Konfigurieren von FlexVPN: AnyConnect IKEv2-Remote-Zugriff mit lokaler Benutzerdatenbank

Inhalt

Einleitung

Dieses Dokument beschreibt die Konfiguration eines Cisco IOS®/XE-Headends für den Zugriff über AnyConnect IKEv2/EAP-Authentifizierung mit lokaler Benutzerdatenbank.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- IKEv2-Protokoll

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Cloud Services Router mit Cisco IOS® XE 16.9.2
- AnyConnect-Client Version 4.6.03049, der unter Windows 10 ausgeführt wird

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

AnyConnect-EAP wird auch als Aggregat-Authentifizierung bezeichnet und ermöglicht es einem Flex Server, den AnyConnect-Client über die proprietäre AnyConnect-EAP-Methode von Cisco zu

authentifizieren.

Im Gegensatz zu standardbasierten Extensible Authentication Protocol (EAP)-Methoden wie EAP-Generic Token Card (EAP-GTC), EAP-Message Digest 5 (EAP-MD5) usw. funktioniert der Flex Server nicht im EAP-Passthrough-Modus.

Die gesamte EAP-Kommunikation mit dem Client endet auf dem Flex Server, und der erforderliche Sitzungsschlüssel für die Erstellung der AUTH-Nutzlast wird lokal vom Flex Server berechnet.

Der Flex Server muss sich gegenüber dem Client mit Zertifikaten entsprechend der IKEv2 RFC authentifizieren.

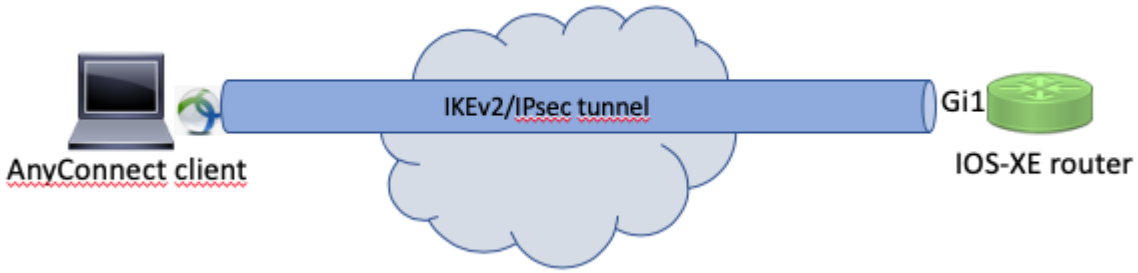
Die lokale Benutzerauthentifizierung wird jetzt auf dem Flex Server unterstützt, und die Remote-Authentifizierung ist optional.

Dies ist ideal für kleinere Bereitstellungen mit weniger Remote-Benutzern und in Umgebungen ohne Zugriff auf einen externen AAA-Server (Authentication, Authorization, and Accounting).

Für umfangreiche Bereitstellungen und in Szenarien, in denen benutzerspezifische Attribute gewünscht werden, wird jedoch weiterhin empfohlen, einen externen AAA-Server für die Authentifizierung und Autorisierung zu verwenden.

Die AnyConnect-EAP-Implementierung ermöglicht die Verwendung von Radius für Remote-Authentifizierung, -Autorisierung und -Accounting.

Netzwerkdiagramm



Konfigurieren

Authentifizierung und Autorisierung von Benutzern mit der lokalen Datenbank

---

> **Hinweis**: Um Benutzer anhand der lokalen Datenbank auf dem Router zu authentifizieren, muss EAP verwendet werden. Um EAP verwenden zu können, muss die lokale Authentifizierungsmethode jedoch rsa-sig sein. Der Router benötigt daher ein entsprechendes Zertifikat, das auf dem Router installiert ist, und es darf sich nicht um ein selbstsigniertes Zertifikat handeln.

Beispielkonfiguration für die lokale Benutzerauthentifizierung, Remote-Benutzer- und Gruppenautorisierung und Remote-Accounting.

Schritt 1: Aktivieren Sie AAA, konfigurieren Sie Authentifizierungs-, Autorisierungs- und

Abrechnungslisten, und fügen Sie der lokalen Datenbank einen Benutzernamen hinzu:

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

Schritt 2: Konfigurieren Sie einen Vertrauenspunkt, der das Routerzertifikat enthalten soll. In diesem Beispiel wird der PKCS12-Dateiimport verwendet. Weitere Optionen finden Sie im PKI-Konfigurationsleitfaden (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
```

Schritt 3: Definieren Sie einen lokalen IP-Pool, um AnyConnect VPN-Clients Adressen zuzuweisen:

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

Schritt 4: Erstellen Sie eine lokale IKEv2-Autorisierungsrichtlinie:

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

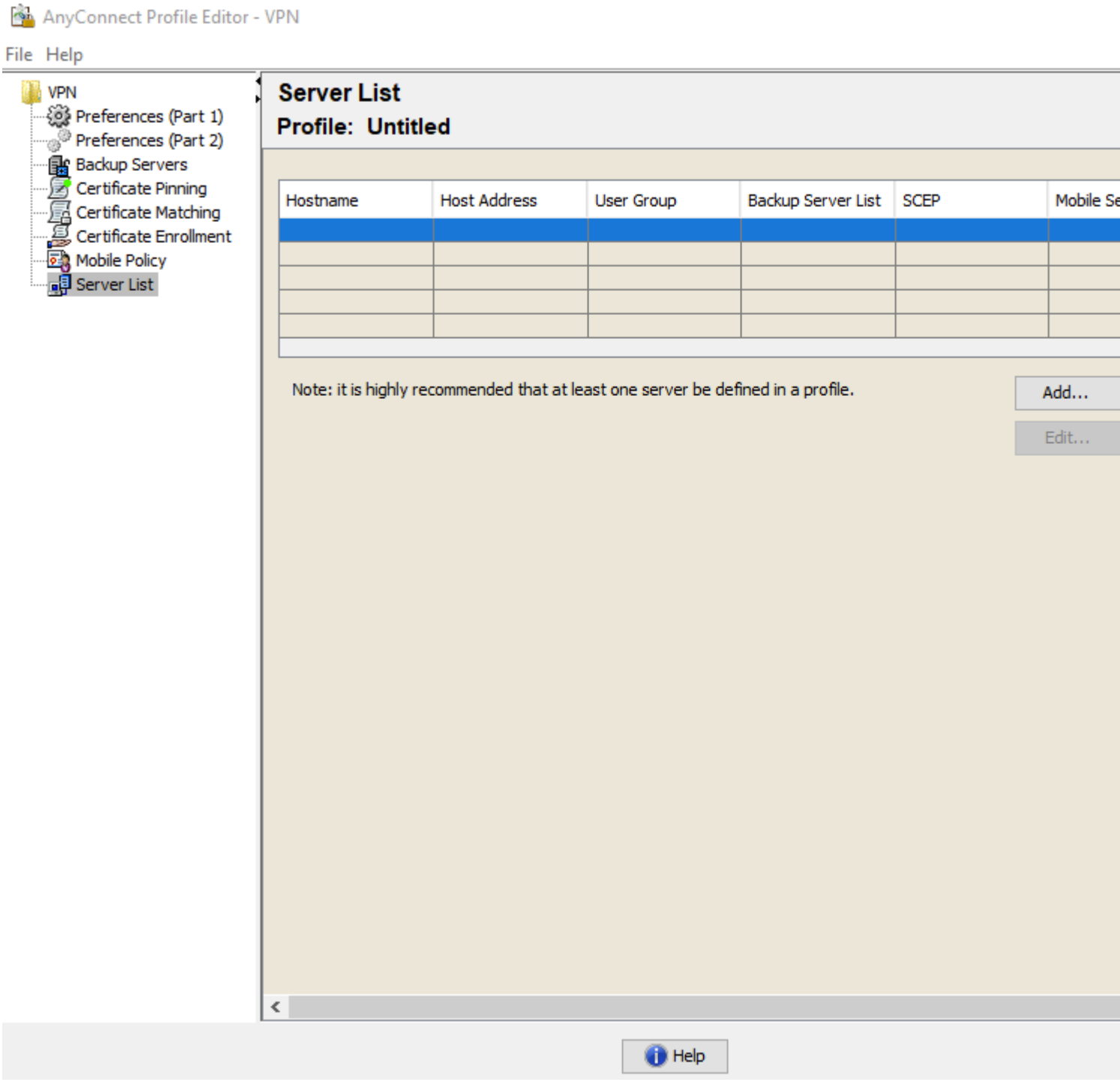
Schritt 5 (optional). Erstellen des gewünschten IKEv2-Angebots und der gewünschten IKEv2-Richtlinie Wenn diese Option nicht konfiguriert ist, werden intelligente Standardeinstellungen verwendet:

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

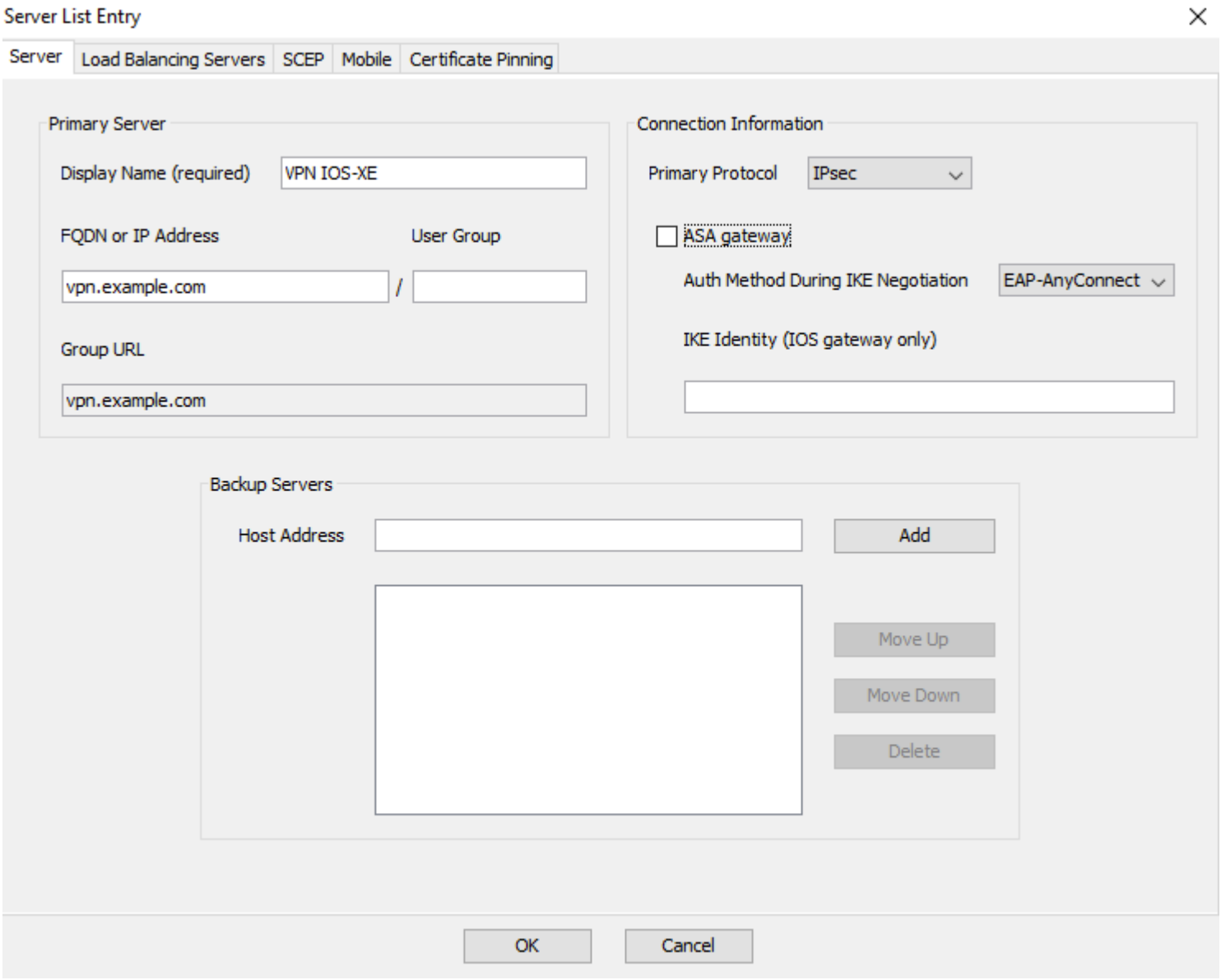
Schritt 6: AnyConnect-Profil erstellen

Hinweis: Das AnyConnect-Profil muss auf dem Client-Computer bereitgestellt werden. Weitere Informationen finden Sie im nächsten Abschnitt.

Konfigurieren Sie das Client-Profil mit dem AnyConnect Profile Editor, wie im Bild gezeigt:



Klicken Sie auf "Hinzufügen", um einen Eintrag für das VPN-Gateway zu erstellen. Wählen Sie "IPsec" als "Primary Protocol" aus. Deaktivieren Sie die Option "ASA-Gateway".



Profil speichern: **FIle -> Speichern unter.** Das XML-Äquivalent des Profils:

```
<?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>
```

Hinweis: AnyConnect verwendet '*$AnyConnectClient$*' als Standard-IKE-Identität des Typs Schlüssel-ID. Diese Identität kann jedoch im AnyConnect-Profil manuell geändert werden, um den Bereitstellungsanforderungen zu entsprechen.

Hinweis: Um das XML-Profil auf den Router hochzuladen, ist Cisco IOS® XE 16.9.1 oder höher erforderlich. Wenn ältere Versionen der Cisco IOS® XE-Software verwendet werden, muss die Funktion zum Herunterladen von Profilen auf dem Client deaktiviert werden. Weitere Informationen finden Sie im Abschnitt "Deaktivieren der AnyConnect-Downloader-Funktion".

Laden Sie das erstellte XML-Profil in den Flash-Speicher des Routers hoch, und definieren Sie das Profil:

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

Hinweis: Der für das XML-Profil von AnyConnect verwendete Dateiname lautet acvpn.xml.

Schritt 7. Erstellen Sie ein IKEv2-Profil für die AnyConnect-EAP-Methode der Client-Authentifizierung.

```
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
```

Hinweis: Die Konfiguration der Remote-Authentifizierungsmethode vor der lokalen Authentifizierungsmethode wird von der CLI akzeptiert, wird jedoch nicht auf Versionen wirksam, die nicht die Korrektur für die Erweiterungsanforderung aufweisen Cisco Bug-ID CSCvb29701, wenn die Remote-Authentifizierungsmethode eap ist. Wenn bei diesen Versionen die EAP-Konfiguration als Remote-Authentifizierungsmethode verwendet wird, stellen Sie sicher, dass die lokale Authentifizierungsmethode zuerst als rsa-sig konfiguriert wird. Dieses Problem tritt bei keiner anderen Form der Remote-Authentifizierung auf.

Hinweis: Bei Codeversionen, die von der Cisco Bug-ID CSCvb24236 betroffen sind, kann nach der Konfiguration der Remote-Authentifizierung vor der lokalen Authentifizierung die Remote-Authentifizierungsmethode auf diesem Gerät nicht mehr konfiguriert werden. Führen Sie ein Upgrade auf eine Version durch, die dieses Problem behebt.

Schritt 8: Deaktivieren Sie die HTTP-URL-basierte Zertifikatssuche und den HTTP-Server auf dem Router:

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

Hinweis: *Überprüfen Sie in* diesem Dokument, ob Ihre Router-Hardware die NGE-Verschlüsselungsalgorithmen unterstützt (im vorherigen Beispiel wurden NGE-Algorithmen verwendet). Andernfalls schlägt die IPSec SA-Installation auf der Hardware in der letzten Verhandlungsphase fehl.

Schritt 9. Definieren der Verschlüsselungs- und Hash-Algorithmen, die zum Schutz von Daten verwendet werden

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

Schritt 10. Erstellen Sie ein IPSec-Profil:

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

Schritt 11. Konfigurieren Sie eine Loopback-Schnittstelle mit einigen Dummy-IP-Adressen. Die Virtual-Access-Schnittstellen leihen sich die IP-Adresse daraus.

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

Schritt 12: Konfigurieren einer virtuellen Vorlage (ordnen Sie die Vorlage dem IKEv2-Profil zu)

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

Schritt 13 (optional). Standardmäßig wird der gesamte Datenverkehr vom Client über den Tunnel gesendet. Sie können Split-Tunnel konfigurieren, der nur ausgewählten Datenverkehr durch den Tunnel leitet.

```
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
```

Schritt 14 (optional). Wenn der gesamte Datenverkehr durch den Tunnel fließen muss, konfigurieren Sie NAT, um die Internetverbindung für Remote-Clients zu ermöglichen.

```
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
```

Deaktivieren Sie die AnyConnect-Download-Funktion (optional).

Dieser Schritt ist nur erforderlich, wenn die Cisco IOS® XE-Softwareversion älter als 16.9.1 verwendet wird. Vor Cisco IOS® XE 16.9.1 war die Möglichkeit zum Hochladen des XML-Profils auf den Router nicht verfügbar. Der AnyConnect-Client versucht nach erfolgreicher Anmeldung standardmäßig, das XML-Profil herunterzuladen. Wenn das Profil nicht verfügbar ist, schlägt die Verbindung fehl. Als

Problemumgehung ist es möglich, die Download-Funktion für AnyConnect-Profile auf dem Client selbst zu deaktivieren. Dazu kann die Datei wie folgt geändert werden:

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

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

Die Option "BypassDownloader" ist auf "true" gesetzt, z. B.:

```
<?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>
```

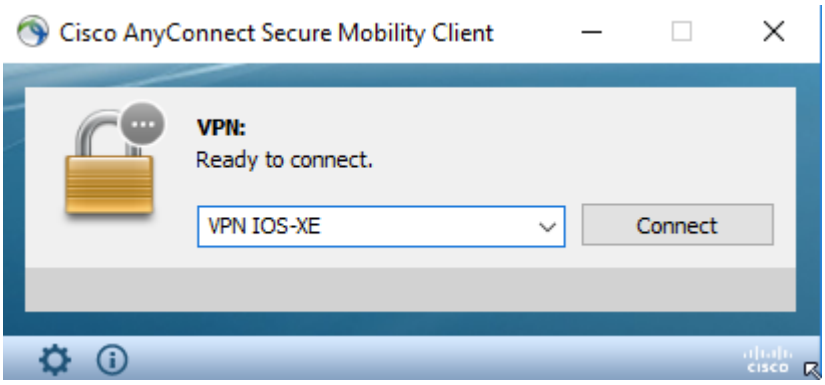
Nach der Änderung muss der AnyConnect-Client neu gestartet werden.

Bereitstellung von AnyConnect XML-Profilen

Nach der Neuinstallation von AnyConnect (ohne Hinzufügen von XML-Profilen) kann der Benutzer den FQDN des VPN-Gateways manuell in die Adressleiste des AnyConnect-Clients eingeben. Daraus ergibt sich die SSL-Verbindung zum Gateway. Der AnyConnect-Client versucht nicht, standardmäßig den VPN-Tunnel mit IKEv2/IPsec-Protokollen einzurichten. Aus diesem Grund muss das XML-Profil auf dem Client installiert sein, damit der IKEv2/IPsec-Tunnel mit dem Cisco IOS® XE VPN-Gateway eingerichtet werden kann.

Das Profil wird verwendet, wenn es in der Dropdown-Liste der AnyConnect-Adressleiste ausgewählt ist.

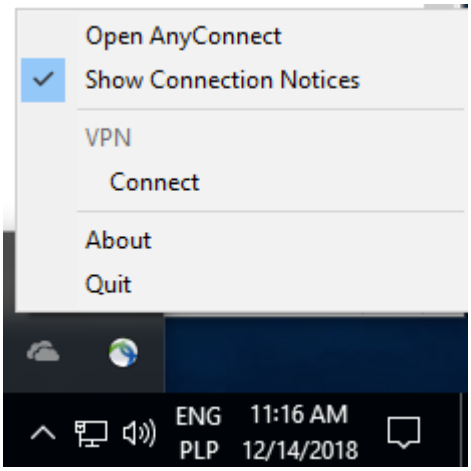
Der angezeigte Name entspricht dem Namen, der im Profil-Editor von AnyConnect unter "Anzeigename" angegeben wurde.



Das XML-Profil kann manuell in diesem Verzeichnis abgelegt werden:

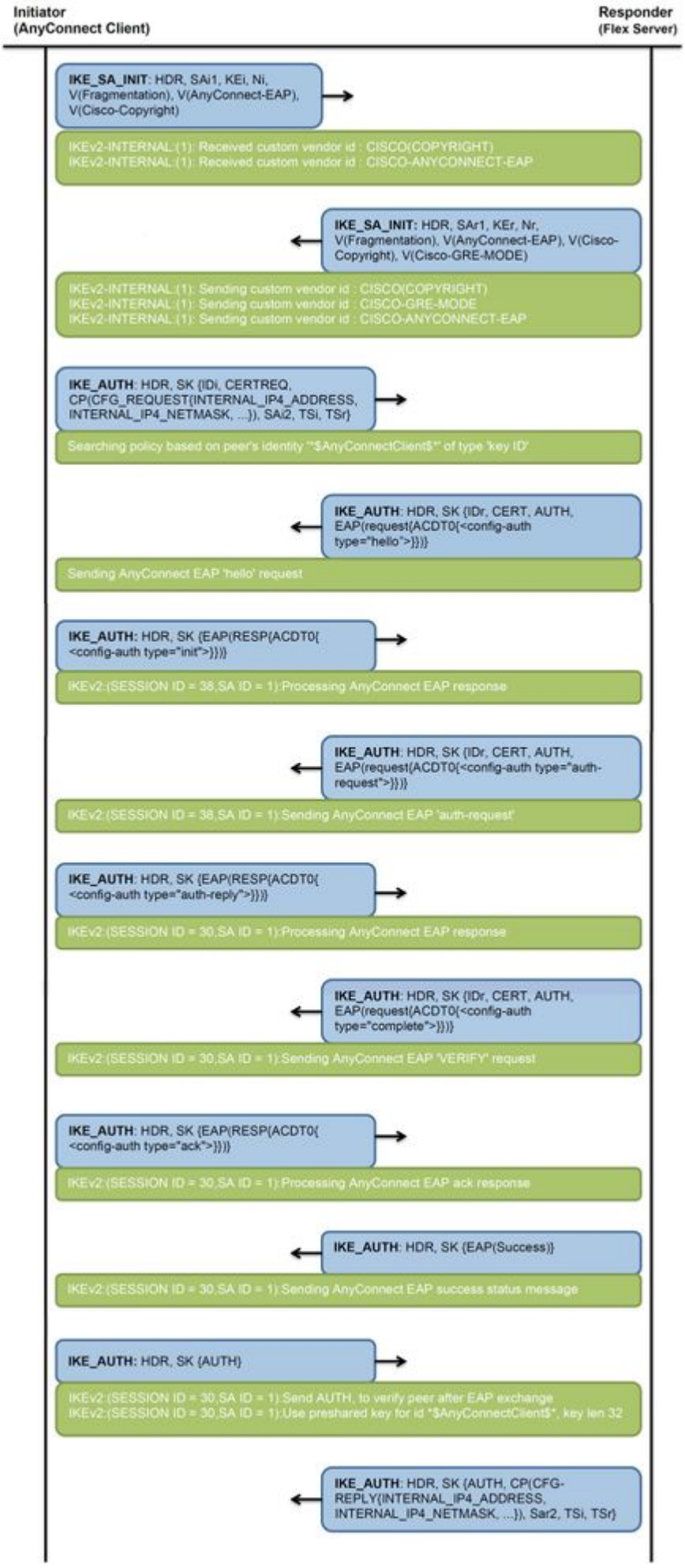
```
For Windows:
C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile

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

Der AnyConnect-Client muss neu gestartet werden, damit das Profil in der GUI sichtbar wird. Es reicht nicht aus, das AnyConnect-Fenster zu schließen. Der Prozess kann neu gestartet werden, indem Sie mit der rechten Maustaste auf das AnyConnect-Symbol in der Windows-Taskleiste klicken und die Option "Beenden" auswählen:



Kommunikationsfluss

IKEv2- und EAP-Austausch



Überprüfung

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
```

Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden

können.

1. IKEv2-Debugs zum Erfassen vom Headend:

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

2. AAA-Fehlersuche zur Anzeige der Zuweisung von lokalen und/oder Remote-Attributen:

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

3. DART vom AnyConnect-Client.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.