FlexVPN configureren: AnyConnect IKEv2 externe toegang met lokale gebruikersdatabase

Inhoud

Inleiding

Dit document beschrijft hoe u een Cisco IOS®/XE-head-end kunt configureren voor toegang via AnyConnect IKEv2/EAP-verificatie met lokale gebruikersdatabase.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- IKEv2-protocol

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Cloud-services router met Cisco IOS® XE 16.9.2
- AnyConnect-clientversie 4.6.03049 onder Windows 10

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

AnyConnect-EAP, ook bekend als aggregaatverificatie, stelt een Flex Server in staat de AnyConnect-client te verifiëren via de bedrijfseigen Cisco AnyConnect-EAP-methode.

Anders dan standaard gebaseerde EAP-methoden zoals EAP-Generic Token Card (EAP-GTC), EAP-Message Digest 5 (EAP-MD5) en dergelijke, werkt de Flex Server niet in de EAP-doorvoermodus.

Alle EAP-communicatie met de client eindigt op de Flex Server en de vereiste sessiesleutel die wordt gebruikt om de AUTH-payload te construeren, wordt lokaal door de Flex Server berekend.

De Flex Server moet zichzelf verifiëren bij de client met certificaten zoals vereist door de IKEv2 RFC.

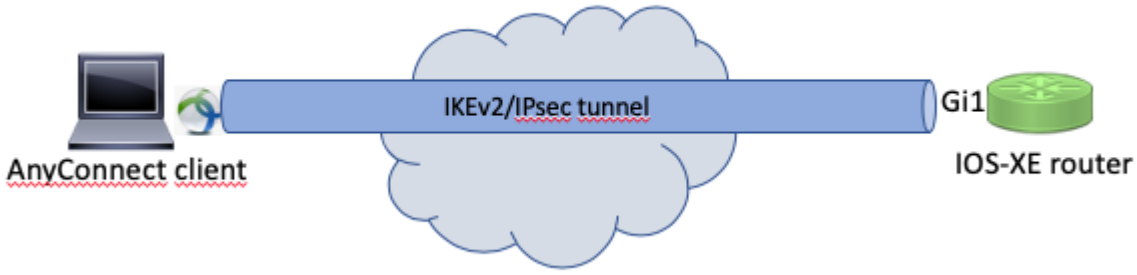
Lokale gebruikersverificatie wordt nu ondersteund op de Flex Server en externe verificatie is optioneel.

Dit is ideaal voor kleinschalige implementaties met minder gebruikers van externe toegang en in omgevingen zonder toegang tot een externe verificatie-, autorisatie- en accounting (AAA) server.

Voor implementaties op grote schaal en in scenario's waarin kenmerken per gebruiker gewenst zijn, wordt het echter nog steeds aanbevolen om een externe AAA-server te gebruiken voor verificatie en autorisatie.

De AnyConnect-EAP-implementatie maakt het gebruik van Radius voor externe verificatie, autorisatie en accounting mogelijk.

Netwerkdiagram



Configureren

Verificatie en autorisatie van gebruikers met de lokale database

---

> **Opmerking**: om gebruikers te verifiëren aan de hand van de lokale database op de router, moet EAP worden gebruikt. Om EAP te gebruiken, moet de lokale verificatiemethode echter rsa-sig zijn, zodat de router een correct certificaat nodig heeft dat erop geïnstalleerd is, en het kan geen zelfondertekend certificaat zijn.

Voorbeeldconfiguratie die gebruik maakt van lokale gebruikersverificatie, autorisatie van externe gebruikers en groepen en externe accounting.

Stap 1. Schakel AAA in, configureer verificatie-, autorisatie- en accounting lijsten en voeg een gebruikersnaam toe aan de lokale database:

```
aaa new-model
!
aaa authentication login a-eap-authen-local local
```

```
aaa authorization network a-eap-author-grp local
!
username test password cisco123
```

Stap 2. Configureer een trustpoint dat is bedoeld om het routercertificaat te bevatten. PKCS12-bestandsimport wordt in dit voorbeeld gebruikt. Raadpleeg voor andere opties de configuratiehandleiding PKI (Public Key Infrastructure):

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
```

Stap 3. Een lokale IP-pool definiëren om adressen toe te wijzen aan AnyConnect VPN-clients:

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

Stap 4. Maak een IKEv2 lokaal autorisatiebeleid:

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

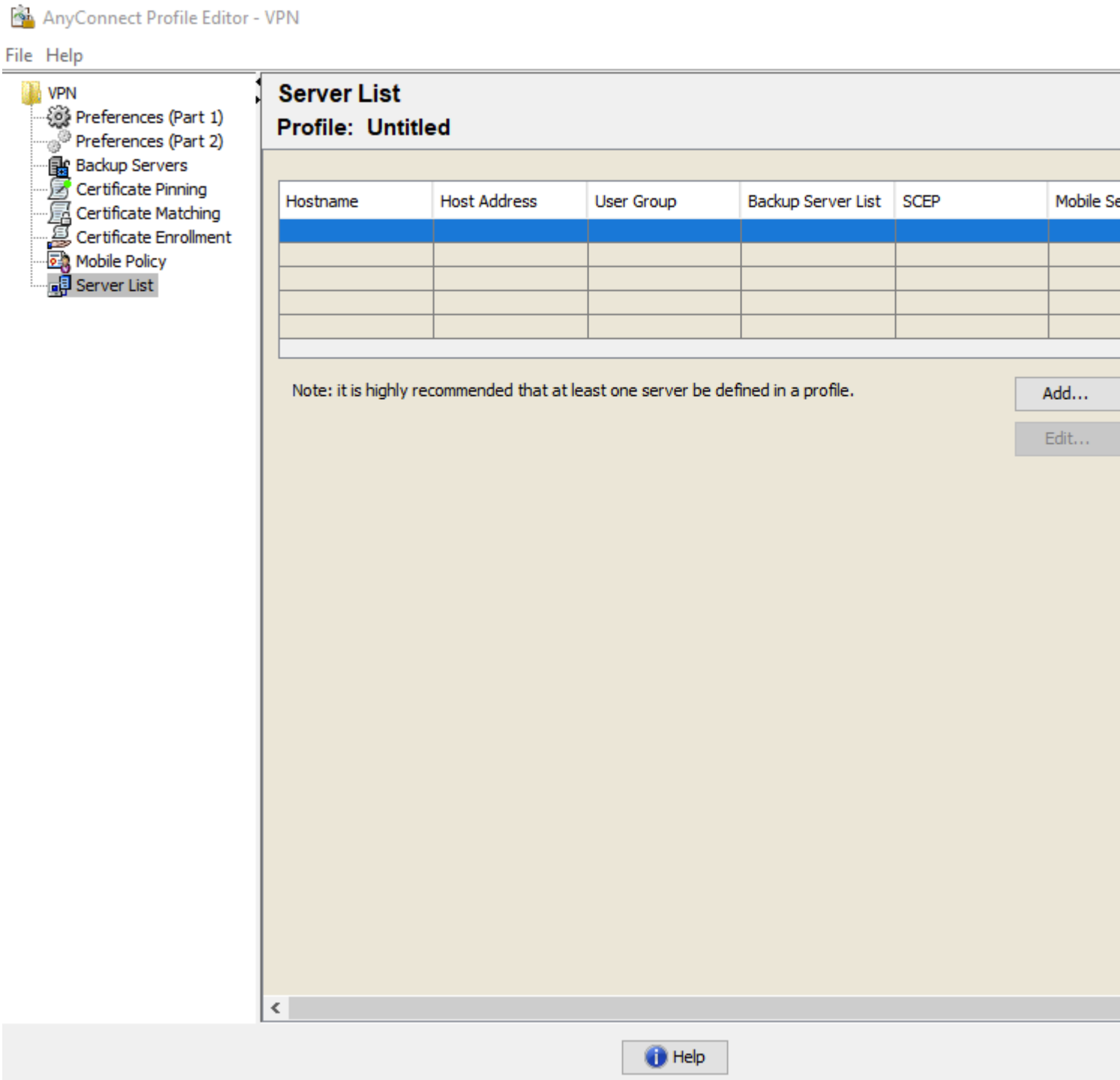
Stap 5 (optioneel). Maak het gewenste IKEv2 voorstel en beleid. Indien niet geconfigureerd worden slimme standaardwaarden gebruikt:

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

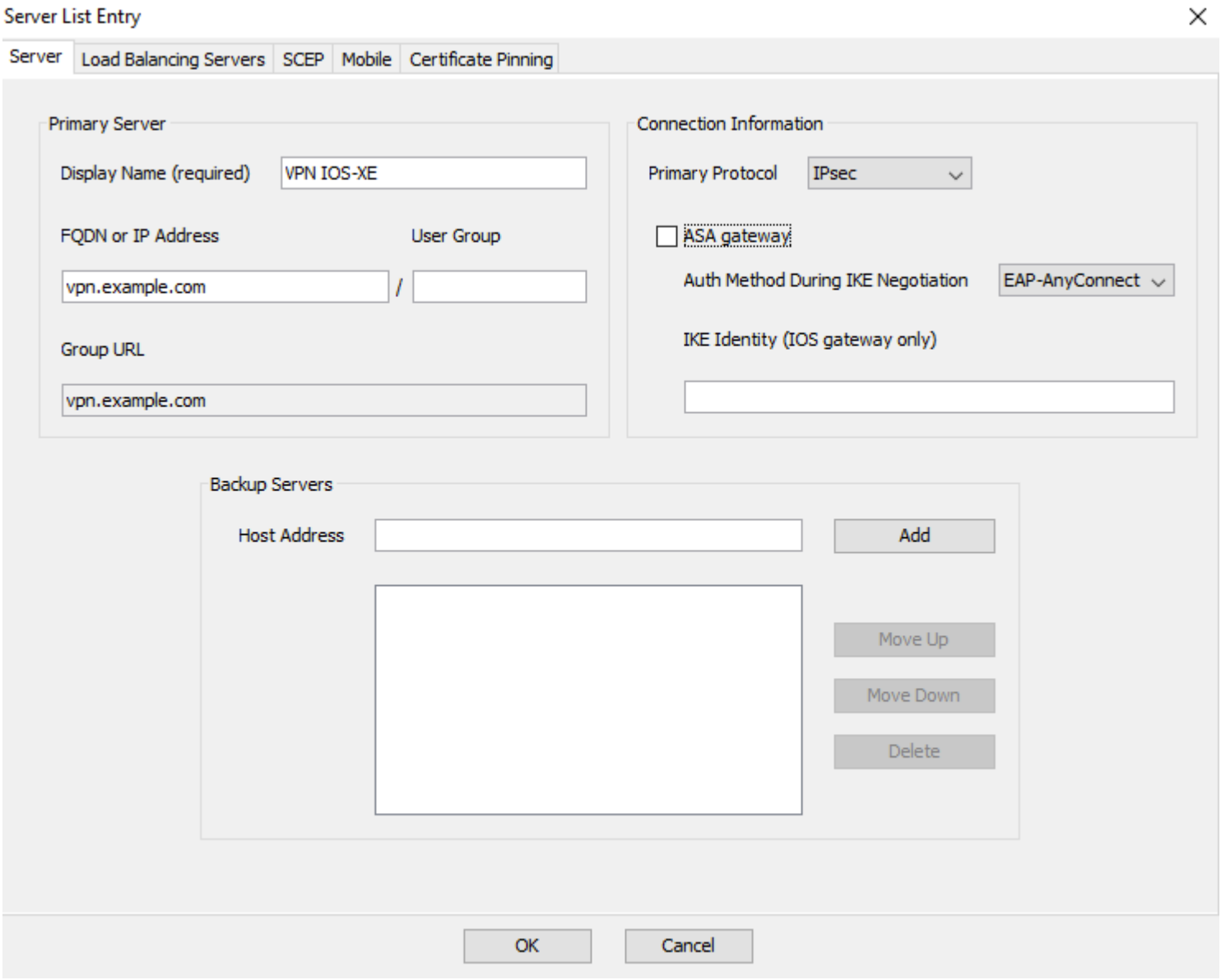
Stap 6. AnyConnect-profiel maken

> **Opmerking**: het AnyConnect-profiel moet worden geleverd aan de clientmachine. Zie de volgende sectie voor meer informatie.

Configureer het clientprofiel met de AnyConnect Profile Editor zoals in de afbeelding:



Klik op "Add" om een ingang voor de VPN gateway te maken. Zorg ervoor dat u "IPsec" selecteert als "Primair protocol". Schakel de optie "ASA gateway" uit.



Sla het profiel op: **Blad -> Opslaan als.** Het XML-equivalent van het profiel:

```
<?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>
```

Opmerking: AnyConnect gebruikt '*$AnyConnectClient$*' als de standaard IKE-identiteit van het type key-id. Deze identiteit kan echter handmatig worden gewijzigd in het AnyConnect-profiel om aan de implementatiebehoeften te voldoen.

Opmerking: voor het uploaden van het XML-profiel naar de router is Cisco IOS® XE 16.9.1 of hoger vereist. Als er een oudere versie van Cisco IOS® XE-software wordt gebruikt, moet de mogelijkheid voor het downloaden van profielen op de client worden uitgeschakeld. Raadpleeg het gedeelte "De AnyConnect-downloader uitschakelen" voor meer informatie.

Upload het gemaakte XML-profiel naar het flitsgeheugen van de router en definieer het profiel:

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

Opmerking: de bestandsnaam die wordt gebruikt voor AnyConnect XML-profiel is acvpn.xml.

Stap 7. Maak een IKEv2-profiel voor AnyConnect-EAP-methode voor clientverificatie.

```
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
```

> **Opmerking**: de configuratie van de verificatiemethode op afstand vóór de lokale verificatiemethode wordt door de CLI geaccepteerd, maar is niet van toepassing op versies die niet over de oplossing voor het verbeteringsverzoek beschikken, zoals Cisco bug ID CSCvb29701, als de verificatiemethode op afstand niet beschikbaar is. Zorg er bij deze versies, wanneer de WAP-configuratie de methode voor externe verificatie is, voor dat de lokale verificatiemethode eerst als rsa-sig is geconfigureerd. Dit probleem wordt niet gezien met een andere vorm van externe verificatiemethode.

> **Opmerking:** op versies van code die worden beïnvloed door Cisco bug ID CSCvb24236 , kan de methode voor externe verificatie niet meer op dat apparaat worden geconfigureerd als externe verificatie is geconfigureerd vóór lokale verificatie. Upgrade naar een versie met de fix voor deze code.

Stap 8. Schakel op HTTP-URL gebaseerde certificaat lookup en HTTP-server op de router uit:

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

> **Opmerking**: *Verwijs naar* dit document om te bevestigen of uw router hardware de NGE encryptie algoritmen (het vorige voorbeeld heeft NGE algoritmen) ondersteunt, anders IPSec SA installatie op de hardware mislukt tijdens de laatste fase van onderhandeling.

Stap 9. Definieer de versleuteling en hashalgoritmen die worden gebruikt om gegevens te beveiligen

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

Stap 10. Een IPSec-profiel maken:

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

Stap 11. Configureer een loopback-interface met een of ander dummy IP-adres. De Virtual-Access interfaces lenen het IP-adres ervan.

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

Stap 12. Een virtuele sjabloon configureren (de sjabloon in het IKEv2-profiel koppelen)

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

Stap 13 (optioneel). Standaard wordt al het verkeer van de client via de tunnel verzonden. U kunt gesplitste tunnel configureren, waardoor alleen geselecteerd verkeer door de tunnel kan gaan.

```
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
```

Stap 14 (optioneel). Als al verkeer door de tunnel moet gaan, vorm NAT om internetconnectiviteit voor verre cliënten toe te staan.

```
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
```

Schakel de AnyConnect-downloader uit (optioneel).

Deze stap is alleen nodig als de softwareversie van Cisco IOS® XE ouder dan 16.9.1 wordt gebruikt. Vóór Cisco IOS® XE 16.9.1 was de mogelijkheid om het XML-profiel te uploaden naar de router niet beschikbaar. De AnyConnect-client probeert standaard het XML-profiel te downloaden na succesvolle aanmelding. Als het profiel niet beschikbaar is, mislukt de verbinding. Als tijdelijke oplossing is het mogelijk om de downloadmogelijkheid van het AnyConnect-profiel op de client zelf uit te schakelen. Om

dat te doen, kan dit bestand gewijzigd worden:

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

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

De optie "BypassDownloader" is ingesteld op "true", bijvoorbeeld:

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

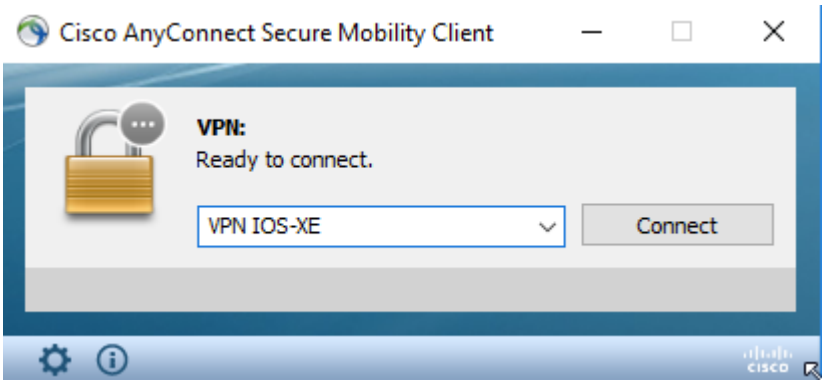
Na de wijziging moet de AnyConnect-client opnieuw worden gestart.

AnyConnect XML-profiellevering

Met de nieuwe installatie van de AnyConnect (zonder XML-profielen toegevoegd), kan de gebruiker de FQDN van de VPN-gateway handmatig invoeren in de adresbalk van AnyConnect-client. Dit resulteert in de SSL verbinding aan de gateway. De AnyConnect-client probeert standaard niet de VPN-tunnel met IKEv2/IPsec-protocollen tot stand te brengen. Dit is de reden dat het XML-profiel op de client is geïnstalleerd. Dit is verplicht om de IKEv2/IPsec-tunnel met Cisco IOS® XE VPN-gateway te maken.

Het profiel wordt gebruikt wanneer het is geselecteerd in de vervolgkeuzelijst van de AnyConnect-adresbalk.

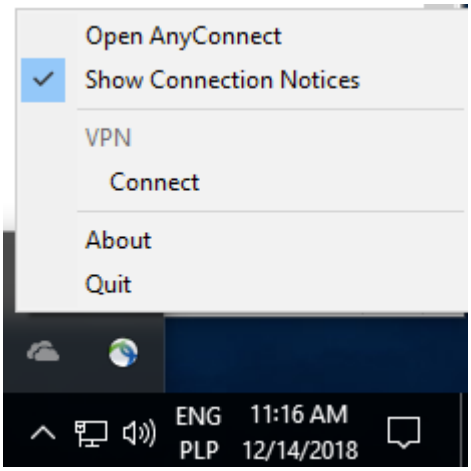
De naam die wordt weergegeven, is dezelfde naam als die is opgegeven in "Naam weergeven" in de AnyConnect-profieleditor.



Het XML-profiel kan handmatig in deze map worden gezet:

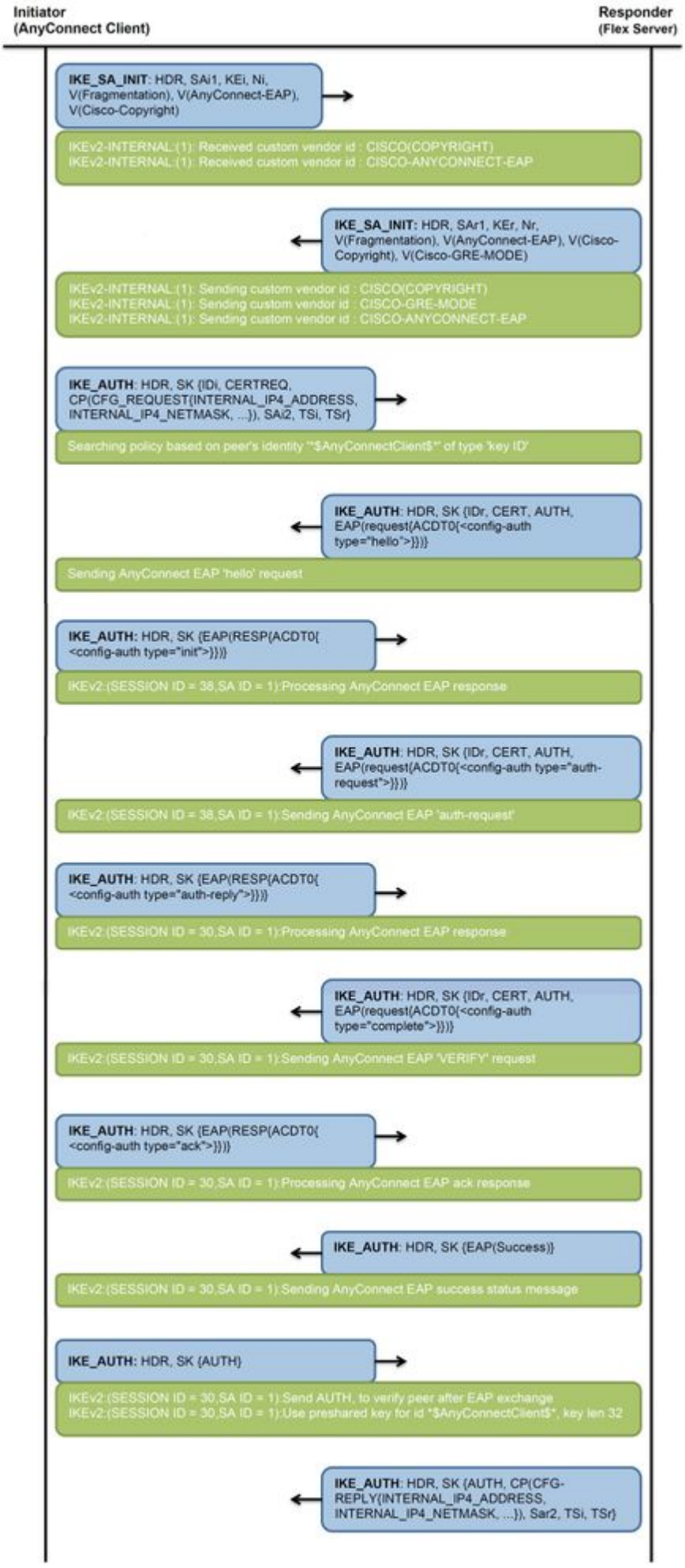
```
For Windows:
C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile

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

De AnyConnect-client moet opnieuw worden opgestart om het profiel in de GUI zichtbaar te maken. Het is niet voldoende om het AnyConnect-venster te sluiten. U kunt het proces opnieuw starten door met de rechtermuisknop op het pictogram AnyConnect in het Windows-vak te klikken en de optie "Ophouden" te selecteren:



Communicatiestroom

IKEv2- en EAP-uitwisseling


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
IKE_AUTH: HDR, SK {EAP(RESP{ACDT0{ <config-auth type="ack">}}}}
IKEv2:(SESSION ID = 30,SA ID = 1):Processing AnyConnect EAP ack response
IKE_AUTH: HDR, SK {EAP(Success)}
IKEv2:(SESSION ID = 30,SA ID = 1):Sending AnyConnect EAP success status message
IKE_AUTH: HDR, SK {AUTH}
IKEv2:(SESSION ID = 30,SA ID = 1):Send AUTH, to verify peer after EAP exchange
IKEv2:(SESSION ID = 30,SA ID = 1):Use preshared key for id *$AnyConnectClient$*, key len 32
IKE_AUTH: HDR, SK {AUTH, CP(CFG-REPLY(INTERNAL_IP4_ADDRESS, INTERNAL_IP4_NETMASK, ...)), Sar2, TSi, TSr}

Verifiëren

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: An
      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
```

Problemen oplossen

Deze sectie bevat informatie die u kunt gebruiken om problemen met de configuratie te troubleshooten.

1. IKEv2 debugt om te verzamelen van de head-end:

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

2. AAA debugs om de toewijzing van lokale en/of externe kenmerken te zien:

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

3. Start de AnyConnect-client.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.