CCNP Security VPN 642-647 Quick Reference

Cristian Matei

Cisco Press

CCNP Security VPN 642-647

Quick Reference

Cristian Matei

ciscopress.com

Table of Contents

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 Cisco's security, routing, switching and wireless portfolio of products. Cristian started this journey back in 2005 with Microsoft technology and finished MCSE Security and MCSE Messaging tracks. He then joined Datanet Systems, where he quickly obtained his Security CCIE, among other certifications and specializations, such as CCNP, CCSP, and CCDP. Christian 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 Routing & Switching, Service Provider CCIE tracks and can be found as a regular and active member on Internetwork Expert and Cisco forums.

About the Technical Reviewer

Rasheim Myers, CCIE # 11563, holds designations in Service Provider & Routing/Switching. Rasheim has been working for Cisco since 2000, where he is responsible for designing large scale Service Provider network architectures.

Rasheim serves as a featured speaker at Networkers (Cisco Live) and participates at the Design Clinics, where he assists customers with their network design/implementation challenges.

Rasheim is also one of the founders of the Internetwork Learning Institute, now operating as Network Learning Institute, where he is one of the most sought after instructors for a variety of Cisco Certification courses.

 Please see page 190 for more details.

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'm still waiting for a book release from him; it should break all frontiers.

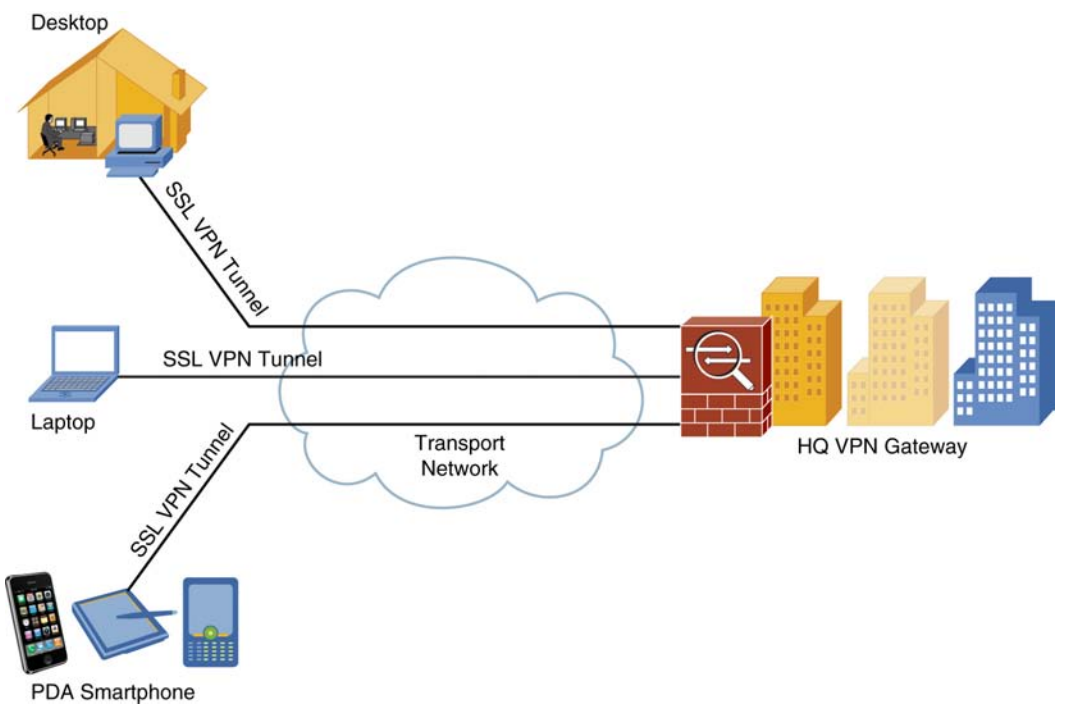
 Please see page 190 for more details.

Chapter 3

Deploying Cisco ASA AnyConnect Remote-Access VPN Solutions

In this chapter, you learn to deploy and manage Secure Sockets Layer (SSL) virtual private networks (VPN) on Cisco Adaptive Security Appliance (ASA) as the VPN gateway with clients using AnyConnect SSL Client software. As you'll see, you can initiate an SSL VPN session from devices that support the install of a dedicated client (desktops, laptops) and from devices that lack administrative privileges to do so (PDA, smartphone, laptop), as shown in Figure 3-1.

FIGURE 3-1
SSL VPN



 Please see page 190 for more details.

Deploying a Basic Cisco AnyConnect Full-Tunnel SSL VPN Solution

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

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 IP address assignment.
4. Configure basic access control.
5. Install the Cisco AnyConnect VPN Client.

As of this writing, AnyConnect Client officially supports only SSL connections. Starting with version 3.0, which is available for download, AnyConnect is composed of multiple modules and supports additional features (including IPsec IKEv2 VPN terminations on Cisco ASA). The problem here is that this requires ASA 8.4(1) and Adaptive Security Device Manager (ASDM) 6.4(1) at a minimum, which are not available for download at the moment of this writing. For these reasons, this book is limited to configuration scenarios supported by AnyConnect versions earlier than 3.0. You can find more information about AnyConnect Secure Mobility Client 3.0 in the official release notes: www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect30/release/notes/anyconnect30rn.html#wp1139431.

Configuring Basic Cisco ASA SSL VPN Gateway Features

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.

 Please see page 190 for more details.

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 by command-line interface (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 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 the 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 **Request from a CA** method, 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 by 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 190 for more details.

Step 2. Load the AnyConnect image onto the ASA.

There are different AnyConnect packages 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 by CLI, use the following commands:

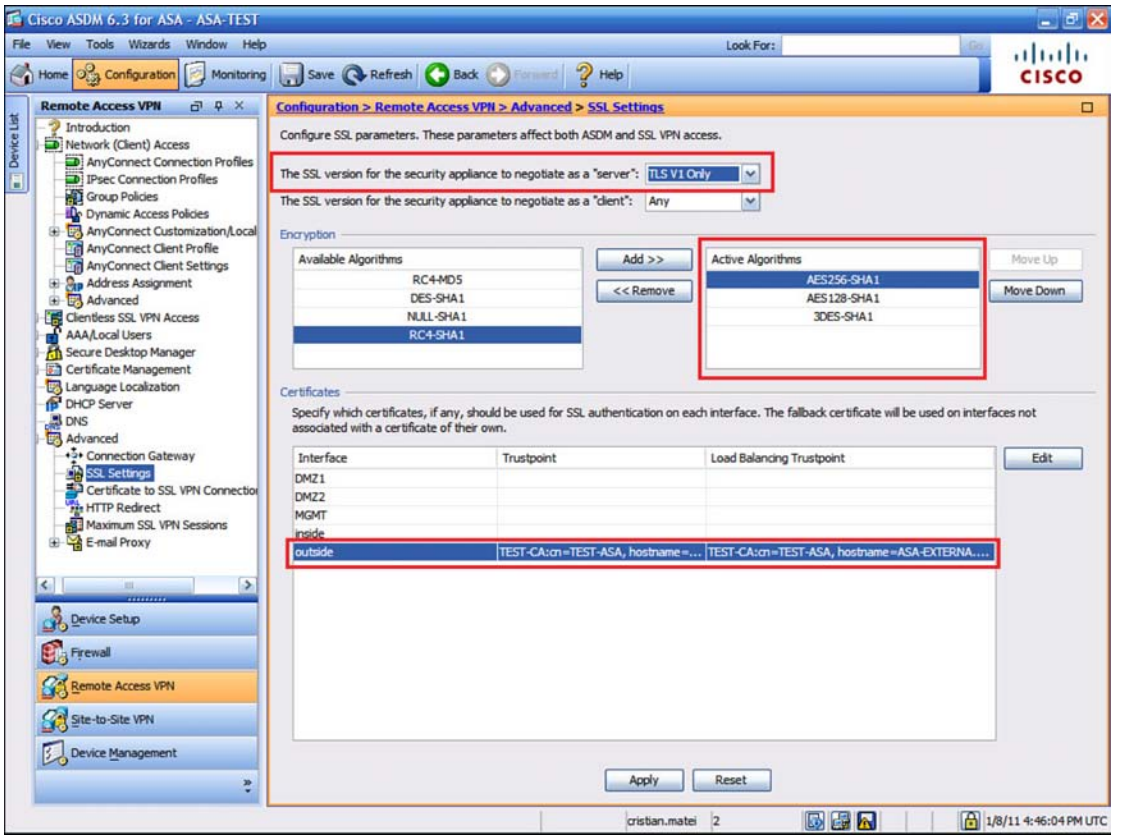
```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# enable outside
ciscoasa(config-webvpn)# svc enable
ciscoasa(config-webvpn)# svc image disk0:/anyconnect-win-2.4.1012-k9.pkg 1
```

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 > Network (Client) Access > AnyConnect Connection Profiles** and click **Click Here to Assign Certificate to Interface** (see Figure 3-2).

 Please see page 190 for more details.

FIGURE 3-2
SSL VPN Tuning



To configure it by CLI, use the following commands:

```
ciscoasa(config)#ssl trustpoint 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
```

Configuring Local Password-Based User Authentication

The simplest authentication method uses local usernames and passwords. We enabled SSL VPN access for AnyConnect clients earlier. Now we need to configure the access, including authentication:

Step 1. Configure a new group policy for AnyConnect connections or modify the default group policy (not recommended because this policy is inherited by all newly created policies, thus making it difficult to differentiate users later).

To create a group policy for AnyConnect connections using the ASDM, navigate to **Configuration > Remote Access VPN > Network (Client) Access > Group Policies** and click **Add**.

To create it by CLI, use the following commands:

```
ciscoasa(config)# group-policy BASIC-ANYCONNECT-POLICY internal
ciscoasa(config)# group-policy BASIC-ANYCONNECT-POLICY attributes
ciscoasa (config-group-policy)# vpn-tunnel-protocol svc
```

Step 2. Configure a connection profile for AnyConnect connections and assign it the new group policy.

To create a connection profile for AnyConnect connections using the ASDM, navigate to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles** and click **Add**.

To create it by CLI, use the following commands:

```
ciscoasa(config)# tunnel-group BASIC-ANYCONNECT-PROFILE type remote-access
ciscoasa(config)# tunnel-group BASIC-ANYCONNECT-PROFILE general-attributes
ciscoasa(config-tunnel-general)# default-group-policy BASIC-ANYCONNECT-POLICY
```

Step 3. Optionally, define an alias for the connection profile.

This option allows users to select the desired connection profile when connecting to the SSL VPN. Navigate in the connection profile configuration to **Advanced > SSL VPN** and click **Add** under Connection Aliases (see Figure 3-3).

 Please see page 190 for more details.