FlexVPN ：与本地用户数据库的AnyConnect IKEv2远程访问

Contents

Introduction

本文提供配置示例如何配置远程访问的IOS/IOS-XE数据转发器使用AnyConnect IKEv2和AnyConnect EAP认证方法本地用户数据库。

Prerequisites

Requirements

Cisco 建议您了解以下主题：

- IKEv2协议

Components Used

本文档中的信息基于以下软件和硬件版本：

- Cisco Cloud服务运行IOS XE 16.9.2的路由器
- 运行在Windows 10的AnyConnect客户端版本4.6.03049

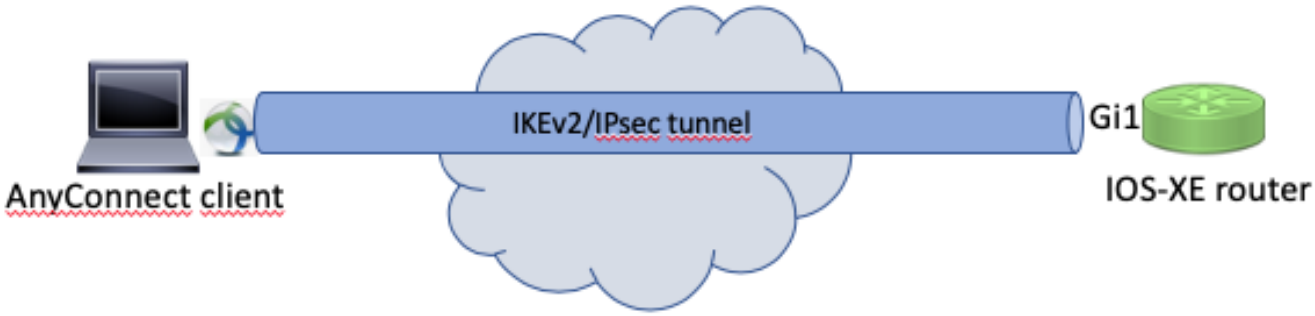
The information in this document was created from the devices in a specific lab environment.All of the devices used in this document started with a cleared (default) configuration.If your network is live, make sure that you understand the potential impact of any command.

背景信息

AnyConnect EAP，亦称聚集认证，允许弹性服务器验证使用Cisco所有权AnyConnect EAP方法的AnyConnect客户端。不同于标准的基于可扩展的认证协议(EAP)方法例如EAP通用的令牌卡(EAP-GTC)，消息摘要5 (EAP-MD5)等，弹性服务器在EAP直通模式下不运行。与客户端的所有EAP通信在弹性服务器终止，并且修建AUTH有效载荷弹性服务器计算用于的必需的会议密钥本地。**弹性服务器必须验证自己对使用证书的客户端据IKEv2 RFC要求。**

弹性服务器现在支持本地用户认证，并且远程验证是可选的。这对与远程访问用户的较少编号的小规模配置是理想的和在环境里没有对一个外部验证、授权和统计(AAA)服务器的访问。然而，对于大规模部署和在每个用户的属性希望的方案仍然推荐使用外部AAA为认证和授权切断。AnyConnect EAP实施允许使用远程验证、授权和记帐的Radius。

Network Diagram



Configure

使用本地数据库的验证和Authorizating用户

> **Note**:为了利用在路由器的本地数据库验证用户，需要使用EAP。然而，为了使用EAP，本地认证方法必须是rsa-sig，因此路由器需要对此安装的一个适当的认证，并且它不可以是自签证书。

步骤1. Enable (event) AAA，和配置认证、授权和记帐列表并且添加用户名到本地数据库：

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

步骤2.配置将有路由器认证的一信任点。PKCS12文件导入用于此示例。对于其它选项，请参见PKI(公共钥匙结构)配置指南：

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
```

步骤3.定义一Ip local pool分配地址到AnyConnect VPN客户端：

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

步骤4.创建一个IKEv2本地授权策略：

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

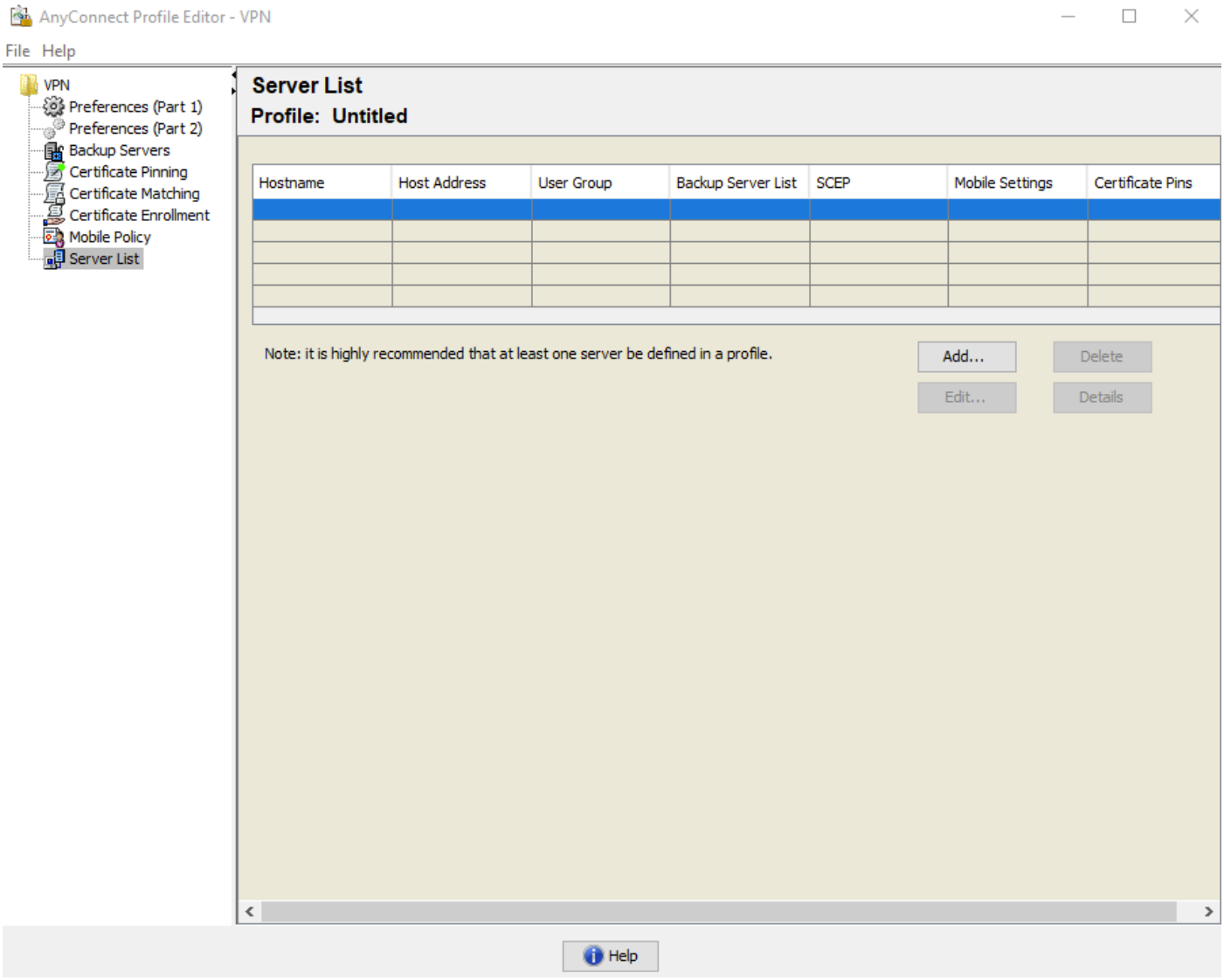
第5步(可选)。create希望IKEv2建议和策略。如果没配置，将使用聪明的默认值：

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

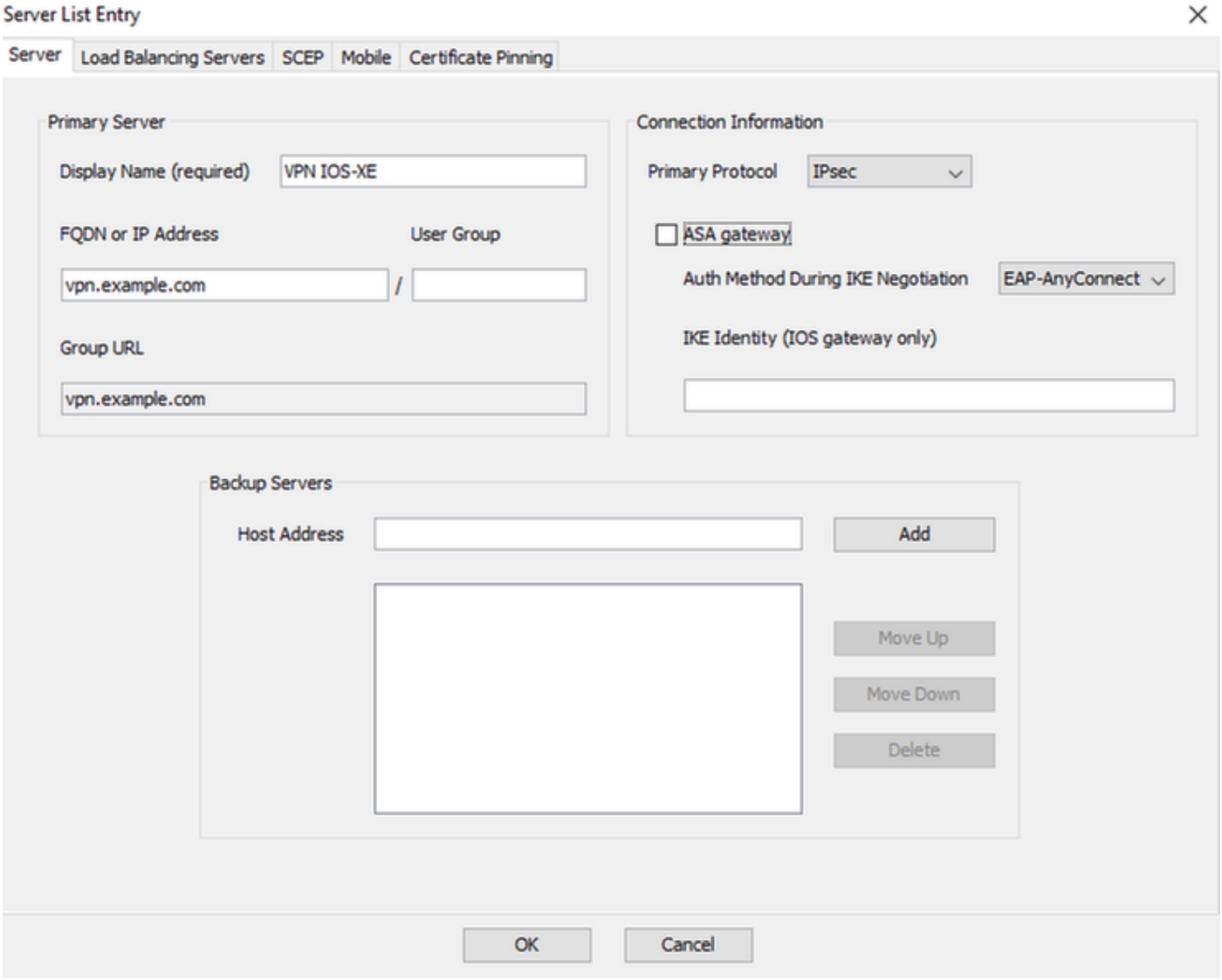
步骤6.创建AnyConnect配置文件

Note:AnyConnect配置文件需要被提供到客户端机器。请参见下个部分欲知更多信息。

如镜像所显示，配置客户端配置文件使用AnyConnect配置文件编辑器：



点击"Add"创建VPN网关的一个条目。保证选择"IPsec"作为“主要的协议”。不选定“ASA网关”选项。



通过去保存配置文件File->Save As。配置文件的XML等同：

```
<?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使用‘*$AnyConnectClient$*’作为其类型密钥ID的默认IKE身份。然而，此身份在AnyConnect配置文件可以手工更改匹配配置需要。

Note:为了加载XML配置文件到路由器，版本或以上需要IOS-XE 16.9.1。如果使用IOS-XE软件早版本，配置文件下载功能在客户端需要被禁用。请参见“禁用AnyConnect下载者功能”欲知更多信息的部分。

加载被创建的XML配置文件到路由器的闪存并且定义配置文件：

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

Note:用于AnyConnect XML配置文件的文件名应该是acvpn.xml。

步骤7.创建客户端验证AnyConnect EAP方法的一个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
```

Note:配置远程验证方法，在本地认证方法将由CLI前接受，但是不会生效对没有增强请求的CSCvb29701修正的版本的，如果远程验证方法是eap。对于这些版本，当配置eap作为远程验证方法时，请保证本地认证方法首先被配置作为rsa-sig。此问题没有在远程验证方法的其他表看到。

Note:在CSCvb24236的影响的编码版本，一旦远程验证在本地认证前被配置，远程验证方法在该设备可能不再被配置。请升级到有此代码的修正的版本。

步骤8.禁用HTTP-URL基于认证查找和HTTP服务器在路由器：

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

Note:*参考*本文确认您的路由器硬件是否支持NGE加密算法(例如的上面的例子有NGE算法)。否则硬件的SA IPSec安装失效在协商最后阶段。

步骤9.定义用于的加密和Hash算法保护数据

```
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.用某个假的IP地址配置一个环回接口。虚拟访问接口从它将借用IP地址。

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

步骤12。配置一个虚拟模板(请关联在IKEv2配置文件的模板)

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

Steap 13 (可选)。默认情况下，从客户端的所有数据流通过隧道将被发送。您能配置分割隧道，允许仅所选的数据流通过隧道。

```
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
```

步骤14 (可选)。如果要求所有数据流通过隧道，您可以配置NAT为了允许远程客户端的互联网连通性。

```
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下载者功能(可选)。

此步骤只是必要的比16.9.1是否使用旧IOS-XE软件版本。在IOS-XE 16.9.1之前加载XML配置文件的功能到路由器不是可用的。默认情况下AnyConnect客户端设法在成功的登录以后执行XML配置文件的下载。如果配置文件不是可用的，连接发生故障。作为解决方法，禁用在客户端的AnyConnect配置文件下载功能是可能的。为了执行那，可以修改以下文件：

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

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

应该设置例如“BypassDownloader”选项到“真”， ：

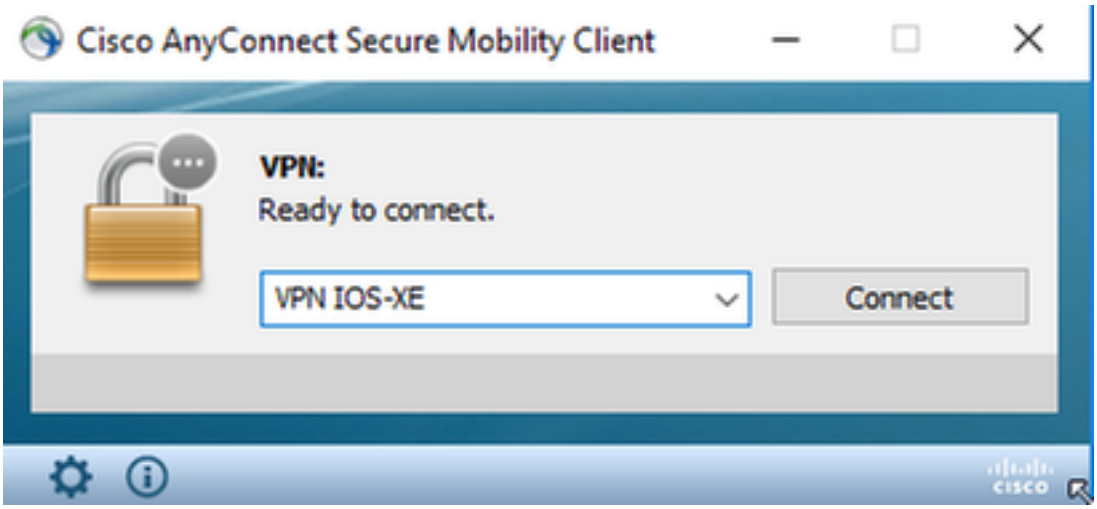
```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectLocalPolicy xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectLocalPolicy.xsd"
acversion="4.6.03049">
<BypassDownloader>true</BypassDownloader>
<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>
```

在修改以后， AnyConnect客户端需要被重新启动。

AnyConnect XML配置文件发运

使用AnyConnect的新安装(没有被添加的XML配置文件)，用户能手工输入VPN网关的FQDN在AnyConnect客户端地址栏。这导致与网关的SSL连接。默认情况下AnyConnect客户端不会尝试设立有IKEv2/IPsec协议的VPN隧道。这是原因为什么有在客户端上安装的XML配置文件是必须设立IKEv2/IPsec隧道用IOS-XE VPN网关。

配置文件，当从AnyConnect地址栏下拉列表时，被挑选使用。将出现的名字是同一个名字在“显示名字上指定”在AnyConnect配置文件编辑器。在本例中用户应该选择以下：

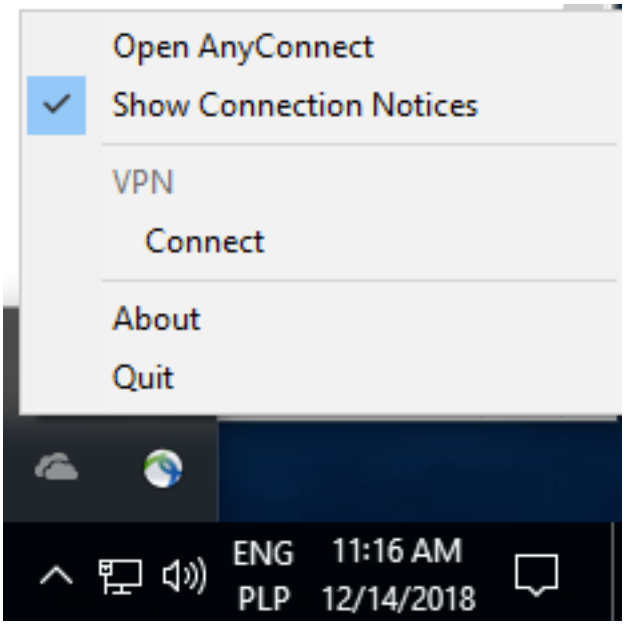


XML配置文件可以手工被放到以下目录：

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

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

AnyConnect客户端需要被重新启动为了配置文件能变得可视在GUI。关上AnyConnect窗口是不满足的。进程在Windows盘上可以通过用鼠标右键单击AnyConnect图标和选择"Quit"选项重新启动：



通信流

IKEv2和EAP交换