与使用的传统SCEP CLI配置示例

目录

简介

本文描述使用在思科可适应安全工具(ASA)的传统简单认证登记协议(SCEP)。

> **警告：**自思科AnyConnect版本3.0，不应该使用此方法。以前是必要的，因为移动设备没有3.x客户端，但是机器人和IP电话当前有SCEP代理的支持，应该使用。只有在它不支持由于ASA处如果配置传统SCEP。然而，均等在这些情况下， ASA升级是推荐的选项。

先决条件

要求

思科建议您有传统SCEP知识。

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是设计为了做分配和撤销数字证书一样可扩展尽可能的协议。想法是所有标准网络用户应该能电子上请求数字证书与从网络管理员的很少干预。对于要求与企业、Certificate Authority (CA)，或者所有第三方CA的证书验证支持SCEP的VPN部署，用户能为从客户端机器的签名证书当前请求，不用网络管理员的介入。

> **注意**：如果希望配置ASA作为CA服务器，则SCEP不是正确的协议方法。参考**配置的数字证书**Cisco文档的本地CA部分。

自ASA版本8.3，有SCEP的两支持的方法：

- 更旧的方法，呼叫Legacy SCEP，在本文讨论。
- SCEP代理方法是新的两个方法， ASA代理证书登记请求代表客户端。此进程是更加干净的，因为不要求一个额外的隧道组并且也是安全的更多。然而，缺点是SCEP代理只与思科AnyConnect版本3.x一起使用。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

此部分提供您能使用为了配置传统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。

这是要记住的一些重要提示，当使用时传统SCEP ：

- 在客户端接收签名证书后， ASA应该认可签署证书的CA，在能验证客户端前。所以，您必须保证ASA用CA服务器也登记。因为保证那， ASA的登记进程应该是第一步：

  如果使用URL登记方法， CA正确地配置并且能通过SCEP发行证书。

  ASA能通信与CA。所以，如果客户端不能，然后有在客户端和ASA之间的一个问题。
- 当第一个连接尝试被做，将没有签名证书。必须有能使用为了验证客户端的另一个选项。
- 在证书登记进程， ASA不服务角色。它只担当VPN聚合器，以便客户端能构建通道为了安全地获取签名证书。当通道设立时，客户端一定能到达CA服务器。否则，它不是能登记。

登记ASA

ASA登记进程是相对容易，并且不要求任何最新信息。 参考登记思科ASA对CA使用SCEP文档关于如何登记ASA的更多信息到第三方CA。

配置通道为登记使用

如被提及以前，为了客户端能能获取证书，安全隧道必须用ASA建立通过验证不同的说法。为了执行此，您必须配置只使用第一个连接尝试的一隧道群，当证书请求被做时。这是使用，定义了此隧道群配置的快照(重要线路显示以博尔德***斜体字***) ：

```
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
```

这是可能或者粘贴到Notepad文件和导入到ASA的客户端配置文件，或者可以配置与直接可适应安全设备管理器(ASDM) ：

```
<?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>
```

> **注意**：group-url没有为此隧道群配置。因为传统SCEP不与URL一起使用，这是重要。您必须选择有其别名的隧道群。这是由于Cisco Bug ID CSCtq74054。 如果遇到问题由于group-url，您在此bug也许需要接着。

配置用户证书验证的通道

当签字的ID证书接收时，与证书验证的连接是可能的。 然而，使用为了连接的实际隧道群未配置。此配置类似于其他连接配置文件的配置。此期限与隧道群是同义的和与客户端配置文件不混淆，使用证书验证。

这是使用此通道配置的快照：

```
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
```

更新用户证书

当用户证书超时或取消时，思科AnyConnect发生故障证书验证。唯一选择是重新连接对证书登记隧道群为了再触发SCEP登记。

验证

请使用在此部分被提供为了确认的信息您的配置适当地工作。

注意：因为应该只实现传统SCEP方法与使用移动设备，与移动客户端的仅此部分交易。

要验证配置，请完成以下步骤：

1. 当您尝试第一次时连接，请输入ASA主机名或IP地址。
2. 选择certenroll或者组别名您在配置配置登记本文的使用部分的一个通道。然后提示对于用户名和密码，并且**获得证书**按钮显示。
3. 点击**获得证书**按钮。

如果检查您的客户端日志，此输出应该显示：

```
[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.
```

即使最后一条消息显示**错误**，是只通知用户此步骤是必要为了该客户端能用于导航尝试，在第二个连接配置文件在配置配置本文的用户证书Authentication部分的一个通道。

相关信息

- CSCtq74054 SCEP没有启动，当曾经URL时(ASA IP/隧道群别名)
- 技术支持和文档