CLI を使用するレガシー SCEP の設定例

目次

概要

この資料はのレガシー Simple Certificate Enrollment Protocol （ SCEP ）の使用を Cisco 適応型セキュリティ アプライアンス (ASA) ソフトウェア記述したものです (ASA) 。

> **注意**： Cisco AnyConnect リリース 3.0 現在で、この方式は使用するべきではありません。それはモバイルデバイスが 3.x クライアントを備えなかったが、Android におよび iPhone に両方今代りに使用する必要がある SCEP プロキシのためのサポートがありますので以前に必要でした。 もしレガシー SCEP を設定すればそれが ASA が理由でサポートされなければだけ。 ただし、このような場合、ASA アップグレードは推奨されるオプションです。

前提条件

要件

Cisco はレガシー SCEP のナレッジがあることを推奨します。

使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

背景説明

スケーラブル な デジタル証明書のディストリビューションおよび失効をできるだけするために設計されている SCEP はプロトコルです。 概念はどの標準ネットワーク ユーザでもネットワーク管理者からの少しだけ介入とデジタル認証を電子的に要求できるはずであることです。 企業、認証局 （CA）、または SCEP をサポートするサード パーティ CA の証明書認証を必要とする VPN 配置に関しては、ユーザはネットワーク管理者の介入なしでクライアントマシンからの署名入り認証のための Now 要求できます。

> **注:** CA サーバで ASA を設定することを望む場合 SCEP は適切なプロトコル メソッドではないです。 **デジタル証明書** Ciscoドキュメントの**設定**のローカル CA セクションを代りに参照して下さい。

ASA リリース 8.3 現在で、SCEP における 2 つのサポートされた方法があります:

- Legacy SCEP と呼ばれるより古い方式はこの資料で説明されています。
- SCEP プロキシ 方式がクライアントに代わって 2 つのメソッドのより新しい、ASA プロキシ 証明書登録 要求。 このプロセスは余分トンネル グループを必要としないで、またセキュアですのでよりきれい。 ただし、欠点は SCEP プロキシが Cisco AnyConnect リリース 3.x をだけ使用することです。 これはモバイルデバイスのための AnyConnect 現在のクライアントバージョンが SCEP プロキシをサポートしないことを意味します。

設定

このセクションはレガシー SCEP プロトコル 方式を設定するために使用できる情報を提供します。

> **注:** このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

レガシー SCEP が使用されるとき留意するべきいくつかの注記はここにあります:

- クライアントが署名入り認証を受け取った後、ASA はそれがクライアントを認証ことはできる前に認証に署名した CA を認識する必要があります。 従って、ASA がまた CA サーバと登録するようにして下さい。 ASA のための登録プロセスはそれを確認するので第一歩であるはずです:

  CA は URL 登録方式を使用する場合正しく設定され、SCEP によって認証を発行できます。

  ASA は CA と通信できます。 従ってクライアントができなければ、そしてクライアントと

ASA 間に問題があります。
- 最初の接続の試みが試みられる場合、署名入り認証がありません。 クライアントを認証するために使用できる別のオプションがある必要があります。

- 証明書登録 プロセスでは、ASA はロールを動作しません。 それは VPN 集約機能として安全に 署名入り認証を得るためにクライアントがトンネルを構築できるようにだけ動作します。 トンネルが確立されるとき、クライアントは CA サーバに達できます必要があります。 さもなければ、それは登録ことはできることではないです。

ASA を登録して下さい

ASA 登録プロセスは比較的容易で、新しい情報を必要としません。 サード パーティ CA に ASA を登録する方法に関する詳細については SCEP 資料を使用して CA に Cisco ASA を登録することを参照して下さい。

登録使用のためのトンネルを設定して下さい

クライアントが認証の異った方法による ASA と認証を得られるセキュアトンネル構築する必要があることができるように、以前に述べられるように。 これをするために、証明書要求がなされるときだけ最初の接続の試みのために使用する 1 つのトンネル グループを設定して下さい。 使用する設定のスナップショットはここにあります、このトンネル グループを定義する (重要な行は ***太イタリック体***で示されています) :

```
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
```

Notepad ファイルに貼り付けられ、ASA にインポートすることができるまたは直接 Adaptive

Security Device Manager（ASDM）で設定することができますクライアント プロファイルはここにありますか、：

```
<?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>
```

注: グループ URL はこのトンネル グループのために設定されません。 これはレガシー SCEP が URL を使用しないので重要です。 エイリアスのトンネル グループを選択して下さい。 これは Cisco バグ ID CSCtq74054 が理由でそうなったものです。 グループ URL が理由で問題に直面する場合、この不具合で追う必要があるかもしれません。

ユーザ許可証 認証のためのトンネルを設定して下さい

署名された ID 認証が受け取られるとき、証明書認証を用いる接続は可能性のあるです。 ただし、接続するために使用する実際のトンネル グループはまだ設定されていません。 この設定は他のどの接続プロファイルのための設定に類似したです。 この条件は証明書認証を使用するトンネル グループと同義クライアント プロファイルと混同しないためにであり。

このトンネルのために使用する設定のスナップショットはここにあります:

```
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
```

ユーザ許可証を更新して下さい

ユーザ許可証が切れるか、または取り消されるとき、Cisco AnyConnect は証明書認証失敗します。 唯一のオプションは SCEP 登録を再度引き起こすために証明書登録 トンネル グループへ再接続することです。

確認

情報を使用して下さい設定はきちんと機能することを確認するためにこのセクションで提供される。

> **注:** レガシー SCEP 方式がモバイルデバイスの使用としか設定する必要がないのでセクション モービル クライアントとの取り引きだけこの。

設定を確認するには、次の手順を実行します。

1. はじめて接続するように試みるとき ASA ホスト名か IP アドレスを入力して下さい。
2. certenroll を、か設定でこの資料の登録使用 セクションのためのトンネルを設定したグルー

プ エイリアスを選択して下さい。 ユーザ名 および パスワードのためにそれからプロンプト表示され、**得 Certificate ボタンは**表示する。

3. **得 Certificate ボタンを**クリックして下さい。

クライアント ログをチェックする場合、この出力は下記のものを表示する必要があります:

```
[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.
```

最後のメッセージは**エラーを**示すのに、そのクライアントが設定でこの資料のユーザ許可証 Authentication セクションのためのトンネル設定される第 2 接続プロファイルにある次の接続の試みに使用することができるようにこのステップが必要であることユーザを知らせることです。

関連情報

- **URL（ASA IP/トンネル グループ エイリアス）を使用するとき CSCtq74054 SCEP は始められません**
- **テクニカル サポートとドキュメント**