

Configurar FlexVPN: acesso remoto IKEv2 do AnyConnect com banco de dados de usuário local

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Diagrama de Rede](#)

[Configurar](#)

[Autenticação e autorização de usuários com o banco de dados local](#)

[Desabilite o recurso de downloader do AnyConnect \(opcional\).](#)

[Entrega de perfil XML do AnyConnect](#)

[Fluxo de comunicação](#)

[Intercâmbio de IKEv2 e EAP](#)

[Verificar](#)

[Troubleshooting](#)

Introdução

Este documento descreve como configurar um headend Cisco IOS®/ XE para acesso através da autenticação IKEv2 / EAP do AnyConnect com o banco 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 Cloud Services Router executando o Cisco IOS® XE 16.9.2
- Cliente AnyConnect versão 4.6.03049 em execução no 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 rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O AnyConnect-EAP, também conhecido como autenticação agregada, permite que um servidor Flex autentique o cliente AnyConnect por meio do método AnyConnect-EAP, propriedade da Cisco.

Diferentemente dos métodos EAP (Extensible Authentication Protocol) baseados em padrões, como EAP-Generic Token Card (EAP-GTC), EAP-Message Digest 5 (EAP-MD5) e outros, o Flex Server não opera no modo de passagem EAP.

Toda a comunicação EAP com o cliente é encerrada no servidor Flex e a chave de sessão necessária usada para construir a carga útil AUTH é calculada localmente pelo servidor Flex.

O servidor Flex precisa se autenticar no cliente com certificados como exigido pelo RFC IKEv2.

A autenticação de usuário local agora é suportada no servidor Flex e a autenticação remota é opcional.

Isso é ideal para implantações em pequena escala com menos usuários de acesso remoto e em ambientes sem acesso a um servidor externo de Autenticação, Autorização e Contabilização (AAA).

No entanto, para implantações em larga escala e em cenários onde atributos por usuário são desejados, ainda é recomendável usar um servidor AAA externo para autenticação e autorização.


A implementação do AnyConnect-EAP permite o uso do Radius para autenticação, autorização e tarifação remotas.

Diagrama de Rede



Configurar

Autenticação e autorização de usuários com o banco de dados local

 Observação: para autenticar usuários no banco de dados local no roteador, o EAP precisa ser usado. No entanto, para usar o EAP, o método de autenticação local deve ser rsa-sig, portanto, o roteador precisa de um certificado apropriado instalado nele e não pode ser um certificado autoassinado.

Exemplo de configuração que usa autenticação de usuário local, autorização de usuário remoto e de grupo e contabilidade remota.

Etapa 1. Ative o AAA e configure as listas de autenticação, autorização e contabilização e adicione um nome de usuário ao banco 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. Configure um ponto de confiança destinado a manter o certificado do roteador. A importação do arquivo PKCS12 é usada neste exemplo. Para outras opções, consulte o guia de configuração da PKI (Public Key Infrastructure):

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/xr-3s/sec-pki-xr-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 pool IP local para atribuir endereços a clientes AnyConnect VPN:

```
ip local pool ACP00L 192.168.10.5 192.168.10.10
```


Etapa 4. Criar uma diretiva de autorização local IKEv2:

```
crypto ikev2 authorization policy ikev2-auth-policy
 pool ACP00L
 dns 10.0.1.1
```

Etapa 5 (opcional). Crie a proposta e a política de IKEv2 desejadas. Se não forem configurados, os padrões inteligentes 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. Criar perfil do AnyConnect

 Observação: o perfil do AnyConnect precisa ser entregue à máquina cliente. Consulte a próxima seção para obter mais informações.

Configure o perfil do cliente com o AnyConnect Profile Editor conforme mostrado na imagem:

File Help

The screenshot shows the 'Server List' configuration window in the AnyConnect Profile Editor. The window title is 'AnyConnect Profile Editor - VPN'. The menu bar includes 'File' and 'Help'. On the left, a tree view shows the configuration hierarchy: VPN, Preferences (Part 1), Preferences (Part 2), Backup Servers, Certificate Pinning, Certificate Matching, Certificate Enrollment, Mobile Policy, and Server List (selected). The main area is titled 'Server List' and 'Profile: Untitled'. It contains a table with the following columns: Hostname, Host Address, User Group, Backup Server List, SCEP, Mobile Settings, and Certificate Pins. The table is currently empty. Below the table, there is a note: 'Note: it is highly recommended that at least one server be defined in a profile.' To the right of the note are four buttons: 'Add...', 'Delete', 'Edit...', and 'Details'. At the bottom center of the window is a 'Help' button.

Server List
Profile: Untitled

Hostname	Host Address	User Group	Backup Server List	SCEP	Mobile Settings	Certificate Pins

Note: it is highly recommended that at least one server be defined in a profile.

Add... Delete
Edit... Details

Help

Clique em "Adicionar" para criar uma entrada para o gateway VPN. Certifique-se de selecionar "IPsec" como "Primary Protocol" (Protocolo principal). Desmarque a opção "Gateway ASA".

Server **Load Balancing Servers** SCEP Mobile Certificate Pinning

Primary Server

Display Name (required)

FQDN or IP Address /

Group URL

Connection Information

Primary Protocol

ASA gateway

Auth Method During IKE Negotiation

IKE Identity (IOS gateway only)

Backup Servers

Host Address	
	<input type="button" value="Add"/> <input type="button" value="Move Up"/> <input type="button" value="Move Down"/> <input type="button" value="Delete"/>


Salve o perfil: Arquivo -> Salvar como. O equivalente XML do 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>
  </ClientInitialization>
</AnyConnectProfile>
```

```

<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>


```

 Observação: o AnyConnect usa "\$AnyConnectClient\$" como sua identidade IKE padrão do tipo key-id. No entanto, essa identidade pode ser alterada manualmente no perfil do AnyConnect para corresponder às necessidades de implantação.

 Observação: para carregar o perfil XML para o roteador, é necessário o Cisco IOS® XE versão 16.9.1 ou posterior. Se uma versão mais antiga do software Cisco IOS® XE for usada, o recurso de download do perfil precisará ser desativado no cliente. Consulte a seção "Desabilitar o recurso de downloader do AnyConnect" para obter mais informações.

Carregue o perfil XML criado na memória flash do roteador e defina o perfil:


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


 Observação: o nome de arquivo usado para o perfil XML do AnyConnect é acvpn.xml.

Passo 7. Crie um perfil IKEv2 para o método AnyConnect-EAP de autenticação de 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
```

 Observação: a configuração do método de autenticação remota antes que o método de autenticação local seja aceito pela CLI, mas não entra em vigor em versões que não tenham a correção para a solicitação de aprimoramento ID de bug da Cisco [CSCvb29701](#), [se o método de autenticação remota for eap](#). Para essas versões, quando a configuração eap for o método de autenticação remota, verifique se o método de autenticação local está configurado como rsa-sig primeiro. Esse problema não é visto com nenhuma outra forma de método de autenticação remota.

 Nota: Em versões de código afetadas pelo bug da Cisco ID [CSCvb24236](#), uma vez que a autenticação remota é configurada antes da autenticação local, o método de autenticação remota não pode mais ser configurado nesse dispositivo. Atualize para uma versão que tenha a correção para este código.

Etapa 8. Desabilite a pesquisa de certificado baseada em URL HTTP e o servidor HTTP no roteador:

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

 Observação: consulte [este documento](#) para confirmar se o hardware do roteador suporta os algoritmos de criptografia NGE (o exemplo anterior tem algoritmos NGE), caso contrário, a instalação IPsec SA no hardware falha [no último estágio da negociação](#).

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

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

Etapa 10. Criar um perfil IPsec:


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

Etapa 11. Configure uma interface de loopback com algum endereço IP fictício. As interfaces de acesso virtual pegam emprestado o endereço IP dele.

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

Etapa 12. Configurar um modelo virtual (associe o modelo ao perfil IKEv2)

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

Etapa 13 (opcional). Por padrão, todo o tráfego do cliente é enviado através do túnel. Você pode configurar o túnel dividido, que permite que apenas o tráfego selecionado passe pelo 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 for necessário para passar pelo túnel, configure o NAT para permitir a conectividade da 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
```

Desabilite o recurso de downloader do AnyConnect (opcional).

Esta etapa só é necessária se for usada a versão do software Cisco IOS® XE anterior à 16.9.1. Antes do Cisco IOS® XE 16.9.1, a capacidade de carregar o perfil XML para o roteador não estava disponível. O cliente AnyConnect tenta fazer download do perfil XML após o login bem-sucedido por padrão. Se o perfil não estiver disponível, a conexão falhará. Como solução alternativa, é possível desativar o recurso de download de perfil do AnyConnect no próprio cliente. Para fazer isso, este arquivo pode ser modificado:

For Windows:

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

For MAC OS:

```
/opt/cisco/anyconnect/AnyConnectLocalPolicy.xml
```

A opção "BypassDownloader" está definida como "true", por exemplo:

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectLocalPolicy xmlns="http://schemas.xmlsoap/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSchema"
<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>
```

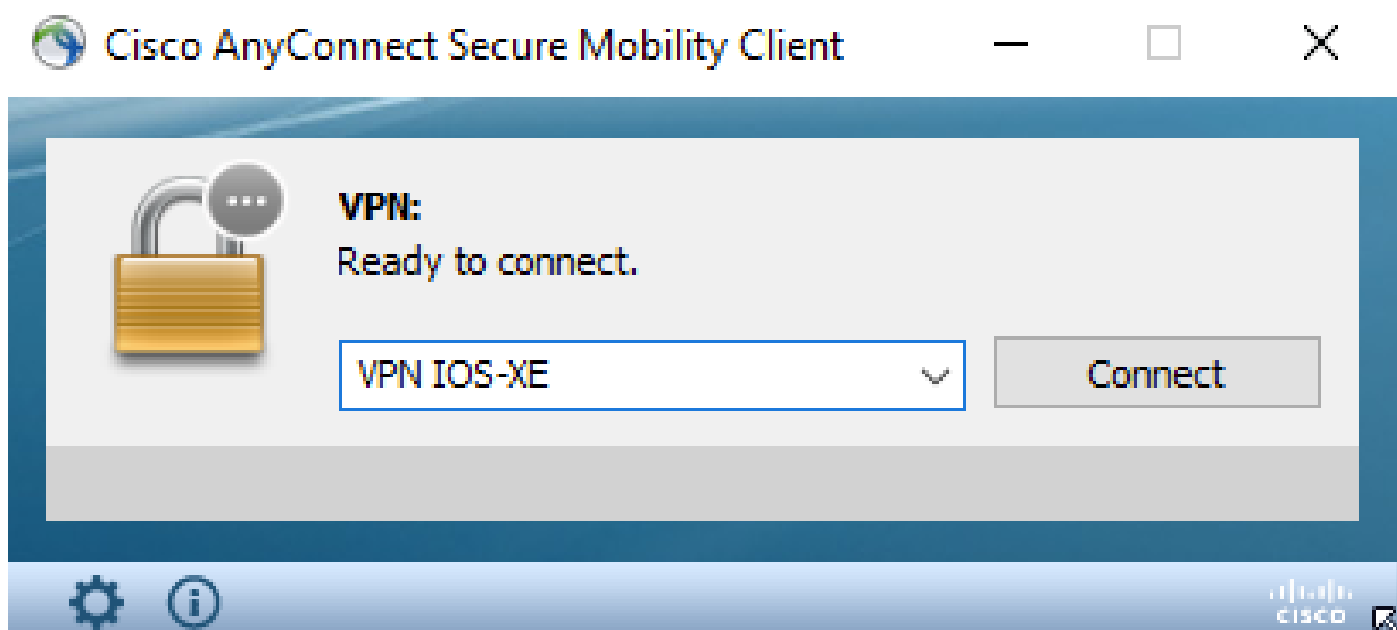
Após a modificação, o cliente AnyConnect precisa ser reiniciado.

Entrega de perfil XML do AnyConnect

Com a nova instalação do AnyConnect (sem perfis XML adicionados), o usuário pode inserir manualmente o FQDN do gateway VPN na barra de endereços do cliente AnyConnect. Isso resulta na conexão SSL com o gateway. O cliente AnyConnect não tenta estabelecer o túnel VPN com protocolos IKEv2/IPsec por padrão. Esta é a razão pela qual o perfil XML está instalado no cliente é obrigatório para estabelecer o túnel IKEv2/IPsec com o gateway Cisco IOS® XE VPN.

O perfil é usado quando é selecionado na lista suspensa da barra de endereços do AnyConnect.

O nome que aparece é o mesmo nome especificado em "Nome de exibição" no editor de perfil do AnyConnect.



O perfil XML pode ser colocado manualmente neste diretório:

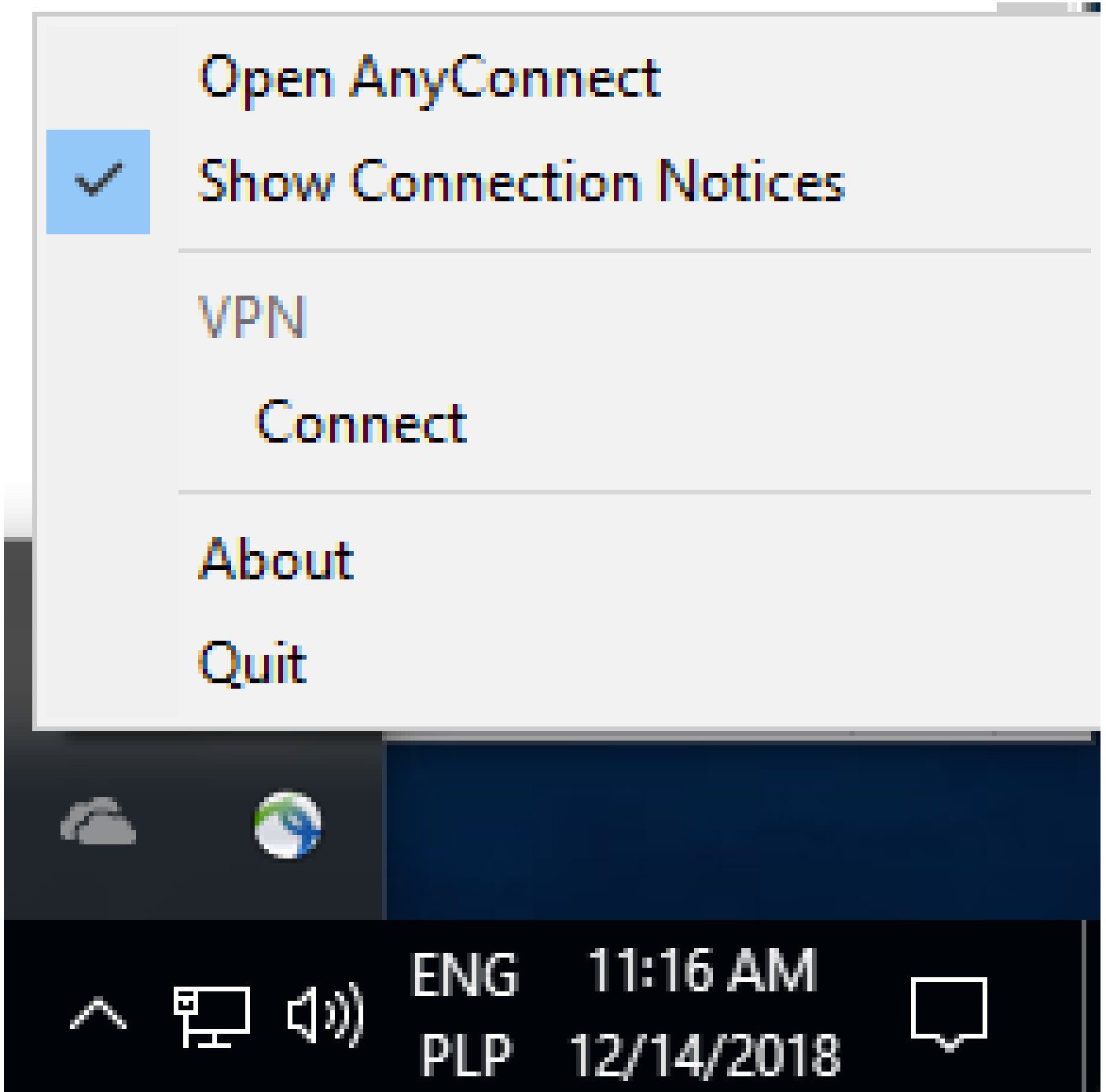
For Windows:

C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile

For MAC OS:

/opt/cisco/anyconnect/profile

O cliente AnyConnect precisa ser reiniciado para que o perfil se torne visível na GUI. Não é suficiente fechar a janela do AnyConnect. O processo pode ser reiniciado clicando com o botão direito do mouse no ícone do AnyConnect na bandeja do Windows e selecionando a opção "Sair":



Fluxo de comunicação

Intercâmbio de IKEv2 e EAP

IKE_SA_INIT: HDR, SAi1, KEi, Ni,
V(Fragmentation), V(AnyConnect-EAP),
V(Cisco-Copyright)

IKEv2-INTERNAL (1): Received custom vendor id : CISCO(COPYRIGHT)
IKEv2-INTERNAL (1): Received custom vendor id : CISCO-ANYCONNECT-EAP

IKE_SA_INIT: HDR, SAr1, KEr, Nr,
V(Fragmentation), V(AnyConnect-EAP), V(Cisco-
Copyright), V(Cisco-GRE-MODE)

IKEv2-INTERNAL (1): Sending custom vendor id : CISCO(COPYRIGHT)
IKEv2-INTERNAL (1): Sending custom vendor id : CISCO-GRE-MODE
IKEv2-INTERNAL (1): Sending custom vendor id : CISCO-ANYCONNECT-EAP

IKE_AUTH: HDR, SK (IDi, CERTREQ,
CP(CFG_REQUEST(INTERNAL_IP4_ADDRESS,
INTERNAL_IP4_NETMASK, ...)), SAi2, TSi, TSr)

Searching policy based on peer's identity "\$AnyConnectClient\$" of type 'key ID'

IKE_AUTH: HDR, SK (IDr, CERT, AUTH,
EAP(request{ACDT0{<config-auth
type="hello">}}))

-Sending AnyConnect EAP 'hello' request

IKE_AUTH: HDR, SK (EAP(ESP{ACDT0{
<config-auth type="init">}}))

IKEv2: (SESSION ID = 38, SA ID = 1): Processing AnyConnect EAP response

IKE_AUTH: HDR, SK (IDr, CERT, AUTH,
EAP(request{ACDT0{<config-auth type="auth-
request">}}))

IKEv2: (SESSION ID = 38, SA ID = 1): Sending AnyConnect EAP 'auth-request'

IKE_AUTH: HDR, SK (EAP(ESP{ACDT0{
<config-auth type="auth-reply">}}))

IKEv2: (SESSION ID = 30, SA ID = 1): Processing AnyConnect EAP response

IKE_AUTH: HDR, SK (IDr, CERT, AUTH,
EAP(request{ACDT0{<config-auth
type="complete">}}))

IKEv2: (SESSION ID = 30, SA ID = 1): Sending AnyConnect EAP 'VERIFY' request

Router# show crypto ikev2 sa detailed

IPv4 Crypto IKEv2 SA

Tunnel-id	Local	Remote	fvr/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: A

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-Access 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
```

Troubleshooting

Esta seção disponibiliza informações para a solução de problemas de configuração.

1. Depurações IKEv2 para coletar do headend:

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

2. Depurações AAA para ver a atribuição de atributos locais e/ou remotos:

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

3. do cliente AnyConnect.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.