authentication server group
	Specifies the DN of the peer certificate used as secondary username for authorization
	Enables strip group processing
	Enables strip realm processing
	Specifies the DN of the peer certificate used as a username for authorization and/or authentication

Table 9-5 Storage Locations for AnyConnect Client Profiles

OS	Location
	%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile
	/opt/cisco/anyconnect/profile
	/opt/cisco/anyconnect/profile

Appendix D. Memory Tables Answer Key

Chapter 2

Table 2-3 Comparing VPN Options

Network Design	DMVPN (mGRE)	GETVPN (tunnel-less)	SSLVPN (TLS)	FlexVPN (DVTI, IKEv2)	EasyVPN (dynamic Crypto Map/DVTI, IKEv1)	Static IPsec (Crypto Map, SVTI, IPsec/GRE)
Remote access (software client)	N/A	N/A	Supported	Supported	Not supported	N/A
Hub-and-spoke only (hardware client)	Supported	N/A	N/A	Supported	Not supported	Not supported
Hub-and-spoke with spoke-and-spoke	Dynamic mesh supported	Any to any (full-mesh) supported	N/A	Not supported	N/A	Not supported

Chapter 3

Table 3-2 Comparison of IKEv1 and IKEv2

Parameter	IKEv1	IKEv2
		One
Exchange messages	Nine for main mode; six for aggressive mode	
Authentication methods		
Authentication	Both peers use the same authentication	Each peer can use different authentication (for example, one using PSK and the other using RSA-Sig)
Number of combinations of a source IP range, a destination IP range, a source port, and a destination port allowed per IPsec SA	One	Multiple (IPv4 and IPv6 addresses can be configured for the same child SA)
Multi-hosting	Not supported	
Rekeying	Not defined	Defined
NAT traversal and dead peer detection	Can be defined as an extension	Supported by default
Remote access VPN	Not defined but supported by vender-specific implementations such as Mode config and Xauth	Supported by default; options including the following:
Multi-homing, mobile clients, and DoS protection	Not supported	Supported, as described in RFC 4555 (DoS protection includes anti-replay function, cookies for mitigating flooding attacks, and vulnerabilities found with IKEv1)

Chapter 5

Table 5-3 DMVPN Troubleshooting Commands

Troubleshooting Part	Commands
Crypto configuration (ISAKMP/IPSEC)	
Tunnel configuration	
NHRP configuration	
Routing configuration	

Chapter 6

Table 6-6 Key FlexVPN Troubleshooting Commands

Troubleshooting FlexVPN Building Block	Commands
Step 1: IKEv2 proposal and IKEv2 policy troubleshooting	
Step 2: IKEv2 authorization policy troubleshooting	
Step 3: Keyring and IKEv2 profile troubleshooting	
Step 4: IPsec profile troubleshooting	
NHRP troubleshooting	
Routing troubleshooting	

Chapter 8

Table 8-2 Comparison Between a Clientless SSLVPN and an AnyConnect VPN

Feature	Clientless SSLVPN	Client VPN
Common use cases		
Client		
Installation		
Protocols used		
Connectivity to resources		
IP address seen on internal servers		
Applications supported		

Table 8-5 Group Policy Attributes for Clientless SSLVPNs

Command	Description
	Creates a banner or welcome text to be displayed on the VPN remote client
	Specifies the name of an existing tunnel group that users are required to connect with
	Configures periodic authentication
	Specifies the VLAN onto which VPN traffic for this group will be forwarded.
	Specifies the name of a configured time-range policy
	Specifies the idle timeout period, in minutes
	Specifies the maximum user connection time, in minutes, or none for unlimited time
	Specifies the maximum number of simultaneous logins allowed
	Specifies the permitted tunneling protocols
	Configures additional group policy attributes for the WebVPN

Table 8-6 WebVPN Group Policy Attributes for Clientless SSLVPNs

Command	Description
	Lets a user who has established a clientless SSLVPN session use a browser to launch Microsoft Office applications. The applications use the session to download and upload ActiveX. The ActiveX relay remains in force until the clientless SSLVPN session closes.
	Sets values for auto sign-on, which requires that the user enter username and password credentials only once for a clientless SSLVPN connection.
	Assigns a customization object to a group policy or user.
	Specifies the message delivered to a remote user who logs in to clientless SSLVPN successfully but has no VPN privileges.
	Enables CIFS file browsing for file servers and shares. Browsing requires NBNS (Master Browser or WINS).
	Allows users to enter names of file servers to access.
	Sets the name of the web type access list.
	Controls the visibility of hidden shares for CIFS files.
	Sets the URL of the web page that displays upon login.
	Configures the content and objects to filter from the HTML for this group policy.
	Configures compression.
	Configures the ASA to use an external proxy server to handle HTTP requests.
	Sets the maximum object size to ignore for updating the session timer.
	Applies a list of clientless SSLVPN TCP ports to forward. The user interface displays the applications in this list.
	Sets the maximum object size to post.
	Configures a list of programs and several smart tunnel parameters to use a smart tunnel.
	Configures storage objects for the data stored between sessions.
	Configures SSLVPN client attributes.
	Sets the UNIX group ID.
	Sets the UNIX user ID.
	Controls the ability of the user to enter any HTTP/HTTPS URL.
	Applies a list of servers and URLs that the clientless SSLVPN portal page displays for end-user access.
	Configures a location for storing user data between sessions.

Table 8-7 Connection Profile General Attributes for Clientless SSLVPNs

Command	Description
	Specifies the name of the accounting server group
	Indicates that the authenticated username will be associated with the session
	Specifies the authentication server that provides an authorization attribute for the session
	Specifies the name of the authentication server group
	Requires users to authorize successfully in order to connect
	Specifies the name of the authorization server group
	Specifies the name of the default group policy
	Enables password management
	Enables SCEP proxy enrollment
	Specifies the name of the secondary authentication server group
	Specifies the DN of the peer certificate used as the secondary username for authorization
	Enables strip-group processing
	Enables strip-realm processing
	Specifies the DN of the peer certificate used as the username for authorization and/or authentication

Table 8-8 Connection Profile WebVPN Attributes for Clientless SSLVPNs

Command	Description
	Specifies the authentication method (either AAA or certificate).
	Specifies the name of a previously defined customization to apply. Customizations determine the appearance of the windows that the user sees upon login. You configure the customization parameters as part of configuring a clientless SSLVPN.
	Specifies the DNS server group, which indicates the DNS server name, domain name, name server, number of retries, and timeout values for a DNS server to use for a connection profile.
	Specifies the name of the NetBIOS name service server (nbns-server) to use for CIFS name resolution.
	Specifies the one or more alternate names by which the server can refer to a connection profile. At login, the user selects the group name from a drop-down menu.
	Specifies the one or more group URLs. If you configure this attribute, users coming in on a specified URL need not select a group at login.
	Specifies the VPN feature policy if you use the Cisco Secure Desktop Manager to set the Group-Based Policy attribute to Use Failure Group-Policy or Use Success Group-Policy, if Criteria Match.
	Specifies the username-to-certificate binding on this tunnel group.
	Flags this tunnel group as a specific proxy authentication tunnel group.
	Overrides download of the group policy or username attributes configured for downloading the AnyConnect VPN client to the remote user.
	Enables the display of the RADIUS reject message on the login screen when authentication is rejected.
	Configures SAML service.
	Configures a secondary username-to-certificate binding on this tunnel group.
	Disables CSD for a tunnel group.

Chapter 9

Table 9-2 Group Policy Attributes for AnyConnect VPNs

Command	Description
	Specifies a list of up to six address pools from which to assign addresses
	Specifies a list of backup servers to be used by the remote client
	Indicates banner or welcome text to be displayed on the VPN remote client
	Specifies rules permitting/denying access to specific client types and versions
	Specifies client behavior for protocols for which the client has not received an address
	Specifies firewall requirements for users in this group policy
	Indicates the default domain name given to users of this group
	Specifies a range of IP addresses to indicate to the DHCP server for address assignment
	Specifies the primary and secondary DNS servers
	Specifies the gateway FQDN to be sent down to the client
	Specifies the name of an existing tunnel group that users are required to connect with
	Indicates to use group policy for clients requesting Microsoft DHCP
	Enables IP compression (LZS)
	Allows a client to operate through a NAT device using UDP encapsulation
	Specifies the UDP port to be used by the client for IPsec through NAT
	Specifies a list of up to six IPv6 address pools from which to assign addresses
	Indicates the split tunneling method to be used for IPv6 traffic by the remote client
	Specifies the MSIE Browser Proxy settings for a client system
	Enables/disables storage of the login password on the client system
	Configures periodic authentication
	Enables perfect forward secrecy
	Enables reauthentication of the user on IKE rekey
	Specifies the CA SCEP URL to forward the SCEP messages.
	Configures the CTS security group tag to be used for users in this group policy
	Specifies the client action for smart card removal
	Specifies a list of domains to be resolved through the split tunnel
	Indicates how the client should handle DNS queries when split tunneling is enabled
	Specifies the name of the access list for split tunnel configuration
	Specifies the split tunneling method to be used for IPv4 traffic by the remote client
	Indicates the VLAN onto which VPN traffic for this group will be forwarded
	Specifies the name of a configured time range policy
	Specifies the name of a configured ACL to apply to users
	Specifies the idle timeout period, in minutes
	Specifies the maximum user connection time in minutes, with none indicating unlimited time
	Deletes the old tunnel immediately in the event that simultaneous login connection is preempted
vpn-simultaneous-logins	Specifies the maximum number of simultaneous logins allowed
vpn-tunnel-protocol	Specifies the permitted tunneling protocols
wins-server	Specifies primary and secondary WINS servers

Table 9-3 Connection Profile General Attributes for AnyConnect VPNs

Command	Description
	Sets the authentication method (AAA or certificate).
	Identifies the name of a previously defined customization to apply. Customizations determine the appearance of the windows that the user sees upon login. You configure the customization parameters as part of configuring clientless SSLVPN.
	Identifies the name of the NetBIOS Name Service server (nbns-server) to use for CIFS name resolution.
	Specifies one or more alternative names by which the server can refer to a connection profile. At login, the user selects the group name from a drop-down menu.
	Identifies one or more group URLs. If you configure this attribute, users coming in on a specified URL need not select a group at login. A load balancing deployment that uses group URLs for AnyConnect client connectivity requires each ASA node in the cluster to configure a group URL for the virtual cluster address, as well as a group URL for the node's load balancing public address.
	Identifies the DNS server group that specifies the DNS server name, domain name, name server, number of retries, and timeout values for a DNS server to use for a connection profile.
	Specifies a VPN feature policy if you use the Cisco Secure Desktop Manager to set the Group-Based Policy attribute to Use Failure Group-Policy or Use Success Group-Policy, if Criteria Match.
	Overrides downloading the group policy or username attributes configured for downloading the AnyConnect VPN client to the remote user.
	Enables the display of the RADIUS reject message on the login screen when authentication is rejected.

Table 9-4 Connection Profile General Attributes for AnyConnect VPNs

Command	Description
	Specifies the name of the accounting server group
	Specifies a list of address pools from which to assign addresses
	Indicates the authenticated username that will be associated with the session
	Specifies the authentication server that provides authorization attributes for the session
	Specifies the name of the authentication server group
	Requires users to authorize successfully in order to connect
	Specifies the name of the authorization server group
	Specifies the name of the default group policy
	Specifies the IP address or name of the DHCP server
	Specifies a list of IPv6 address pools from which to assign addresses
	Maps the NAT-assigned IP address to a public IP address
	Enables password management
	Enables SCEP proxy enrollment
	Specifies the name of the secondary authentication server group
	Specifies the DN of the peer certificate used as secondary username for authorization
	Enables strip group processing
	Enables strip realm processing
	Specifies the DN of the peer certificate used as a username for authorization and/or authentication

Table 9-5 Storage Locations for AnyConnect Client Profiles

OS	Location
	%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile
	/opt/cisco/anyconnect/profile
	/opt/cisco/anyconnect/profile

Appendix E. Study Planner

This content is currently in development.

Glossary of Key Terms

Authentication Header (AH) A protocol that defines a method for digitally signing IP packets. Signing packets is accomplished by hashing the IP header and data payload.

certificate authority (CA) A trusted entity that is responsible for issuing digital certificates.

Cisco Adaptive Security Device Manager (ASDM) A management option for Cisco ASA appliances that can also manage the Cisco AnyConnect Secure Mobility Client.

Cisco Defense Orchestrator (CDO) A cloud-based management option for Cisco security devices ranging from the ASA Series to other firewall and network devices.

Cisco Secure Firewall Device Manager (FDM) A management option for multiple 1000 Series and 2100 Series devices and select 5500-x Series devices running the Cisco Secure Firewall Threat Defense (FTD) software image. Each FTD image is managed individually through FDM.

Cisco Secure Firewall Management Center (FMC) A centralized management option for Cisco Firepower Next Generation Firewall (NGFW), Cisco Firepower Next Generation IPS (NGIPS), and Cisco AMP (Advanced Malware Protection) for networks as well as threat correlation for network sensors and AMP for Endpoints.

connection profile A VPN profile (formerly called a tunnel group) that identifies the group policy for a specific connection. A connection profile consists of a set of records that determines tunnel connection policies.

crypto map A software configuration entity that selects data flows that need security processing and defines the policy for flows that are selected for security processing and the crypto peer toward which that traffic needs to flow. Crypto maps are applied to interfaces.

Datagram Transport Layer Security (DTLS) protocol A communication protocol that provides security for datagram-based applications, allowing them to communicate in a secure manner.

Diffie–Hellman (DH) A public key cryptography protocol that allows two parties to establish a shared secret over an insecure communications channel. It is used with IKE to establish session keys.

Dynamic Multipoint VPN (DMVPN) A dynamic tunneling VPN supported on Cisco IOS-based routers and other systems.

Easy VPN (EzVPN) A protocol that simplifies IPsec configuration by using the Unity client protocol, which allows most IPsec VPN parameters to be defined at an IPsec gateway (also called an EzVPN server).

elliptic curve algorithm A relatively new alternative to public key cryptography that functions on elliptic curves over finite fields for better efficiency and performance. Diffie–Hellman secure elliptic curve algorithms are typically used for very secure information, such as classified information.

Encapsulating Security Payload (ESP) A protocol that defines a method for encrypting data and ensuring the integrity of data packets.

Extensible Authentication Protocol (EAP) A protocol based on RFC 3748 that supports multiple authentication methods. It can be used across multiple data link layers, such as PPP or IEEE 802 and is commonly found in wireless networks.

FlexVPN A configuration framework designed to simplify the setup of remote access, site-to-site, and DMVPN topologies.

full mesh An architecture in which each site in a VPN can communicate with every other site in that VPN.

Group Domain of Interpretation (GDOI) A cryptographic protocol for group key management based on RFC 6407 and ISAKMP (RFC 2408).

Group Encrypted Transport VPN (GETVPN) A tunnel-less VPN solution that provides highly secure communication between systems grouped together in a network.

group policy A policy applied to a collection of users treated as a single entry.

hash algorithm An irreversible function that provides a fixed size value based on various inputs. Also known as a digital fingerprinting algorithm.

Internet Key Exchange (IKE) An IPsec standard protocol used to ensure

security for VPN negotiation and remote host or network access.

Internet Key Exchange Version 2 (IKEv2) A protocol that dynamically establishes and maintains a shared state between the endpoints of an IP datagram. IKEv2 performs mutual authentication between two devices and establishes an IKEv2 Security Association (SA).

IP-Delivery Delay Detection Protocol (IP-D3P) A header that includes a timestamp that is used by the receivers of the packet to determine whether that packet was generated recently. Receivers compare the timestamp delivered in the IP packet to their local time and to determine whether the packet should be accepted.

IP Security (IPsec) A framework made up of open standards developed by the Internet Engineering Task Force (IETF) that is designed to offer data confidentiality, data integrity, and data authentication between participating peers.

key encryption key (KEK) An encryption rekeying message that group members use to decrypt rekeying messages from the key server.

Layer 2 Tunneling Protocol (L2TP) A tunneling protocol used to support VPNs or part of a service provided by an ISP.

multipoint Generic Routing Encapsulation (mGRE) A tunneling protocol that can encapsulate a wide variety of network layer protocols inside either a point-to-point link or a point-to-multipoint link over IP.

Multiprotocol Label Switching (MPLS) A data forwarding technology that routes data from one node to the next, based on short path labels rather than complex route table lookups.

network access server (NAS) A device that handles remote logins to establish a PPP connection such as a remote access VPN. Also called a media access gateway or remote access server.

Next Hop Resolution Protocol (NHRP) A protocol that enables routing communication and efficiency to occur over a non-broadcast multiple access (NBMA) network.

Point-to-Point Tunneling Protocol (PPTP) A networking standard for connecting to virtual private networks.

pseudorandom function (PRF) An algorithm used to derive keying material and hashing operations required by IKEv2 tunnel encryption.

public key algorithm A cryptographic algorithm that uses different keys for encryption and decryption. It is common to call these algorithms public/private key algorithms since one key is privately held and kept in secret while the other key is publicly available.

remote access VPN A VPN that enables individual users to connect to a private network from remote locations.

Secure Socket Tunneling Protocol (SSTP) A VPN tunnel protocol that provides a mechanism to transport PPP traffic through an SSL/TLS channel.

Secure Sockets Layer (SSL) A security standard for establishing an encrypted link between a server and a client. It typically uses a web server and a host browser.

security association (SA) A logical connections between two network entities to support security communications.

site-to-site VPN A VPN that allows branch offices to use the Internet as a conduit for access to other locations.

split tunneling A networking concept that permits a user to access dissimilar security domains, like the Internet (a public domain) and a local LAN (a private domain), at the same time, using the same or different network connections. This connection state can be facilitated through the use of a VPN client software application without the benefit of access control.

symmetric key algorithm A cryptographic secret key algorithm that uses the same key for encryption and decryption.

Time-Based Anti-Replay (TBAR) A replay mechanism used in a group key environment to prevent replay attacks.

traffic encryption key (TEK) A key that encrypts traffic and that is based on the IPsec security association for a group.

trapdoor function An algorithm that is easier in one direction than the other.

WebVPN A secure remote access VPN tunnel to a security appliance that a user can access by using a web browser. Users do not need a software or hardware client..