使用本地使用者資料庫為安全客戶端(AnyConnect)IKEv2遠端訪問配置FlexVPN頭端

目錄

[簡介](#)

[必要條件](#)

- [需求](#)
- [採用元件](#)

[背景資訊](#)

[網路圖表](#)

[設定](#)

- [使用本地資料庫對使用者進行身份驗證和授權](#)
- [範例：AnyConnect配置檔案下載配置](#)
- [禁用AnyConnect下載程式功能（僅適用於16.9.1以前的版本）。](#)
- [AnyConnect XML配置檔案交付](#)

[通訊流](#)

- [IKEv2和EAP交換](#)

[驗證](#)

[疑難排解](#)

簡介

本文檔介紹如何配置FlexVPN頭端以通過本地使用者資料庫的安全客戶端(AnyConnect)IKEv2/EAP身份驗證進行訪問。

必要條件

需求

思科建議您瞭解以下主題：

- IKEv2通訊協定

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 雲端服務路由器版本16.9.2
- 在Windows 10上運行的AnyConnect客戶030494.6.1版

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設

）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

AnyConnect-EAP或聚合身份驗證允許FlexVPN伺服器通過Cisco專有AnyConnect-EAP方法對AnyConnect客戶端進行身份驗證。

與基於標準的可擴展身份驗證協定(EAP)方法(例如EAP — 通用令牌卡(EAP-GTC)、EAP — 消息摘要5(EAP-MD5)不同，FlexVPN伺服器不以EAP直通模式運行。

與客戶端的所有EAP通訊在FlexVPN伺服器上終止，用於構建AUTH負載的所需會話金鑰由FlexVPN伺服器本地計算。

FlexVPN伺服器必須使用IKEv2 RFC要求的證書向客戶端驗證其自身。

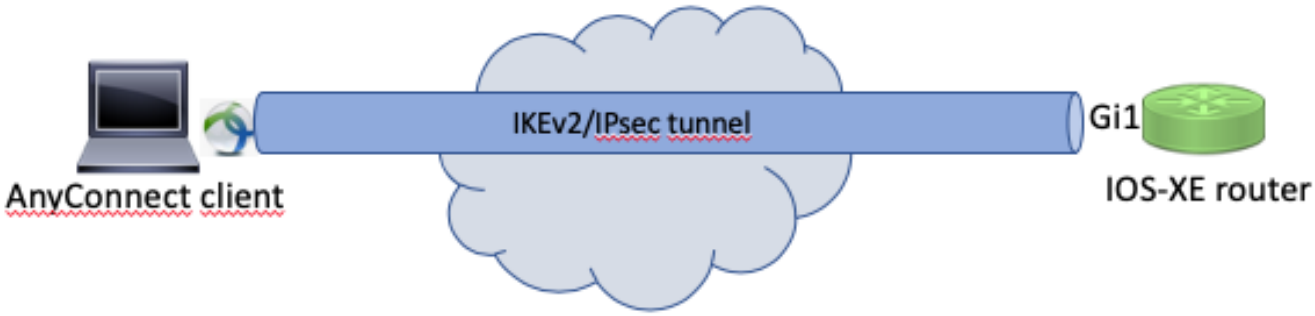
Flex Server現在支援本地使用者身份驗證，並且遠端身份驗證是可選的。

這非常適合於遠端訪問使用者較少的小型部署以及無法訪問外部身份驗證、授權和記帳(AAA)伺服器的環境。

但是，對於大規模部署以及需要每個使用者屬性的情況下，仍建議使用外部AAA伺服器進行身份驗證和授權。

AnyConnect-EAP實施允許使用Radius進行遠端身份驗證、授權和記帳。

網路圖表



設定

使用本地資料庫對使用者進行身份驗證和授權

附註：要根據路由器上的本地資料庫對使用者進行身份驗證，需要使用EAP。但是，要使用EAP，本地身份驗證方法必須是rsa-sig，因此路由器需要正確的身份證書，並且不能使用自簽名證書。

使用本地使用者身份驗證、遠端使用者和組授權以及遠端記帳的示例配置。

步驟1.啟用AAA，配置身份驗證、授權和記帳清單並將使用者名稱新增到本地資料庫：

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

步驟2.配置用於儲存路由器證書的信任點。本示例中使用PKCS12檔案匯入。有關其他選項，請參閱安全和VPN配置指南，IOS XE 17.x，章節：為PKI文檔配置證書註冊。

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

步驟3.定義IP本地池以向AnyConnect VPN客戶端分配地址：

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

步驟4.建立IKEv2本地授權策略：

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

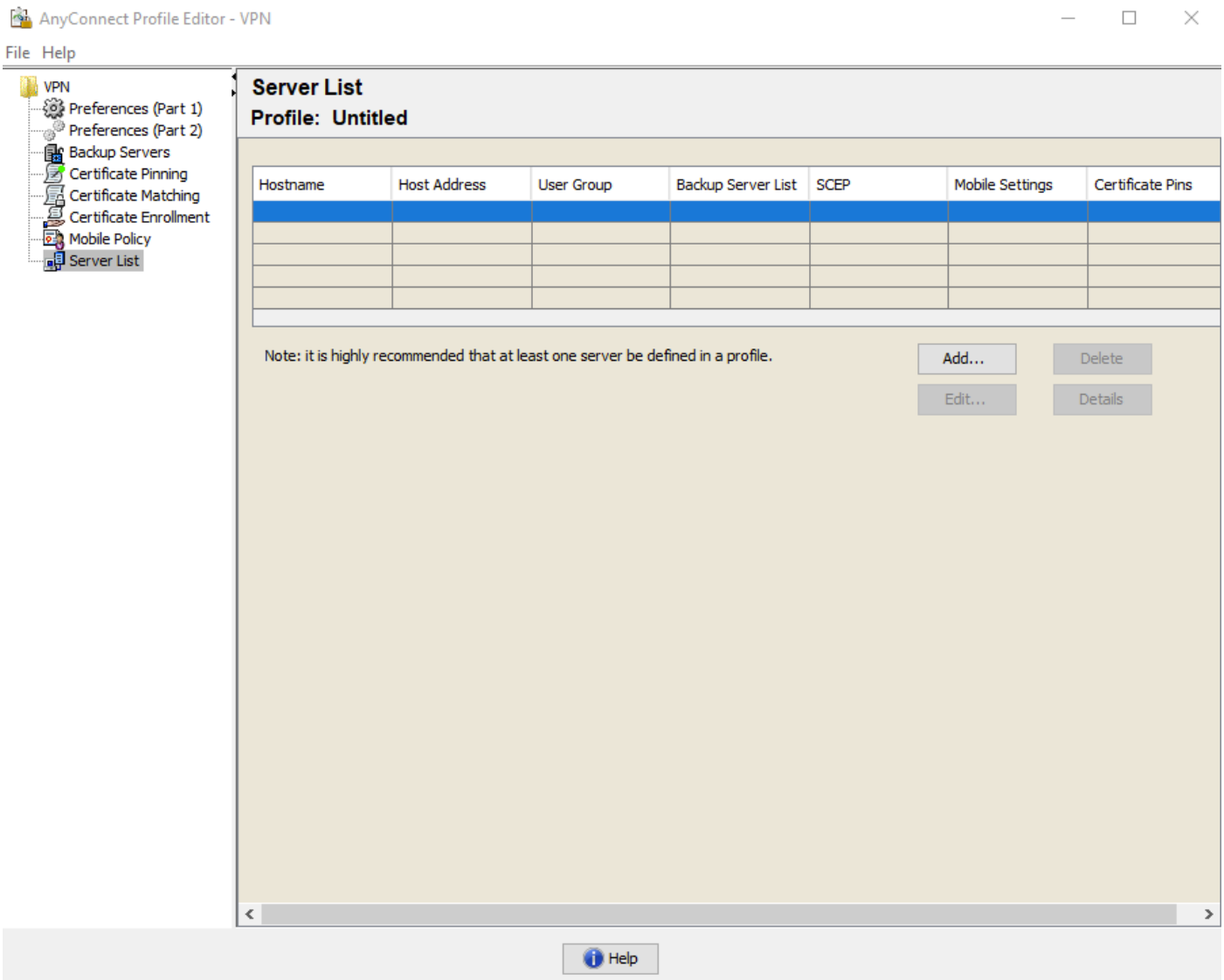
第5步（可選）。 建立所需的IKEv2建議和策略。如果未配置，則使用智慧預設值：

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

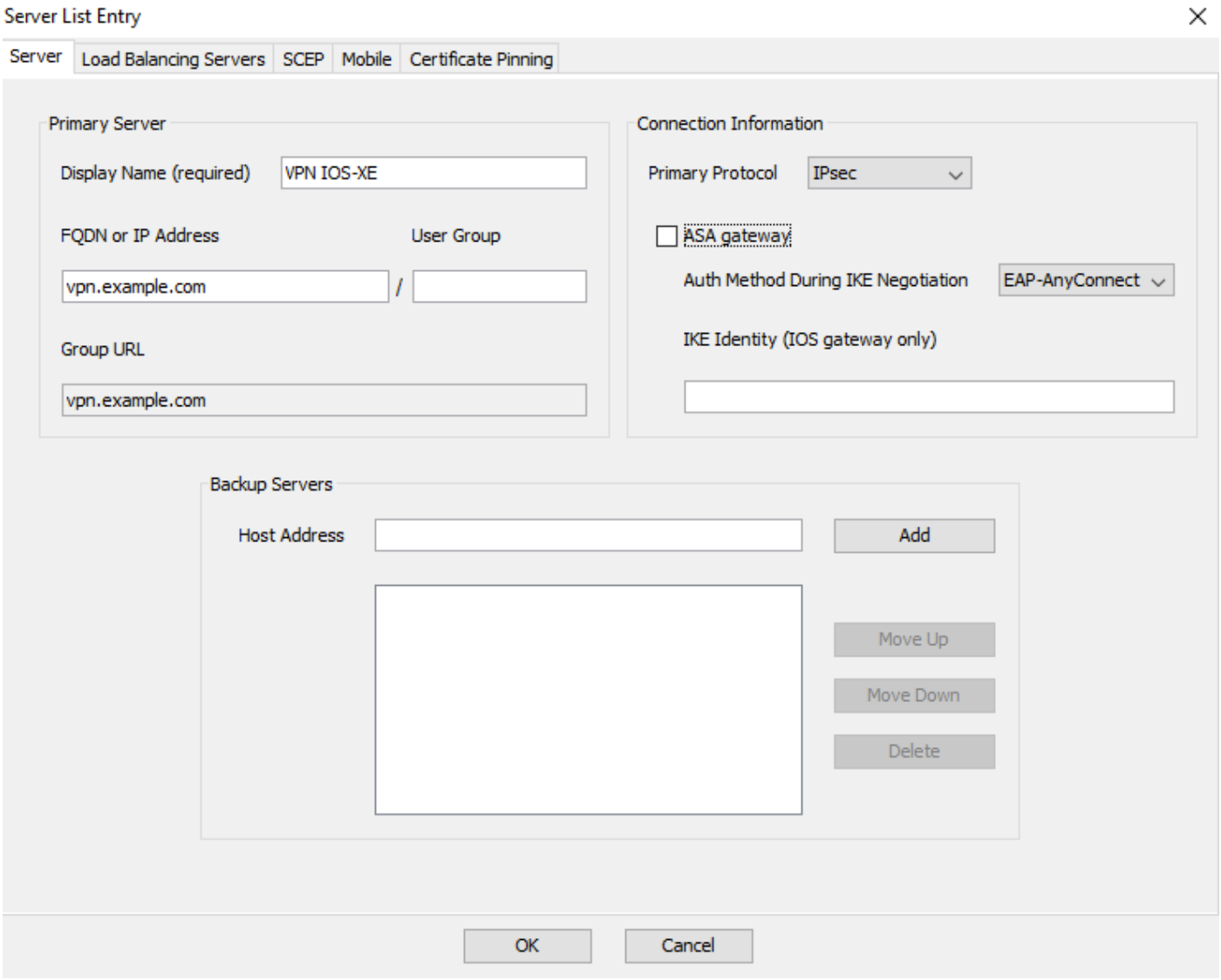
步驟6.建立AnyConnect配置檔案

附註：需要將AnyConnect配置檔案傳送到客戶端電腦。有關詳細資訊，請參閱下一節。

使用AnyConnect配置檔案編輯器配置客戶端配置檔案，如下圖所示：



按一下Add為VPN網關建立條目。確保選擇IPsec作為Primary Protocol。取消選中ASA網關選項。



儲存配置檔案：檔案 — >另存為。配置檔案的XML等效項：

```
<?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>
```

附註：AnyConnect使用*$AnyConnectClient$*作為key-id型別的預設IKE標識。但是，可以在AnyConnect配置檔案中手動更改此標識以滿足部署需求。

附註：要將XML配置檔案上傳到路由器，需要16.9.1版或更高版本。如果使用的是較舊的軟體版本，需要在客戶端上禁用配置檔案下載功能。有關詳細資訊，請參閱禁用AnyConnect下載程式功能部分。

將建立的XML配置檔案上傳到路由器的快閃記憶體並定義配置檔案：

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

附註：用於AnyConnect XML配置檔案的檔名始終為acvpn.xml。即使使用其他檔名，傳送到PC的配置檔案也命名為acvpn.xml。因此，建議不要更改路由器配置中的名稱。

步驟7.為AnyConnect-EAP客戶端身份驗證方法建立IKEv2配置檔案。

```
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
```

附註：對於aaa authentication eap/anyconnect-eap命令，確保在配置遠端身份驗證方法之前，將本地身份驗證方法配置為rsa-sig。

步驟8.在路由器上禁用基於HTTP-URL的證書查詢和HTTP伺服器：

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

附註：請參閱下一代加密支援文檔以確認您的路由器硬體是否支援NGE演算法（例如sha-256、aes-gcm、ecdh、ecdsa），否則，在硬體上安裝IPSec SA會在隧道建立的最後階段失敗。

步驟9.定義用於保護資料的加密和雜湊演算法

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

步驟10.建立IPSec配置檔案：

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

步驟11.使用某個虛擬IP地址配置環回介面。虛擬訪問介面從它借用IP地址。

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

步驟12.配置虛擬模板（關聯IKEv2配置檔案中的模板）

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

第13步（可選）。 預設情況下，來自使用者端的所有流量都會透過通道（全通道）傳送。 您可以配置拆分隧道，僅允許所選流量通過該隧道。

```
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（可選）。 如果所有流量都需要通過隧道，請配置NAT以允許遠端客戶端的Internet連線。

```
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
```

範例：AnyConnect配置檔案下載配置

此示例說明如何配置FlexVPN AnyConnect配置檔案下載功能：

附註：您無需修改Anyconnect客戶端電腦上的本地策略檔案。配置IKEv2的Anyconnect配置檔案下載功能後，VPN下載程式模組工作正常 — 在進行XML配置檔案更新時，客戶端裝置上會自動更新所需的XML配置檔案。

附註：不能同時使用HTTPS伺服器和SSL策略。啟用SSL策略之前，請刪除ip http secure-server命令。如果同時啟用這兩個功能，並且裝置收到傳入的SSL VPN連線，則裝置可能會崩潰。

```
no ip http secure-server
crypto ssl policy ssl-policy
  pki trustpoint IKEv2-TP sign
  ip address local 10.0.0.1 port 443
  no shutdown
crypto ssl profile ssl_prof
    match policy ssl-policy
```

禁用AnyConnect下載程式功能（僅適用於16.9.1以前的版本）。

只有在使用低於16.9.1的版本時，才需要執行此步驟。在此版本之前，無法將XML配置檔案上傳到路由器。預設情況下，成功登入後，安全客戶端(AnyConnect)會嘗試下載XML配置檔案。如果配置檔案不可用，連線將失敗。作為解決方法，可以在客戶端本身上禁用AnyConnect配置檔案下載功能。為此，可以修改此檔案：

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

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

BypassDownloader選項設定為true，例如：

<#root>

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

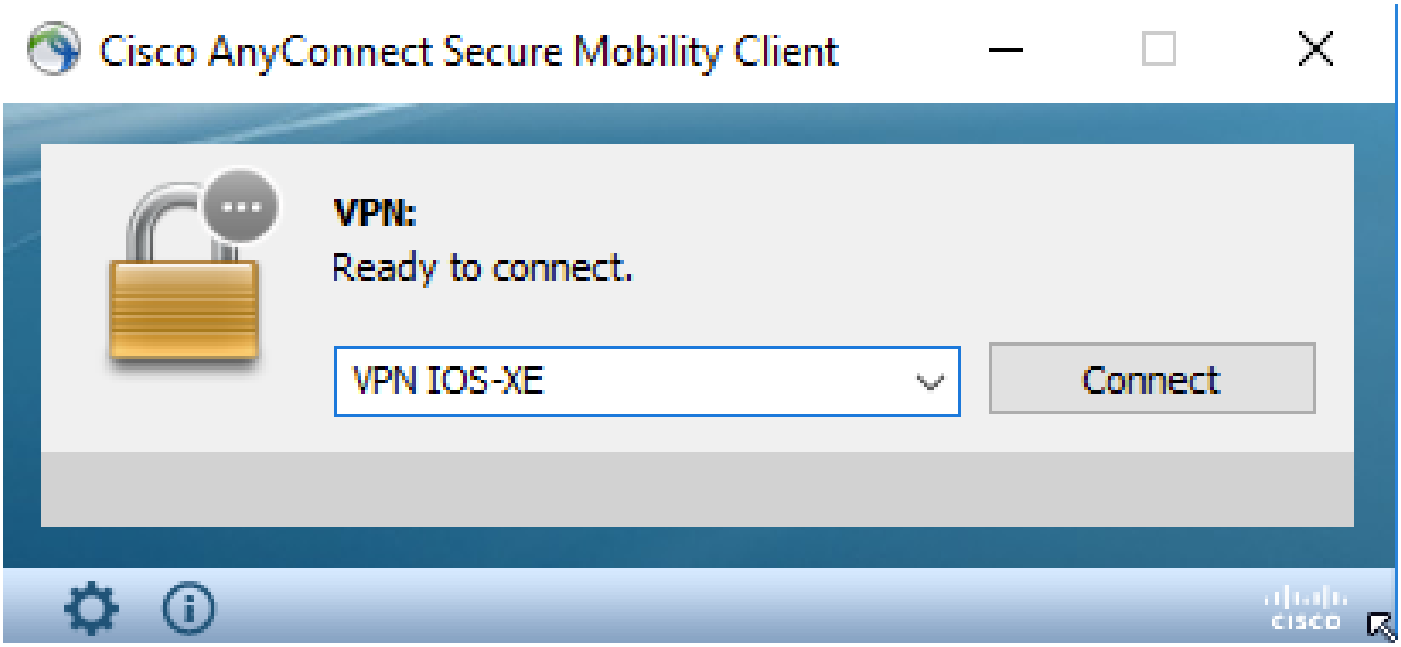
修改完成後，需要重新啟動AnyConnect客戶端。

AnyConnect XML配置檔案交付

通過全新安裝AnyConnect（未新增XML配置檔案），使用者可以在AnyConnect客戶端的位址列中手動輸入VPN網關的FQDN。這會導致到網關的SSL連線。預設情況下，AnyConnect客戶端不會嘗試使用IKEv2/IPsec協定建立VPN隧道。這就是客戶端PC上必須安裝XML配置檔案才能與FlexVPN網關建立IKEv2/IPsec隧道的原因。

從AnyConnect位址列的下拉選單中選擇配置檔案時，將使用該配置檔案。

在AnyConnect Profile Editor -> Server List -> Server List Entry的Display Name欄位中指定清單上顯示的名稱。

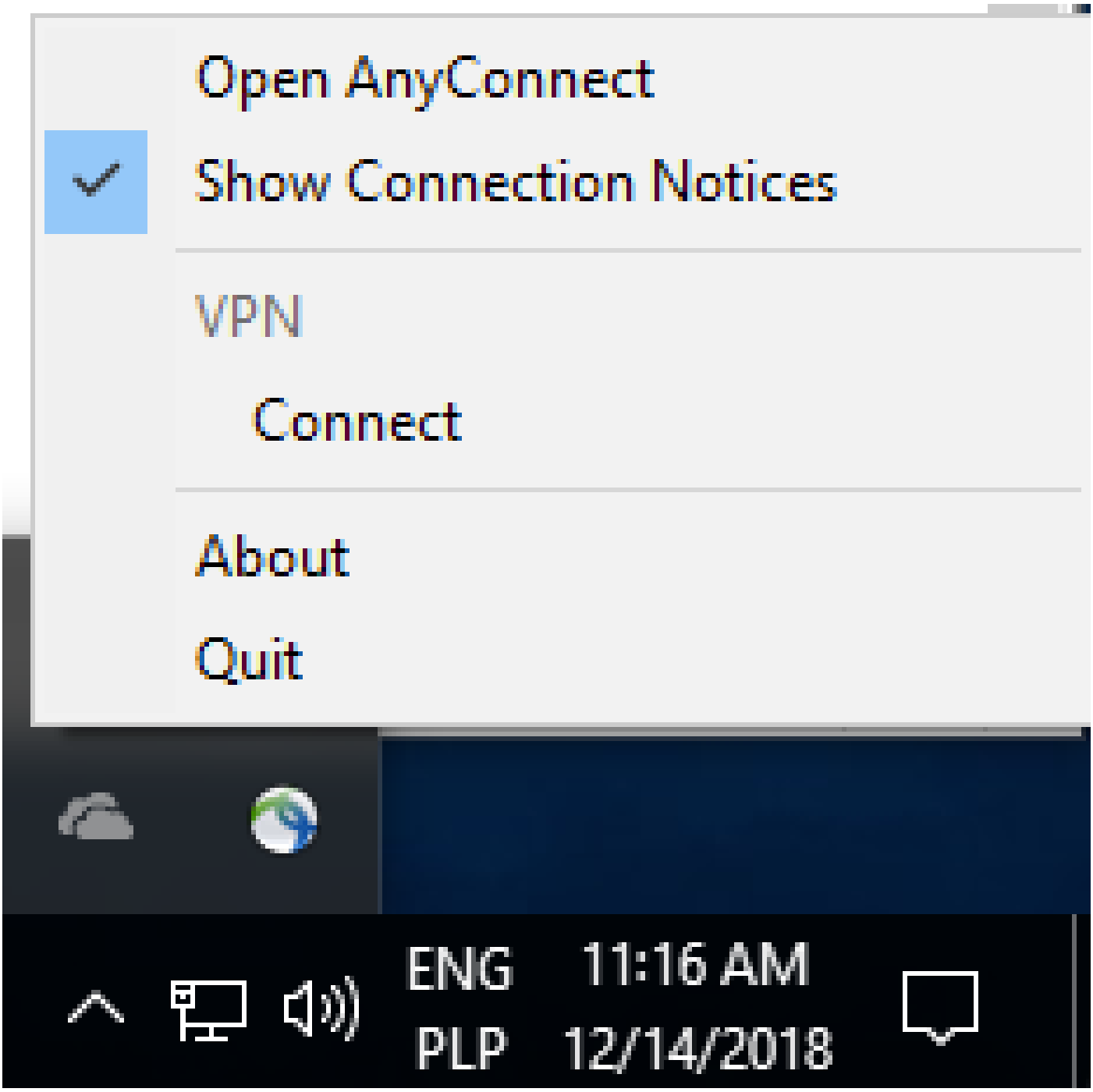


根據客戶端作業系統，可以將XML配置檔案手動放入目錄：

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

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

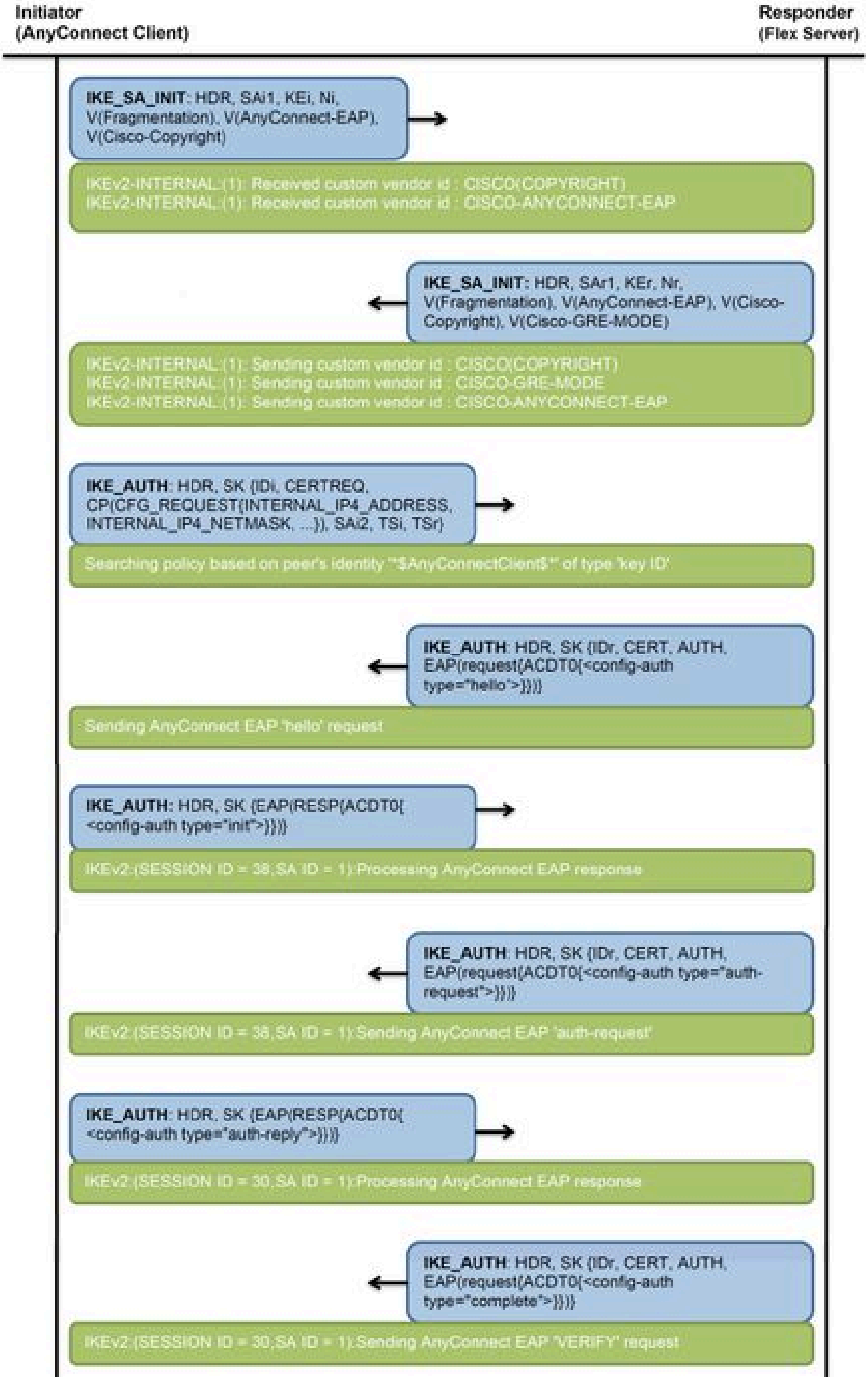
AnyConnect客戶端需要重新啟動，才能在GUI中看到配置檔案。關閉AnyConnect視窗是不夠的。可通過按一下右鍵Windows工作列中的AnyConnect圖示並選擇Quit選項來重新啟動進程：



通訊流

點選此處

IKEv2和EAP交換


Initiator
(AnyConnect Client)
Responder
(Flex Server)
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(RESP{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(RESP{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                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: 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-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
```

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

1. 要從頭端收集的IKEv2調試：

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

2. AAA調試以檢視本地和/或遠端屬性的分配：

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

3. AnyConnect客戶端的診斷和報告工具(DART)。
   要收集DART捆綁包，請執行Cisco Secure Client（包括AnyConnect）管理員指南，版本5，章節：章節：思科安全使用者端疑難排解檔案。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。