FlexVPN : Accès à distance d'AnyConnect IKEv2 avec l'AnyConnect-EAP

Contenu

Introduction

Ce document fournit une configuration d'échantillon de la façon configurer un headend IOS/IOS-XE pour l'Accès à distance suivre AnyConnect IKEv2 et méthode d'authentification d'AnyConnect-EAP.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Version 3.15 IOS-XE (15.5(2)S) ou plus tard
- Release 15.5(2)T IOS ou plus tard
- Version du client 3.0 d'AnyConnect ou plus tard

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco ASR1002-X exécutant IOS XE 3.15
- Version du client 3.1.8009 d'AnyConnect s'exécutant sur le Windows 7
- Serveur ACS 5.3 de Cisco (facultatif)

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

L'AnyConnect-EAP, également connu sous le nom d'authentification d'agrégat, permet à un serveur de flexible pour authentifier le client d'AnyConnect utilisant la méthode de propriété industrielle d'AnyConnect-EAP de Cisco. À la différence des méthodes de Protocole EAP (Extensible Authentication Protocol) de conformité aux normes telles que la carte symbolique Eap-générique (EAP-GTC), le Message Digest 5 EAP- (EAP-MD5) et ainsi de suite, le serveur de flexible ne fonctionne pas en mode d'intercommunication d'EAP. Toute la transmission d'EAP avec le client se termine sur le serveur de flexible et la clé de session exigée utilisée pour construire la charge utile AUTHENTIQUE est calculée localement par le serveur de flexible. **Le serveur de flexible doit s'authentifier au client utilisant des Certificats selon les exigences du RFC IKEv2.**

L'authentification d'utilisateur local est maintenant prise en charge sur le serveur de flexible et l'authentification à distance est facultative. C'est idéal pour des déploiements à échelle réduite avec moins de nombre d'utilisateurs d'Accès à distance et dans les environnements sans l'accès à une authentification externe, à un serveur d'autorisation, et de comptabilité (AAA). Cependant, pour des déploiements à grande échelle et dans les scénarios où des attributs de par-utilisateur sont désirés il est encore recommandé pour utiliser un AAA externe divisent pour l'authentification et l'autorisation. L'implémentation d'AnyConnect-EAP permet l'utilisation du rayon ou du TACACS pour l'authentification à distance, l'autorisation et la comptabilité.

Configurez

Utilisateurs de authentifier et d'Authorizating utilisant la base de données locale

> Remarque: Afin d'authentifier des utilisateurs contre la base de données locale sur le routeur, l'EAP doit être utilisé. Cependant, afin d'utiliser l'EAP, la méthode d'authentification locale doit être RSA-Sig, ainsi le routeur a besoin d'un certificat approprié installé là-dessus, et ce ne peut pas être un certificat auto-signé.

Configuration d'échantillon qui utilise l'authentification d'utilisateur local, l'autorisation d'utilisateur distant et de groupe et la comptabilité de distant.

Configuration illustrée spécifique d'AnyConnect-EAP en gras

Étape 1. Activez l'AAA, et configurez les listes d'authentification, d'autorisation et de comptabilité (l'aaa attribute list est facultatif) et ajoutez un nom d'utilisateur à la base de données locale :

```
aaa new-model
!
aaa authentication login a-eap-authen-local local
```

```
aaa authorization network a-eap-author-grp local
!
aaa attribute list AAA-attr
attribute type interface-config "ip mtu 1300"
!
username test password cisco12
```

Étape 2. Configurez un point de confiance pour obtenir un certificat d'ID d'un serveur CA (le routeur peut être aussi bien configuré comme CA) :

```
crypto pki trustpoint IKEv2-TP
enrollment mode ra
enrollment url http://X.X.X.X:80/certsrv/mscep/mscep.dll
subject-name CN=vpn.example.com,OU=TAC,L=SanJose,C=US
revocation-check none
rsakeypair rsakey
```

Étape 3. Définissez un ip local pool pour assigner des adresses aux clients vpn d'AnyConnect :

```
ip local pool ACPOOL 192.168.10.5 192.168.10.10
```

Étape 4. Créez une stratégie locale de l'autorisation IKEv2 :

```
crypto ikev2 authorization policy ikev2-auth-policy
pool ACPOOL
aaa attribute list AAA-attr
```

Étape 5. Create a désiré la proposition IKEv2 et la stratégie :

```
crypto ikev2 proposal IKEv2-prop1
encryption aes-cbc-256
integrity sha256
group 2
!
crypto ikev2 policy IKEv2-pol
proposal IKEv2-prop1
```

Étape 6. Créez un profil IKEv2 pour la méthode d'AnyConnect-EAP d'authentification client :

```
crypto ikev2 profile AnyConnect-EAP
match identity remote key-id *$AnyConnectClient$*
authentication remote anyconnect-eap aggregate
authentication local rsa-sig
pki trustpoint IKEv2-TP
aaa authentication anyconnect-eap a-eap-authen-local
aaa authorization group anyconnect-eap list a-eap-author-grp ikev2-auth-policy
aaa authorization user anyconnect-eap cached
virtual-template 100
```

> Remarque: Configurer la méthode d'authentification à distance avant que la méthode d'authentification locale soit reçue par le CLI, mais peut ne pas prendre effet sur des versions de code affectées par CSCva46032. Si vous copiez/pâte la configuration de ce document, assurez s'il vous plaît que la méthode d'authentification à distance en fait l'a pris effet et si elle n'a pas veuillez ressaisissent la commande.

Étape 7. Consultation de certificat basée par URL HTTP de débronchement :

```
crypto ikev2 profile AnyConnect-EAP
match identity remote key-id *$AnyConnectClient$*
authentication remote anyconnect-eap aggregate
authentication local rsa-sig
pki trustpoint IKEv2-TP
aaa authentication anyconnect-eap a-eap-authen-local
aaa authorization group anyconnect-eap list a-eap-author-grp ikev2-auth-policy
```

```
aaa authorization user anyconnect-eap cached
virtual-template 100
```

Étape 8. Définissez le cryptage et les algorithmes de hachage utilisés pour protéger des données

```
crypto ikev2 profile AnyConnect-EAP
match identity remote key-id *$AnyConnectClient$*
authentication remote anyconnect-eap aggregate
authentication local rsa-sig
pki trustpoint IKEv2-TP
aaa authentication anyconnect-eap a-eap-authen-local
aaa authorization group anyconnect-eap list a-eap-author-grp ikev2-auth-policy
aaa authorization user anyconnect-eap cached
virtual-template 100
```

> Remarque: *Référez-vous* ce document pour confirmer si vos supports matériels de routeur les algorithmes de chiffrement NGE (par exemple l'exemple ci-dessus a des algorithmes NGE). Autrement l'installation d'IPSec SA sur le matériel échouera à la dernière étape de la négociation.

Étape 9. Créez un profil IPSec :

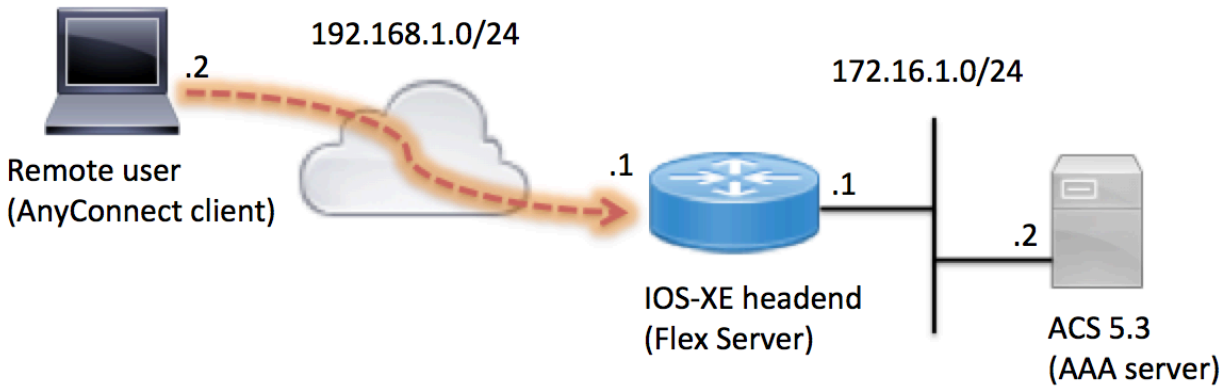
```
crypto ikev2 profile AnyConnect-EAP
match identity remote key-id *$AnyConnectClient$*
authentication remote anyconnect-eap aggregate
authentication local rsa-sig
pki trustpoint IKEv2-TP
aaa authentication anyconnect-eap a-eap-authen-local
aaa authorization group anyconnect-eap list a-eap-author-grp ikev2-auth-policy
aaa authorization user anyconnect-eap cached
virtual-template 100
```

Étape 10. Configurez un virtual-template (associez le modèle dans le profil IKEv2)

```
crypto ikev2 profile AnyConnect-EAP
match identity remote key-id *$AnyConnectClient$*
authentication remote anyconnect-eap aggregate
authentication local rsa-sig
pki trustpoint IKEv2-TP
aaa authentication anyconnect-eap a-eap-authen-local
aaa authorization group anyconnect-eap list a-eap-author-grp ikev2-auth-policy
aaa authorization user anyconnect-eap cached
virtual-template 100
```

Authentification, autorisation et comptabilité utilisant un serveur distant d'AAA

Diagramme du réseau



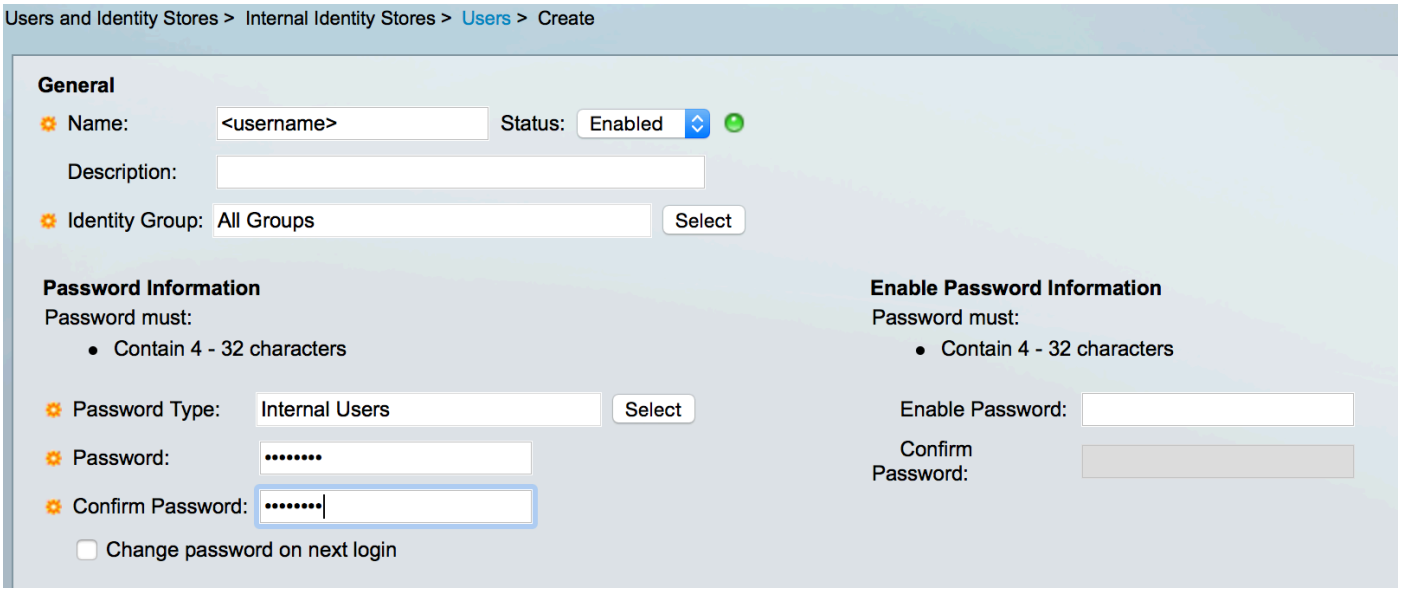
Modifications de configuration de Headend

Remarque: Référez-vous à la section ci-dessus pour le reste de la configuration.

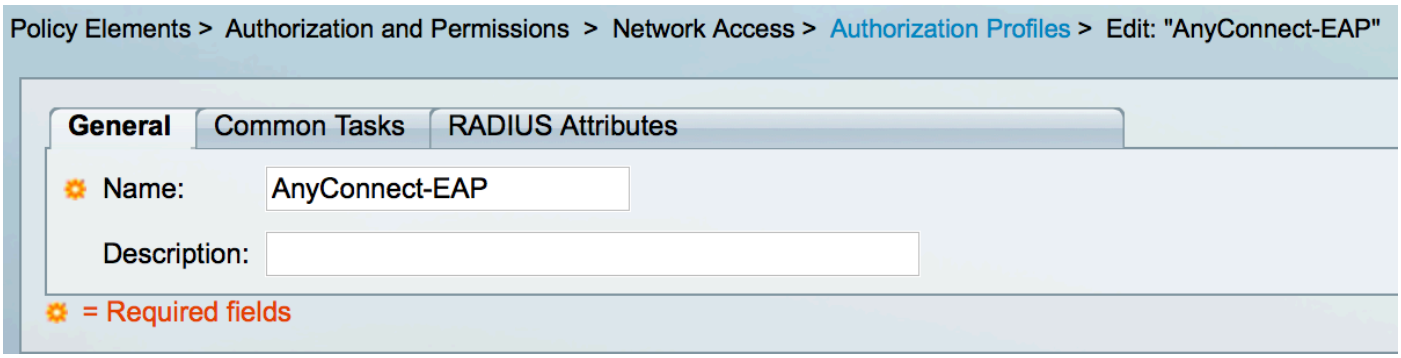
```
aaa group server radius ACS
server name ACS
!
radius server ACS
address ipv4 172.16.1.2 auth-port 1645 acct-port 1646
key Cisco123!
!
aaa authentication login a-eap-authen group ACS
aaa authorization network a-eap-author group ACS
aaa accounting network a-eap-acc start-stop group ACS
!
crypto ikev2 name-mangler NM
eap suffix delimiter @
!
crypto ikev2 profile AnyConnect-EAP
aaa authentication anyconnect-eap a-eap-authen
aaa authorization group anyconnect-eap list a-eap-author <aaa-username>
aaa authorization user anyconnect-eap list a-eap-author name-mangler NM
aaa accounting anyconnect-eap a-eap-acc
```

Configuration du serveur RADIUS

Étape 1. Créez un nom d'utilisateur (pour l'utilisateur et/ou groupez l'authentification et l'autorisation), suivant les indications de l'image :



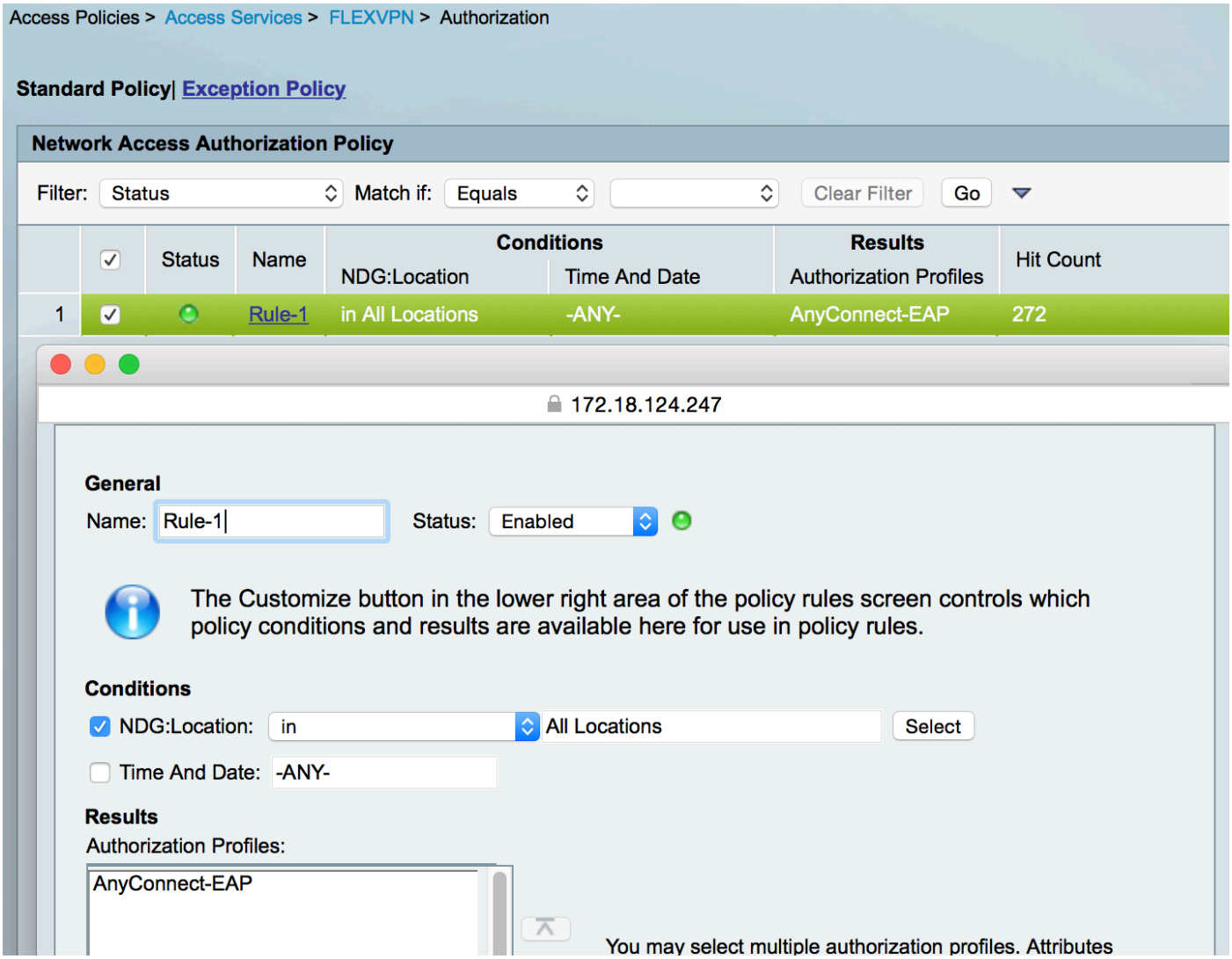
Étape 2. Configurez la stratégie d'autorisation, suivant les indications de l'image :



Étape 3. Ajoutez maintenant les attributs RADIUS, suivant les indications de l'image :

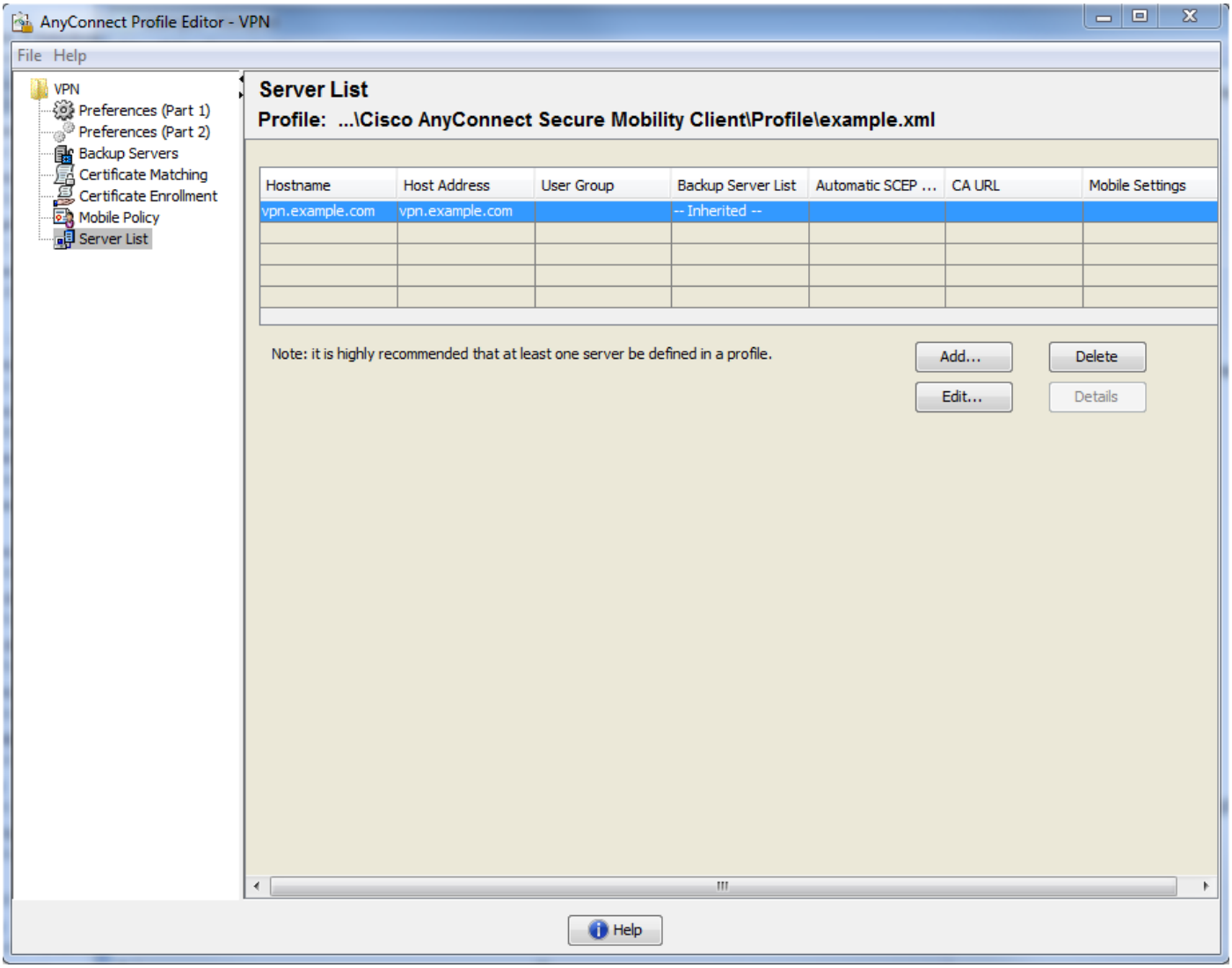
Attribute	Type	Value
cisco-av-pair	String	ipsec:default-domain=ciscotac.com
cisco-av-pair	String	ipsec:banner=AnyConnect
cisco-av-pair	String	ipsec:addr-pool=ACPOOL
cisco-av-pair	String	ipsec:route-set=prefix 172.16.1.0/24
cisco-av-pair	String	ipsec:route-set=access-list split-acl

Étape 4. Suivant les indications de l'image, créez la stratégie d'autorisation de stratégie d'Access et d'associé.



Configuration de profil de client d'AnyConnect

Configurez le profil de client utilisant l'éditeur de profil d'AnyConnect suivant les indications de l'image :



L'équivalent XML du profil :

```
<?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">true</AutomaticCertSelection>
<ShowPreConnectMessage>false</ShowPreConnectMessage>
<CertificateStore>All</CertificateStore>
<CertificateStoreOverride>false</CertificateStoreOverride>
<ProxySettings>Native</ProxySettings>
<AllowLocalProxyConnections>false</AllowLocalProxyConnections>
<AuthenticationTimeout>12</AuthenticationTimeout>
<AutoConnectOnStart UserControllable="true">false</AutoConnectOnStart>
<MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
<LocalLanAccess UserControllable="true">false</LocalLanAccess>
<ClearSmartcardPin UserControllable="true">true</ClearSmartcardPin>
<IPProtocolSupport>IPv4,IPv6</IPProtocolSupport>
<AutoReconnect UserControllable="false">true
<AutoReconnectBehavior UserControllable="false">ReconnectAfterResume</AutoReconnectBehavior>
</AutoReconnect>
<AutoUpdate UserControllable="false">false</AutoUpdate>
<RSASecurIDIntegration UserControllable="false">Automatic</RSASecurIDIntegration>
<WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
<WindowsVPNEstablishment>AllowRemoteUsers</WindowsVPNEstablishment>
<AutomaticVPNPolicy>false</AutomaticVPNPolicy>
```

```
<PPPExclusion UserControllable="false">Automatic
<PPPExclusionServerIP UserControllable="false"></PPPExclusionServerIP>
</PPPExclusion>
<EnableScripting UserControllable="false">false</EnableScripting>
<EnableAutomaticServerSelection UserControllable="true">false
<AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
<AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
</EnableAutomaticServerSelection>
<RetainVpnOnLogoff>false
</RetainVpnOnLogoff>
<AllowManualHostInput>true</AllowManualHostInput>
</ClientInitialization>
<ServerList>
<HostEntry>
<HostName>vpn.example.com</HostName>
<HostAddress>vpn.example.com</HostAddress>
 <PrimaryProtocol>IPsec</PrimaryProtocol>
</HostEntry>
</ServerList>
</AnyConnectProfile>
```

> Remarque: AnyConnect utilise « *$AnyConnectClient$* » en tant que son identité par défaut d'IKE de clé-id de type. Cependant, cette identité peut être manuellement changée dans le profil d'AnyConnect pour apparier les besoins de déploiement. StandardAuthenticationOnly devrait être placé à faux en utilisant l'AnyConnect-EAP suivant les indications de l'image.

Changez l'identity(Optional) par défaut d'IKE d'AnyConnect

Si vous ne voulez pas utiliser l'id par défaut d'IKE utilisé par le client, vous pouvez changer l'id d'IKE dans le profil de client, toutefois il a également exigé de l'id d'IKE d'être changé sous le profil ikev2 configuré sur le serveur de Flexvpn.

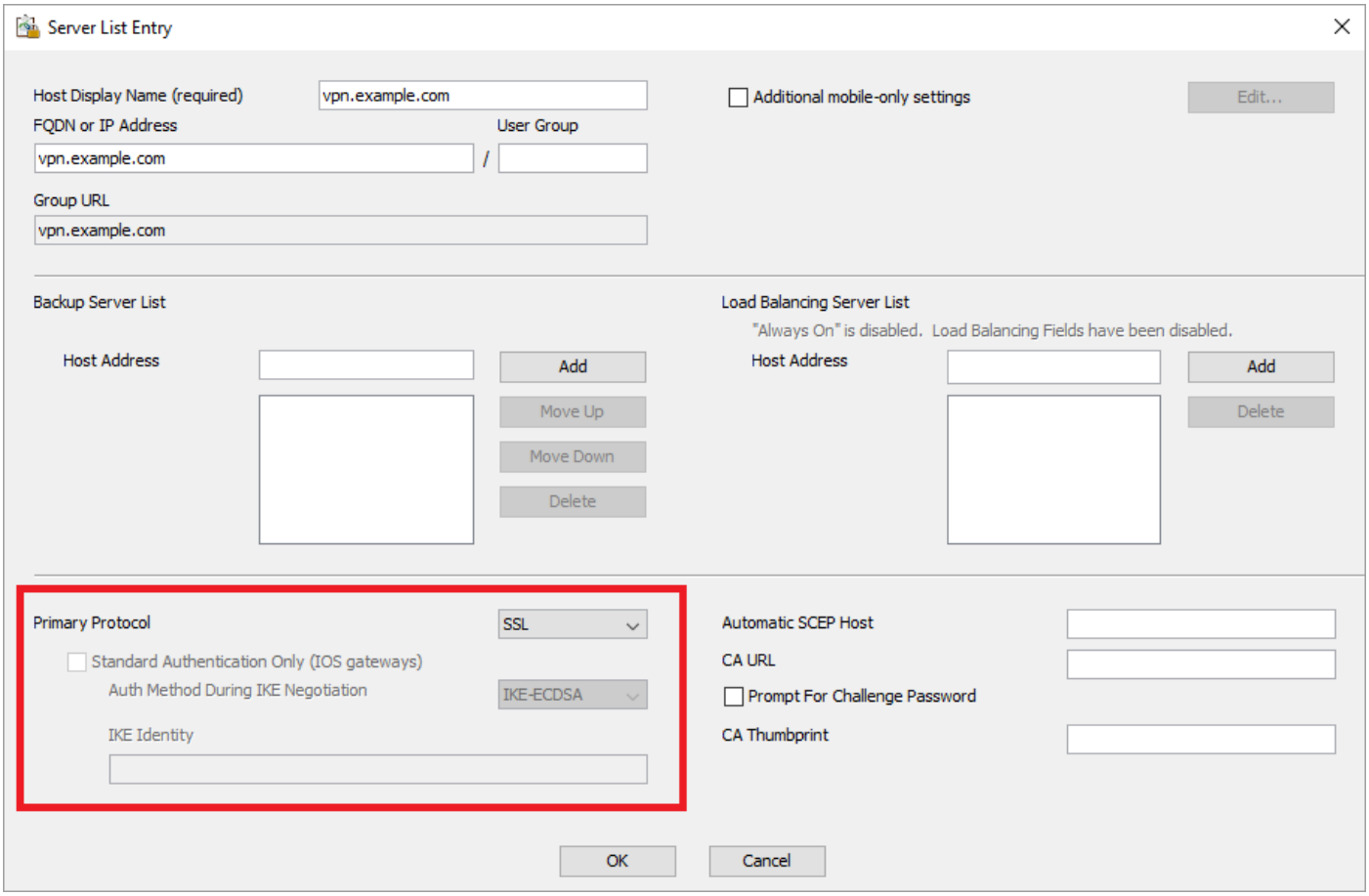
Profil de client :

```
 <ServerList>
<HostEntry>
<HostName>vpn.example.com</HostName>
<HostAddress>vpn.example.com</HostAddress>
<PrimaryProtocol>IPsec
<StandardAuthenticationOnly>false
     <IKEIdentity>ANYCONNECT-IKEID</IKEIdentity>
</StandardAuthenticationOnly>
</PrimaryProtocol>
</HostEntry>
</ServerList>
```

Configuration de FlexServer :

```
crypto ikev2 profile AnyConnect-EAP
match identity remote key-id ANYCONNECT-IKEID
```

Ceci peut également être placé utilisant l'éditeur de profil de client :



Conseil : En utilisant l'éditeur de profil de client, l'ID d'IKE peut seulement être changé si l'authentification standard est vérifiée. C'est un problème connu et la bogue CSCva64390 a été classée pour aborder cette question. Entre-temps vous pouvez manuellement éditer le fichier de xml utilisant n'importe quel éditeur de texte de sorte que la valeur pour l'attribut « StandardAuthenticationOnly » soit placée à faux.

Contournement Downloader(Optional)

Actuellement, la caractéristique qui permet au client d'Anyconnect pour télécharger la version mise à jour du client de la passerelle n'est pas prise en charge sur des Routeurs IOS-XE. Ainsi si la version du client étant utilisée pour se connecter à la passerelle est inférieure que la version configurée sur la passerelle ceci aura comme conséquence la connexion une panne. Afin de le désactiver, un changement du fichier de stratégie local sur la machine cliente est nécessaire. Le pour en savoir plus comprenant l'emplacement du fichier de stratégie local se rapportent s'il vous plaît à des paramètres locaux de stratégie de modification manuellement.

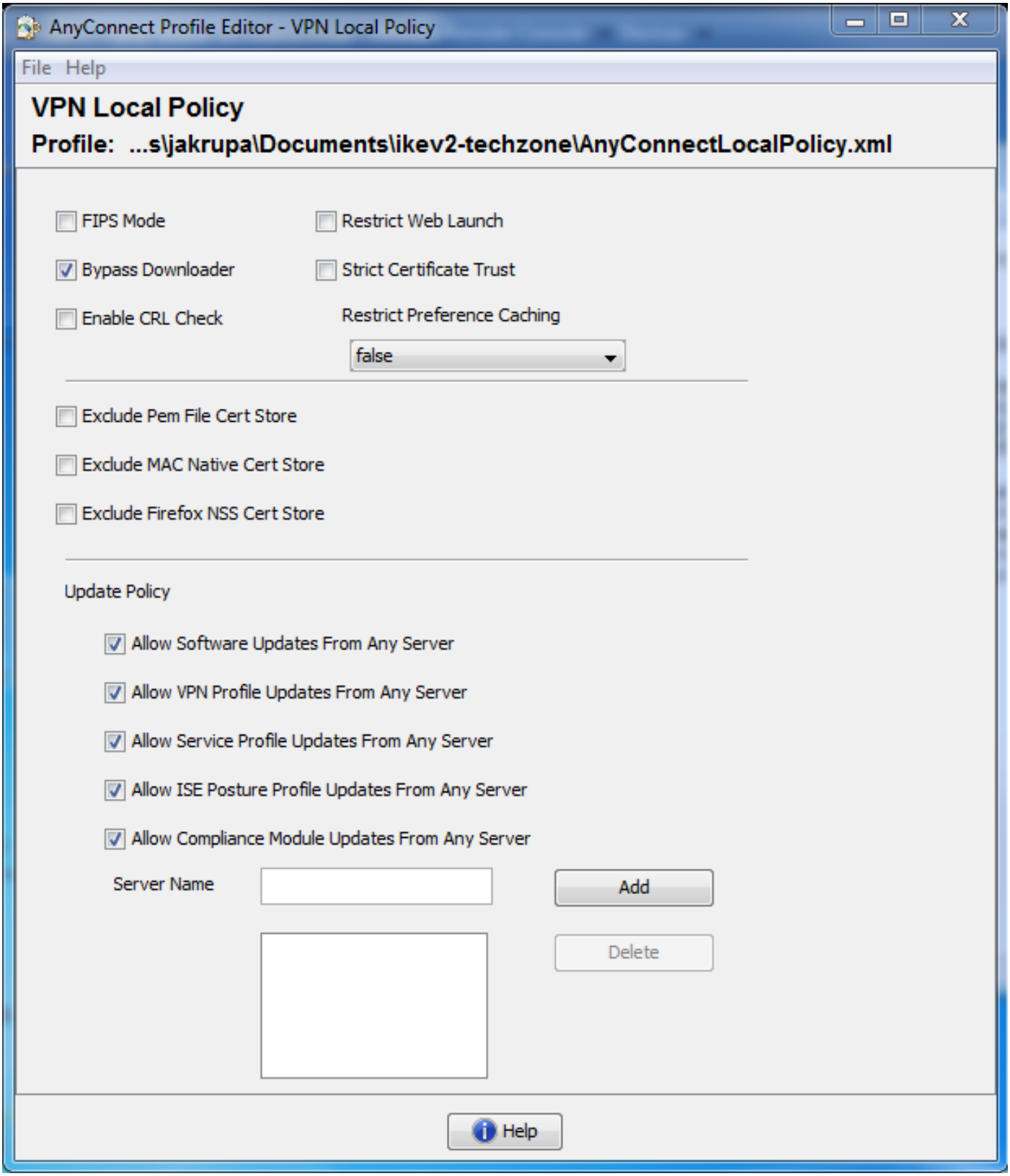
Valeur de **BypassDownloader de** modification à rectifier.

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectLocalPolicy xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectLocalPolicy.xsd"
acversion="3.0.0592">
   <FipsMode>false</FipsMode>
   <BypassDownloader>true</BypassDownloader>
   <RestrictWebLaunch>false</RestrictWebLaunch>
   <StrictCertificateTrust>false</StrictCertificateTrust>
   <EnableCRLCheck>false</EnableCRLCheck>
   <RestrictPreferenceCaching>false</RestrictPreferenceCaching>
```

```
   <ExcludePemFileCertStore>false</ExcludePemFileCertStore>
   <ExcludeMacNativeCertStore>false</ExcludeMacNativeCertStore>
   <ExcludeFirefoxNSSCertStore>false</ExcludeFirefoxNSSCertStore>
   <UpdatePolicy>
       <AllowSoftwareUpdatesFromAnyServer>true</AllowSoftwareUpdatesFromAnyServer>
       <AllowVPNProfileUpdatesFromAnyServer>true</AllowVPNProfileUpdatesFromAnyServer>
       <AllowServiceProfileUpdatesFromAnyServer>true</AllowServiceProfileUpdatesFromAnyServer>
       <AllowISEProfileUpdatesFromAnyServer>true</AllowISEProfileUpdatesFromAnyServer>

 <AllowComplianceModuleUpdatesFromAnyServer>true</AllowComplianceModuleUpdatesFromAnyServer>
   </UpdatePolicy>
</AnyConnectLocalPolicy>
```

Il peut être fait en éditant manuellement du fichier ou à l'aide de l'outil d'éditeur de profil d'AnyConnect :



Écoulement de transmission

Échange IKEv2 et d'EAP