

Configurazione dell'headend FlexVPN per l'accesso remoto AnyConnect IKEv2 del client sicuro con il database degli utenti locali

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Esempio di rete](#)

[Configurazione](#)

[Autenticazione e autorizzazione degli utenti con il database locale](#)

[Esempio: configurazione del download dei profili AnyConnect](#)

[Disabilitare la funzionalità AnyConnect Download \(solo per le versioni precedenti alla 16.9.1\).](#)

[Recapito del profilo XML AnyConnect](#)

[Flusso di comunicazione](#)

[Scambio IKEv2 e EAP](#)

[Verifica](#)

[Risoluzione dei problemi](#)

Introduzione

In questo documento viene descritta la configurazione di un headend FlexVPN per l'accesso tramite autenticazione AnyConnect IKEv2/EAP con un database utenti locale.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- protocollo IKEv2

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cloud Services Router versione 16.9.2

- Client AnyConnect versione 4.6.03049 in esecuzione su Windows 10

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

AnyConnect-EAP, o autenticazione aggregata, consente a un server FlexVPN di autenticare il client AnyConnect tramite il metodo AnyConnect-EAP proprietario di Cisco.

A differenza dei metodi EAP (Extensible Authentication Protocol) basati su standard, quali EAP-Generic Token Card (EAP-GTC), EAP-Message Digest 5 (EAP-MD5) e così via, il server FlexVPN non funziona in modalità pass-through EAP.

Tutte le comunicazioni EAP con il client terminano sul server FlexVPN e la chiave di sessione richiesta utilizzata per costruire il payload AUTH viene calcolata localmente dal server FlexVPN.

Il server FlexVPN deve autenticarsi al client con i certificati richiesti dalla RFC IKEv2.

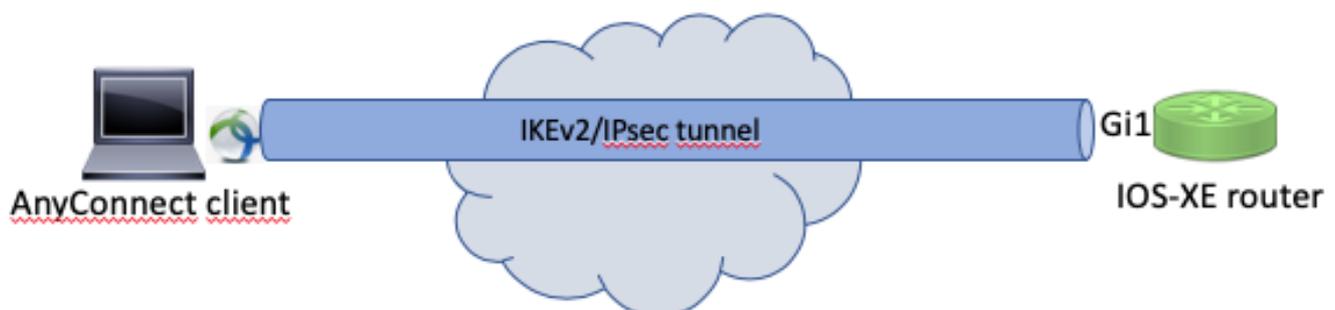
L'autenticazione dell'utente locale è ora supportata sul server Flex e l'autenticazione remota è facoltativa.

Questa soluzione è ideale per le implementazioni su piccola scala con un numero inferiore di utenti e ambienti di accesso remoto senza accesso a un server esterno di autenticazione, autorizzazione e accounting (AAA).

Tuttavia, per implementazioni su larga scala e negli scenari in cui si desidera ottenere gli attributi per utente, si consiglia di utilizzare un server AAA esterno per l'autenticazione e l'autorizzazione.

L'implementazione AnyConnect-EAP consente l'uso di Radius per l'autenticazione, l'autorizzazione e l'accounting remoti.

Esempio di rete



Configurazione

Autenticazione e autorizzazione degli utenti con il database locale

 Nota: per autenticare gli utenti sul database locale sul router, è necessario usare EAP. Tuttavia, per utilizzare EAP, il metodo di autenticazione locale deve essere rsa-sig, quindi il router deve disporre di un certificato di identità valido e non può utilizzare un certificato autofirmato.

Configurazione di esempio che utilizza l'autenticazione degli utenti locali, l'autorizzazione di utenti e gruppi remoti e l'accounting remoto.

Passaggio 1. Abilitare il server AAA, configurare gli elenchi di autenticazione, autorizzazione e accounting e aggiungere un nome utente al database locale:

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

Passaggio 2. Configurare un trust point che contenga il certificato del router. In questo esempio viene utilizzata l'importazione di file PKCS12. Per altre opzioni, consultare la [guida alla configurazione di sicurezza e VPN, IOS XE 17.x, capitolo: Configurazione della registrazione dei certificati per un documento PKI](#).

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

Passaggio 3. Definire un pool locale IP per assegnare gli indirizzi ai client VPN AnyConnect:

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

Passaggio 4. Creare un criterio di autorizzazione locale IKEv2:

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

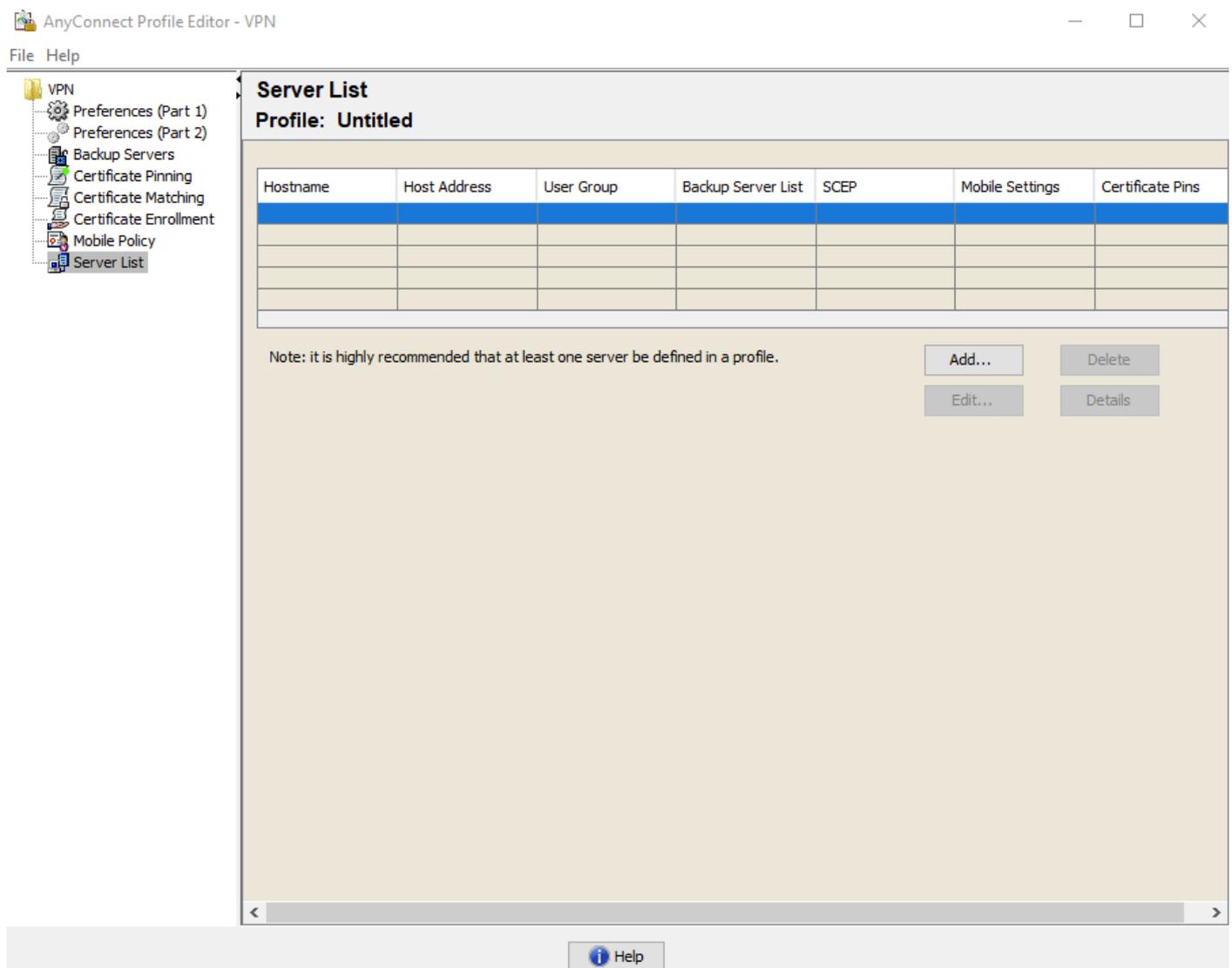
Passaggio 5 (facoltativo). Creare la proposta e il criterio IKEv2 desiderati. Se non configurata, vengono utilizzati i valori predefiniti intelligenti:

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

Passaggio 6. Crea profilo AnyConnect

 Nota: il profilo AnyConnect deve essere consegnato al computer client. Per ulteriori informazioni, consultare la sezione successiva.

Configurare il profilo client con l'Editor di profili AnyConnect, come mostrato nell'immagine:



Fare clic su Add (Aggiungi) per creare una voce per il gateway VPN. Selezionare IPsec come protocollo primario. Deselezionare l'opzione ASA gateway.

Salvare il profilo: File -> Salva con nome. L'equivalente XML del profilo:

```
<?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>
  </ClientInitialization>
</AnyConnectProfile>
```

```

<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>

```

 Nota: AnyConnect utilizza *\$AnyConnectClient\$* come identità IKE predefinita con tipo key-id. Tuttavia, è possibile modificare manualmente l'identità nel profilo AnyConnect in base alle esigenze di distribuzione.

 Nota: per caricare il profilo XML sul router, è necessaria la versione 16.9.1 o successive. Se si utilizza una versione precedente del software, è necessario disabilitare la funzionalità di download del profilo sul client. Per ulteriori informazioni, consultare la sezione Disabilitazione della funzione di download di AnyConnect.

Caricare il profilo XML creato nella memoria flash del router e definire il profilo:

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

 Nota: il nome file usato per il profilo AnyConnect XML è sempre acvpn.xml. Anche se si utilizza un nome di file diverso, il profilo inviato al PC è denominato acvpn.xml. Si consiglia pertanto di non modificare il nome nella configurazione del router.

Passaggio 7. Creare un profilo IKEv2 per il metodo di autenticazione client AnyConnect-EAP.

```
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
```



Nota: per il comando `aaa authentication eap/ anyconnect-eap` verificare che il metodo di autenticazione locale sia configurato come `rsa-sig` prima di configurare il metodo di autenticazione remota.

Passaggio 8. Disabilitare la ricerca dei certificati basata su URL HTTP e il server HTTP sul router:

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



Nota: per verificare se l'hardware del router in uso supporta gli algoritmi NGE (ad esempio sha-256, aes-gcm, ecdh, ecdsa), consultare il documento sul [supporto della crittografia di nuova generazione](#); in caso contrario, l'installazione dell'associazione di protezione IPsec sull'hardware non riesce nell'ultima fase della creazione del tunnel.

Passaggio 9. Definire gli algoritmi di crittografia e hash utilizzati per proteggere i dati

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

Passaggio 10. Creare un profilo IPsec:

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

Passaggio 11. Configurare un'interfaccia di loopback con un indirizzo IP fittizio. Le interfacce di accesso virtuale prendono in prestito l'indirizzo IP da esso.

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

Passaggio 12. Configurare un modello virtuale (associare il modello nel profilo IKEv2)

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

Passaggio 13 (facoltativo). Per impostazione predefinita, tutto il traffico proveniente dal client viene inviato attraverso il tunnel (tunnel completo). È possibile configurare un tunnel suddiviso in modo che solo il traffico selezionato possa passare attraverso il tunnel.

```
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
```

Passaggio 14 (facoltativo). Se tutto il traffico deve passare attraverso il tunnel, configurare NAT in modo da consentire la connettività Internet per i client remoti.

```
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
```

Esempio: configurazione del download dei profili AnyConnect

Nell'esempio viene mostrato come configurare la funzione di download del profilo AnyConnect di

FlexVPN:

 Nota: non è necessario modificare il file dei criteri locali sul computer client Anyconnect. Dopo aver configurato la funzione di download dei profili Anyconnect con IKEv2, il modulo VPN Downloader funziona correttamente - il profilo XML richiesto viene aggiornato automaticamente sul dispositivo client in caso di aggiornamento del profilo XML.

 Nota: non utilizzare il server HTTPS insieme ai criteri SSL. Prima di abilitare il criterio SSL, rimuovere il comando `ip http secure-server`. Se entrambe le funzionalità sono attivate contemporaneamente e il dispositivo riceve una connessione VPN SSL in ingresso, è possibile che si verifichi un arresto anomalo del dispositivo.

```
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
```

Disabilitare la funzionalità AnyConnect Download (solo per le versioni precedenti alla 16.9.1).

Questo passaggio è necessario solo se si utilizza una versione precedente alla 16.9.1. In precedenza, non era possibile caricare il profilo XML sul router. Secure Client (AnyConnect) cerca di eseguire il download del profilo XML dopo aver eseguito l'accesso per impostazione predefinita. Se il profilo non è disponibile, la connessione non riesce. Per risolvere questo problema, è possibile disabilitare la funzionalità di download dei profili AnyConnect sul client stesso. A tale scopo, è possibile modificare il file:

For Windows:

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

For MAC OS:

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

L'opzione `BypassDownloader` è impostata su `true`, ad esempio:

```
<#root>
```

```
<?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>
```

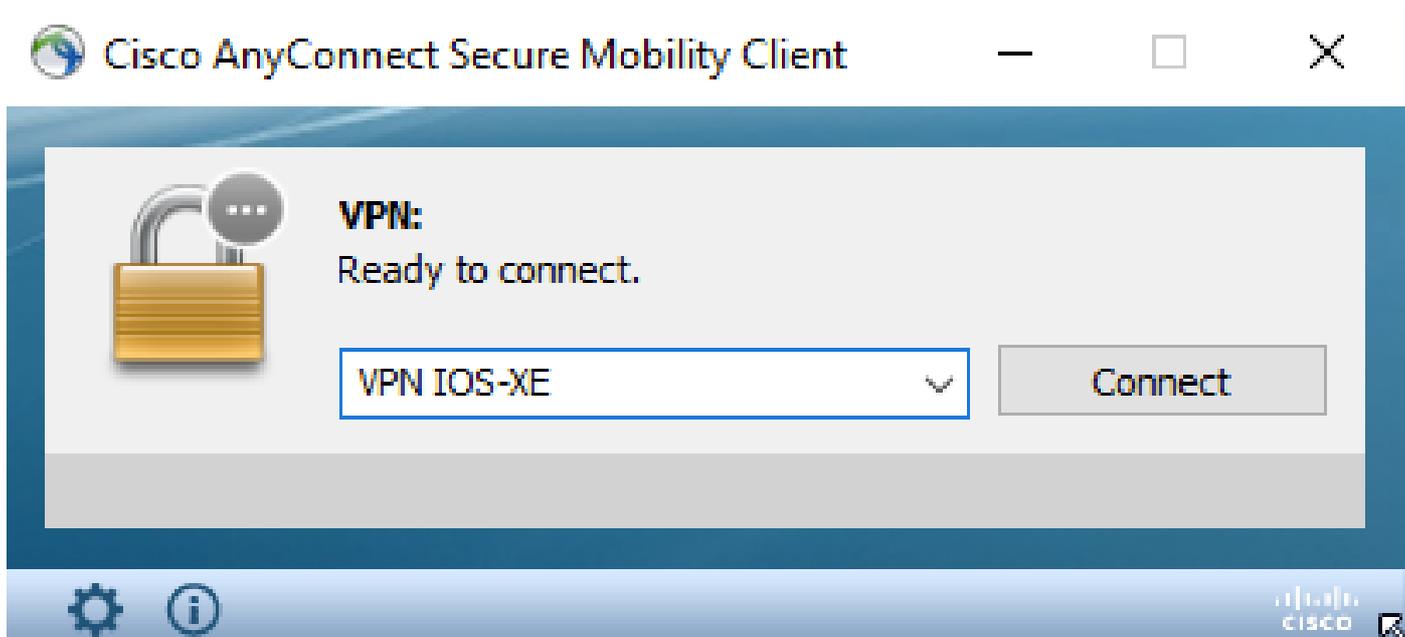
Dopo la modifica, il client AnyConnect deve essere riavviato.

Recapito del profilo XML AnyConnect

Con la nuova installazione di AnyConnect (senza profili XML aggiunti), l'utente può immettere manualmente il nome di dominio completo (FQDN) del gateway VPN nella barra degli indirizzi del client AnyConnect. Il risultato è la connessione SSL al gateway. Per impostazione predefinita, il client AnyConnect non tenta di stabilire il tunnel VPN con i protocolli IKEv2/IPsec. Per questo motivo, l'installazione del profilo XML sul PC client è obbligatoria per stabilire il tunnel IKEv2/IPsec con il gateway FlexVPN.

Il profilo viene usato quando viene selezionato dall'elenco a discesa della barra degli indirizzi di AnyConnect.

Il nome visualizzato nell'elenco è specificato nel campo Display Name (Nome visualizzato) in AnyConnect Profile Editor -> Server List -> Server List Entry (Editor profili AnyConnect -> Elenco server -> Voce elenco server).



Il profilo XML può essere inserito manualmente in una directory, a seconda del sistema operativo del client:

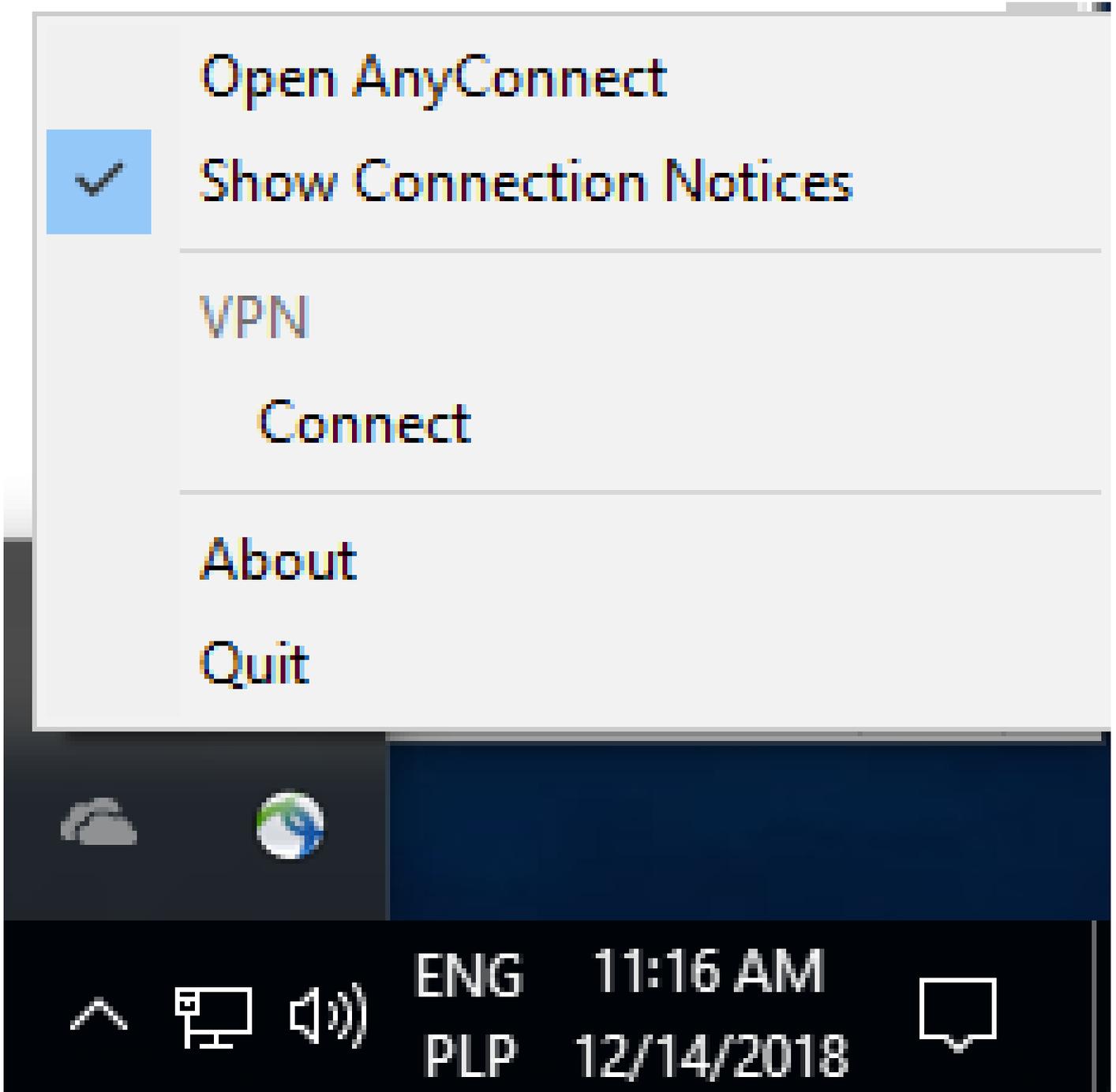
For Windows:

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

For MAC OS:

/opt/cisco/anyconnect/profile

Affinché il profilo sia visibile nella GUI, è necessario riavviare il client AnyConnect. Non è sufficiente chiudere la finestra AnyConnect. Per riavviare il processo, fare clic con il pulsante destro del mouse sull'icona AnyConnect nell'area di notifica di Windows e selezionare l'opzione Quit (Esci):



Flusso di comunicazione

fare clic qui

Scambio 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
```

Risoluzione dei problemi

In questa sezione vengono fornite informazioni utili per risolvere i problemi di configurazione.

1. Debug IKEv2 da raccogliere dall'headend:

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

2. Esegue il debug di AAA per verificare l'assegnazione degli attributi locali e/o remoti:

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

3. Strumento di diagnostica e report (DART) per il client AnyConnect.

Per raccogliere il pacchetto DART, attenersi alla procedura descritta nella [Guida dell'amministratore di Cisco Secure Client \(incluso AnyConnect\), versione 5, capitolo: Risoluzione dei problemi relativi a Cisco Secure Client](#).

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).