使用CLI的傳統SCEP配置示例

目錄

簡介

本檔案介紹舊版簡單憑證註冊通訊協定(SCEP)在思科調適型安全裝置(ASA)上的使用。

> **注意**：自Cisco AnyConnect 3.0版起，不應使用此方法。以前之所以需要這樣做，是因為流動裝置沒有3.x客戶端，但是Android和iPhone現在都支援SCEP代理，而應該使用它。只有在由於ASA不支援的情況下，才應配置傳統SCEP。但是，即使在這些情況下，建議使用ASA升級。

必要條件

需求

思科建議您瞭解傳統SCEP。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

SCEP是一種協定，旨在使數位證書的分發和撤銷儘可能的可擴充性。其理念是，任何標準網路使用者都應該能夠以電子方式請求數位證書，而網路管理員只需極少干預。對於需要向企業、證書頒發機構(CA)或任何支援SCEP的第三方CA進行證書身份驗證的VPN部署，使用者現在無需網路管理員的參與即可從客戶端電腦請求已簽名的證書。

> **附註**：如果您希望將ASA配置為CA伺服器，則SCEP不是正確的協定方法。請改為參閱**設定數位憑證** Cisco檔案的本地CA一節。

自ASA 8.3版起，SCEP支援兩種方法：

- 本文檔將討論較舊的方法，稱為傳統SCEP。
- SCEP代理方法是兩種方法中的較新方法，其中ASA代表客戶端代理證書註冊請求。此過程更乾淨，因為它不需要額外的隧道組，而且更安全。但是缺點是SCEP代理僅適用於Cisco AnyConnect 3.x版。這表示目前流動裝置的AnyConnect客戶端版本不支援SCEP代理。

設定

本節提供的資訊可用於配置傳統SCEP協定方法。

> **附註**：使用命令查詢工具(僅供已註冊客戶使用)可獲取本節中使用的命令的更多資訊。

以下是使用傳統SCEP時需要記住的一些重要說明：

- 客戶端收到簽名證書後，ASA應識別簽名證書的CA，然後才能夠對客戶端進行身份驗證。因此，您必須確保ASA也向CA伺服器註冊。ASA的註冊過程應該是第一步，因為它確保：

  CA已正確設定，且如果您使用URL註冊方法，則能夠透過SCEP發出憑證。

  ASA能夠與CA通訊。因此，如果客戶端無法訪問，則客戶端和ASA之間出現問題。
- 進行第一次連線嘗試時，不會存在已簽名的證書。必須有另一個選項可用於對客戶端進行身份驗證。
- 在證書註冊過程中，ASA不發揮作用。它僅充當VPN聚合器，以便客戶端可以建立隧道來安全地獲取已簽名的證書。建立通道後，使用者端必須能夠連線至CA伺服器。否則，它將無法註冊。

註冊ASA

ASA註冊過程相對簡單，不需要任何新資訊。有關如何將ASA註冊到第三方CA的詳細資訊，請參閱使用SCEP將Cisco ASA註冊到CA文檔。

配置用於註冊的隧道

如前所述，為了使客戶端能夠獲取證書，必須使用ASA通過不同的身份驗證方法構建安全隧道。為此，您必須配置一個隧道組，該組僅在發出證書請求時用於第一次連線嘗試。以下是已使用的組態的快照，其中定義了該通道組(重要線路以***粗斜體顯***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
```

以下是可以貼上到記事本檔案中並匯入到ASA的客戶端配置檔案，也可以直接使用自適應安全裝置管理器(ASDM)進行配置：

```
<?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>
```

附註：沒有為此隧道組配置group-url。這非常重要，因為傳統SCEP不能與URL一起使用。您必須選擇具有其別名的隧道組。這是因為思科錯誤ID CSCtq74054。如果由於group-url而遇到問題，則可能需要追蹤此錯誤。

為使用者證書身份驗證配置隧道

收到簽名的ID證書時，可以連線到證書身份驗證。但是，尚未配置用於連線的實際隧道組。此配置類似於任何其他連線配置檔案的配置。此術語與隧道組同義，請勿與使用證書身份驗證的客戶端配置檔案混淆。

以下是用於此通道的組態的快照：

```
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
```

續訂使用者證書

當使用者證書到期或被吊銷時，Cisco AnyConnect無法進行證書身份驗證。唯一的選項是重新連線到證書註冊隧道組，以便再次觸發SCEP註冊。

驗證

使用本節提供的資訊以確認您的組態是否正常運作。

附註：由於傳統SCEP方法只能使用流動裝置實現，因此本節只處理移動客戶端。

完成以下步驟以驗證您的設定：

1. 當您首次嘗試連線時，輸入ASA主機名或IP地址。
2. 選擇**certenroll**，或您在本文檔的配置用於註冊的隧道部分中配置的組別名。系統提示您輸入使用者名稱和密碼，並顯示**get certificate**按鈕。
3. 按一下**get certificate**按鈕。

如果檢查客戶端日誌，應顯示以下輸出：

```
[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]
```

即使最後一條消息顯示**錯誤**，也只是為了通知使用者必須執行此步驟才能將該客戶端用於下一次連

線嘗試，該連線嘗試位於本文檔的為使用者證書身份驗證配置隧道部分中配置的第二個連線配置檔案中。

相關資訊

- 使用URL(asa-IP/tunnel-group alias)時不會啟動CSCtq74054 SCEP
- 技術支援與檔案