FlexVPN: Acceso Remoto de AnyConnect IKEv2 con el AnyConnect-EAP

Contenido

Introducción

Este documento proporciona una configuración de muestra de cómo configurar un headend IOS/IOS-XE para el Acceso Remoto usando el método de autentificación IKEv2 y AnyConnect-EAP de AnyConnect.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Versión 3.15 (15.5(2)S) IOS-XE o más adelante
- Versión del IOS 15.5(2)T o más adelante
- 3.0 de la versión de cliente de AnyConnect o más adelante

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco ASR1002-X que ejecuta IOS XE 3.15
- Versión de cliente 3.1.8009 de AnyConnect que se ejecuta en Windows 7
- Servidor ACS de Cisco 5.3 (opcional)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

El AnyConnect-EAP, también conocido como autenticación global, permite que un servidor de la flexión autentique al cliente de AnyConnect que usa el método propietario AnyConnect-EAP de Cisco. Los métodos basados a diferencia del estándar del Protocolo de Autenticación Extensible (EAP) tales como placa Token EAP-genérica (EAP-GTC), la publicación de mensaje EAP 5 (EAP-MD5) y así sucesivamente, el servidor de la flexión no actúan en el modo de transferencia EAP. Toda la comunicación EAP con el cliente termina en el servidor de la flexión y la clave de la sesión requerida usada para construir el payload AUTH es computada localmente por el servidor de la flexión. **El servidor de la flexión tiene que autenticarse al cliente que usa los Certificados de acuerdo con del IKEv2 RFC.**

La autenticación de usuario local ahora se soporta en el servidor de la flexión y la autenticación remota es opcional. Esto es ideal para las implementaciones de la pequeña escala con menos número de usuarios de acceso remoto y en los entornos sin el acceso a una autenticación externa, a un servidor de la autorización, y de las estadísticas (AAA). Sin embargo, para los despliegues a grandes escala y en los escenarios donde se desean los atributos de usuario todavía se recomienda para utilizar un externo AAA separa para la autenticación y autorización. La implementación AnyConnect-EAP permite el uso del radius or tacacs para la autenticación remota, la autorización y las estadísticas.

Configurar

Usuarios de la autenticidad y de Authorizating que usan la base de datos local

> Nota: Para autenticar a los usuarios contra la base de datos local en el router, el EAP necesita ser utilizado. Sin embargo, para utilizar el EAP, el método de autenticación local tiene que ser RSA-SIG, así que el router necesita un certificado apropiado instalado en él, y no puede ser un certificado autofirmado.

Configuración de muestra que utiliza la autenticación de usuario local, autorización del usuario remoto y del grupo y las estadísticas del telecontrol.

Configuración específica AnyConnect-EAP mostrada en intrépido

Paso 1. Habilite el AAA, y configure las listas de la autenticación, de la autorización y de las estadísticas (la lista de atribución aaa es opcional) y agregue un nombre de usuario a la base de datos local:

```
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
```

Paso 2. Configure un trustpoint para obtener un certificado ID de un servidor de CA (el router puede ser configurado como CA también):

```
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
```

Paso 3. Defina a una agrupación local IP para asignar los direccionamientos a los clientes VPN de AnyConnect:

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

Paso 4. Cree una directiva de la autorización local IKEv2:

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

Paso 5. Create deseó la oferta IKEv2 y la directiva:

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

Paso 6. Cree un perfil IKEv2 para el método AnyConnect-EAP de autenticación de cliente:

```
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
```

> Nota: Configurar el método de autenticación remota antes de que el método de autenticación local sea validado por el CLI, pero puede no tomar el efecto sobre las versiones del código afectadas por CSCva46032. Si usted copia/goma la configuración de este documento, asegúrese por favor que el método de autenticación remota de hecho haya tomado el efecto y si no tiene satisfaga entran el comando de nuevo.

Paso 7. La neutralización HTTP URL basó las operaciones de búsqueda del certificado:

```
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
```

Paso 8. Defina el cifrado y los algoritmos de troceo usados para proteger los datos

```
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
```

> Nota: *Refiera* este documento para confirmar si su hardware de router soporta los algoritmos de encripción NGE (por ejemplo el ejemplo anterior tiene algoritmos NGE). Si no la instalación IPSec SA en el hardware fallará en la etapa más reciente de la negociación.

Paso 9. Cree un perfil de ipsec:

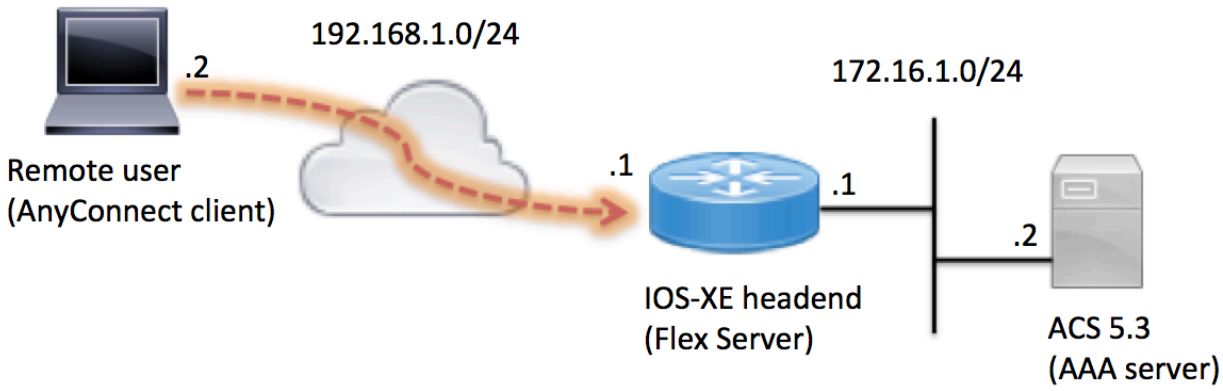
```
crypto ikev2 profile AnyConnect-EAP
match identity remote key-id *$AnyConnectClient$*
authentication remote anyconnect-eap aggregate
authentication local rsa-sig
pki trustpoint IKEv2-TP
aaa authentication anyconnect-eap a-eap-authen-local
aaa authorization group anyconnect-eap list a-eap-author-grp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

Paso 10. Configure una virtual-plantilla (asocie la plantilla en el perfil 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
```

Autenticación, autorización y estadísticas usando un servidor de AAA remoto

Diagrama de la red



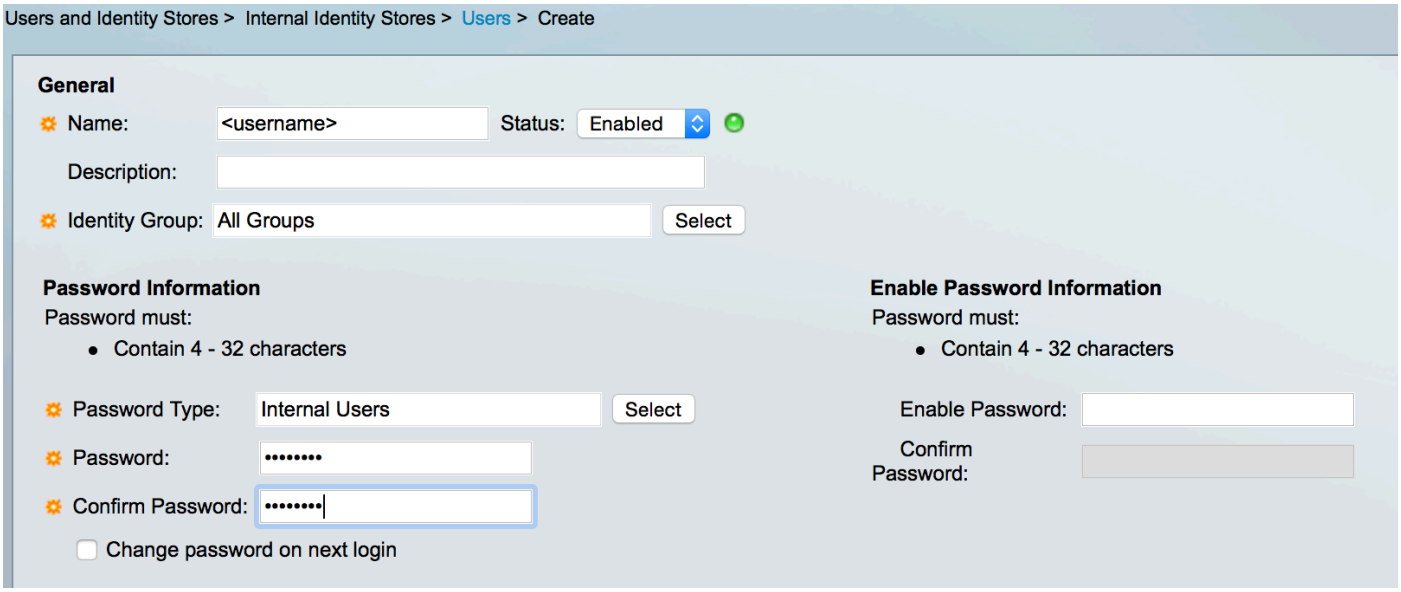
Cambios de configuración del headend

Nota: Refiera a la sección antedicha para el resto de la configuración.

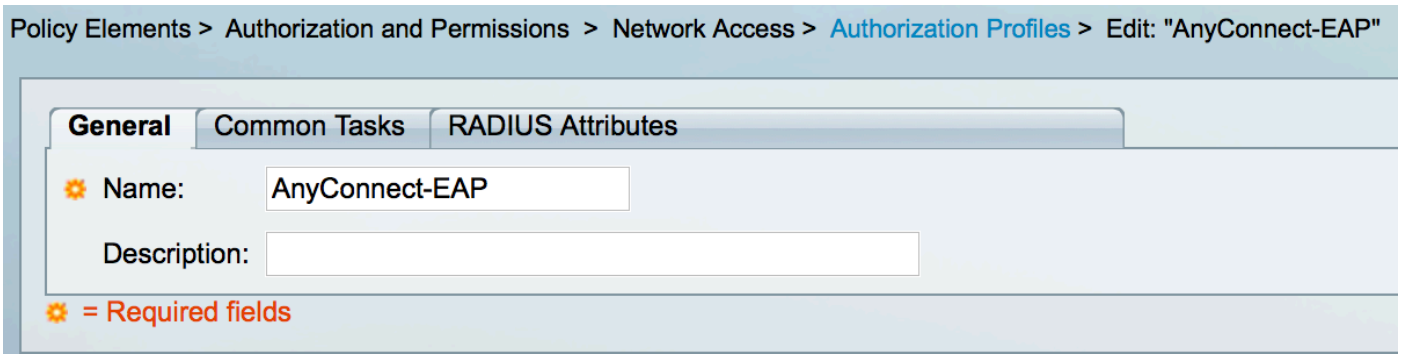
```
aaa group server radius ACS
server name ACS
!
radius server ACS
address ipv4 172.16.1.2 auth-port 1645 acct-port 1646
key Cisco123!
!
aaa authentication login a-eap-authen group ACS
aaa authorization network a-eap-author group ACS
aaa accounting network a-eap-acc start-stop group ACS
!
crypto ikev2 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
```

Configuración de servidor de RADIUS

Paso 1. Cree un nombre de usuario (para la autenticación y autorización del usuario y/o del grupo), tal y como se muestra en de la imagen:



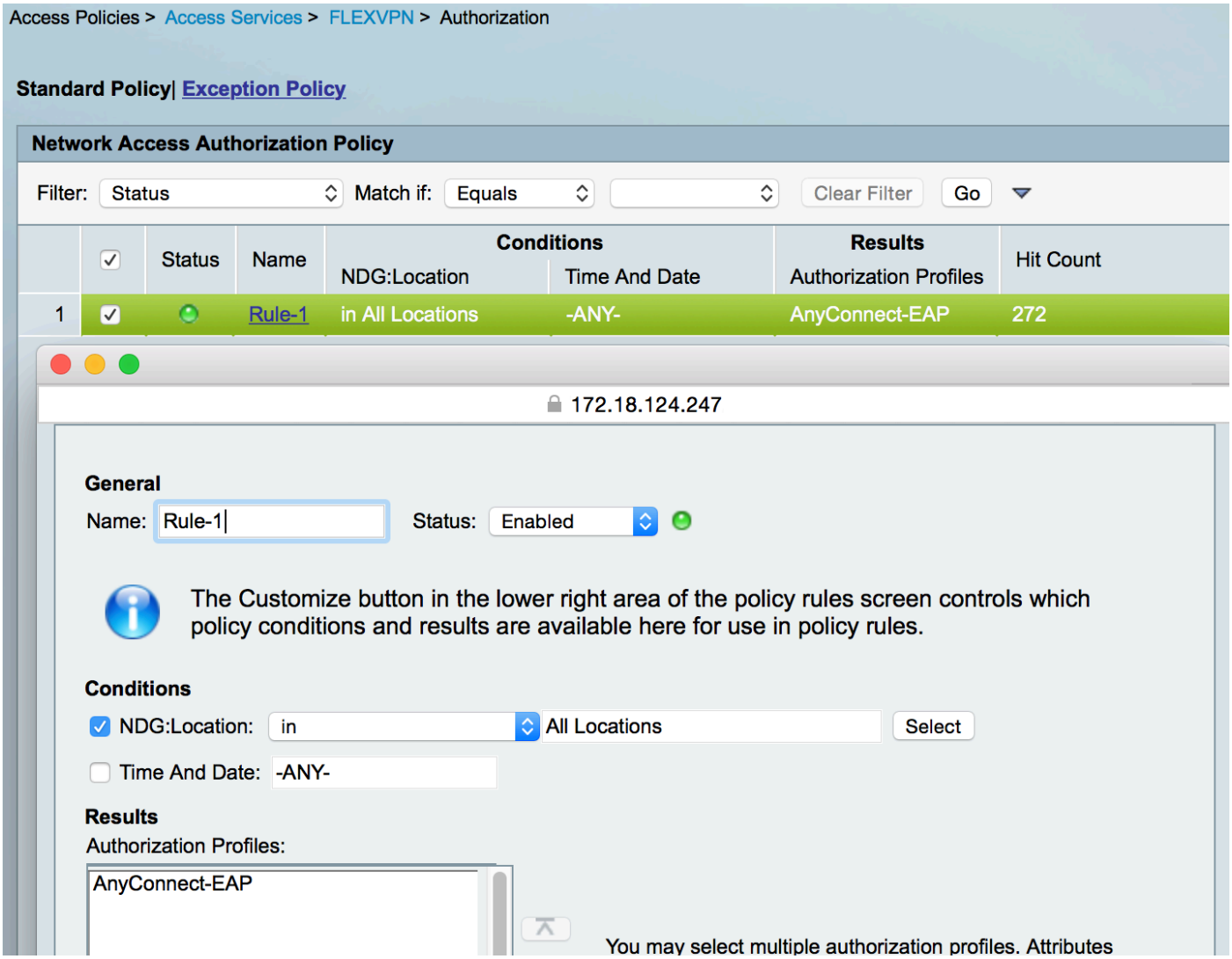
Paso 2. Directiva de la autorización de la configuración, tal y como se muestra en de la imagen:



Paso 3. Ahora agregue los atributos de RADIUS, tal y como se muestra en de la imagen:

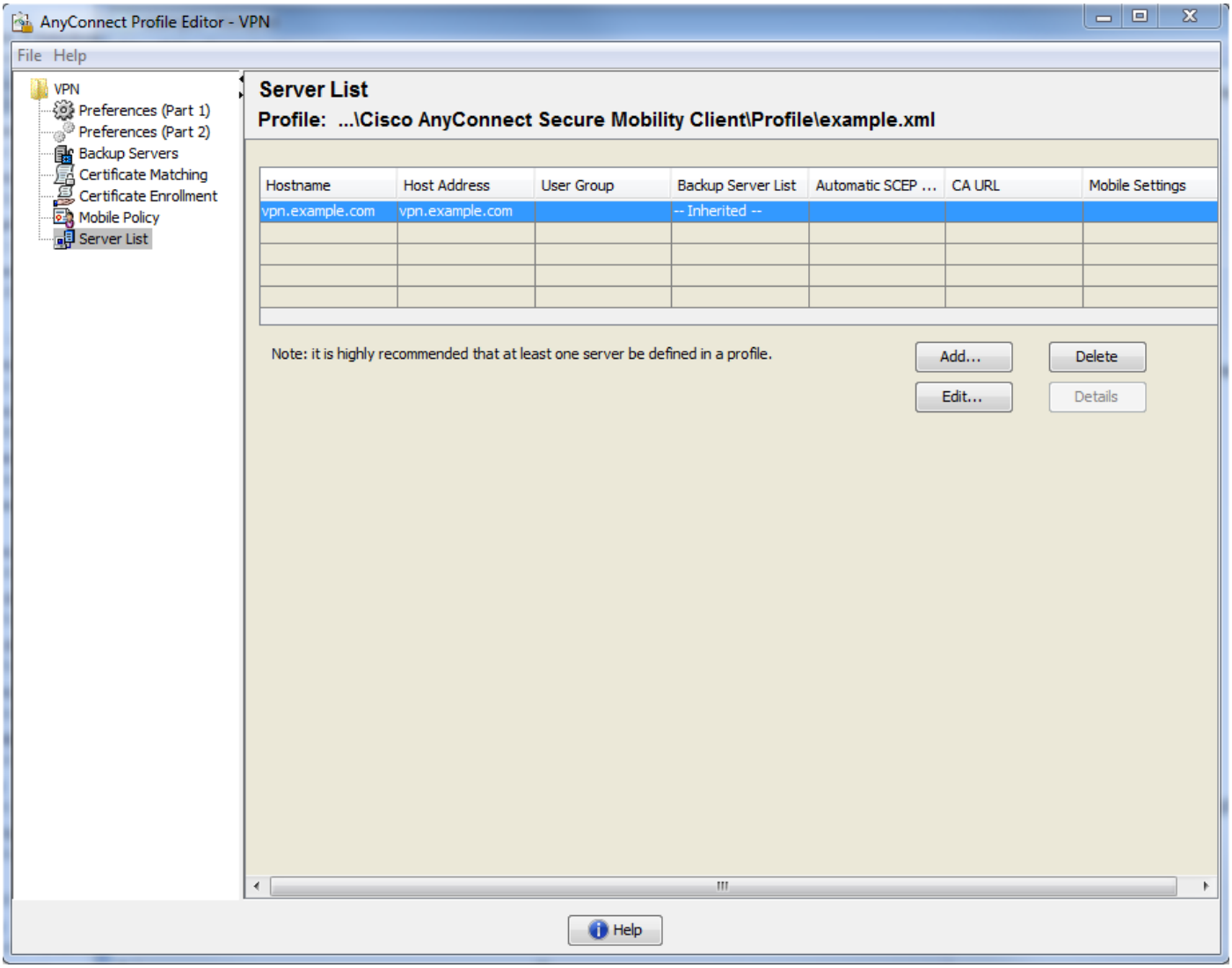
Attribute	Type	Value
cisco-av-pair	String	ipsec:default-domain=ciscotac.com
cisco-av-pair	String	ipsec:banner=AnyConnect
cisco-av-pair	String	ipsec:addr-pool=ACPOOL
cisco-av-pair	String	ipsec:route-set=prefix 172.16.1.0/24
cisco-av-pair	String	ipsec:route-set=access-list split-acl

Paso 4. Tal y como se muestra en de la imagen, cree la directiva de la autorización de la política de acceso y del socio.



Configuración del perfil del cliente de AnyConnect

Configure el perfil del cliente usando el editor del perfil de AnyConnect tal y como se muestra en de la imagen:



El equivalente XML del perfil:

```
<?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>
```

> Nota: AnyConnect utiliza “*$AnyConnectClient$*” como su identidad del valor por defecto IKE de la clave-identificación del tipo. Sin embargo, esta identidad se puede cambiar manualmente en el perfil de AnyConnect para hacer juego las necesidades del despliegue. **StandardAuthenticationOnly** se debe fijar a falso al usar el AnyConnect-EAP tal y como se muestra en de la imagen.

Cambie el identity(Optional) predeterminado de AnyConnect IKE

Si usted no quiere utilizar la identificación predeterminada del ike usada por el cliente, usted puede cambiar la identificación del ike en el perfil del cliente, no obstante también requirió la identificación del ike ser cambiado bajo perfil ikev2 configurado en el servidor de Flexvpn.

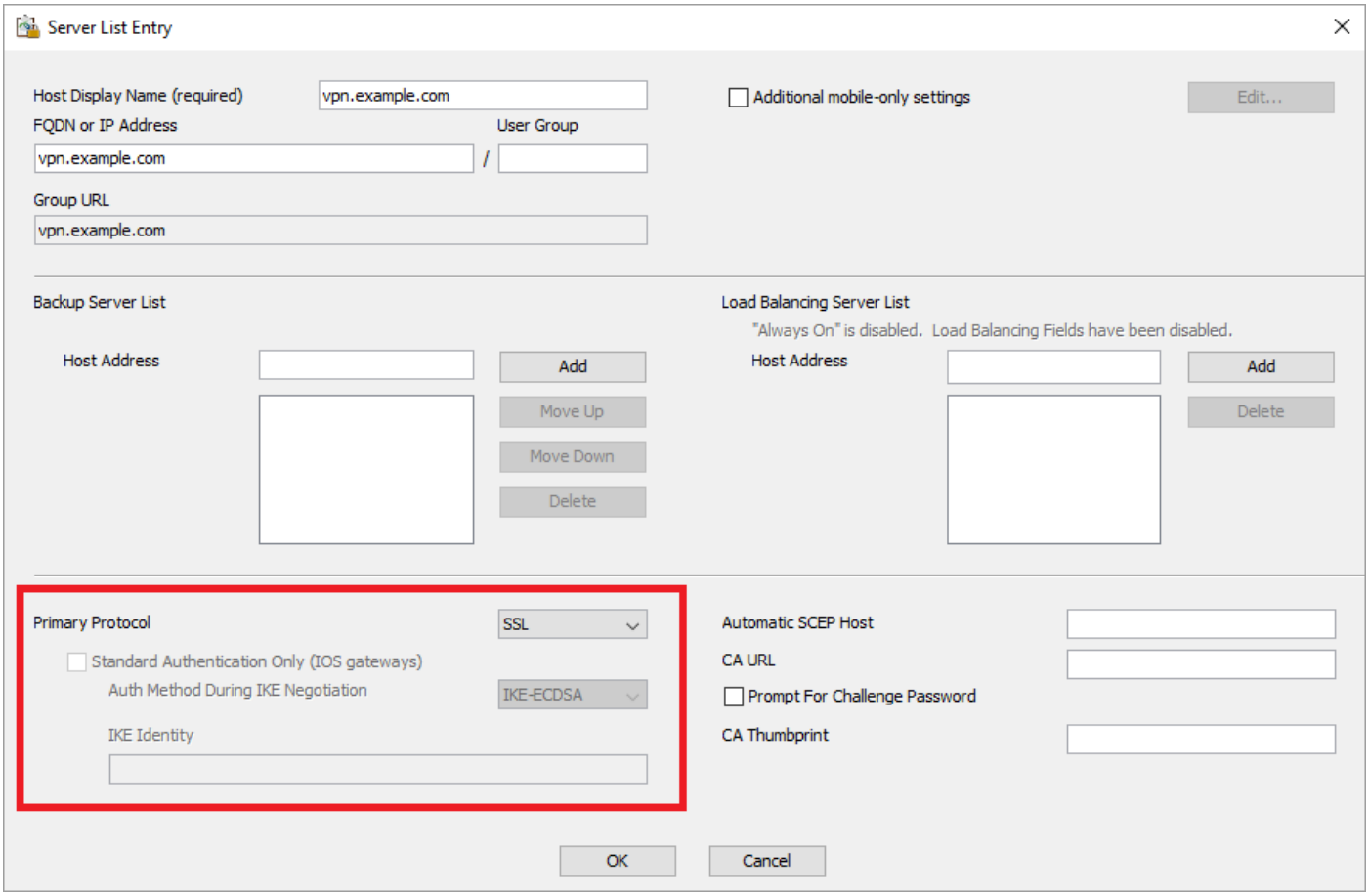
Perfil del cliente:

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

Configuración de FlexServer:

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

Esto se puede también fijar usando el editor del perfil del cliente:



> Consejo: Al usar el editor del perfil del cliente, el ike ID puede ser cambiado solamente si se marca la autenticación estándar. Esto es un problema conocido y el bug CSCva64390 se ha clasifiado para abordar este problema. Usted puede editar mientras tanto manualmente el archivo del xml usando cualquier editor de textos para fijar el valor para el atributo “StandardAuthenticationOnly” a falso.

Puente Downloader(Optional)

Actualmente, la característica que permite que el cliente de Anyconnect descargue la versión actualizada del cliente del gateway no se soporta en el Routers IOS-XE. Tan si la versión de cliente que es utilizada para conectar con el gateway es más baja que la versión configurada en el gateway esto dará lugar a la conexión un error. Para inhabilitarlo, un cambio en el archivo de la política local en la máquina del cliente es necesario. Para más información incluyendo la ubicación del archivo de la política local refiera por favor a los parámetros de la política local del cambio manualmente.

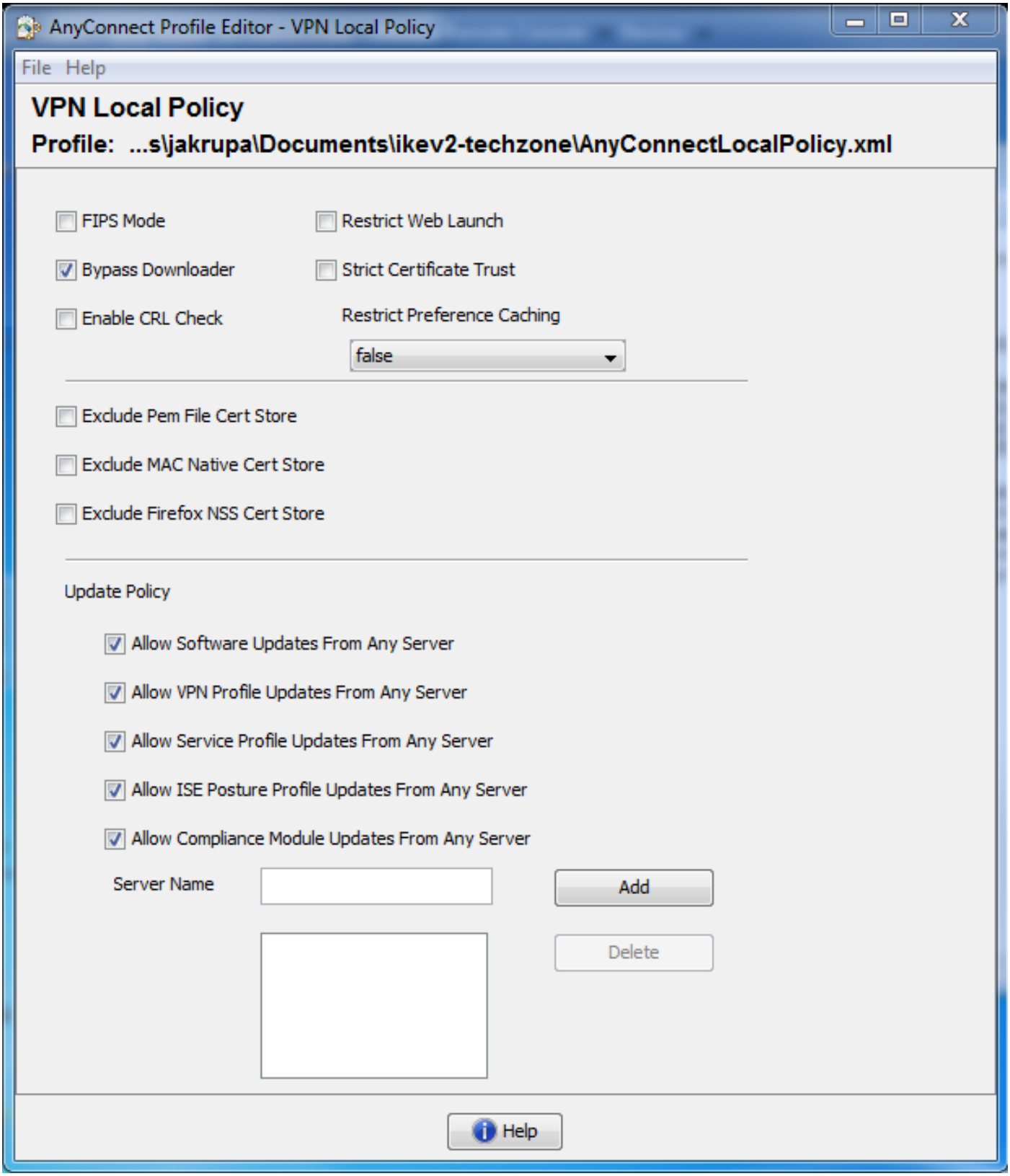
Cambie el valor de **BypassDownloader** para verdad.

```
<?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>
```

Puede ser hecho con manualmente editar del archivo o usando la herramienta del editor del perfil de AnyConnect:



Flujo de la comunicación

Intercambio IKEv2 y EAP