FlexVPN: Acesso remoto de AnyConnect IKEv2 com base de dados de usuário local

Índice

Introdução

Este original fornece uma configuração de exemplo de como configurar um final do cabeçalho IOS/IOS-XE para o Acesso remoto usando o método de autenticação IKEv2 e AnyConnect-EAP de AnyConnect com base de dados de usuário local.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Protocolo IKEv2

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco nubla-se o roteador dos serviços que executa IO XE 16.9.2
- Versão de cliente 4.6.03049 de AnyConnect que é executado em Windows 10

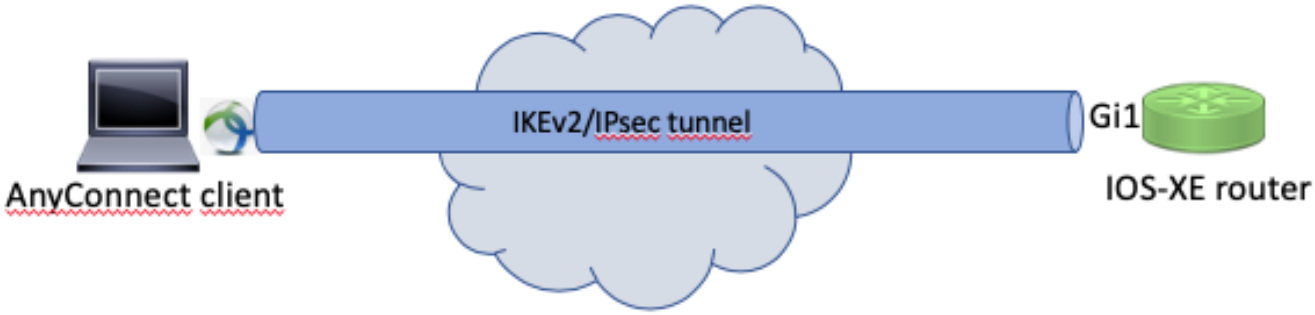
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

O AnyConnect-EAP, igualmente conhecido como a autenticação agregada, permite que um server do cabo flexível autentique o cliente de AnyConnect que usa o método AnyConnect-EAP proprietário de Cisco. Ao contrário do padrão baseado os métodos do Extensible Authentication Protocol (EAP) tais como a placa de token EAP-genérica (EAP-GTC), o resumo de mensagem EAP 5 (EAP-MD5) e assim por diante, o server do cabo flexível não se operam no modo de passagem EAP. Toda a comunicação EAP com o cliente termina no server do cabo flexível e a chave de sessão exigida usada para construir o payload do AUTH é computada localmente pelo server do cabo flexível. **O server do cabo flexível tem que autenticar-se ao cliente que usa Certificados segundo as exigências do IKEv2 RFC.**

A autenticação de usuário local é apoiada agora no server do cabo flexível e a autenticação remota é opcional. Isto é ideal para disposições da pequena escala com menos número de usuários de acesso remotos e nos ambientes sem o acesso a uma autenticação externa, a um server da autorização, e da contabilidade (AAA). Contudo, para distribuições em larga escala e nas encenações onde os atributos por usuário são desejados ainda recomenda-se usar um AAA externo separa para a authentication e autorização. A aplicação AnyConnect-EAP permite o uso do raio para a autenticação remota, a autorização e a contabilidade.

Diagrama de Rede



Configurar

Usuários da autenticação e do Authorizating que usam o base de dados local

> **Note**: A fim autenticar usuários contra o base de dados local no roteador, o EAP precisa de ser usado. Contudo, a fim usar o EAP, o método de autenticação local tem que ser RSA-SIG, assim que o roteador precisa um certificado apropriado instalado nele, e não pode ser um certificado auto-assinado.

Configuração de exemplo que usa a autenticação de usuário local, a autorização do usuário remoto e do grupo e contabilidade remota.

Etapa 1. Permita o AAA, e configurar lista da autenticação, da autorização e da contabilidade e

adicionar um username ao base de dados local:

```
aaa new-model
!
aaa authentication login a-eap-authen-local local
aaa authorization network a-eap-author-grp local
!
username test password cisco123
```

Etapa 2. Configurar um trustpoint que guarde o certificado de roteador. A importação do arquivo do PKCS12 é usada neste exemplo. Para outras opções, consulte por favor o manual de configuração PKI (infraestrutura de chave pública):

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
```

Etapa 3. Defina um conjunto local IP para atribuir endereços aos clientes VPN de AnyConnect:

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

Etapa 4. Crie uma política da autorização local IKEv2:

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

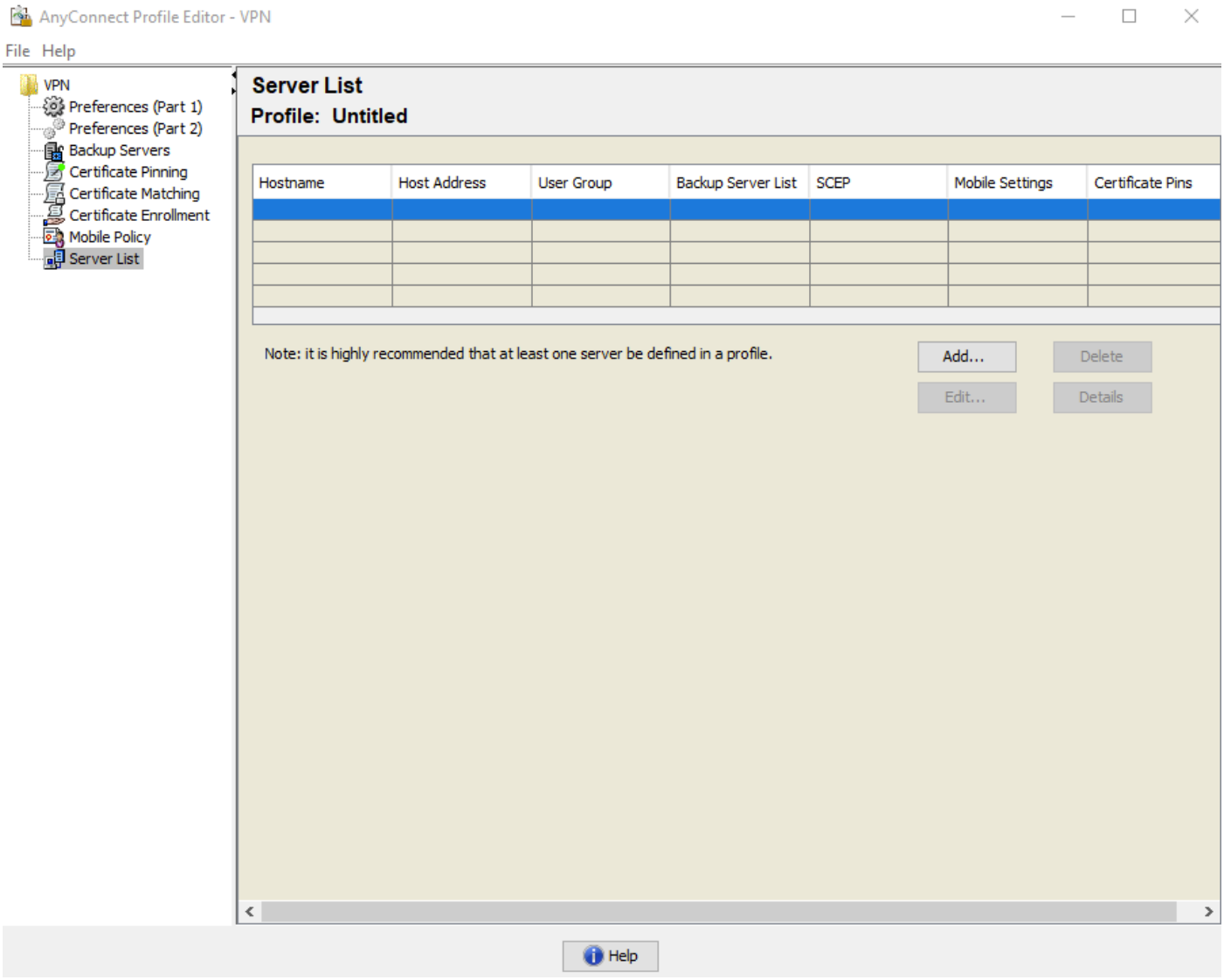
Etapa 5 (opcional). Create desejou a proposta IKEv2 e a política. Se não os padrões configurados, espertos serão usados:

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

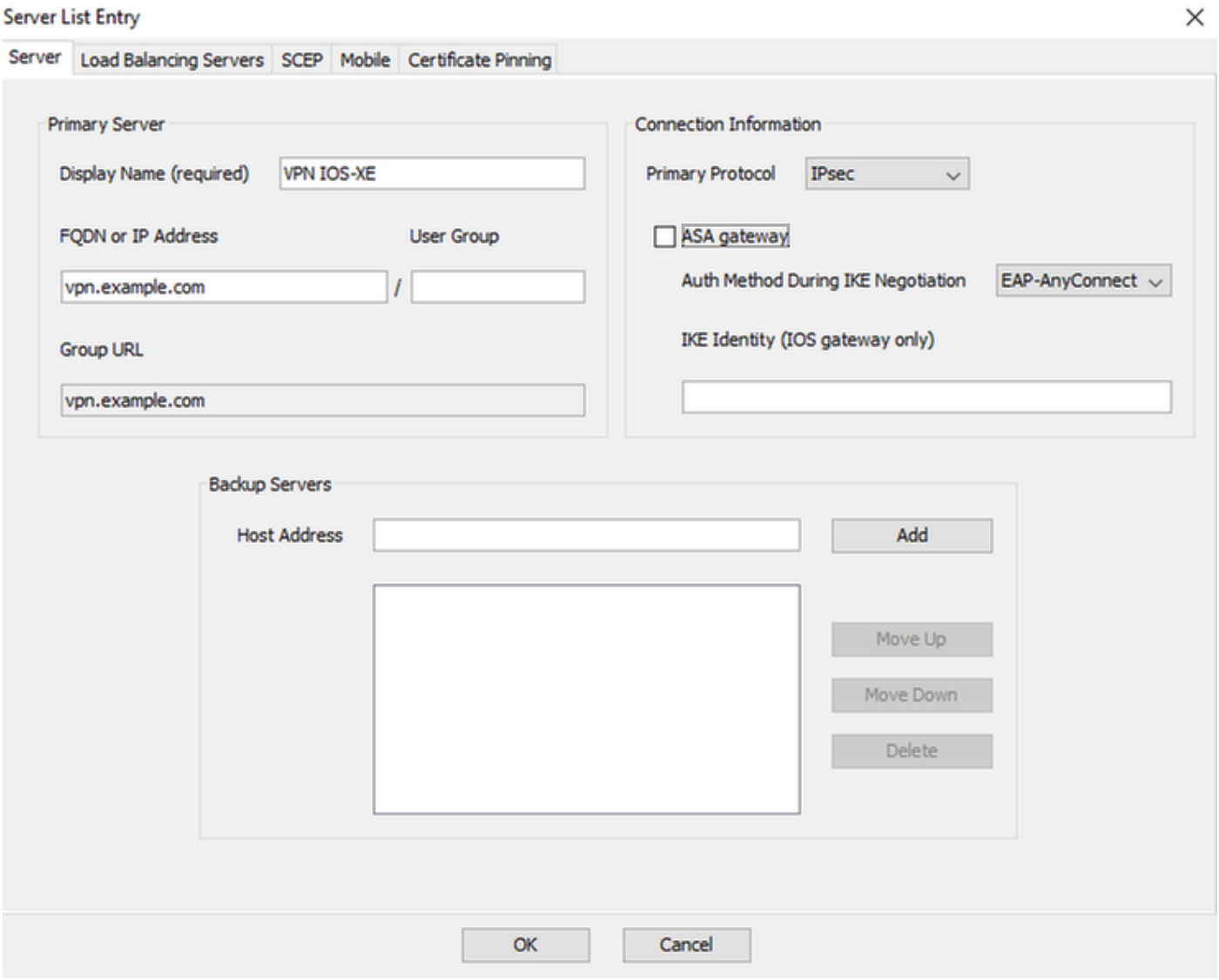
Etapa 6. Crie o perfil de AnyConnect

> **Note**: O perfil de AnyConnect precisa de ser entregado à máquina cliente. Refira por favor a próxima seção para mais informação.

Configurar o perfil do cliente usando o editor do perfil de AnyConnect segundo as indicações da imagem:



O clique “adiciona” para criar uma entrada para o gateway de VPN. Certifique-se selecionar “IPsec” como “o protocolo preliminar”. Uncheck “a opção do gateway ASA”.



Salvar o perfil indo arquivar - > salvaguarda como. O equivalente XML do 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">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>
```

Note: AnyConnect usa “*$AnyConnectClient$*” como sua identidade do padrão IKE do tipo chave-identificação. Contudo, esta identidade pode manualmente ser mudada no perfil de AnyConnect para combinar necessidades do desenvolvimento.

Note: A fim transferir arquivos pela rede o perfil XML ao roteador, são exigidos a versão IOS-XE 16.9.1 ou mais tarde. Se uma versão mais velha do software IOS-XE é usada, a capacidade da transferência do perfil precisa de ser desabilitada no cliente. Refira por favor a seção “que desabilita a capacidade do descargador de AnyConnect” para mais informação.

Transfira arquivos pela rede o perfil criado XML à memória Flash do roteador e defina o perfil:

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

Note: O nome de arquivo usado para o perfil de AnyConnect XML deve ser acvpn.xml.

Etapa 7. Crie um perfil IKEv2 para o método AnyConnect-EAP de authenticação do cliente.

```
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
```

> **Note**: Configurar o método de autenticação remota antes que o método de autenticação local estiver aceitado pelo CLI, mas não tomará o efeito nas versões que não têm o reparo para a requisição de aprimoramento CSCvb29701, se o método de autenticação remota é eap. Para estas versões, ao configurar o eap como o método de autenticação remota, assegure-se de que o método de autenticação local esteja configurado como o RSA-SIG primeiramente. Este problema não é considerado com nenhum outro formulário do método de autenticação remota.

> **Nota:** Nas versões de código afetadas por CSCvb24236, uma vez que a autenticação remota é configurada antes da autenticação local, o método de autenticação remota pode já não ser configurado nesse dispositivo. Promova por favor a uma versão que tenha o reparo para este código.

Etapa 8. Desabilite a consulta baseada URL DO HTTP e o Server do HTTP do certificado no roteador:

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

> **Note**: *Consulte* este original para confirmar se seu hardware de roteador apoia os algoritmos de criptografia NGE (por exemplo o exemplo acima tem algoritmos NGE). Se não a instalação IPSec SA no hardware falhará na última fase da negociação.

Etapa 9. Defina a criptografia e os algoritmos de hash usados para proteger dados

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

Etapa 10. Crie um perfil IPSec:

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

Etapa 11. Configurar uma interface de loopback com algum IP address do manequim. As interfaces de acesso virtual pedirão o IP address dele.

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

Etapa 12. Configurar um virtual-molde (associe o molde no perfil IKEv2)

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

Steap 13 (opcional). À revelia, todo o tráfego do cliente será enviado através do túnel. Você pode configurar o túnel em divisão, que permite que somente o tráfego selecionado atravesse o 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
```

Etapa 14 (opcional). Se todo o tráfego é exigido para atravessar o túnel, você pode configurar o NAT a fim permitir a conectividade de Internet para 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
```

Desabilitando a capacidade do descargador de AnyConnect (opcional).

Esta etapa é somente necessária se a versão de software IOS-XE mais velha de 16.9.1 está sendo usada. Antes de IOS-XE 16.9.1 a capacidade de transferir arquivos pela rede o perfil XML ao roteador não estava disponível. O cliente de AnyConnect tenta executar à revelia a transferência do perfil XML após o login bem-sucedido. Se o perfil não está disponível, a conexão falha. Como uma ação alternativa, é possível desabilitar a capacidade no cliente própria da transferência do perfil de AnyConnect. A fim fazer isso, o seguinte arquivo pode ser alterado:

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

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

A opção de “BypassDownloader” deve ser ajustada “verdadeira”, por exemplo:

```
<?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="4.6.03049">
<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>
```

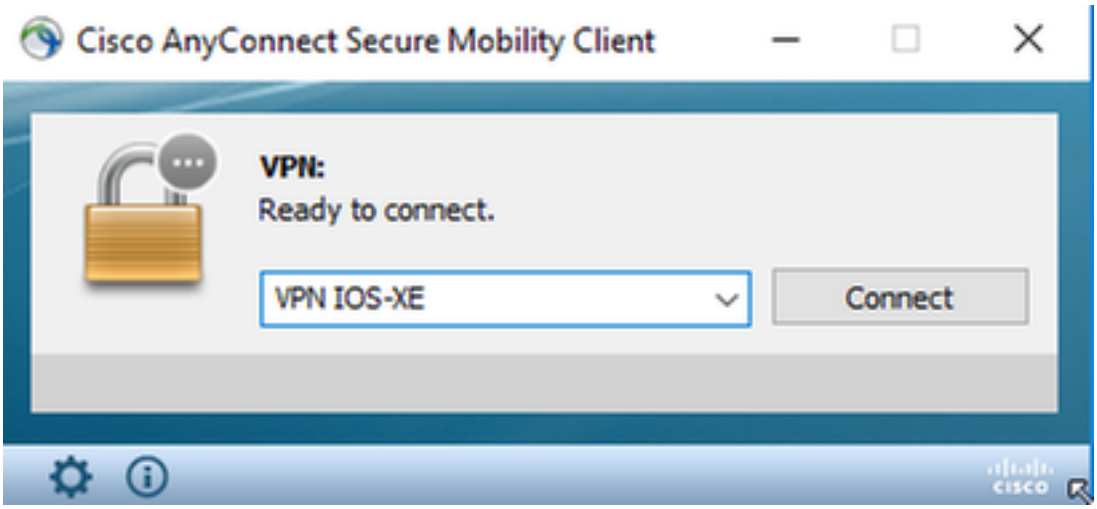
```
<AllowComplianceModuleUpdatesFromAnyServer>true</AllowComplianceModuleUpdatesFromAnyServer>
<AllowISEProfileUpdatesFromAnyServer>true</AllowISEProfileUpdatesFromAnyServer>
<AllowServiceProfileUpdatesFromAnyServer>true</AllowServiceProfileUpdatesFromAnyServer>
<AllowSoftwareUpdatesFromAnyServer>true</AllowSoftwareUpdatesFromAnyServer>
<AllowVPNProfileUpdatesFromAnyServer>true</AllowVPNProfileUpdatesFromAnyServer></UpdatePolicy>
</AnyConnectLocalPolicy>
```

Após a alteração, o cliente de AnyConnect precisa de ser reiniciado.

Entrega do perfil de AnyConnect XML

Com a instalação de atualização do AnyConnect (sem o XML perfila adicionado), o usuário pode incorporar manualmente o FQDN do gateway de VPN à barra de endereços do cliente de AnyConnect. Isto conduz à conexão SSL ao gateway. O cliente de AnyConnect não tentará estabelecer à revelia o túnel VPN com protocolos IKEv2/IPsec. Esta é a razão pela qual ter o perfil XML instalado no cliente é imperativo para estabelecer o túnel IKEv2/IPsec com gateway de VPN IOS-XE.

O perfil é usado quando está sendo selecionado da lista de drop-down da barra de endereços de AnyConnect. O nome que aparecerá é o mesmo nome como especificado do “no nome indicador” no editor do perfil de AnyConnect. Neste exemplo o usuário deve selecionar o seguinte:

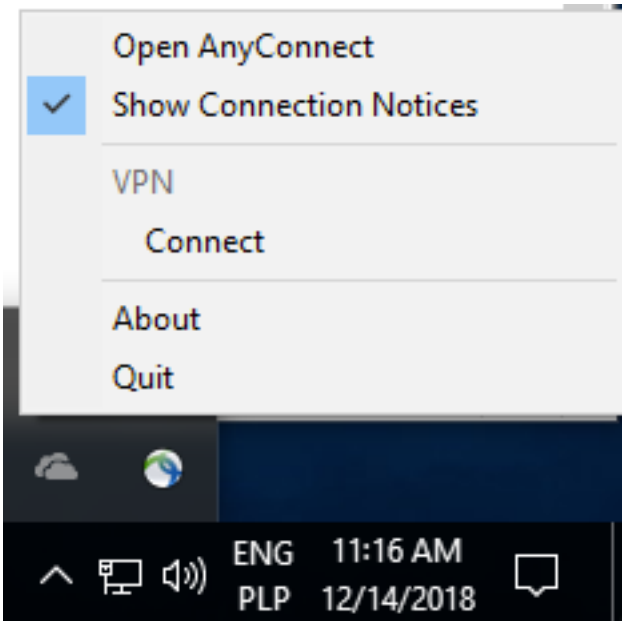


O perfil XML pode manualmente ser posto no seguinte diretório:

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

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

O cliente de AnyConnect precisa de ser reiniciado para que o perfil torne-se visível no GUI. Não é suficiente fechar o indicador de AnyConnect. O processo pode ser reiniciado pelo ícone declique de AnyConnect na bandeja e em selecionar de Windows a opção “parada”:



Fluxo de comunicação

Troca IKEv2 e EAP