使用CLI的传统SCEP配置示例

目录

简介

本文档介绍在思科自适应安全设备(ASA)上使用传统简单证书注册协议(SCEP)。

> **警告：**自Cisco AnyConnect版本3.0起，不应使用此方法。之前需要使用SCEP代理，因为移动设备没有3.x客户端，但Android和iPhone现在都支持SCEP代理，应使用SCEP代理。仅在因ASA而不支持SCEP的情况下，您才应配置传统SCEP。但是，即使在这些情况下，也建议使用ASA升级。

先决条件

要求

思科建议您了解传统SCEP。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

SCEP是一种协议，旨在使数字证书的分发和撤销尽可能具有可扩展性。其思想是，任何标准网络用户都应该能够以电子方式请求数字证书，而网络管理员几乎无需干预。对于需要与企业、证书颁发机构(CA)或任何支持SCEP的第三方CA进行证书身份验证的VPN部署，用户现在无需网络管理员的参与即可从客户端计算机请求签名证书。

> **注意：**如果要将ASA配置为CA服务器，则SCEP不是正确的协议方法。请参阅配置数字证书思科文**档的本地**CA部分。

自ASA 8.3版起，SCEP支持两种方法：

- 本文档将讨论较旧的方法，称为传统SCEP。
- SCEP代理方法是两种方法中较新的一种，其中ASA代表客户端代理证书注册请求。此过程更简洁，因为它不需要额外的隧道组，也更加安全。但是，缺点是SCEP代理仅与Cisco AnyConnect版本3.x配合使用。这意味着移动设备的当前AnyConnect客户端版本不支持SCEP代理。

配置

本节提供可用于配置传统SCEP协议方法的信息。

> **注意：**使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

使用传统SCEP时，请记住以下重要注意事项：

- 客户端收到签名证书后，ASA应先识别签名证书的CA，然后才能对客户端进行身份验证。因此，您必须确保ASA也注册到CA服务器。ASA的注册过程应是第一步，因为它可确保：

  CA配置正确，如果使用URL注册方法，它可以通过SCEP颁发证书。

  ASA能够与CA通信。因此，如果客户端不能，则客户端和ASA之间会出现问题。
- 首次尝试连接时，将不会有签名证书。必须使用另一个选项来验证客户端。
- 在证书注册过程中，ASA不起任何作用。它仅用作VPN聚合器，以便客户端可以构建隧道以安全地获取签名证书。隧道建立后，客户端必须能够到达CA服务器。否则，它将无法注册。

注册ASA

ASA注册过程相对简单，不需要任何新信息。有关如何将ASA注册到第三方CA的详细信息，请参阅使用SCEP将Cisco ASA注册到CA文档。

配置隧道以供注册使用

如前所述，为使客户端能够获得证书，必须通过不同的身份验证方法与ASA建立安全隧道。为此，您必须配置一个隧道组，该隧道组仅用于发出证书请求时的首次连接尝试。以下是所用配置的快照，它定义此隧道组(重要行以粗体斜体***显示***):

```
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
```

以下是可粘贴到记事本文件并导入到ASA的客户端配置文件，或者可以直接使用自适应安全设备管理器(ASDM)进行配置：

```
<?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>
```

> **注意：**未为此隧道组配置group-url。这很重要，因为传统SCEP不与URL配合使用。必须选择具有其别名的隧道组。这是因为Cisco Bug ID CSCtq74054。如果由于group-url而遇到问题，则可能需要跟进此Bug。

为用户证书身份验证配置隧道

收到签名的ID证书时，可能会连接证书身份验证。但是，尚未配置用于连接的实际隧道组。此配置类似于任何其他连接配置文件的配置。此术语与隧道组同义，不要与使用证书身份验证的客户端配置文件相混淆。

以下是用于此隧道的配置的快照：

```
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
```

续订用户证书

当用户证书过期或被撤销时，Cisco AnyConnect将失败证书身份验证。唯一的选项是重新连接到证书注册隧道组，以再次触发SCEP注册。

验证

使用本节中提供的信息确认您的配置工作正常。

注意：由于传统SCEP方法只应使用移动设备实施，因此本部分仅处理移动客户端。

要验证配置，请完成以下步骤：

1. 首次尝试连接时，输入ASA主机名或IP地址。
2. 选择**certenroll**或您在本文档的“配置隧道以供注册使用”部分中配置的组别名。系统随后提示您输入用户名和密码，并**显示**“获取证书”按钮。
3. 单击“获取**证书**”按钮。

如果检查客户端日志，应显示以下输出：

```
[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]
```

即使最后一条消息显示**错误**，它也只是通知用户此步骤是必要的，以便该客户端用于下次连接尝试

，该连接配置文件位于本文档的“配置用户证书身份验证的隧道”部分中配置的第二个连接配置文件中。

相关信息

- 使用URL（asa-IP/隧道组别名）时，CSCtq74054 SCEP未启动
- 技术支持和文档