Legs SCEP avec l'utilisation de l'exemple de configuration CLI

Contenu

Introduction

Ce document décrit l'utilisation de l'inscription de certificat simple existante Protocol (SCEP) sur l'appliance de sécurité adaptable Cisco (ASA).

> **Attention** : En date de la version 3.0 de Cisco AnyConnect, cette méthode ne devrait pas être utilisée. Il était précédemment nécessaire parce que les périphériques mobiles n'ont pas eu le client 3.x, mais Android et les iPhones ont maintenant le soutien du proxy SCEP, qui devrait être utilisé à la place. Seulement dans les cas où il n'est pas pris en charge en raison de l'ASA si vous configurez le legs SCEP. Cependant, même dans des ces cas, une mise à jour ASA est l'option recommandée.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance du legs SCEP.

Composants utilisés

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

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

Le SCEP est un protocole qui est conçu afin de faire la distribution et la révocation des Certificats numériques aussi extensibles comme possible. L'idée est que n'importe quel utilisateur du réseau standard devrait pouvoir demander un certificat numérique électroniquement avec l'intervention très petite des administrateurs réseau. Pour les déploiements VPN qui exigent l'authentification de certificat avec l'entreprise, l'Autorité de certification (CA), ou n'importe quelle tierce partie CA qui prend en charge SCEP, les utilisateurs peuvent maintenant demander pour les Certificats signés des machines cliente sans implication des administrateurs réseau.

> Remarque: Si vous désirez configurer l'ASA en tant que serveur CA, alors SCEP n'est pas la méthode appropriée de protocole. Référez-vous à la section des gens du pays CA du document Cisco **configurant de Certificats numériques** à la place.

En date de la version 8.3 ASA, il y a deux méthodes prises en charge pour SCEP :

- La méthode plus ancienne, appelée Legacy SCEP, est discutée dans ce document.
- La méthode de proxy SCEP est la plus nouvelle des deux méthodes, où les proxys ASA la demande d'inscription de certificat au nom du client. Ce processus est plus propre parce qu'il n'exige pas un groupe supplémentaire de tunnel et est également plus sécurisé. Cependant, l'inconvénient est que les travaux de proxy SCEP seulement avec le Cisco AnyConnect libèrent 3.x. Ceci signifie que la version du client en cours d'AnyConnect pour des périphériques mobiles ne prend en charge pas le proxy SCEP.

Configurez

Cette section fournit les informations que vous pouvez employer afin de configurer la méthode de protocole du legs SCEP.

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

Voici quelques informations importantes à maintenir dans l'esprit quand le legs SCEP est utilisé :

- Après que le client reçoive le certificat signé, l'ASA devrait identifier le CA qui a signé le certificat avant qu'il puisse authentifier le client. Par conséquent, vous devez s'assurer que l'ASA s'inscrit également avec le serveur CA. Le procédé d'inscription pour l'ASA devrait être la première étape parce qu'il assure cela :

Le CA est configuré correctement et peut délivrer des Certificats par l'intermédiaire de SCEP si vous utilisez la méthode d'inscription URL.

L'ASA peut communiquer avec le CA. Par conséquent, si le client ne peut pas, puis il y a une question entre le client et l'ASA.

- Quand la première tentative de connexion est faite, il n'y aura pas un certificat signé. Il doit y avoir une autre option qui peut être utilisée afin d'authentifier le client.

- Dans le procédé d'inscription de certificat, l'ASA ne sert aucun rôle. Il sert seulement d'agrégateur VPN de sorte que le client puisse construire un tunnel afin d'obtenir sécurisé le certificat signé. Quand le tunnel est établi, le client doit pouvoir atteindre le serveur CA. Autrement, il n'est pas de pouvoir s'inscrire.

Inscrivez-vous l'ASA

Le procédé d'inscription ASA est relativement facile et n'exige pas n'importe quelles nouvelles informations. Référez-vous à s'inscrire Cisco ASA à un CA utilisant le document SCEP pour plus d'informations sur la façon s'inscrire l'ASA à une tierce partie CA.

Configurez un tunnel pour l'usage d'inscription

Comme mentionné précédemment, pour que le client puissiez obtienne un certificat, un tunnel sécurisé doit être construit avec l'ASA par une différente méthode de l'authentification. Afin de faire ceci, vous devez configurer un groupe de tunnels qui est seulement utilisé pour la première tentative de connexion quand une demande de certificat est faite. Voici un instantané de la configuration qui est utilisée, qui définit ce groupe de tunnels (les importantes lignes sont affichées en ***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 <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
```

Voici le profil de client qui peut ou être collé dans un fichier de Notepad et être importé à l'ASA, ou elle peut être configurée avec Adaptive Security Device Manager (ASDM) directement :

```
<?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>
```

Remarque: Un groupe-URL n'est pas configuré pour ce groupe de tunnels. C'est important

parce que le legs SCEP ne fonctionne pas avec l'URL. Vous devez sélectionner le groupe de tunnels avec le son alias. C'est en raison de l'ID de bogue Cisco CSCtq74054. Si vous éprouvez des questions en raison du groupe-URL, vous pourriez devoir continuer sur cette bogue.

Configurez un tunnel pour l'authentification de certificat utilisateur

Quand le certificat signé d'ID est reçu, la connexion avec l'authentification de certificat est possible. Cependant, le groupe de tunnels réel qui est utilisé afin de se connecter n'a pas été encore configuré. Cette configuration est semblable à la configuration pour n'importe quel autre connexion-profil. Ce terme est synonyme de groupe de tunnels et ne pas être confondu avec le profil de client, qui utilise l'authentification de certificat.

Voici un instantané de la configuration qui est 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
```

Renouvelez le certificat utilisateur

Quand le certificat utilisateur expire ou est retiré, le Cisco AnyConnect échoue l'authentification de certificat. La seule option est de rebrancher au groupe de tunnels d'inscription de certificat afin de déclencher l'inscription SCEP de nouveau.

Vérifiez

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

Remarque: Puisque la méthode du legs SCEP devrait seulement être appliquée avec l'utilisation des périphériques mobiles, des affaires de cette section seulement avec les

clients mobiles.

Terminez-vous ces étapes afin de vérifier votre configuration :

1. Quand vous tentez de se connecter pour la première fois, écrivez l'adresse Internet ou l'adresse IP ASA.

2. **Certenroll** choisi, ou le groupe alias que vous avez configuré dans le configurer un tunnel pour la section d'utilisation d'inscription de ce document. Vous êtes alors incité pour un nom d'utilisateur et mot de passe, et le bouton de **certificat d'obtenir** est affiché.

3. Cliquez sur le bouton de **certificat d'obtenir**.

Si vous vérifiez vos logs de client, cette sortie devrait 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] <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.
```

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

Informations connexes

- CSCtq74054 SCEP n'est pas initié en utilisant un URL (asa-IP/groupe de tunnels alias)
- Soutien technique et documentation