Configuration de la tête de réseau FlexVPN pour l'accès à distance IKEv2 Secure Client (AnyConnect) à l'aide de la base de données utilisateur locale

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Informations générales

Diagramme du réseau

Configurer

- Authentification et autorisation des utilisateurs avec la base de données locale
- Exemple : Configuration du téléchargement du profil AnyConnect
- Désactivez la fonction de téléchargement AnyConnect (uniquement pour les versions antérieures à 16.9.1).
- Remise du profil XML AnyConnect

Flux de communication

- Échange IKEv2 et EAP

Vérifier

Dépannage

Introduction

Ce document décrit la configuration d'une tête de réseau FlexVPN pour l'accès via l'authentification IKEv2/EAP Secure Client (AnyConnect) avec une base de données d'utilisateurs locaux.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Protocole IKEv2

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Routeur de services cloud version 16.9.2
- Client AnyConnect version 4.6.03049 sous Windows 10

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

AnyConnect-EAP, ou authentification globale, permet à un serveur FlexVPN d'authentifier le client AnyConnect via la méthode propriétaire AnyConnect-EAP de Cisco.

Contrairement aux méthodes EAP (Extensible Authentication Protocol) basées sur la norme, telles que EAP-GTC (Generic Token Card), EAP-MD5 (Message Digest 5), etc., le serveur FlexVPN ne fonctionne pas en mode Pass-Through EAP.

Toutes les communications EAP avec le client se terminent sur le serveur FlexVPN et la clé de session requise utilisée pour construire la charge utile AUTH est calculée localement par le serveur FlexVPN.

Le serveur FlexVPN doit s'authentifier auprès du client à l'aide des certificats requis par la RFC IKEv2.

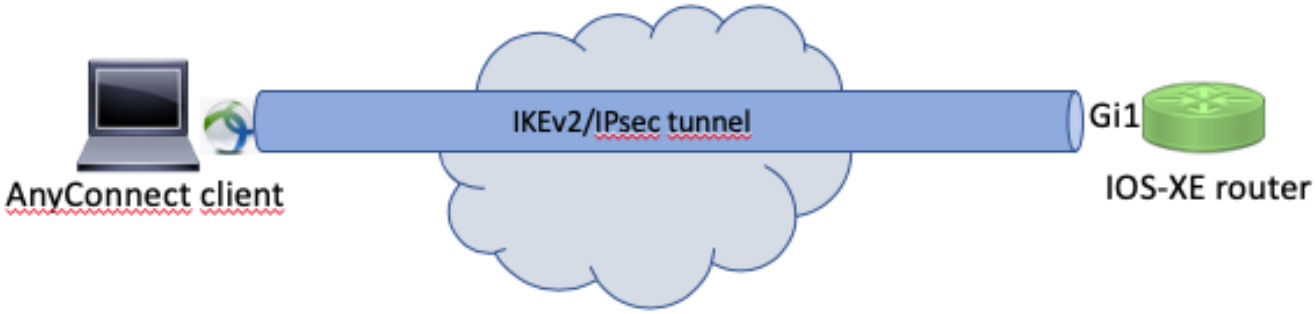
L'authentification des utilisateurs locaux est désormais prise en charge sur le serveur Flex Server et l'authentification à distance est facultative.

Cette solution est idéale pour les déploiements à petite échelle avec moins d'utilisateurs et d'environnements d'accès à distance sans accès à un serveur AAA (Authentication, Authorization, and Accounting) externe.

Cependant, pour les déploiements à grande échelle et dans les scénarios où les attributs par utilisateur sont souhaités, il est toujours recommandé d'utiliser un serveur AAA externe pour l'authentification et l'autorisation.

L'implémentation AnyConnect-EAP permet l'utilisation de Radius pour l'authentification, l'autorisation et la comptabilité à distance.

Diagramme du réseau



Configurer

Authentification et autorisation des utilisateurs avec la base de données locale

> Remarque : Afin d'authentifier les utilisateurs par rapport à la base de données locale sur le routeur, EAP doit être utilisé. Cependant, pour utiliser EAP, la méthode d'authentification locale doit être rsa-sig, de sorte que le routeur a besoin d'un certificat d'identité approprié, et il ne peut pas utiliser un certificat auto-signé.

Exemple de configuration qui utilise l'authentification des utilisateurs locaux, l'autorisation des utilisateurs et des groupes distants et la comptabilité à distance.

Étape 1 : activation de AAA, configuration des listes d'authentification, d'autorisation et de gestion des comptes et ajout d'un nom d'utilisateur à la base de données locale

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

Étape 2 : configuration d'un point de confiance destiné à contenir le certificat du routeur L'importation de fichiers PKCS12 est utilisée dans cet exemple. Pour d'autres options, consultez le Guide de configuration de la sécurité et du VPN, IOS XE 17.x, Chapitre : Configuration de l'inscription de certificat pour un document PKI.

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

Étape 3. Définition d’un pool local IP pour attribuer des adresses aux clients VPN AnyConnect :

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

Étape 4 : création d’une stratégie d’autorisation locale IKEv2

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

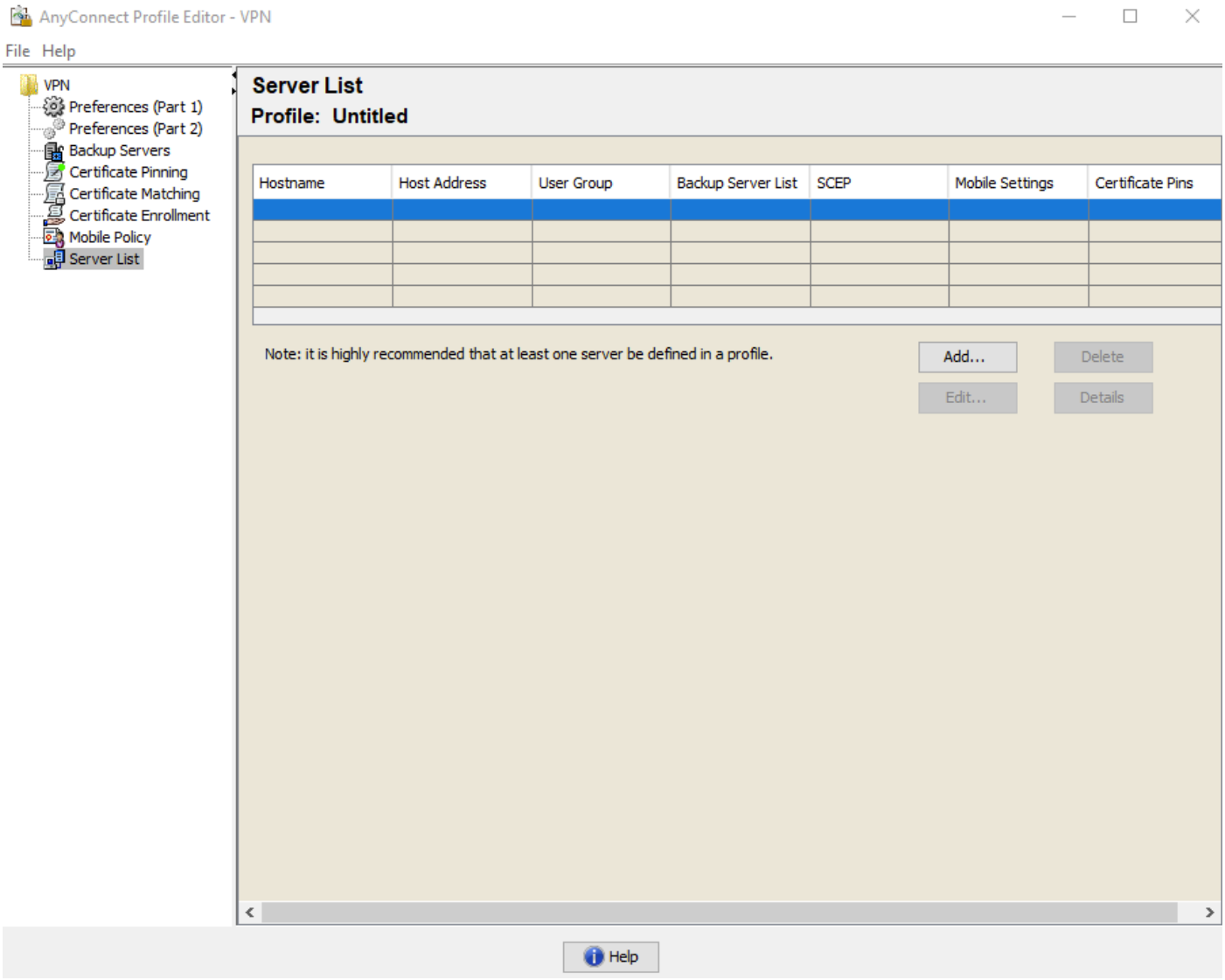
Étape 5 (facultatif). Créez la proposition et la stratégie IKEv2 souhaitées. S'ils ne sont pas configurés, les paramètres Smart par défaut sont utilisés :

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

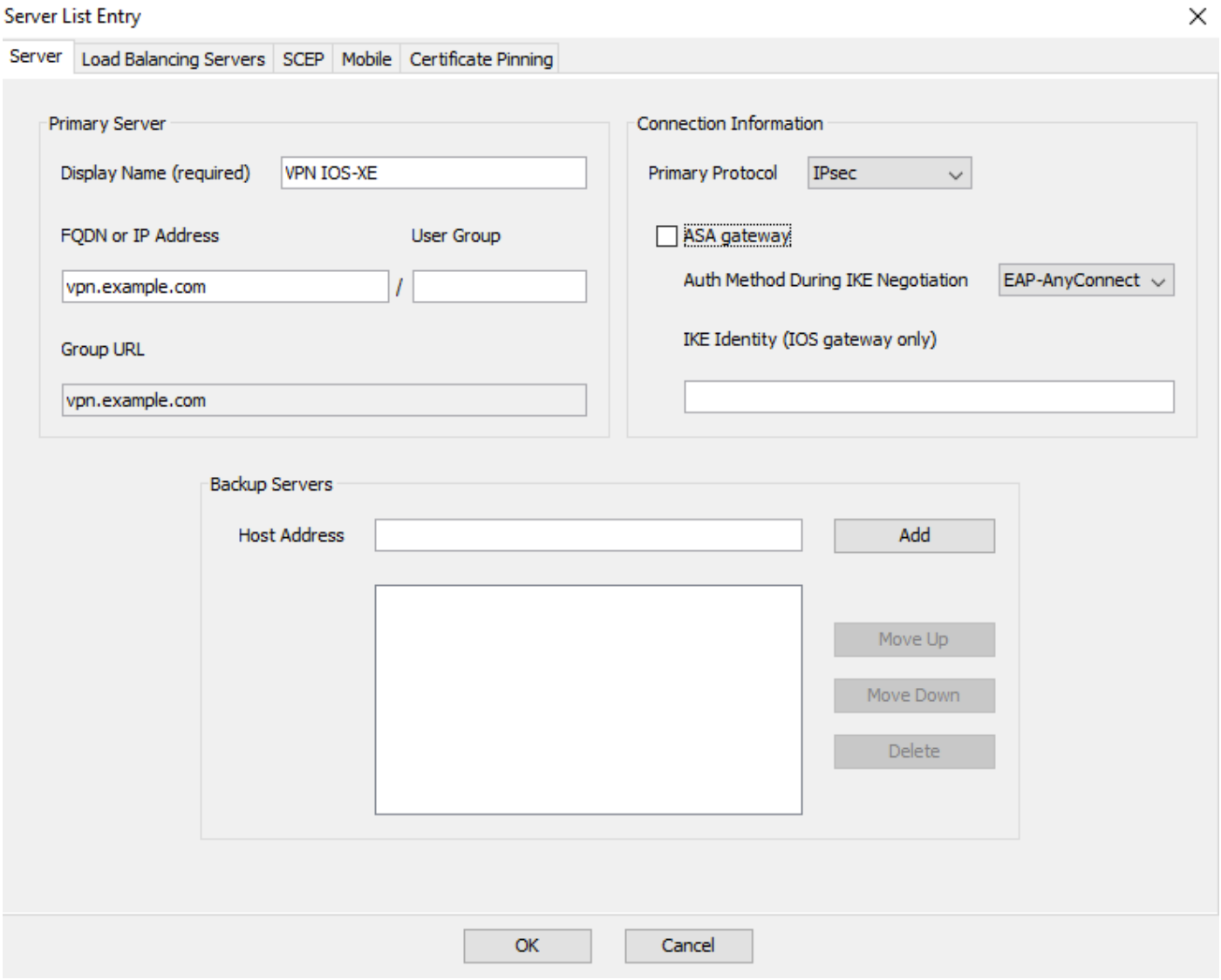
Étape 6. Créer un profil AnyConnect

Remarque : Le profil AnyConnect doit être fourni à l’ordinateur client. Reportez-vous à la section suivante pour plus d'informations.

Configurez le profil client à l’aide de l’Éditeur de profil AnyConnect, comme illustré dans l’image :



Cliquez sur Add pour créer une entrée pour la passerelle VPN. Veillez à sélectionner IPsec comme protocole principal. Décochez l'option de passerelle ASA.



Enregistrez le profil : Fichier -> Enregistrer sous. L'équivalent XML du profil :

```
<?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>
```

Remarque : AnyConnect utilise *$AnyConnectClient$* comme identité IKE par défaut de type key-id. Toutefois, cette identité peut être modifiée manuellement dans le profil AnyConnect pour correspondre aux besoins de déploiement.

Remarque : Pour télécharger le profil XML sur le routeur, la version 16.9.1 ou ultérieure est requise. Si une version logicielle plus ancienne est utilisée, la fonctionnalité de téléchargement de profil doit être désactivée sur le client. Référez-vous à la section Désactiver la fonctionnalité de téléchargement d'AnyConnect pour plus d'informations.

Téléchargez le profil XML créé dans la mémoire flash du routeur et définissez le profil :

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

Remarque : Le nom de fichier utilisé pour le profil XML AnyConnect est toujours acvpn.xml. Même si un nom de fichier différent est utilisé, le profil envoyé au PC est nommé acvpn.xml. Par conséquent, il est recommandé de ne pas modifier le nom dans la configuration du routeur.

Étape 7 : création d'un profil IKEv2 pour la méthode AnyConnect-EAP d'authentification client

```
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
```

Remarque : Pour la commande aaa authentication eap / anyconnect-eap, assurez-vous que la méthode d'authentification locale est configurée comme rsa-sig avant que la méthode d'authentification distante soit configurée.

Étape 8. Désactivez la recherche de certificat basée sur HTTP-URL et le serveur HTTP sur le routeur :

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

Remarque : Reportez-vous au document Next Generation Encryption Support pour confirmer si votre matériel de routeur prend en charge les algorithmes NGE (par exemple sha-256, aes-gcm, ecdh, ecdsa), sinon, l'installation de la SA IPSec sur le matériel échoue à la dernière étape de l'établissement du tunnel.

Étape 9. Définition des algorithmes de chiffrement et de hachage utilisés pour protéger les données

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

Étape 10. Créer un profil IPSec :

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

Étape 11. Configuration d’une interface de bouclage avec une adresse IP factice Les interfaces d'accès virtuel lui empruntent l'adresse IP.

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

Étape 12. Configurer un modèle virtuel (associer le modèle dans le profil IKEv2)

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

Étape 13 (facultatif). Par défaut, tout le trafic provenant du client est envoyé via le tunnel (tunnel complet). Vous pouvez configurer un tunnel partagé, qui permet uniquement au trafic sélectionné de traverser le 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
```

Étape 14 (facultatif). Si tout le trafic doit passer par le tunnel, configurez NAT afin d'autoriser la connectivité Internet pour les clients distants.

```
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
```

Exemple : Configuration du téléchargement du profil AnyConnect

Cet exemple montre comment configurer la fonctionnalité de téléchargement de profil FlexVPN

AnyConnect :

Remarque : Il n'est pas nécessaire de modifier le fichier de stratégie locale sur l'ordinateur client Anyconnect. Une fois la fonction de téléchargement de profil Anyconnect avec IKEv2 configurée, le module de téléchargement VPN fonctionne correctement - le profil XML requis est automatiquement mis à jour sur le périphérique client en cas de mise à jour du profil XML.

Remarque : Vous ne devez pas utiliser simultanément le serveur HTTPS et la stratégie SSL. Avant d'activer la stratégie SSL, supprimez la commande ip http secure-server. Si ces deux fonctionnalités sont activées en même temps et que le périphérique reçoit une connexion VPN SSL entrante, le périphérique peut se bloquer.

```
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
```

Désactivez la fonction de téléchargement AnyConnect (uniquement pour les versions antérieures à 16.9.1).

Cette étape n'est nécessaire que si une version antérieure à 16.9.1 est utilisée. Avant cette version, la capacité de télécharger le profil XML sur le routeur n'était pas disponible. Par défaut, le client sécurisé (AnyConnect) tente d'effectuer le téléchargement du profil XML après une connexion réussie. Si le profil n'est pas disponible, la connexion échoue. Pour contourner ce problème, il est possible de désactiver la fonctionnalité de téléchargement de profil AnyConnect sur le client lui-même. Pour ce faire, ce fichier peut être modifié :

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

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

L'option BypassDownloader est définie sur true, par exemple :

<#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>
```

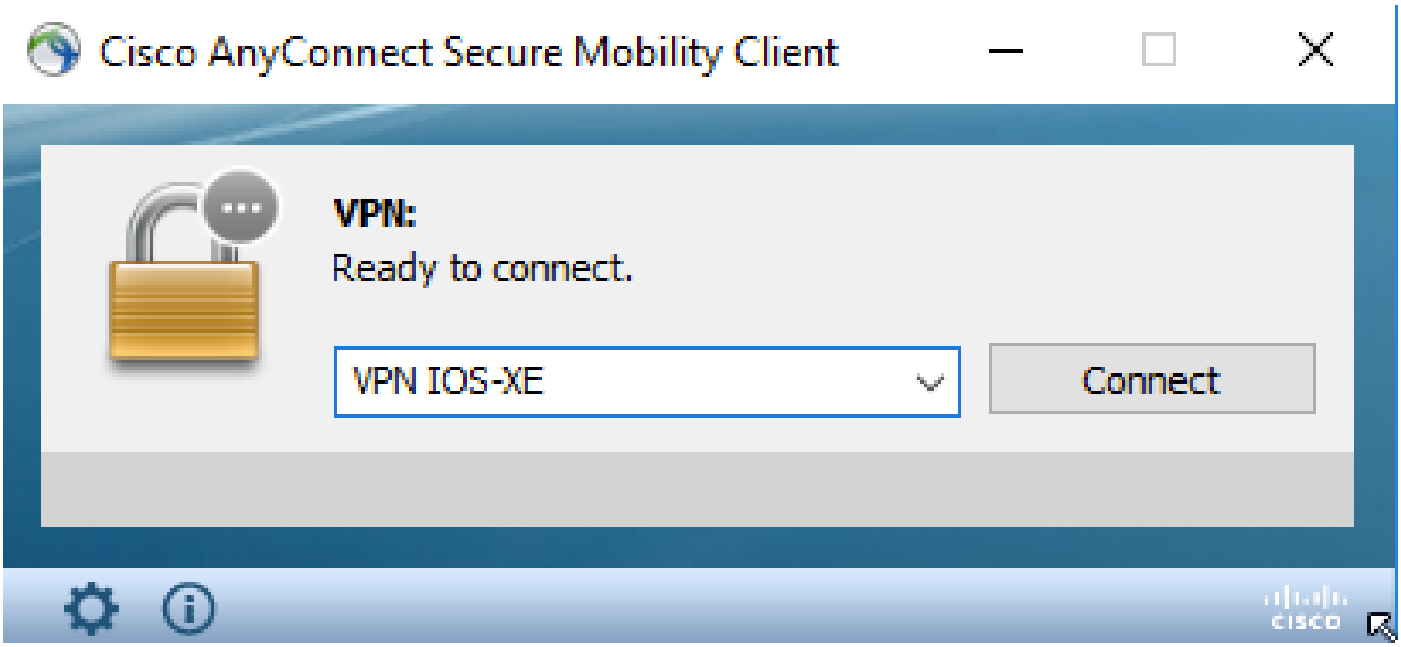
Après la modification, le client AnyConnect doit être redémarré.

Remise du profil XML AnyConnect

Avec la nouvelle installation d'AnyConnect (sans ajout de profils XML), l'utilisateur peut entrer manuellement le nom de domaine complet de la passerelle VPN dans la barre d'adresse du client AnyConnect. Il en résulte une connexion SSL à la passerelle. Par défaut, le client AnyConnect ne tente pas d’établir le tunnel VPN avec les protocoles IKEv2/IPsec. C'est la raison pour laquelle l'installation du profil XML sur le PC client est obligatoire pour établir le tunnel IKEv2/IPsec avec la passerelle FlexVPN.

Le profil est utilisé lorsqu’il est sélectionné dans la liste déroulante de la barre d’adresses AnyConnect.

Le nom qui apparaît dans la liste est spécifié dans le champ Display Name dans AnyConnect Profile Editor -> Server List -> Server List Entry.

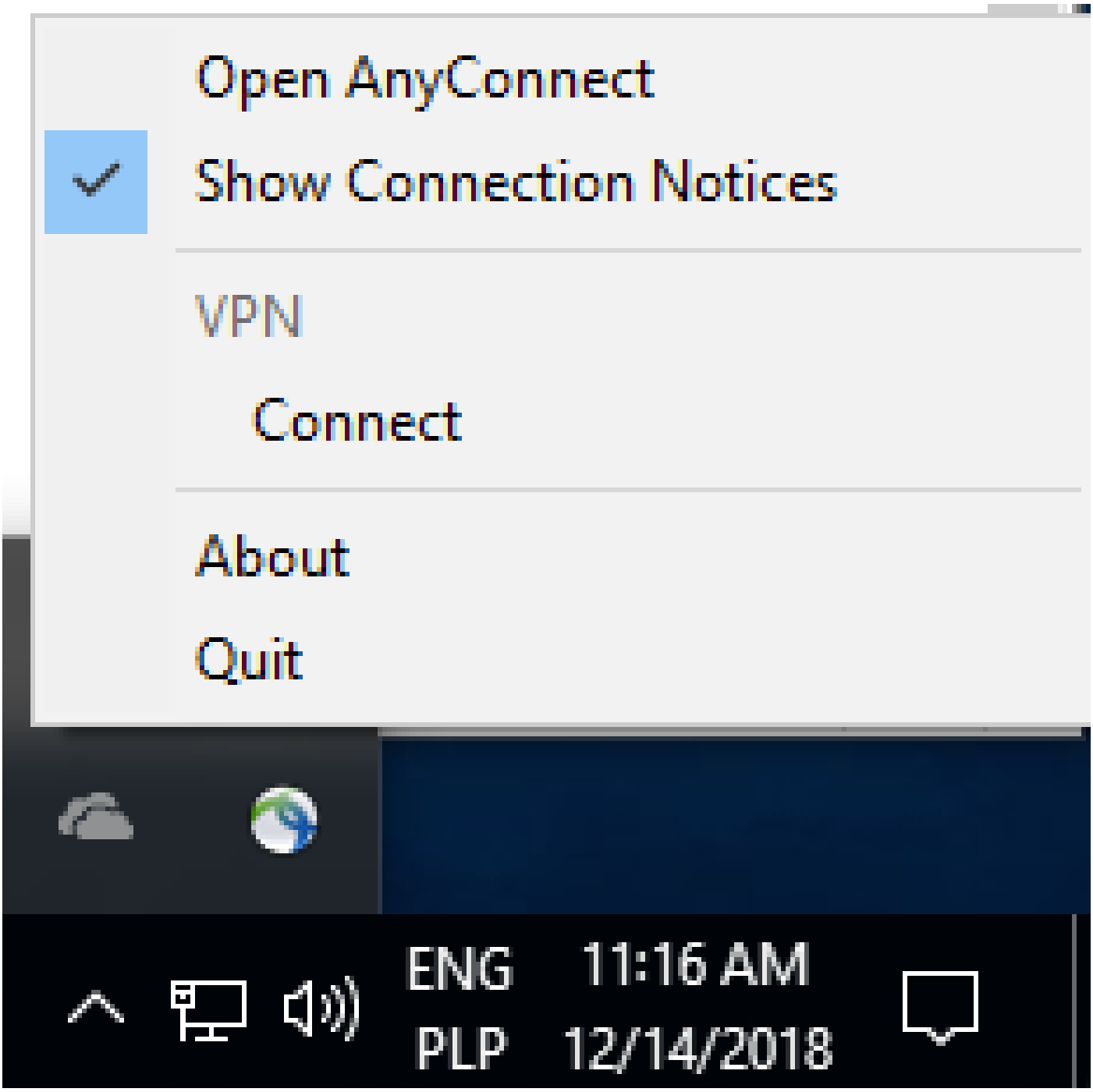


Le profil XML peut être placé manuellement dans un répertoire, selon le système d'exploitation client :

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

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

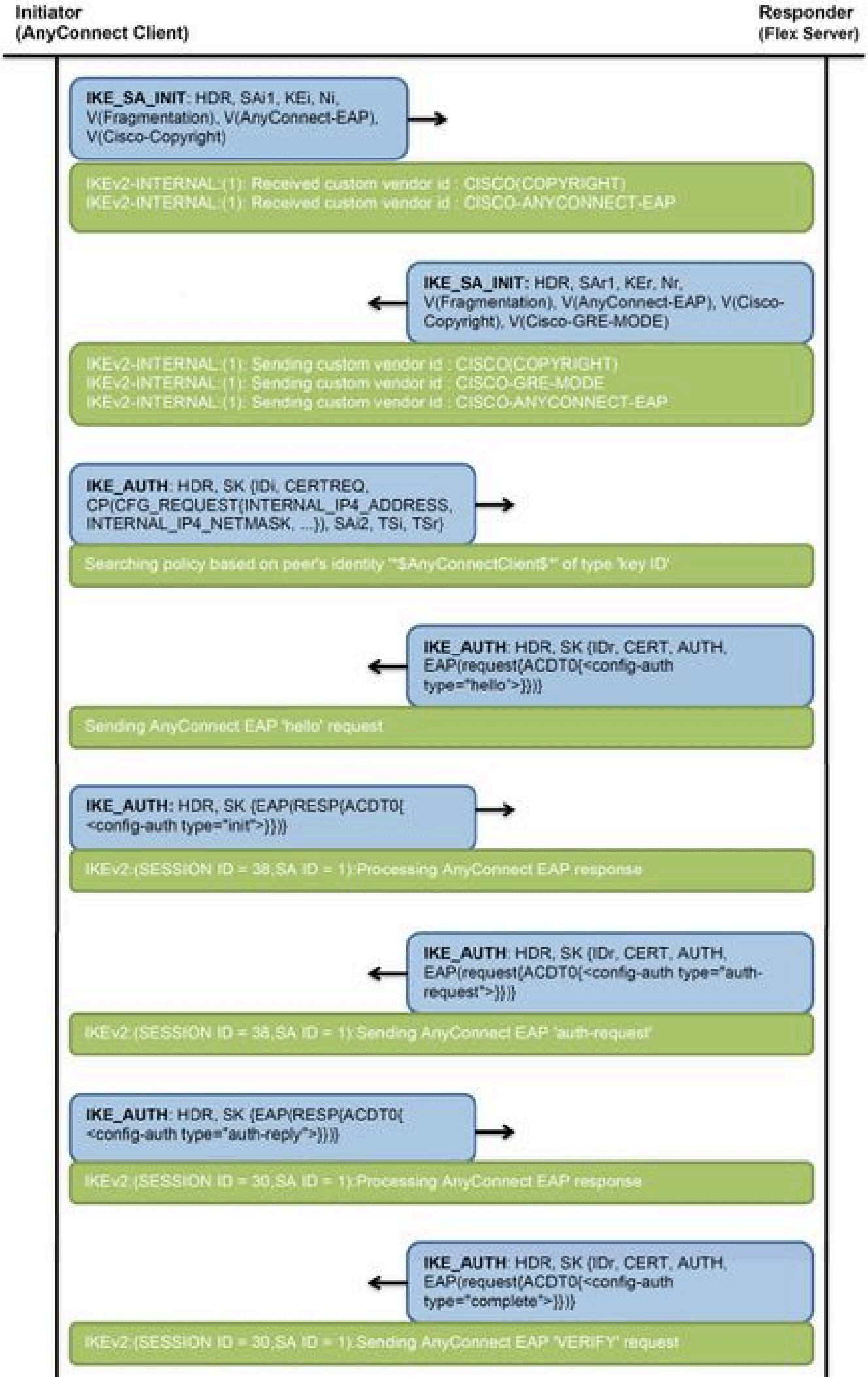
Le client AnyConnect doit être redémarré pour que le profil soit visible dans l'interface utilisateur graphique. Il ne suffit pas de fermer la fenêtre AnyConnect. Vous pouvez redémarrer le processus en cliquant avec le bouton droit sur l'icône AnyConnect dans la barre d'état système de Windows et en sélectionnant Quit option :



Flux de communication

cliquez ici

Échange IKEv2 et EAP


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
```

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

1. Débogages IKEv2 à collecter à partir de la tête de réseau :

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

2. Débogages AAA pour voir l'attribution des attributs locaux et/ou distants :

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

3. Outil DART (Diagnostic and Reporting Tool) pour le client AnyConnect.
   Pour collecter l'ensemble DART, suivez les étapes décrites dans le Guide de l'administrateur de Cisco Secure Client (y compris AnyConnect), version 5, chapitre : Chapitre : Dépannez le document Cisco Secure Client.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.