Exemple de configuration SCEP hérité avec l'utilisation de l'interface de ligne de commande

Contenu

Introduction

Ce document décrit l'utilisation du protocole SCEP (Simple Certificate Enrollment Protocol) existant sur l'appliance de sécurité adaptative (ASA) de Cisco.

> **Attention** : Depuis Cisco AnyConnect version 3.0, cette méthode ne doit pas être utilisée. Cela était auparavant nécessaire parce que les appareils mobiles n'avaient pas le client 3.x, mais Android et les iPhones ont maintenant pris en charge le proxy SCEP, qui devrait être utilisé à la place. Ce n'est que dans les cas où il n'est pas pris en charge en raison de l'ASA que vous devez configurer le SCEP hérité. Cependant, même dans ces cas, une mise à niveau ASA est recommandée.

Conditions préalables

Conditions requises

Cisco vous recommande de connaître le SCEP existant.

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informations générales

Le SCEP est un protocole conçu pour rendre la distribution et la révocation des certificats numériques aussi évolutives que possible. L'idée est que tout utilisateur réseau standard doit pouvoir demander un certificat numérique par voie électronique avec très peu d'intervention de la part des administrateurs réseau. Pour les déploiements VPN qui nécessitent une authentification de certificat avec l'entreprise, l'autorité de certification (CA) ou toute autorité de certification tierce prenant en charge SCEP, les utilisateurs peuvent désormais demander des certificats signés aux machines clientes sans l'intervention des administrateurs réseau.

> **Note**: Si vous souhaitez configurer l'ASA en tant que serveur AC, SCEP n'est pas la méthode de protocole appropriée. Reportez-vous à la section Autorité de certification locale du document **Configuration des certificats numériques** Cisco à la place.

Depuis la version 8.3 d'ASA, deux méthodes sont prises en charge pour SCEP :

- L'ancienne méthode, appelée Legacy SCEP, est traitée dans ce document.
- La méthode proxy SCEP est la plus récente des deux méthodes, où l'ASA envoie une requête d'inscription de certificat par proxy au nom du client. Ce processus est plus propre car il ne nécessite pas de groupe de tunnels supplémentaire et est également plus sécurisé. Cependant, le problème est que le proxy SCEP fonctionne uniquement avec Cisco AnyConnect version 3.x. Cela signifie que la version actuelle du client AnyConnect pour les périphériques mobiles ne prend pas en charge le proxy SCEP.

Configuration

Cette section fournit des informations que vous pouvez utiliser afin de configurer la méthode de protocole SCEP existante.

> **Note**: Utilisez l'Outil de recherche de commande (clients inscrits seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Voici quelques remarques importantes à garder à l'esprit lors de l'utilisation du SCEP hérité :

- Une fois que le client a reçu le certificat signé, l'ASA doit reconnaître l'autorité de certification qui a signé le certificat avant de pouvoir authentifier le client. Par conséquent, vous devez vous assurer que l'ASA s'inscrit également au serveur AC. Le processus d'inscription de l'ASA doit être la première étape car il garantit que :

L'autorité de certification est configurée correctement et peut émettre des certificats via SCEP si vous utilisez la méthode d'inscription d'URL.

L'ASA peut communiquer avec l'autorité de certification. Par conséquent, si le client ne peut pas le faire, il y a un problème entre le client et l'ASA.

- Lors de la première tentative de connexion, aucun certificat signé n'est émis. Une autre option doit être utilisée pour authentifier le client.

- Dans le processus d'inscription des certificats, l'ASA ne joue aucun rôle. Il sert uniquement d'agrégateur VPN pour que le client puisse construire un tunnel afin d'obtenir le certificat signé en toute sécurité. Une fois le tunnel établi, le client doit être en mesure d'atteindre le serveur AC. Sinon, il ne peut pas s'inscrire.

Inscrire ASA

Le processus d'inscription à ASA est relativement simple et ne nécessite aucune nouvelle information. Référez-vous au document Inscription de Cisco ASA à une autorité de certification à l'aide de SCEP pour plus d'informations sur la façon d'inscrire l'ASA à une autorité de certification tierce.

Configurer un tunnel pour l'utilisation de l'inscription

Comme mentionné précédemment, pour que le client puisse obtenir un certificat, un tunnel sécurisé doit être construit avec l'ASA via une autre méthode d'authentification. Pour ce faire, vous devez configurer un groupe de tunnels qui n'est utilisé que pour la première tentative de connexion lorsqu'une demande de certificat est faite. Voici un instantané de la configuration utilisée, qui définit ce groupe de tunnels (les lignes importantes sont affichées en ***gras-italique***) :

```
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
```

Voici le profil client qui peut être collé dans un fichier Bloc-notes et importé dans l'ASA, ou qui peut être configuré directement avec l'Adaptive Security Device Manager (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>
```

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

```
</AnyConnectProfile>
```

> **Note**: Une url de groupe n'est pas configurée pour ce groupe de tunnels. Ceci est important car le SCEP hérité ne fonctionne pas avec l'URL. Vous devez sélectionner le groupe de tunnels avec son alias. Ceci est dû au bogue Cisco ID CSCtq74054. Si vous rencontrez des problèmes à cause de l'url de groupe, vous devrez peut-être suivre ce bogue.

Configurer un tunnel pour l'authentification du certificat utilisateur

Lorsque le certificat d'ID signé est reçu, la connexion avec l'authentification de certificat est possible. Cependant, le groupe de tunnels utilisé pour se connecter n'a pas encore été configuré. Cette configuration est similaire à celle de tout autre profil de connexion. Ce terme est synonyme

de groupe de tunnels et ne doit pas être confondu avec le profil client, qui utilise l'authentification de certificat.

Voici un instantané de la configuration utilisée pour ce tunnel :

```
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
```

Renouveler le certificat utilisateur

Lorsque le certificat utilisateur expire ou est révoqué, Cisco AnyConnect échoue à l'authentification du certificat. La seule option est de se reconnecter au groupe de tunnels d'inscription de certificat afin de déclencher à nouveau l'inscription SCEP.

Vérification

Utilisez les informations fournies dans cette section afin de confirmer que votre configuration fonctionne correctement.

> **Note**: Puisque la méthode SCEP héritée ne doit être mise en oeuvre qu'avec l'utilisation d'appareils mobiles, cette section traite uniquement des clients mobiles.

Complétez ces étapes afin de vérifier votre configuration :

1. Lorsque vous tentez de vous connecter pour la première fois, saisissez le nom d'hôte ou l'adresse IP ASA.

2. Sélectionnez **certenroll**, ou l'alias de groupe que vous avez configuré dans la section Configurer un tunnel pour l'utilisation de l'inscription de ce document. Vous êtes ensuite invité à saisir un nom d'utilisateur et un mot de passe, et le bouton **obtenir le certificat**

s'affiche.

3. Cliquez sur le bouton **Obtenir le certificat**.

Si vous vérifiez les journaux de vos clients, cette sortie doit afficher :

```
[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]
```

Même si le dernier message affiche **une erreur**, il suffit d'informer l'utilisateur que cette étape est nécessaire pour que ce client soit utilisé pour la prochaine tentative de connexion, qui se trouve dans le deuxième profil de connexion configuré dans la section Configurer un tunnel pour l'authentification de certificat utilisateur de ce document.

Informations connexes

- CSCtq74054 SCEP n'est pas lancé lors de l'utilisation d'une URL (alias asa-IP/tunnel-group)
- Documentation et assistance techniques