CLI を使用するレガシー SCEP の設定例

内容

概要

このドキュメントでは、Cisco適応型セキュリティアプライアンス(ASA)でのレガシーSimple Certificate Enrollment Protocol(SCEP)の使用について説明します。

> **注意**：Cisco AnyConnectリリース3.0以降では、この方式は使用しないでください。以前は、モバイルデバイスには3.xクライアントがありませんでしたが、AndroidとiPhoneの両方でSCEPプロキシがサポートされるようになり、代わりに使用する必要がありました。レガシーSCEPを設定する必要があるのは、ASAが原因でサポートされていない場合だけです。ただし、このような場合でも、ASAのアップグレードが推奨されるオプションです。

前提条件

要件

レガシーSCEPに関する知識があることが推奨されます。

使用するコンポーネント

このドキュメントの内容は、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ました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

SCEPは、デジタル証明書の配布と取り消しを可能な限りスケーラブルにするために設計されたプロトコルです。ネットワークの標準的なユーザであれば、ネットワーク管理者の介入をほとんど受けずに、電子証明書を要求できるはずです。エンタープライズ、認証局(CA)、またはSCEPをサポートするサードパーティCAとの証明書認証を必要とするVPN展開では、ネットワーク管理者の介入なしにクライアントマシンから署名付き証明書を要求できるようになりました。

> **注**：ASAをCAサーバとして設定する場合、SCEPは適切なプロトコル方式ではありません。代わりに、『デジタル証明書の設定』の「**ローカルCA**」セクションを参照してください。

ASAリリース8.3では、SCEPでサポートされる方式は2つあります。

- このドキュメントでは、レガシーSCEPと呼ばれる古い方法について説明します。
- SCEPプロキシ方式は、2つの方式の新しい方式です。ASAは、クライアントの代わりに証明書登録要求をプロキシします。このプロセスは、追加のトンネルグループを必要とせず、さらに安全であるため、よりクリーンです。ただし、欠点は、SCEPプロキシがCisco AnyConnectリリース3.xでのみ動作することです。これは、モバイルデバイスの現在のAnyConnectクライアントバージョンがSCEPプロキシをサポートしていないことを意味します。

設定

このセクションでは、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るコマンドの詳細については、Command Lookup Tool（登録ユーザ専用）を使用してください。

レガシーSCEPを使用する際に注意すべき重要な注意事項を次に示します。

- クライアントが署名付き証明書を受信した後、ASAはクライアントを認証する前に、証明書に署名したCAを認識する必要があります。したがって、ASAがCAサーバにも登録されていることを確認する必要があります。ASAの登録プロセスは最初のステップである必要があります。これは、次のことを保証するためです。

  CAは正しく設定されており、URL登録方法を使用すると、SCEP経由で証明書を発行できます。

ASAはCAと通信できます。したがって、クライアントが接続できない場合、クライアントとASAの間に問題があります。
- 最初の接続が試行されても、署名付き証明書は存在しません。クライアントの認証に使用できる別のオプションが必要です。

- 証明書登録プロセスでは、ASAは役割を果たしません。クライアントが署名付き証明書を安全に取得するためにトンネルを構築できるように、VPNアグリゲータとしてのみ機能します。トンネルが確立されると、クライアントはCAサーバに到達できる必要があります。そうしないと、登録できません。

ASAの登録

ASAの登録プロセスは比較的簡単で、新しい情報は必要ありません。ASAをサードパーティCAに登録する方法の詳細については、「SCEPを使用したCAへのCisco ASAの登録」を参照してください。

登録用のトンネルの設定

前述のように、クライアントが証明書を取得できるようにするには、別の認証方式を使用してASAとセキュアトンネルを構築する必要があります。これを行うには、証明書要求が行われたときに最初の接続の試行にのみ使用される1つのトンネルグループを設定する必要があります。次に、このトンネルグループを定義する設定のスナップショットを示します(重要な行は太字斜体で示***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
```

```
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
```

次に、メモ帳ファイルに貼り付けてASAにインポートできるクライアントプロファイルを示します。または、Adaptive Security Device Manager(ASDM)を使用して直接設定することもできます。

```
<?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>
```

```
<EnableAutomaticServerSelection UserControllable="false">false
<AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
<AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
</EnableAutomaticServerSelection>
<RetainVpnOnLogoff>false</RetainVpnOnLogoff>
</ClientInitialization>
```

```
</AnyConnectProfile>
```

注：このトンネルグループにグループURLが設定されていません。レガシーSCEPはURLで機能しないため、これは重要です。エイリアスを持つトンネルグループを選択する必要があります。これは、Cisco Bug ID CSCtq74054が原因です。グループURLが原因で問題が発生した場合は、このバグをフォローアップする必要があります。

ユーザ証明書認証用のトンネルの設定

署名付きID証明書を受信すると、証明書認証を使用して接続できます。ただし、接続に使用され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、他の接続プロファイルの設定に似ています。この用語はtunnel-groupと同義であり、証明書認証を使用するクライアントプロファイルと混同しないでください。

このトンネルに使用される設定のスナップショットを次に示します。

```
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
```

ユーザ証明書の更新

ユーザ証明書の有効期限が切れるか、または失効すると、Cisco AnyConnectは証明書認証に失敗します。唯一のオプションは、証明書登録トンネルグループに再接続して、SCEP登録を再びトリガーすることです。

確認

このセクションに記載されている情報を使用して、設定が正しく動作していることを確認します。

> **注**：レガシーSCEP方式はモバイルデバイスの使用でのみ実装する必要があるため、このセクションではモバイルクライアントのみを扱います。

設定を確認するには、次の手順を実行します。

1. 初めて接続するときは、ASAのホスト名またはIPアドレスを入力します。
2. certenroll**または**、このドキュメントの「Configure a Tunnel for Enrollment Use」セクションで設定したグループエイリアスを選択します。次に、ユーザ名とパスワードの入力を求めるプロンプトが表示され、証明書**の取得ボタン**が表示されます。
3. 証明書の取得ボタン**をクリック**します。

クライアントログを確認すると、次の出力が表示されます。

```
[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]



[06-22-12 11:23:52:764]



[06-22-12 11:23:52:771]



[06-22-12 11:23:55:642]



[06-22-12 11:24:02:756]
```

最後のメッセージにerrorが示されている場合でも、このステップが次の接続試行に使用するために必要であることをユーザに通知することだけです。このステップは、このドキュメントの「ユーザ証明書認証のためのトンネルの設定」セクションで設定した2番目の接続プロファイルです。

関連情報

- CSCtq74054 SCEPは、URL(asa-IP/tunnel-group alias)を使用している場合は開始されません
- テクニカル サポートとドキュメント