

# 配置FlexVPN：使用本地用户数据库的AnyConnect IKEv2远程访问

## 目录

---

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[网络图](#)

[配置](#)

[使用本地数据库对用户进行身份验证和授权](#)

[禁用AnyConnect下载程序功能（可选）。](#)

[AnyConnect XML配置文件交付](#)

[通信流](#)

[IKEv2和EAP交换](#)

[验证](#)

[故障排除](#)

---

## 简介

本文档介绍如何配置Cisco IOS®/XE头端，以便通过本地用户数据库的AnyConnect IKEv2/EAP身份验证进行访问。

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- IKEv2协议

### 使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行Cisco IOS® XE 16.9.2的思科云服务路由器
- 在Windows 10上运行的AnyConnect客户03049版本4.6.

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

## 背景信息

AnyConnect-EAP (也称为聚合身份验证) 允许Flex服务器通过Cisco专有的AnyConnect-EAP方法对AnyConnect客户端进行身份验证。

与基于标准的可扩展身份验证协议(EAP)方法(例如EAP — 通用令牌卡(EAP-GTC)、EAP — 消息摘要5(EAP-MD5)等不同, Flex服务器不以EAP直通模式运行。

与客户端的所有EAP通信在Flex Server上终止, 用于构建AUTH负载所需的会话密钥由Flex Server在本地计算。

Flex Server必须使用IKEv2 RFC要求的证书向客户端验证其自身。

Flex Server现在支持本地用户身份验证, 并且远程身份验证是可选的。

这非常适合远程访问用户数量较少的小型部署, 以及无法访问外部身份验证、授权和记帐(AAA)服务器的环境。

但是, 对于大规模部署以及需要每用户属性的情况下, 仍建议使用外部AAA服务器进行身份验证和授权。

AnyConnect-EAP实施允许使用Radius进行远程身份验证、授权和记帐。


## 网络图



## 配置

使用本地数据库对用户进行身份验证和授权

---

 注: 要根据路由器上的本地数据库对用户进行身份验证, 需要使用EAP。但是, 要使用EAP, 本地身份验证方法必须是rsa-sig, 因此路由器需要安装适当的证书, 并且它不能是自签名证书。

---

使用本地用户身份验证、远程用户和组授权以及远程记帐的示例配置。

步骤1:启用AAA，配置身份验证、授权和记账列表并将用户名添加到本地数据库：

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

第二步：配置用于持有路由器证书的信任点。本示例中使用PKCS12文件导入。有关其他选项，请参阅PKI(Public Key Infrastructure)配置指南：

[https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec\\_conn\\_pki/configuration/xs-3s/sec-pki-xe-3s-book/sec-cert-enroll-pki.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/xs-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
```

第三步：定义IP本地池以向AnyConnect VPN客户端分配地址：

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


第四步：创建IKEv2本地授权策略：

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

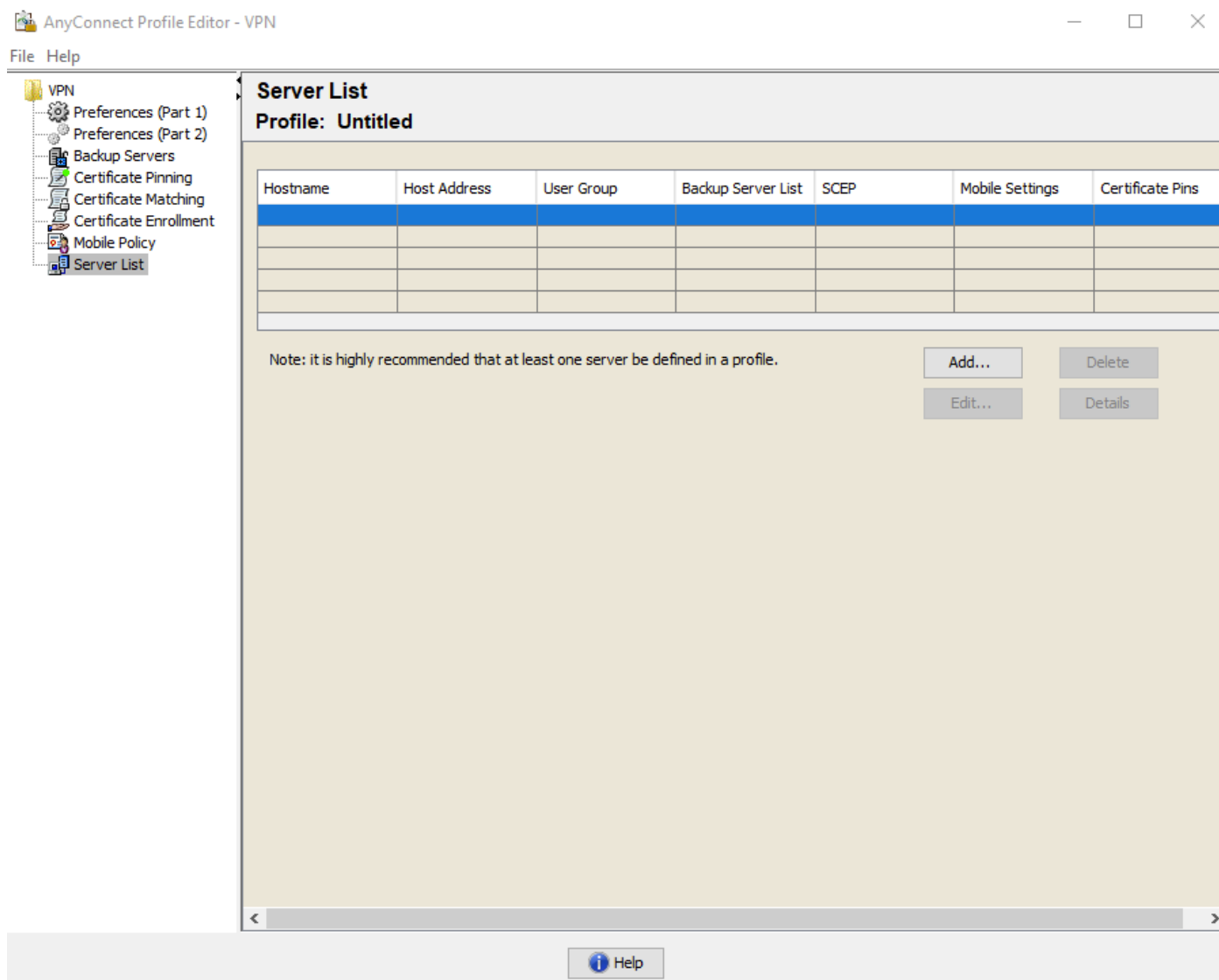
第5步（可选）：创建所需的IKEv2建议和策略。如果未配置，则使用智能默认值：

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

## 第六步：创建AnyConnect配置文件

 **注意：** AnyConnect配置文件需要传送到客户端计算机。有关详细信息，请参阅下一节。

使用AnyConnect配置文件编辑器配置客户端配置文件，如图所示：



点击“Add”为VPN网关创建条目。确保选择“IPsec”作为“主协议”。取消选中“ASA网关”选项。

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"/>

保存配置文件：文件 —>另存为。配置文件的XML等效项：


```
<?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>

```

---

 **注意：** AnyConnect使用“\*\$AnyConnectClient\$\*”作为其类型为key-id的默认IKE标识。但是，可以在AnyConnect配置文件中手动更改此标识以满足部署需求。

---

 **注意：** 要将XML配置文件上传到路由器，需要Cisco IOS® XE 16.9.1版或更高版本。如果使用的是旧版本Cisco IOS® XE软件，则需要在客户端上禁用配置文件下载功能。有关详细信息，请参阅“禁用AnyConnect下载程序功能”部分。

---

将创建的XML配置文件上传到路由器的闪存并定义配置文件：

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

---

 **注：** 用于AnyConnect XML配置文件的文件名为acvpn.xml。

---

步骤 7.为AnyConnect-EAP客户端身份验证方法创建IKEv2配置文件。


```

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
```

---

 **注意：**CLI接受本地身份验证方法之前的远程身份验证方法配置。但是，如果远程身份验证方法是eap，则对于没有增强请求Cisco bug ID [CSCvb29701](#)的修复程序的版本不会生效。对于这些版本，当eap配置为远程身份验证方法时，请确保首先将本地身份验证方法配置为rsa-sig。任何其他形式的远程身份验证方法均未出现此问题。

---

 **注：**在受Cisco bug ID [CSCvb24236](#)（仅限注册用户）影响的代码版本上，一旦在本地身份验证之前配置了远程身份验证，则无法再在该设备上配置远程身份验证方法。请升级到具有此代码的修复程序的版本。

---

步骤 8在路由器上禁用基于HTTP-URL的证书查找和HTTP服务器：

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

---

 **注：**请参阅本文档以确认您的路由器硬件是否支持NGE加密算法（上一个示例包含NGE算法），否则，在协商的最后阶段，硬件上的IPSec SA安装将失败。

---

步骤 9定义用于保护数据的加密和哈希算法

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

步骤 10创建IPSec配置文件：

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

步骤 11使用某些虚构IP地址配置环回接口。虚拟访问接口从它借用IP地址。

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

## 步骤 12配置虚拟模板 ( 关联IKEv2配置文件中的模板 )

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

Step 13 ( 可选 )。默认情况下，来自客户端的所有流量通过隧道发送。您可以配置拆分隧道，只允许选定的流量通过隧道。

```
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
```

第 14 步 ( 可选 )：如果所有流量都需要通过隧道，请配置NAT以允许远程客户端的Internet连接。

```
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
```

## 禁用AnyConnect下载程序功能 ( 可选 )。

仅当使用Cisco IOS® XE软件版本低于16.9.1时，才需要执行此步骤。在Cisco IOS® XE 16.9.1之前，无法将XML配置文件上传到路由器。默认情况下，AnyConnect客户端在成功登录后尝试下载XML配置文件。如果配置文件不可用，则连接失败。作为解决方法，可以在客户端本身上禁用AnyConnect配置文件下载功能。为此，可以修改此文件：

For Windows:

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



For MAC OS:

/opt/cisco/anyconnect/AnyConnectLocalPolicy.xml

“BypassDownloader”选项设置为“true”，例如：

```
<?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>
```

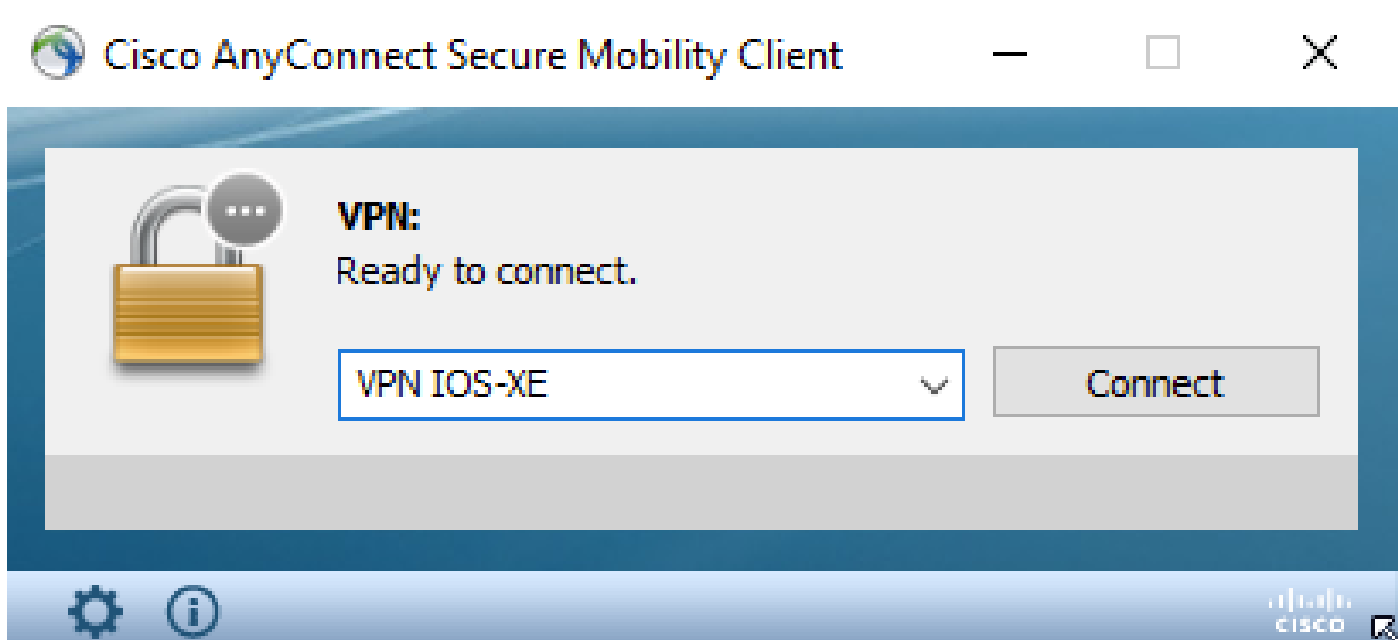
修改后，需要重新启动AnyConnect客户端。

## AnyConnect XML配置文件交付

通过全新安装AnyConnect（未添加XML配置文件），用户可以在AnyConnect客户端的地址栏中手动输入VPN网关的FQDN。这会导致与网关的SSL连接。默认情况下，AnyConnect客户端不会尝试使用IKEv2/IPsec协议建立VPN隧道。这就是客户端上必须安装XML配置文件才能建立与Cisco IOS® XE VPN网关的IKEv2/IPsec隧道的原因。

从AnyConnect地址栏的下拉列表中选择配置文件时，会使用该配置文件。

显示的名称与AnyConnect配置文件编辑器中“显示名称”中指定的名称相同。



可以将XML配置文件手动放入此目录：

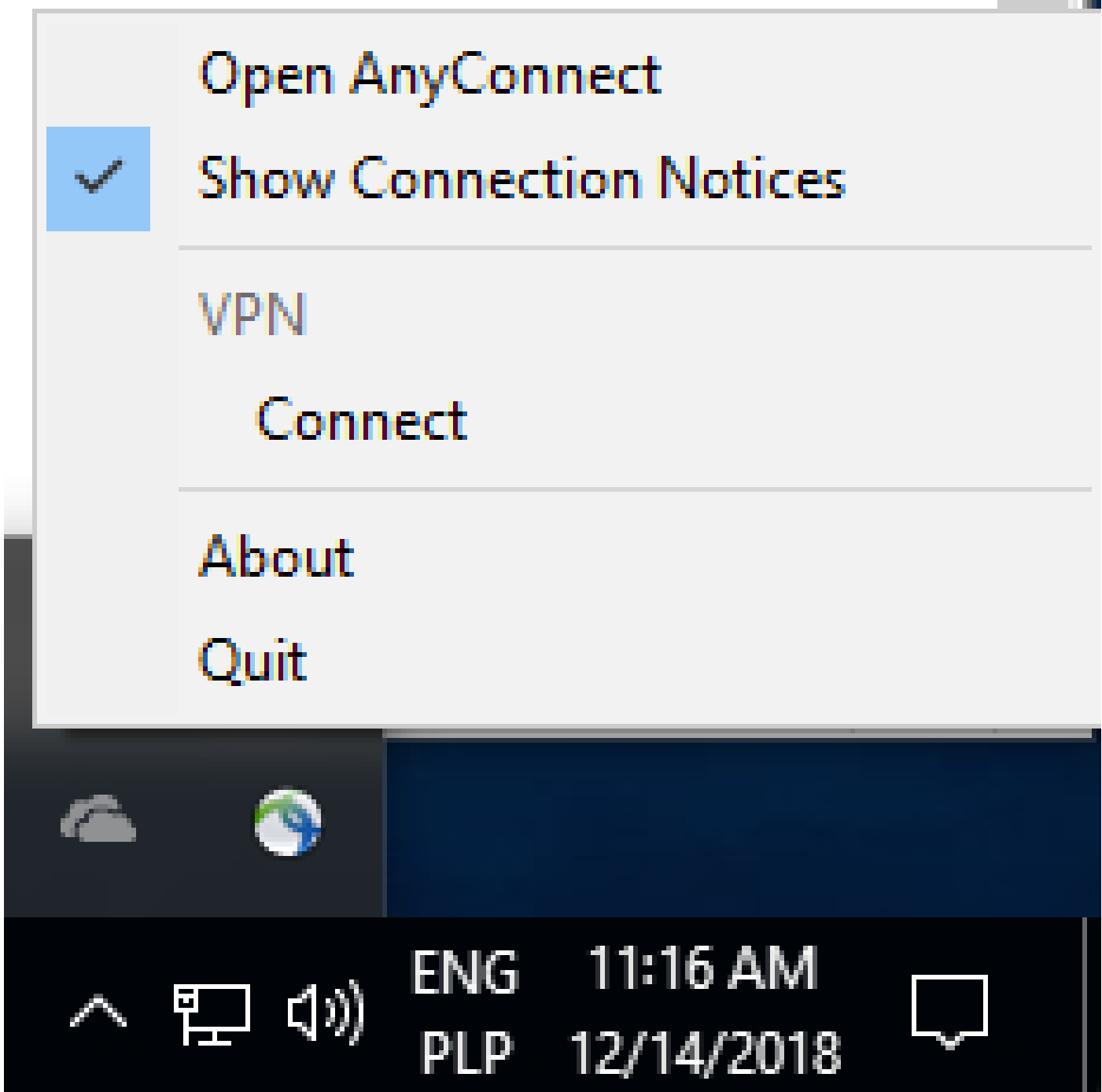
For Windows:

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

For MAC OS:

/opt/cisco/anyconnect/profile

AnyConnect客户端需要重新启动，才能在GUI中看到配置文件。关闭AnyConnect窗口是不够的。可通过右键单击Windows托盘中的AnyConnect图标并选择“退出”选项重新启动该进程：



通信流

IKEv2和EAP交换

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

## 故障排除

本部分提供了可用于对配置进行故障排除的信息。

1. 要从头端收集的IKEv2调试：

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

2. AAA调试，以查看本地和/或远程属性的分配：

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

3. AnyConnect客户端的DART。

## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。