CCNP Security VPN 642-648 Quick Reference

Cristian Matei

Cisco Press

CCNP Security VPN 642-648 Quick Reference

Cristian Matei

ciscopress.com

Table of Contents

Chapter 1
Evaluating the Cisco ASA
VPN Subsystem 3

Chapter 2
Deploying Cisco ASA
IPsec VPN Solutions..... 42

Chapter 3
Deploying Cisco ASA
AnyConnect Remote-Access
SSL VPN Solutions.....109

Chapter 4
Deploying Clientless Remote-
Access SSL VPN Solutions.....148

Chapter 5
Deploying Advanced Cisco
ASA VPN Solutions.....184

About the Author

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

About the Technical Editor

Sean Wilkins is an accomplished networking consultant for SR-W Consulting (http://www.sr-wconsulting.com) and has been in the field of IT since the mid 1990s, working with companies such as Cisco, Lucent, Verizon, and AT&T. Sean currently holds certifications with Cisco (CCNP/CCDP), Microsoft (MCSE), and CompTIA (A+ and Network+). He also has a master's of science degree in Information Technology with a focus in Network Architecture and Design, a master's of science degree in Organizational Management, a master's certificate in Network Security, a bachelor's of science degree in Computer Networking, and an associate's degree of Applied Science in Computer Information systems. In addition to working as a consultant, Sean spends a lot of his time as a technical writer and editor for various companies.

Dedications

To Bianca Mihaela, a beautiful and lovely girl who actually became my wife in 2010. Thank you for loving and supporting me throughout all these years. Your morning smile makes my day.

To Petr Lapukhov from Internetwork Expert. His technical mentoring and level of knowledge are purely outstanding. I am still waiting for a book release from him; it should break all frontiers.

 Please see page 219 for more details.

Chapter 3

Deploying Cisco ASA AnyConnect Remote-Access SSL VPN Solutions

In this chapter, you learn to deploy and manage client-based Secure Sockets Layer (SSL) virtual private networks (VPN) on Cisco Adaptive Security Appliance (ASA) as the VPN gateway using AnyConnect Secure Mobility Client software. As you'll see, you can initiate a client-based SSL VPN session from a broad range of devices and operating systems that support the install of AnyConnect Client (desktops, laptops, mobile devices), as shown in Figure 3-1.

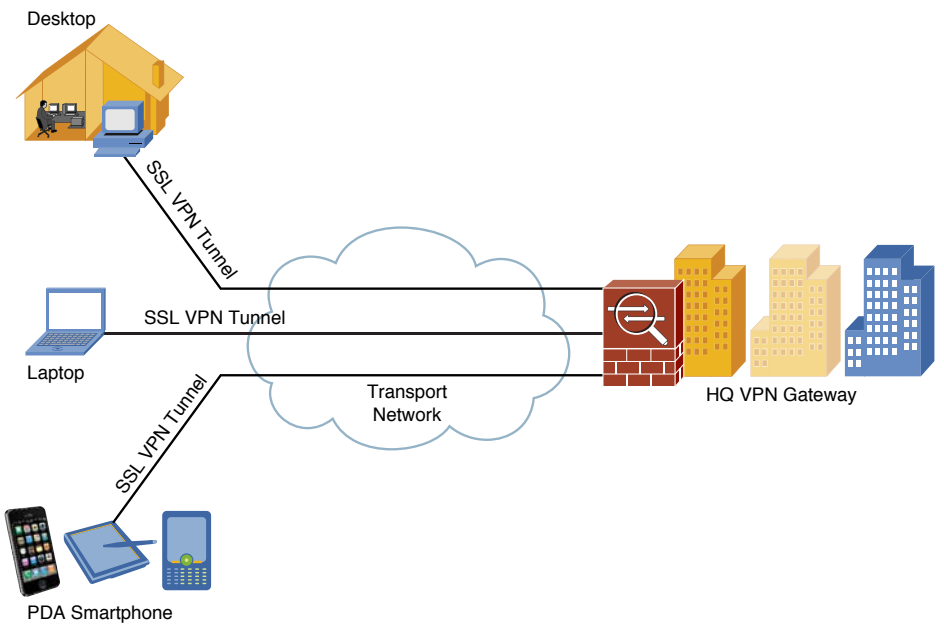

Figure 3-1 AnyConnect SSL VPN

Deploying a Basic Cisco AnyConnect Full-Tunnel SSL VPN Solution

Basic Cisco AnyConnect full-tunnel SSL VPN uses user authentication by username and password, provides IP address assignment to the client, and uses a basic access control policy. The client also authenticates the ASA with identity certificate-based authentication. Deployment tasks for this scenario are as follows:

1. Configure the basic ASA SSL VPN gateway features.
2. Configure local user authentication.
3. Configure IPv4/IPv6 address assignment.
4. Configure basic access control.
5. Install the Cisco AnyConnect Secure Mobility Client.

Initially, AnyConnect was an SSL-only VPN client. Starting with Version 3.0, AnyConnect became a modular client with additional features (including IPsec IKEv2 VPN terminations on Cisco ASA), but it requires a minimum of ASA 8.4(1) and ASDM 6.4(1).

Configuring Basic Cisco ASA SSL VPN Gateway Features

Note
Starting with version 2.5, AnyConnect is called ***AnyConnect Secure Mobility Client***.

To initially prepare the ASA for SSL VPN termination, complete the following steps:

STEP 1. Provision the ASA with an identity certificate. Your options are as follows:

- Use a self-signed certificate.
- Enroll ASA in Public Key Infrastructure (PKI) with Simple Certificate Enrollment Protocol (SCEP).
- Enroll ASA in PKI with manual cut-and-paste method enrollment.

To install a self-signed certificate using the ASDM, navigate to **Configuration > Remote Access VPN > Certificate Management > Identity Certificate**s and click **Add**. Give the PKI trustpoint a name, choose **Add a New Identity Certificate**, check **Generate Self-Signed Certificate**, and then click **Add Certificate**.To configure a self-signed certificate via the command-line interface (CLI), use the following commands:

 Please see page 219 for more details.

```
ciscoasa(config)# crypto key generate rsa label SELF-SIGNED modulus 2048
ciscoasa(config)# crypto ca trustpoint TEST-CA
ciscoasa(config-ca-trustpoint)# id-usage ssl-ipsec
ciscoasa(config-ca-trustpoint)# subject-name CN=cisco.com
ciscoasa(config-ca-trustpoint)# enrollment self
ciscoasa(config-ca-trustpoint)# keypair SELF-SIGNED
ciscoasa(config)# crypto ca enroll TEST-CA noconfirm
```

To enroll with SCEP by using the ASDM, navigate to same section as for self-signed certificates. Give the PKI trustpoint a name, choose **Add a New Identity Certificate** (do not check Generate Self-Signed Certificate), and click the **Advanced** button for enrollment options. From here, you have two options:

- For SCEP enrollment, navigate to **Enrollment Mode** and choose the **Request from a CA** method and complete the URL (which is in the form http://*IP_ADDRESS*/certserv/mscep/mscep.dll). Navigate to **SCEP Challenge Password** and provide the challenge in case the certificate authority (CA) requires it.
- For manual enrollment, navigate to **Enrollment Mode** and choose **Request by Manual Enrollment**. This requires an additional step: After the certificate is issued, it needs to be imported onto the ASA from a file. For this, select the created trustpoint and click **Install**. In the new window, choose **Install from a File** and provide the full path to the base64-encoded certificate.

To configure SCEP enrollment via the CLI, use the following commands:

```
ciscoasa(config)# crypto key generate rsa label SELF-SIGNED modulus 2048
ciscoasa(config)# crypto ca trustpoint TEST-CA
ciscoasa(config-ca-trustpoint)# id-usage ssl-ipsec
ciscoasa(config-ca-trustpoint)# subject-name CN=cisco.com
ciscoasa(config-ca-trustpoint)# enrollment url http://10.10.10.10/certsrv/mscep/mscep.dll
ciscoasa(config-ca-trustpoint)# keypair SELF-SIGNED
ciscoasa(config)# crypto ca authenticate TEST-CA nointeractive
ciscoasa(config)# crypto ca enroll TEST-CA
```

 Please see page 219 for more details.

STEP 2. Load the AnyConnect image onto the ASA.

There are different AnyConnect web deployment packages (PKG files) for different client operating systems. Choose the one you need, download it from Cisco.com, and load it into ASA flash memory. To make the transfer using the ASDM, navigate to **Tools > File Management**.

STEP 3. Enable SSL VPN termination on desired interfaces.

To enable SSL using the ASDM, navigate to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles** and check the **Enable Cisco AnyConnect VPN Client Access on the Interfaces Selected in the Table Below** check box. In the pop-up window, select the AnyConnect image. Choose **Allow Access** and, optionally, **Enable DTLS** for desired interfaces.

To enable SSL via the CLI, use the following commands:

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# enable outside
ciscoasa(config-webvpn)# anyconnect enable
ciscoasa(config-webvpn)# anyconnect image disk0:/ anyconnect-win-3.0.1047-k9.pkg 1
```

STEP 4. Configure and optionally tune SSL Transport Layer Security (TLS) settings.Here, you can tune SSL VPN by allowing only certain SSL/TLS versions and algorithms and by specifying the identity certificate used (if many exist). To configure it using the ASDM, navigate to **Configuration > Remote Access VPN > Advanced > SSL Settings** (see Figure 3-2).

 Please see page 219 for more details.

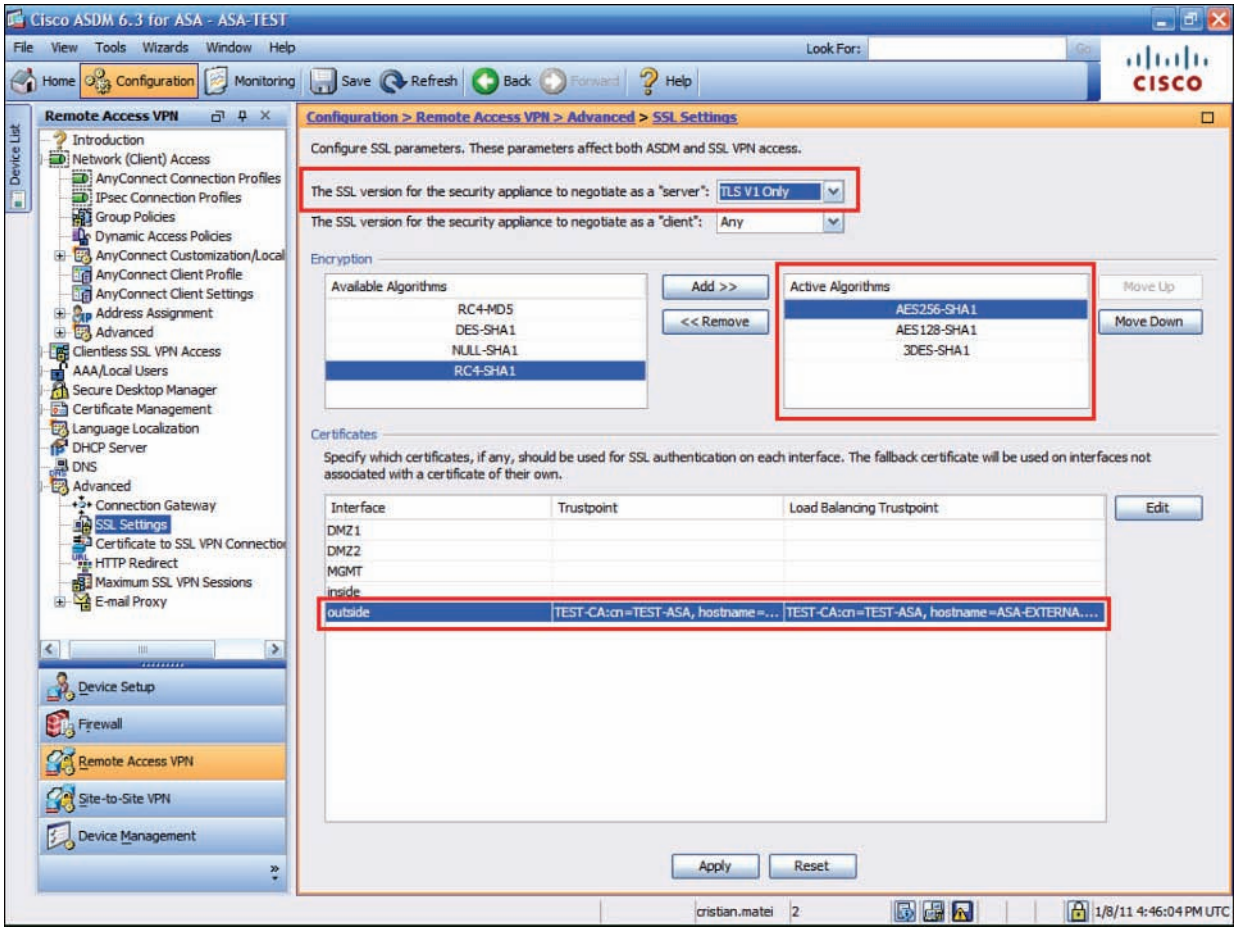

Figure 3-2 SSL VPN Tuning

To configure it via the CLI, use the following commands:

```
ciscoasa(config)#ssl trust-point TEST-CA outside
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)#ssl server-version tlsv1
ciscoasa(config-webvpn)#ssl encryption aes128-sha1 aes256-sha1 3des-sha1 des-sha1
```

 Please see page 219 for more details.

CCNP Security VPN 642-648 Quick Reference

Cristian Matei

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

First Release May 2012

ISBN-13: 978-1-58714-315-1

Warning and Disclaimer

This digital Quick Reference is designed to provide information about the CCNP Security Certification. Every effort has been made to make this digital Quick Reference as complete and accurate as possible, but no warranty or fitness is implied.
The information is provided on an "as is" basis. The author, 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 digital Quick Reference.

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

Trademark Acknowledgments

All terms mentioned in this digital Quick Reference 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 digital Quick Reference should not be regarded as affecting the validity of any trademark or service mark.

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 of the professional technical community.
Reader feedback is a natural continuation of this process. If you have any comments on how we could improve the quality of this digital Quick Reference, or otherwise alter it to better suit your needs, you can contact us through e-mail at feedback@ciscopress.com. Please be sure to include the digital Quick Reference title and ISBN in your message.

We greatly appreciate your assistance.

Corporate and Government Sales

The publisher offers excellent discounts on this digital Quick Reference when ordered in quantity for bulk purchases or special sales, which may include electronic versions and/or custom covers and content particular to your business, training goals, marketing focus, and branding interests. For more information, please contact: U.S. Corporate and Government Sales 1-800-382-3419 corpsales@pearsontechgroup.com.
For sales outside the United States please contact: International Sales international@pearsoned.com

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

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

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

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