Legacy SCEP with the Use of the CLI Configuration Example

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Components Used](#)
[Background Information](#)
[Configure](#)
[Enroll the ASA](#)
[Configure a Tunnel for Enrollment Use](#)
[Configure a Tunnel for User Certificate Authentication](#)
[Renew the User Certificate](#)
[Verify](#)
[Related Information](#)

Introduction

This document describes the use of Legacy Simple Certificate Enrollment Protocol (SCEP) on the Cisco Adaptive Security Appliance (ASA).

> **Caution**: As of Cisco AnyConnect Release 3.0, this method should not be used. It was previously necessary because mobile devices did not have the 3.x client, but both Android and iPhones now have support for SCEP proxy, which should be used instead. Only in cases where it is not supported because of the ASA should you configure Legacy SCEP. However, even in these cases, an ASA upgrade is the recommended option.

Prerequisites

Requirements

Cisco recommends that you have knowledge of Legacy SCEP.

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Background Information

The SCEP is a protocol that is designed in order to make the distribution and revocation of digital certificates as scalable as possible. The idea is that any standard network user should be able to request a digital certificate electronically with very little intervention from network administrators. For VPN deployments that require certificate authentication with the enterprise, Certificate Authority (CA), or any third-party CA that supports SCEP, users can now request for signed certificates from the client machines without the involvement of the network administrators.

> **Note**: If you desire to configure the ASA as the CA server, then SCEP is not the proper protocol method. Refer to The Local CA section of the **Configuring Digital Certificates** Cisco document instead.

As of ASA Release 8.3, there are two supported methods for SCEP:

- The older method, called Legacy SCEP, is discussed in this document.
- The SCEP proxy method is the newer of the two methods, where the ASA proxies the certificate enrollment request on behalf of the client. This process is cleaner because it does not require an extra tunnel group and is also more secure. However, the drawback is that SCEP proxy only works with Cisco AnyConnect Release 3.x. This means that the current AnyConnect client version for mobile devices does not support SCEP proxy.

Configure

This section provides information that you can use in order to configure the Legacy SCEP protocol method.

> **Note**: Use the Command Lookup Tool (registered customers only) in order to obtain more information on the commands used in this section.

Here are some important notes to keep in mind when Legacy SCEP is used:

- After the client receives the signed certificate, the ASA should recognize the CA that signed the certificate before it is able to authenticate the client. Therefore, you must ensure that the ASA also enrolls with the CA server. The enrollment process for the ASA should be the first step because it ensures that:

  The CA is configured correctly and is able to issue certificates via SCEP if you use the URL enrollment method.

  The ASA is able to communicate with the CA. Therefore, if the client cannot, then there is an

issue between the client and the ASA.

- When the first connection attempt is made, there will not be a signed certificate. There must be another option that can be used in order to authenticate the client.

- In the certificate enrollment process, the ASA serves no role. It only serves as the VPN aggregator so that the client can build a tunnel in order to securely obtain the signed certificate. When the tunnel is established, the client must be able to reach the CA server. Otherwise, it is not be able to enroll.

Enroll the ASA

The ASA enrollment process is relatively easy and does not require any new information. Refer to the Enrolling the Cisco ASA to a CA Using SCEP document for more information about how to enroll the ASA to a third-party CA.

Configure a Tunnel for Enrollment Use

As mentioned previously, in order for the client to be able to obtain a certificate, a secure tunnel must be built with the ASA through a different method of authentication. In order to do this, you must configure one tunnel-group that is only used for the first connection attempt when a certificate request is made. Here is a snapshot of the configuration that is used, which defines this tunnel-group (the important lines are shown in ***bold-italics***):

```
rtpvpnoutbound6(config)# show run user
username cisco password ffIRPGpDSOJh9YLq encrypted privilege 0

rtpvpnoutbound6# show run group-policy gp_certenroll
group-policy gp_certenroll internal
group-policy gp_certenroll attributes
wins-server none
dns-server value <dns-server-ip-address>

vpn-tunnel-protocol ikev2 ssl-client ssl-clientless
group-lock value certenroll
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value acl_certenroll
default-domain value cisco.com
webvpn
anyconnect profiles value pro-sceplegacy type user

rtpvpnoutbound6# show run access-l acl_certenroll
access-list acl_certenroll remark to allow access to the CA server
access-list acl_certenroll standard permit host <ca-server-ipaddress>

rtpvpnoutbound6# show run all tun certenroll
tunnel-group certenroll type remote-access
tunnel-group certenroll general-attributes
address-pool ap_fw-policy
authentication-server-group LOCAL
secondary-authentication-server-group none
default-group-policy gp_certenroll
tunnel-group certenroll webvpn-attributes
authentication aaa
 group-alias certenroll enable
```

Here is the client profile that can either be pasted into a Notepad file and imported to the ASA, or it

can be configured with the Adaptive Security Device Manager (ASDM) directly:

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
<ClientInitialization>
<UseStartBeforeLogon UserControllable="true">false</UseStartBeforeLogon>
<AutomaticCertSelection UserControllable="true">false</AutomaticCertSelection>
<ShowPreConnectMessage>false</ShowPreConnectMessage>
<CertificateStore>All</CertificateStore>
<CertificateStoreOverride>false</CertificateStoreOverride>
<ProxySettings>Native</ProxySettings>
<AllowLocalProxyConnections>true</AllowLocalProxyConnections>
<AuthenticationTimeout>12</AuthenticationTimeout>
<AutoConnectOnStart UserControllable="true">false</AutoConnectOnStart>
<MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
<LocalLanAccess UserControllable="true">false</LocalLanAccess>
<ClearSmartcardPin UserControllable="true">true</ClearSmartcardPin>
<AutoReconnect UserControllable="false">true
<AutoReconnectBehavior UserControllable="false">ReconnectAfterResume
</AutoReconnectBehavior>
</AutoReconnect>
<AutoUpdate UserControllable="false">true</AutoUpdate>
<RSASecurIDIntegration UserControllable="false">Automatic</RSASecurIDIntegration>
<WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
<WindowsVPNEstablishment>LocalUsersOnly</WindowsVPNEstablishment>
<AutomaticVPNPolicy>false</AutomaticVPNPolicy>
<PPPExclusion UserControllable="false">Disable
<PPPExclusionServerIP UserControllable="false"></PPPExclusionServerIP>
</PPPExclusion>
<EnableScripting UserControllable="false">false</EnableScripting>
 <CertificateEnrollment>
 <AutomaticSCEPHost>rtpvpnoutbound6.cisco.com/certenroll</AutomaticSCEPHost>
 <CAURL PromptForChallengePW="false" >scep_url</CAURL>
 <CertificateImportStore>All</CertificateImportStore>
 <CertificateSCEP>
 <Name_CN>%USER%</Name_CN>
 <KeySize>2048</KeySize>
 <DisplayGetCertButton>true</DisplayGetCertButton>
 </CertificateSCEP>
 </CertificateEnrollment>
<EnableAutomaticServerSelection UserControllable="false">false
<AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
<AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
</EnableAutomaticServerSelection>
<RetainVpnOnLogoff>false</RetainVpnOnLogoff>
</ClientInitialization>
 <ServerList>
 <HostEntry>
 <HostName>rtpvpnoutbound6.cisco.com</HostName>
 <HostAddress>rtpvpnoutbound6.cisco.com</HostAddress>
 </HostEntry>
 </ServerList>
</AnyConnectProfile>
```

> **Note**: A group-url is not configured for this tunnel-group. This is important because Legacy SCEP does not work with the URL. You must select the tunnel-group with its alias. This is because of Cisco bug ID CSCtq74054. If you experience issues because of the group-url, you might need to follow up on this bug.

Configure a Tunnel for User Certificate Authentication

When the signed ID certificate is received, connection with certificate authentication is possible. However, the actual tunnel-group that is used in order to connect has not yet been configured. This configuration is similar to the configuration for any other connection-profile. This term is synonymous with tunnel-group and not to be confused with client profile, which uses certificate authentication.

Here is a snapshot of the configuration that is used for this tunnel:

```
rtpvpnoutbound6(config)# show run access-l acl_fw-policy

access-list acl_fw-policy standard permit 192.168.1.0 255.255.255.0

rtpvpnoutbound6(config)# show run group-p gp_legacyscep
group-policy gp_legacyscep internal
group-policy gp_legacyscep attributes
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelspecified
split-tunnel-network-list value acl_fw-policy
default-domain value cisco.com
webvpn
anyconnect modules value dart

rtpvpnoutbound6(config)# show run tunnel tg_legacyscep
tunnel-group tg_legacyscep type remote-access
tunnel-group tg_legacyscep general-attributes
address-pool ap_fw-policy
 default-group-policy gp_legacyscep
tunnel-group tg_legacyscep webvpn-attributes
 authentication certificate
group-alias legacyscep enable
group-url https://rtpvpnoutbound6.cisco.com/legacyscep enable
```

Renew the User Certificate

When the user certificate expires or is revoked, Cisco AnyConnect fails the certificate authentication. The only option is to reconnect to the certificate enrollment tunnel-group in order to trigger the SCEP enrollment again.

Verify

Use the information that is provided in this section in order to confirm that your configuration works properly.

> **Note**: Since the Legacy SCEP method should only be implemented with the use of mobile devices, this section only deals with mobile clients.

Complete these steps in order to verify your configuration:

1. When you attempt to connect for the first time, enter the ASA hostname or IP address.

2. Select **certenroll**, or the group alias that you configured in the Configure a Tunnel for Enrollment Use section of this document. You are then prompted for a username and password, and the **get certificate** button is displayed.

3. Click the **get certificate** button.

If you check your client logs, this output should display:

```
[06-22-12 11:23:45:121] <Information> - Contacting https://rtpvpnoutbound6.cisco.com.
[06-22-12 11:23:45:324] <Warning> - No valid certificates available for authentication.
[06-22-12 11:23:51:767] <Information> - Establishing VPN session...
[06-22-12 11:23:51:879] <Information> - Establishing VPN session...
[06-22-12 11:23:51:884] <Information> - Establishing VPN - Initiating connection...
[06-22-12 11:23:52:066] <Information> - Establishing VPN - Examining system...
[06-22-12 11:23:52:069] <Information> - Establishing VPN - Activating VPN adapter...
[06-22-12 11:23:52:594] <Information> - Establishing VPN - Configuring system...
[06-22-12 11:23:52:627] <Information> - Establishing VPN...
[06-22-12 11:23:52:734] <Information> - VPN session established to
https://rtpvpnoutbound6.cisco.com.
[06-22-12 11:23:52:764] <Information> - Certificate Enrollment - Initiating, Please Wait.
[06-22-12 11:23:52:771] <Information> - Certificate Enrollment - Request forwarded.
[06-22-12 11:23:55:642] <Information> - Certificate Enrollment - Storing Certificate
[06-22-12 11:24:02:756] <Error> - Certificate Enrollment - Certificate successfully
imported. Please manually associate the certificate with your profile and reconnect.
```

Even though the last message shows **error**, it is only to inform the user that this step is necessary in order for that client to be used for the next connection attempt, which is in the second connection profile that is configured in the Configure a Tunnel for User Certificate Authentication section of this document.

Related Information

- **CSCtq74054 SCEP is not initiated when using a URL (asa-IP/tunnel-group alias)**
- **Technical Support & Documentation**