Configuración de FlexVPN: acceso remoto IKEv2 de AnyConnect con base de datos de usuarios locales

Contenido

Introducción

Este documento describe cómo configurar una cabecera Cisco IOS®/ XE para el acceso a través de la autenticación AnyConnect IKEv2 / EAP con la base de datos de usuario local.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- protocolo IKEv2

Componentes Utilizados

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

- Router de servicios en la nube de Cisco con Cisco IOS® XE 16.9.2
- Cliente AnyConnect versión 4.6.03049 que se ejecuta en Windows 10

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

AnyConnect-EAP, también conocido como autenticación agregada, permite que un servidor Flex autentique al cliente AnyConnect a través del método AnyConnect-EAP propiedad de Cisco.

A diferencia de los métodos de protocolo de autenticación extensible (EAP) basados en estándares, como EAP-Generic Token Card (EAP-GTC), EAP-Message Digest 5 (EAP-MD5), etc., Flex Server no funciona en el modo de paso a través de EAP.

Toda la comunicación EAP con el cliente termina en el servidor Flex y la clave de sesión necesaria utilizada para construir la carga útil AUTH es calculada localmente por el servidor Flex.

El servidor Flex tiene que autenticarse ante el cliente con certificados según lo requiere el RFC IKEv2.

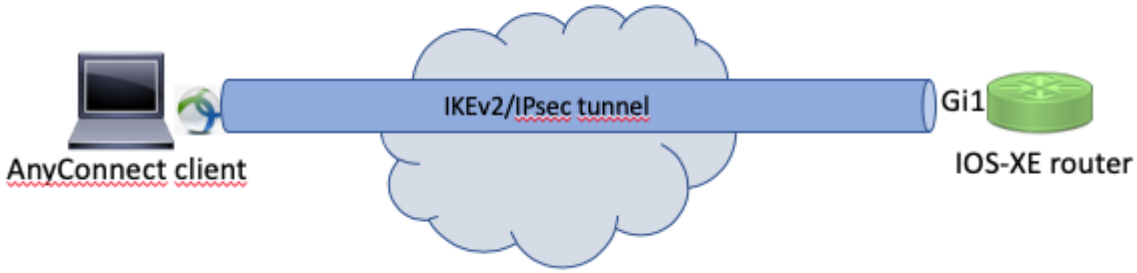
La autenticación de usuario local ahora es compatible con Flex Server y la autenticación remota es opcional.

Esto es ideal para implementaciones a pequeña escala con menos usuarios de acceso remoto y en entornos sin acceso a un servidor externo de autenticación, autorización y contabilidad (AAA).

Sin embargo, para implementaciones a gran escala y en escenarios donde se desean atributos por usuario, se recomienda utilizar un servidor AAA externo para la autenticación y autorización.

La implementación de AnyConnect-EAP permite el uso de Radius para la autenticación, autorización y contabilidad remotas.

Diagrama de la red



Configurar

Autenticación y autorización de usuarios con la base de datos local

---

> **Nota**: Para autenticar a los usuarios en la base de datos local del router, se debe utilizar EAP. Sin embargo, para utilizar EAP, el método de autenticación local debe ser rsa-sig, de modo que el router necesita un certificado adecuado instalado en él y no puede ser un certificado autofirmado.

Configuración de ejemplo que utiliza autenticación de usuario local, autorización de grupo y usuario remoto y cuentas remotas.

Paso 1. Habilite AAA y configure las listas de autenticación, autorización y contabilidad 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
!
username test password cisco123
```

Paso 2. Configure un punto de confianza que contenga el certificado del router. En este ejemplo se utiliza la importación de archivos PKCS12. Para otras opciones, consulte la guía de configuración PKI (Public Key Infrastructure):

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/xe-3s/sec-pki-xe-3s-book/sec-cert-enroll-pki.html

```
Router(config)# crypto pki import IKEv2-TP pkcs12 bootflash:IKEv2-TP.p12 password cisco123
```

Paso 3. Defina un conjunto local de IP para asignar direcciones a los clientes VPN de AnyConnect:

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

Paso 4. Cree una política de autorización local IKEv2:

```
crypto ikev2 authorization policy ikev2-auth-policy
 pool ACPOOL
 dns 10.0.1.1
```

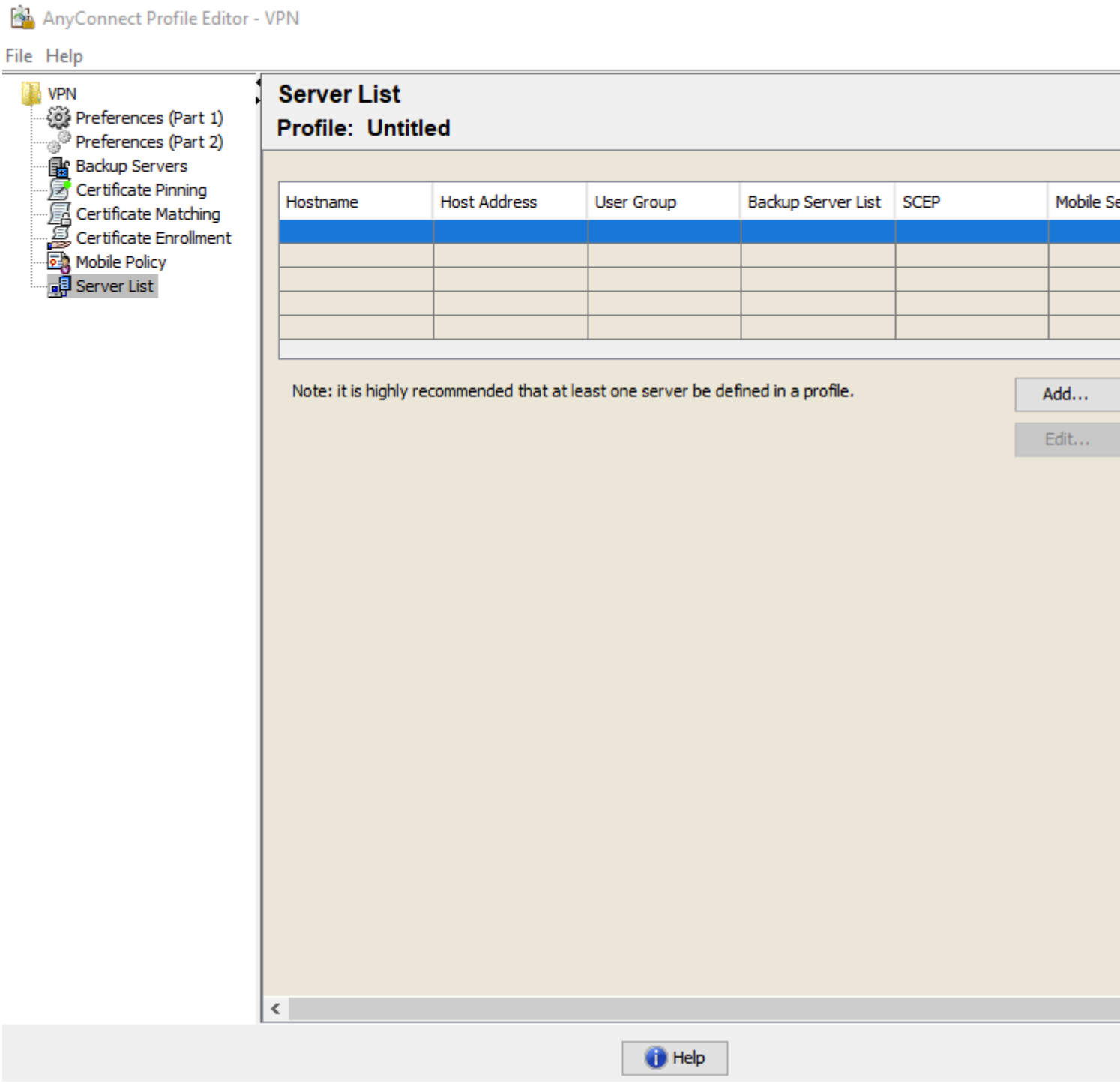
Paso 5 (opcional). Cree la propuesta y la política IKEv2 que desee. Si no se configura, se utilizan los valores predeterminados inteligentes:

```
crypto ikev2 proposal IKEv2-prop1
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy IKEv2-pol
 proposal IKEv2-prop1
```

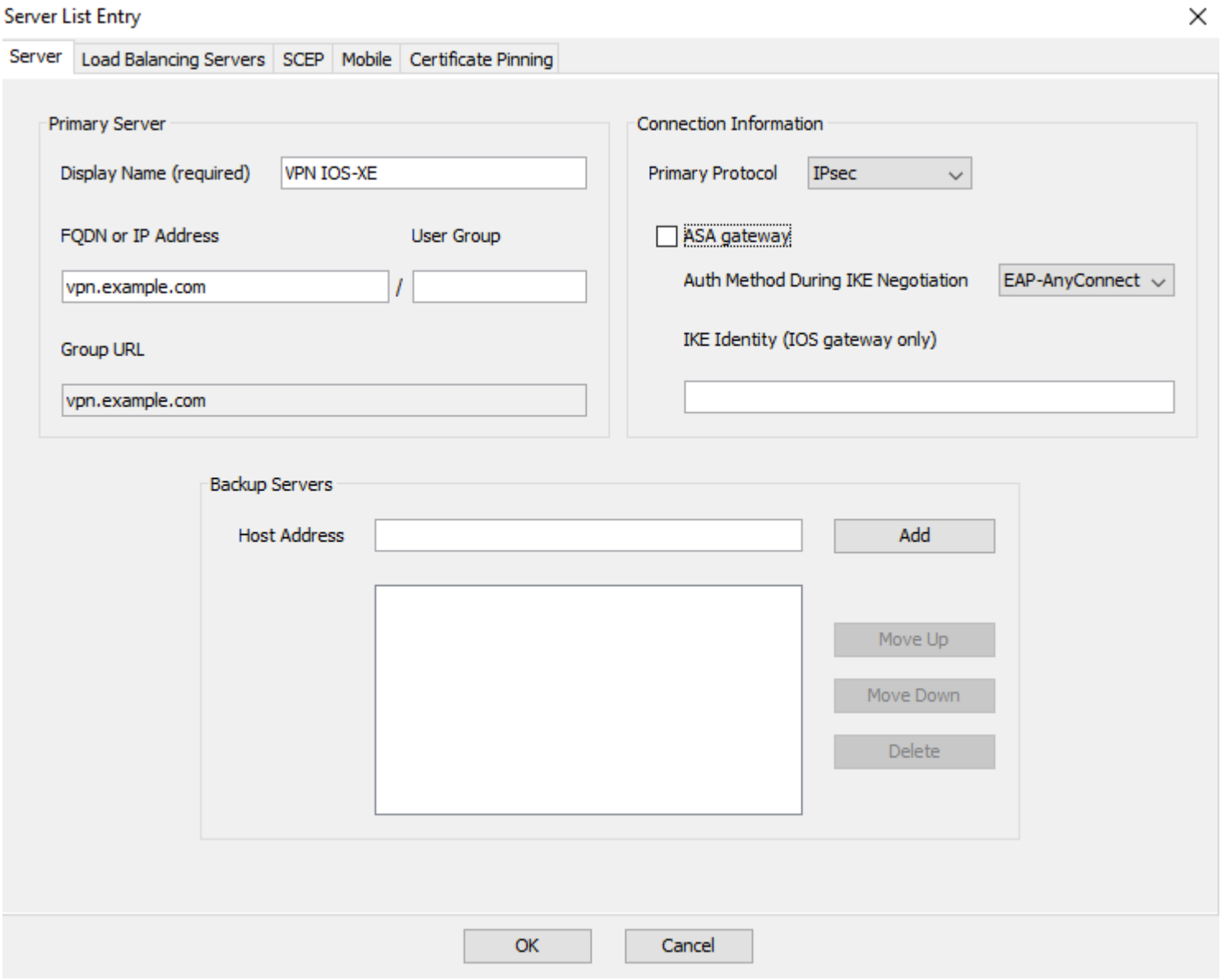
Paso 6. Crear perfil de AnyConnect

> **Nota**: el perfil de AnyConnect debe entregarse al equipo cliente. Consulte la siguiente sección para obtener más información.

Configure el perfil del cliente con el editor de perfiles de AnyConnect como se muestra en la imagen:



Haga clic en "Agregar" para crear una entrada para el gateway VPN. Asegúrese de seleccionar "IPSec" como "Protocolo principal". Desmarque la opción "ASA gateway".



Guardar el perfil: **Archivo -> Guardar como.** El equivalente XML del perfil:

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    <ClientInitialization>
        <UseStartBeforeLogon UserControllable="true">false</UseStartBeforeLogon>
        <AutomaticCertSelection UserControllable="true">false</AutomaticCertSelection>
        <ShowPreConnectMessage>false</ShowPreConnectMessage>
        <CertificateStore>All</CertificateStore>
        <CertificateStoreMac>All</CertificateStoreMac>
        <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>
        <DisableCaptivePortalDetection UserControllable="true">false</DisableCaptivePortalDetection>
        <ClearSmartcardPin UserControllable="true">true</ClearSmartcardPin>
        <IPProtocolSupport>IPv4,IPv6</IPProtocolSupport>
        <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>
        <AllowManualHostInput>true</AllowManualHostInput>
    </ClientInitialization>
    <ServerList>
        <HostEntry>
            <HostName>VPN IOS-XE</HostName>
            <HostAddress>vpn.example.com</HostAddress>
            <PrimaryProtocol>IPsec
                <StandardAuthenticationOnly>true
                    <AuthMethodDuringIKENegotiation>EAP-AnyConnect</AuthMethodDuringIKENegotiation>
                </StandardAuthenticationOnly>
            </PrimaryProtocol>
        </HostEntry>
    </ServerList>
</AnyConnectProfile>
```

Nota: AnyConnect utiliza '*$AnyConnectClient$*' como su identidad IKE predeterminada de tipo key-id. Sin embargo, esta identidad se puede cambiar manualmente en el perfil de AnyConnect para que coincida con las necesidades de implementación.

Nota: Para cargar el perfil XML en el router, se requiere la versión Cisco IOS® XE 16.9.1 o posterior. Si se utiliza una versión anterior del software Cisco IOS® XE, la capacidad de descarga del perfil debe estar inhabilitada en el cliente. Consulte la sección "Desactivar la función de descarga de AnyConnect" para obtener más información.

Cargue el perfil XML creado en la memoria flash del router y defina el perfil:

```
crypto vpn anyconnect profile acvpn bootflash:/acvpn.xml
```

Nota: El nombre de archivo utilizado para el perfil XML de AnyConnect es acvpn.xml.

Paso 7. Cree un perfil IKEv2 para el método de autenticación de cliente AnyConnect-EAP.

```
crypto ikev2 profile AnyConnect-EAP
```

```
 match identity remote key-id *$AnyConnectClient$*
 authentication local rsa-sig
 authentication remote anyconnect-eap aggregate
 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
 anyconnect profile acvpn
```

Nota: La CLI acepta la configuración del método de autenticación remota antes del método de autenticación local, pero no tiene efecto en las versiones que no tienen la corrección para la solicitud de mejora Cisco bug ID CSCvb29701**,** si el método de autenticación remota es eap. Para estas versiones, cuando la configuración eap sea el método de autenticación remota, asegúrese de que el método de autenticación local esté configurado primero como rsa-sig. Este problema no se observa con ninguna otra forma de método de autenticación remota.

Nota: En las versiones de código afectadas por el Id. de error de Cisco CSCvb24236 **, una vez que la autenticación remota se configura antes de la autenticación local, el método de autenticación remota ya no se puede configurar en ese dispositivo.** Actualice a una versión que tenga la corrección para este código.

Paso 8. Inhabilite la búsqueda de certificados basada en HTTP-URL y el servidor HTTP en el router:

```
no crypto ikev2 http-url cert
no ip http server
no ip http secure-server
```

Nota: *Consulte* este documento **para confirmar si el hardware del router admite los algoritmos de cifrado NGE (el ejemplo anterior tiene algoritmos NGE); de lo contrario, la instalación de SA IPSec en el hardware falla** en la última etapa de la negociación.

Paso 9. Definir los algoritmos de cifrado y hash utilizados para proteger los datos

```
crypto ipsec transform-set TS esp-aes 256 esp-sha256-hmac
 mode tunnel
```

Paso 10. Cree un perfil IPSec:

```
crypto ipsec profile AnyConnect-EAP
 set transform-set TS
 set ikev2-profile AnyConnect-EAP
```

Paso 11. Configure una interfaz de loopback con alguna dirección IP ficticia. Las interfaces de acceso virtual le piden prestada la dirección IP.

```
interface loopback100
 ip address 10.0.0.1 255.255.255.255
```

Paso 12. Configure una plantilla virtual (asocie la plantilla en el perfil IKEv2)

```
interface Virtual-Template100 type tunnel
 ip unnumbered Loopback100
 ip mtu 1400
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile AnyConnect-EAP
```

Paso 13 (opcional). De forma predeterminada, todo el tráfico del cliente se envía a través del túnel. Puede configurar el túnel dividido, que permite que sólo el tráfico seleccionado pase a través del túnel.

```
ip access-list standard split_tunnel
 permit 10.0.0.0 0.255.255.255
!
crypto ikev2 authorization policy ikev2-auth-policy
 route set access-list split_tunnel
```

Paso 14 (opcional). Si se requiere que todo el tráfico pase a través del túnel, configure NAT para permitir la conectividad a Internet para los clientes remotos.

```
ip access-list extended NAT
 permit ip 192.168.10.0 0.0.0.255 any
!
ip nat inside source list NAT interface GigabitEthernet1 overload
!
interface GigabitEthernet1
 ip nat outside
!
interface Virtual-Template 100
 ip nat inside
```

Desactive la función de descarga de AnyConnect (opcional).

Este paso sólo es necesario si se utiliza la versión del software Cisco IOS® XE anterior a 16.9.1. Antes de Cisco IOS® XE 16.9.1, la capacidad de cargar el perfil XML en el router no estaba disponible. El cliente AnyConnect intenta descargar el perfil XML después de iniciar sesión correctamente de forma predeterminada. Si el perfil no está disponible, la conexión falla. Como solución alternativa, es posible inhabilitar la capacidad de descarga del perfil de AnyConnect en el propio cliente. Para ello, este archivo se

puede modificar:

```
For Windows:
C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\AnyConnectLocalPolicy.xml

For MAC OS:
/opt/cisco/anyconnect/AnyConnectLocalPolicy.xml
```

La opción "BypassDownloader" se establece en "true", por ejemplo:

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectLocalPolicy xmlns="http://schemas.xmlsoap/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSch
<BypassDownloader>true</BypassDownloader>
<EnableCRLCheck>false</EnableCRLCheck>
<ExcludeFirefoxNSSCertStore>false</ExcludeFirefoxNSSCertStore>
<ExcludeMacNativeCertStore>false</ExcludeMacNativeCertStore>
<ExcludePemFileCertStore>false</ExcludePemFileCertStore>
<ExcludeWinNativeCertStore>false</ExcludeWinNativeCertStore>
<FipsMode>false</FipsMode>
<RestrictPreferenceCaching>false</RestrictPreferenceCaching>
<RestrictTunnelProtocols>false</RestrictTunnelProtocols>
<RestrictWebLaunch>false</RestrictWebLaunch>
<StrictCertificateTrust>false</StrictCertificateTrust>
<UpdatePolicy>
<AllowComplianceModuleUpdatesFromAnyServer>true</AllowComplianceModuleUpdatesFromAnyServer>
<AllowISEProfileUpdatesFromAnyServer>true</AllowISEProfileUpdatesFromAnyServer>
<AllowServiceProfileUpdatesFromAnyServer>true</AllowServiceProfileUpdatesFromAnyServer>
<AllowSoftwareUpdatesFromAnyServer>true</AllowSoftwareUpdatesFromAnyServer>
<AllowVPNProfileUpdatesFromAnyServer>true</AllowVPNProfileUpdatesFromAnyServer></UpdatePolicy>
</AnyConnectLocalPolicy>
```

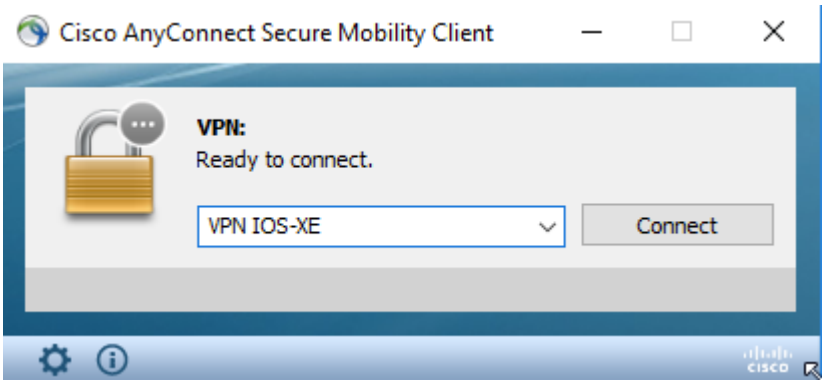
Después de la modificación, es necesario reiniciar el cliente AnyConnect.

Entrega de perfil XML de AnyConnect

Con la nueva instalación de AnyConnect (sin perfiles XML agregados), el usuario puede introducir manualmente el FQDN del gateway VPN en la barra de direcciones del cliente AnyConnect. Esto da como resultado la conexión SSL con el gateway. El cliente AnyConnect no intenta establecer el túnel VPN con los protocolos IKEv2/IPsec de forma predeterminada. Esta es la razón por la que el perfil XML está instalado en el cliente y es obligatorio establecer el túnel IKEv2/IPsec con el gateway de VPN Cisco IOS® XE.

El perfil se utiliza cuando se selecciona en la lista desplegable de la barra de direcciones de AnyConnect.

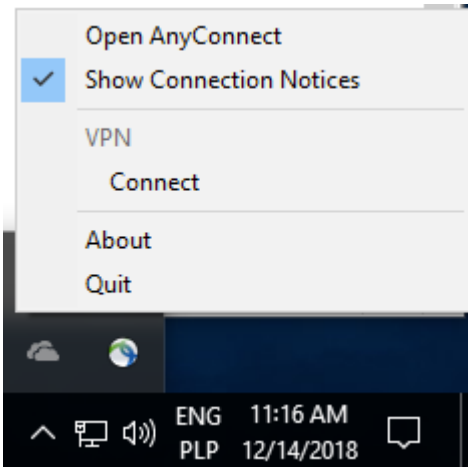
El nombre que aparece es el mismo que el especificado en "Display Name" en el editor de perfiles de AnyConnect.



El perfil XML se puede colocar manualmente en este directorio:

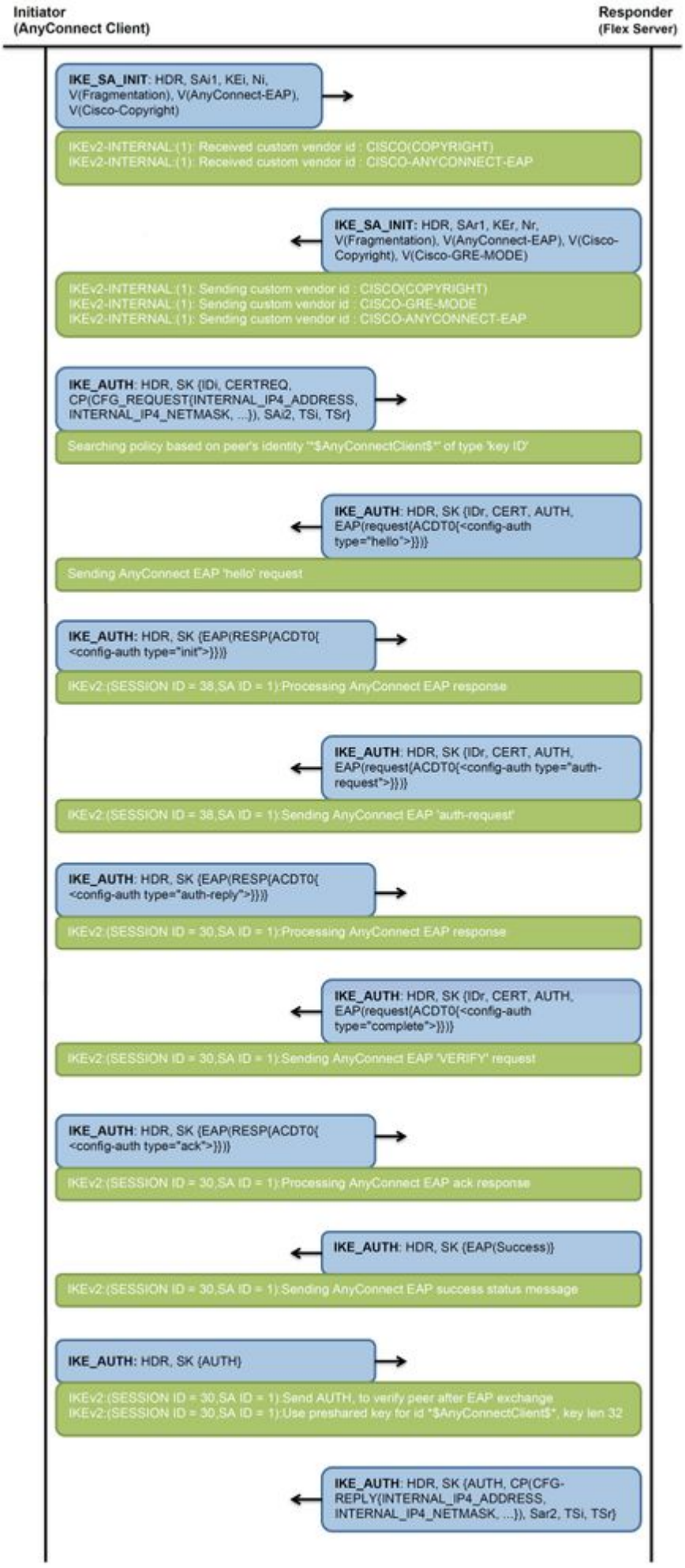
```
For Windows:
C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile

For MAC OS:
/opt/cisco/anyconnect/profile
```

El cliente AnyConnect debe reiniciarse para que el perfil sea visible en la GUI. No es suficiente con cerrar la ventana de AnyConnect. El proceso se puede reiniciar haciendo clic con el botón derecho del ratón en el icono de AnyConnect en la bandeja de Windows y seleccione la opción "Salir":



Flujo de comunicación

Intercambio IKEv2 y EAP



Verificación

Router# show crypto ikev2 sa detailed

```
 IPv4 Crypto IKEv2  SA

Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         192.0.2.1/4500
```

192.0.2.100/50899

```
    none/none            READY
      Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:14, Auth sign: RSA, Auth verify: An
      Life/Active Time: 86400/758 sec
      CE id: 1004, Session-id: 4
      Status Description: Negotiation done
      Local spi: 413112E83D493428       Remote spi: 696FA78292A21EA5
      Local id: 192.0.2.1
      Remote id: *$AnyConnectClient$*
```

Remote EAP id: test

<------ username

```
      Local req msg id:  0              Remote req msg id:  31
      Local next msg id: 0              Remote next msg id: 31
      Local req queued:  0              Remote req queued:  31
      Local window:      5              Remote window:      1
      DPD configured for 0 seconds, retry 0
      Fragmentation not  configured.
      Dynamic Route Update: disabled
      Extended Authentication not configured.
      NAT-T is detected  outside
      Cisco Trust Security SGT is disabled
```

Assigned host addr: 192.168.10.8. <---- Assigned IP

```
      Initiator of SA : No
```

! Check the crypto session information

Router# show crypto session detail

```
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation
R - IKE Auto Reconnect, U - IKE Dynamic Route Update
S - SIP VPN
```

Interface: Virtual-Access1. <----- Virtual interface associated with the client

```
Profile: AnyConnect-EAP
Uptime: 00:14:54
Session status: UP-ACTIVE
```

Peer: 192.0.2.100

```
 port 50899 fvrf: (none) ivrf: (none).
```

<----- Public IP of the remote client

```
      Phase1_id: *$AnyConnectClient$*
      Desc: (none)
  Session ID: 8
  IKEv2 SA: local 192.0.2.1/4500 remote 192.0.2.100/50899 Active
          Capabilities:N connid:1 lifetime:23:45:06
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 host 192.168.10.8
        Active SAs: 2, origin: crypto map
```

Inbound: #pkts dec'ed 89

```
 drop 0 life (KB/Sec) 4607990/2705.
```

<------ Packets received from the client

Outbound: #pkts enc'ed 2

```
 drop 0 life (KB/Sec) 4607999/2705.
```

<------ Packets sent to the client

! Check the actual configuration applied for the Virtual-Acces interface associated with client

Router# show derived-config interface virtual-access 1.

```
Building configuration...

Derived configuration : 258 bytes
!
interface Virtual-Access1
 ip unnumbered Loopback100
 ip mtu 1400
 ip nat inside
 tunnel source 192.0.2.1
 tunnel mode ipsec ipv4
 tunnel destination 192.0.2.100
 tunnel protection ipsec profile AnyConnect-EAP
 no tunnel protection ipsec initiate
end
```

Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

1. Depuraciones IKEv2 para recopilar datos del equipo de cabecera:

```
debug crypto ikev2
debug crypto ikev2 packet
debug crypto ikev2 error
```

2. Depuraciones AAA para ver la asignación de atributos locales y/o remotos:

```
debug aaa authorization
debug aaa authentication
```

3. DART del cliente AnyConnect.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).