تكوين وحدة الاستقبال والبث FlexVPN للوصول عن بعد لعميل آمن (AnyConnect) IKEv2 باستخدام قاعدة بيانات المستخدم المحلي

المحتويات

المقدمة

المتطلبات الأساسية

المتطلبات

المكونات المستخدمة

معلومات أساسية

الرسم التخطيطي للشبكة

التكوين

المصادقة والتفويض للمستخدمين باستخدام قاعدة البيانات المحلية

مثال: تكوين تنزيل ملف تعريف AnyConnect

تمكين تنزيل AnyConnect (للإصدارات الأقدم من 16.9.1 فقط).

تسليم ملف تعريف AnyConnect XML

تدفق الاتصالات

تبادل IKEv2 و EAP

التحقق من الصحة

استكشاف الأخطاء وإصلاحها

المقدمة

يصف هذا المستند تكوين وحدة الاستقبال والبث الخاصة ب FlexVPN للوصول عبر مصادقة IKEv2/EAP الخاصة بالعميل الآمن (AnyConnect) باستخدام قاعدة بيانات مستخدم محلية.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- بروتوكول IKEv2

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- موجه خدمات السحابة الإصدار 16.9.2
- AnyConnect Client الإصدار 4.6.03049 الذي يعمل على Windows 10

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

يتيح AnyConnect-EAP أو المصادقة التجميعية لخادم FlexVPN إمكانية مصادقة عميل AnyConnect عبر طريقة AnyConnect-EAP الخاصة من Cisco.

ليس كطرق بروتوكول المصادقة الموسع (EAP) القياسية المستندة إلى مثل بطاقة الرمز المميز العام EAP (EAP-GTC) و EAP- Message Digest 5 (EAP-MD5) وما إلى ذلك، لا يعمل خادم FlexVPN في وضع تمرير EAP.

ينتهي جميع إتصالات EAP مع العميل على خادم FlexVPN ومفتاح الجلسة المطلوب المستخدم لإنشاء حمولة المصادقة ويتم حسابه محليا بواسطة خادم FlexVPN.

يجب أن يقوم خادم FlexVPN بمصادقة نفسه لدى العميل باستخدام الشهادات المطلوبة بواسطة IKEv2 RFC.

مصادقة المستخدم المحلي مدعومة الآن على Flex Server والمصادقة عن بعد إختيارية.

ويعد هذا الخيار مثاليا لعمليات النشر على نطاق صغير التي تتميز بعدد أقل من مستخدمي الوصول عن بعد وبيئاته التي لا تتوفر لها إمكانية الوصول إلى خادم المصادقة والتفويض والمحاسبة (AAA) الخارجي.

ومع ذلك، فبالنسبة لعمليات النشر واسعة النطاق وفي السيناريوهات التي تكون فيها سمات كل مستخدم مرغوبة، لا يزال يوصى باستخدام خادم AAA خارجي للمصادقة والتفويض.

يتيح تنفيذ AnyConnect-EAP إستخدام RADIUS للمصادقة عن بعد والتخويل والمحاسبة.

الرسم التخطيطي للشبكة

التكوين

المصادقة والتفويض للمستخدمين باستخدام قاعدة البيانات المحلية

> ملاحظة: لمصادقة المستخدمين مقابل قاعدة البيانات المحلية على الموجه، يلزم إستخدام EAP. ومع ذلك، لاستخدام EAP، يجب أن يكون أسلوب المصادقة المحلي rsa-sig، لذلك يحتاج الموجه إلى شهادة هوية مناسبة، ولا يمكنه إستخدام شهادة موقعة ذاتيا.

نموذج التكوين الذي يستخدم مصادقة المستخدم المحلي وتخويل المستخدم البعيد والمجموعة والمحاسبة عن بعد.

الخطوة 1. تمكين المصادقة والتفويض والمحاسبة (AAA) وتكوين قوائم المصادقة والتفويض والمحاسبة وإضافة اسم مستخدم إلى قاعدة البيانات المحلية:

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

الخطوة 2. تكوين نقطة ثقة تهدف إلى الاحتفاظ بشهادة الموجه. يتم إستخدام إستيراد ملف PKCS12 في هذا المثال. للحصول على خيارات أخرى، راجع دليل تكوين الأمان وشبكة VPN، IOS XE 17.x، الفصل: تكوين تسجيل الشهادة لمستند PKI.

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

الخطوة 3. حدد تجمع IP المحلي لتعيين العناوين إلى عملاء AnyConnect VPN:

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

الخطوة 4. إنشاء سياسة ترخيص محلية لـ IKEv2:

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

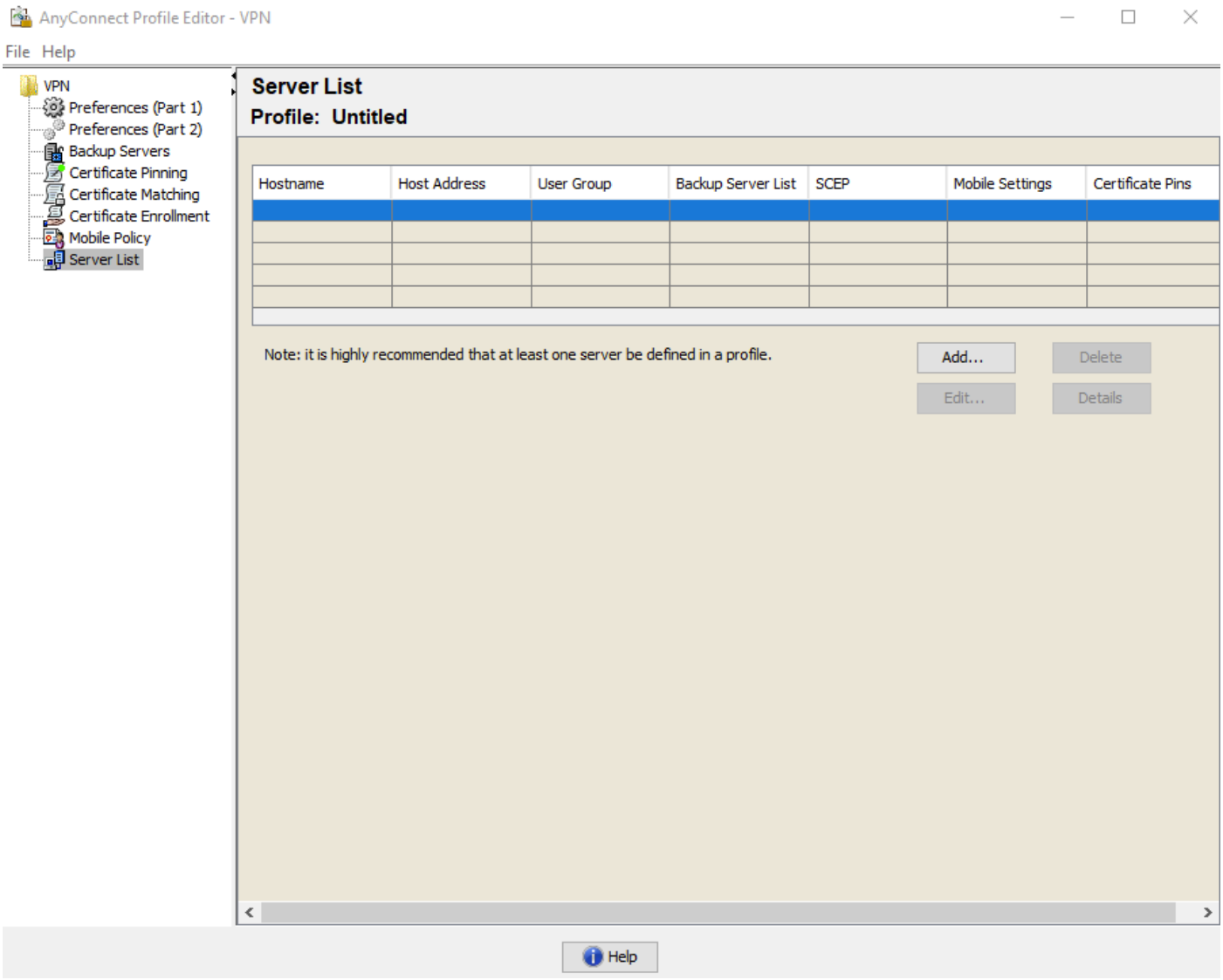
الخطوة 5 (اختيارية). قم بإنشاء مقترح وسياسة IKEv2 المطلوبين. في حالة عدم تكوين هذا الخيار، يتم إستخدام الافتراضيات الذكية:

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

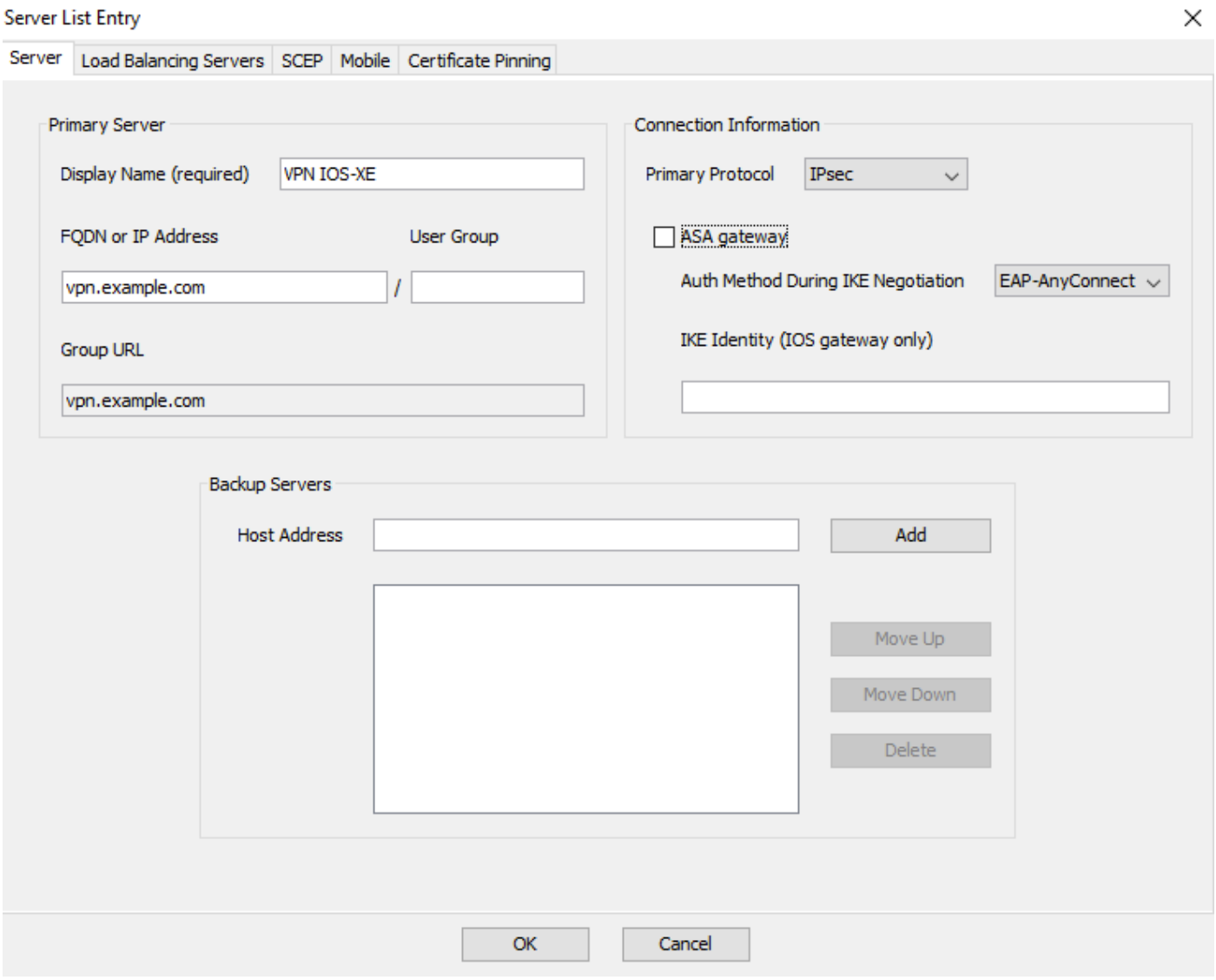
الخطوة 6. إنشاء ملف تعريف AnyConnect

> ملاحظة: يلزم تسليم ملف تعريف AnyConnect إلى جهاز العميل. راجع القسم التالي للحصول على مزيد من المعلومات.

قم بتكوين ملف تعريف العميل باستخدام محرر ملف تعريف AnyConnect كما هو موضح في الصورة:



طقطقة يضيف أن يخلق مدخل ل ال VPN مدخل. تأكد من تحديد IPsec كبروتوكول أساسي. قم بإلغاء تحديد خيار عبارة ASA.



حفظ التوصيف: FIle -> حفظ باسم. مرادف XML لملف التعريف:

```
<?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>
```

ملاحظة: يستخدم AnyConnect *$AnyConnectClient$* كهوية IKE الافتراضية من النوع key-id. ومع ذلك، يمكن تغيير هذه الهوية يدويا في ملف تعريف AnyConnect لمطابقة إحتياجات النشر.

ملاحظة: لتحميل ملف تعريف XML إلى الموجه، يلزم الإصدار 16.9.1 وأ إصدار أحدث. في حالة إستخدام إصدار برنامج قديم، يلزم تعطيل إمكانية تنزيل ملف التعريف على العميل. راجع القسم تعطيل إمكانية تنزيل AnyConnect للحصول على مزيد من المعلومات.

قم بتحميل ملف تعريف XML الذي تم إنشاؤه إلى ذاكرة Flash (الذاكرة المؤقتة) للموجه وحدد ملف التعريف:

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

ملاحظة: اسم الملف الذي يتم إستخدامه لملف تعريف AnyConnect XML يكون دائما acvpn.xml. حتى في حالة إستخدام اسم ملف مختلف، يتم تسمية ملف التعريف الذي

تم إرساله إلى الكمبيوتر الشخصي acvpn.xml. لذلك، يوصى بعدم تغيير الاسم في تكوين الموجه.

الخطوة 7. قم بإنشاء توصيف IKEv2 لأسلوب AnyConnect-EAP لمصادقة العميل.

```
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
```

ملاحظة: للحصول على الأمر AAA authentication eap /anyConnect-eap، تأكد من تكوين أسلوب المصادقة المحلي على أنه rsa-sig قبل تكوين أسلوب المصادقة عن بعد.

الخطوة 8. قم بتعطيل بحث الشهادة المستند إلى HTTP-URL وخادم HTTP على الموجه:

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

ملاحظة: ارجع إلى مستند دعم التشفير من الجيل التالي لتأكيد ما إذا كانت أجهزة Cisco الموجه لديك تدعم خوارزميات NGE (على سبيل المثال SHA-256 و AES-GCM و ECDH و ECDSA)، وإلا فإن تثبيت IPSec SA على الجهاز يفشل في المرحلة الأخيرة من إنشاء النفق.

الخطوة 9. تحديد التشفير وخوارزميات التجزئة المستخدمة لحماية البيانات

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

الخطوة 10. إنشاء ملف تعريف IPSec:

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

الخطوة 11. قم بتكوين واجهة إسترجاع باستخدام عنوان IP وهمي. تستعير واجهات الوصول الظاهري عنوان IP منها.

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

الخطوة 12. تكوين قالب ظاهري (إقران القالب في ملف تعريف IKEv2)

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

الخطوة 13 (اختيارية). بشكل افتراضي، يتم إرسال جميع حركات مرور البيانات من العميل عبر النفق (النفق الكامل). يمكنك تكوين نفق تقسيمي، والذي يسمح لحركة المرور المحددة فقط بالمرور عبر النفق.

```
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
```

الخطوة 14 (اختيارية). إن يتطلب كل حركة مرور أن يذهب من خلال النفق، شكلت NAT in order to سمحت إنترنت موصولية لزبون بعيد.

```
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
```

مثال: تكوين تنزيل ملف تعريف AnyConnect

يوضح هذا المثال كيفية تكوين ميزة تنزيل ملف تعريف AnyConnect ل FlexVPN:

✎ ملاحظة: لا تحتاج إلى تعديل ملف "النهج المحلي" على جهاز عميل AnyConnect. بعد تكوين ميزة تنزيل ملف تعريف AnyConnect باستخدام IKEv2، تعمل وحدة تحميل VPN للتنزيل بشكل صحيح - يتم تحديث ملف تعريف XML المطلوب تلقائيا على جهاز العميل في حالة تحديث ملف تعريف XML.

✎ ملاحظة: يجب عدم إستخدام خادم HTTPS ونهج SSL معا. قبل تمكين نهج SSL، قم بإزالة الأمر ip http secure-server. إذا تم تمكين كل من هذه المميزات في نفس الوقت واستلم الجهاز اتصال SSL VPN وارد، فيمكن أن يتعطل الجهاز.

```
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
```

تعطيل إمكانية تنزيل AnyConnect (للإصدارات الأقدم من 16.9.1 فقط).

تكون هذه الخطوة ضرورية فقط في حالة إستخدام إصدار أقدم من 16.9.1. قبل هذا الإصدار، لم تكن إمكانية تحميل ملف تعريف XML إلى الموجه متوفرة. يحاول العميل الآمن (AnyConnect) إجراء تنزيل ملف تعريف XML بعد تسجيل الدخول الناجح بشكل افتراضي. إذا لم يكن التوصيف متاحا يفشل التوصيل. كحل بديل، من الممكن تعطيل قدرة تنزيل ملف تعريف AnyConnect على العميل نفسه. للقيام بذلك، يمكن تعديل هذا الملف:

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

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

تم تعيين خيار BypassDownloader على true، على سبيل المثال:

<#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>
```

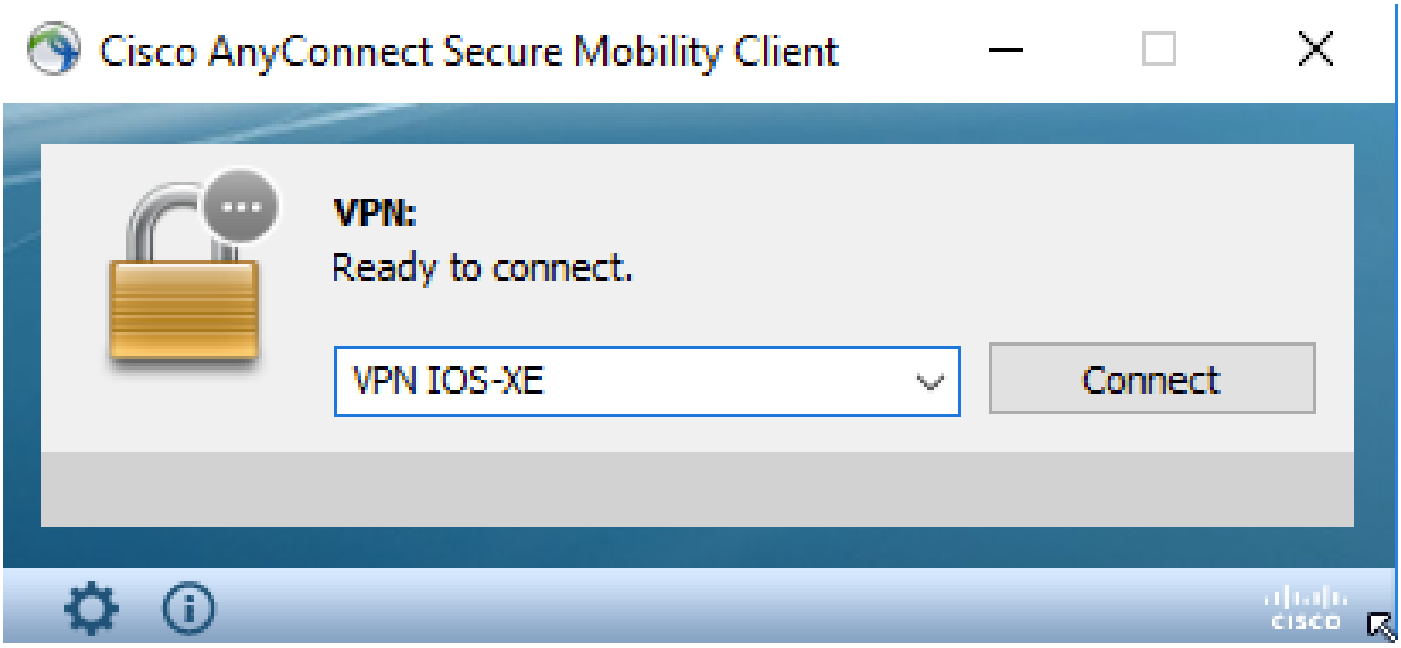
بعد التعديل، يلزم إعادة تشغيل عميل AnyConnect.

تسليم ملف تعريف AnyConnect XML

مع التثبيت الجديد ل AnyConnect (بدون ملفات تعريف XML مضافة)، يمكن للمستخدم إدخال FQDN لعبارة VPN يدويا في شريط عناوين عميل AnyConnect. ينتج عن ذلك اتصال SSL بالبوابة. ال يحاول عميل AnyConnect إنشاء نفق VPN باستخدام بروتوكولات IKEv2/IPsec بشكل افتراضي. هذا هو السبب الذي يجعل تثبيت ملف تعريف XML على كمبيوتر العميل إلزاميا لإنشاء نفق IKEv2/IPsec باستخدام بوابة FlexVPN.

يستخدم التوصيف عند تحديده من القائمة المنسدلة بشريط عناوين AnyConnect.

يتم تحديد الاسم الذي يظهر في القائمة في حقل اسم العرض في محرر ملف تعريف AnyConnect -> قائمة الخوادم -> إدخال قائمة الخوادم.

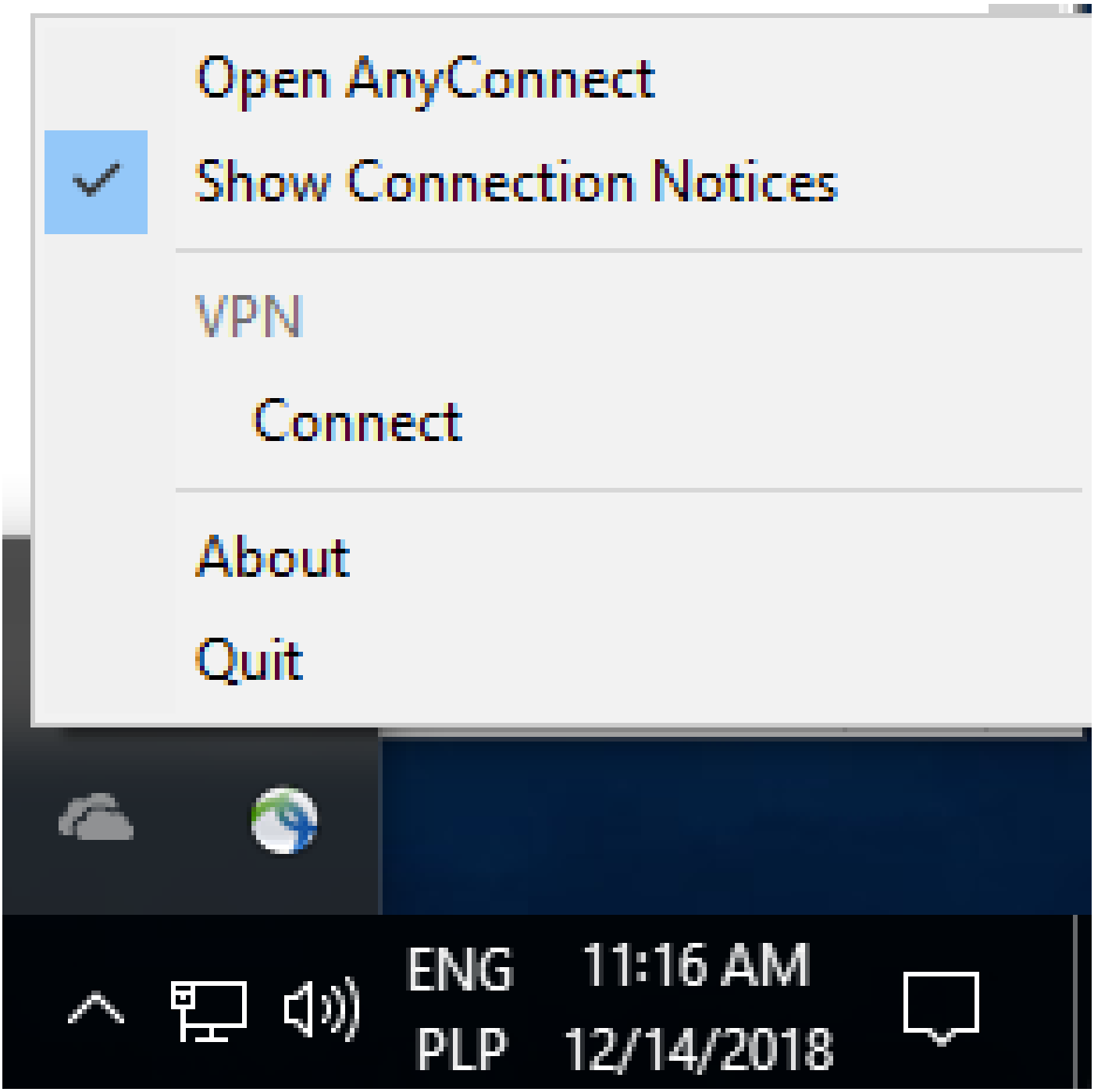


يمكن وضع ملف تعريف XML يدويا في دليل، حسب نظام تشغيل العميل:

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

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

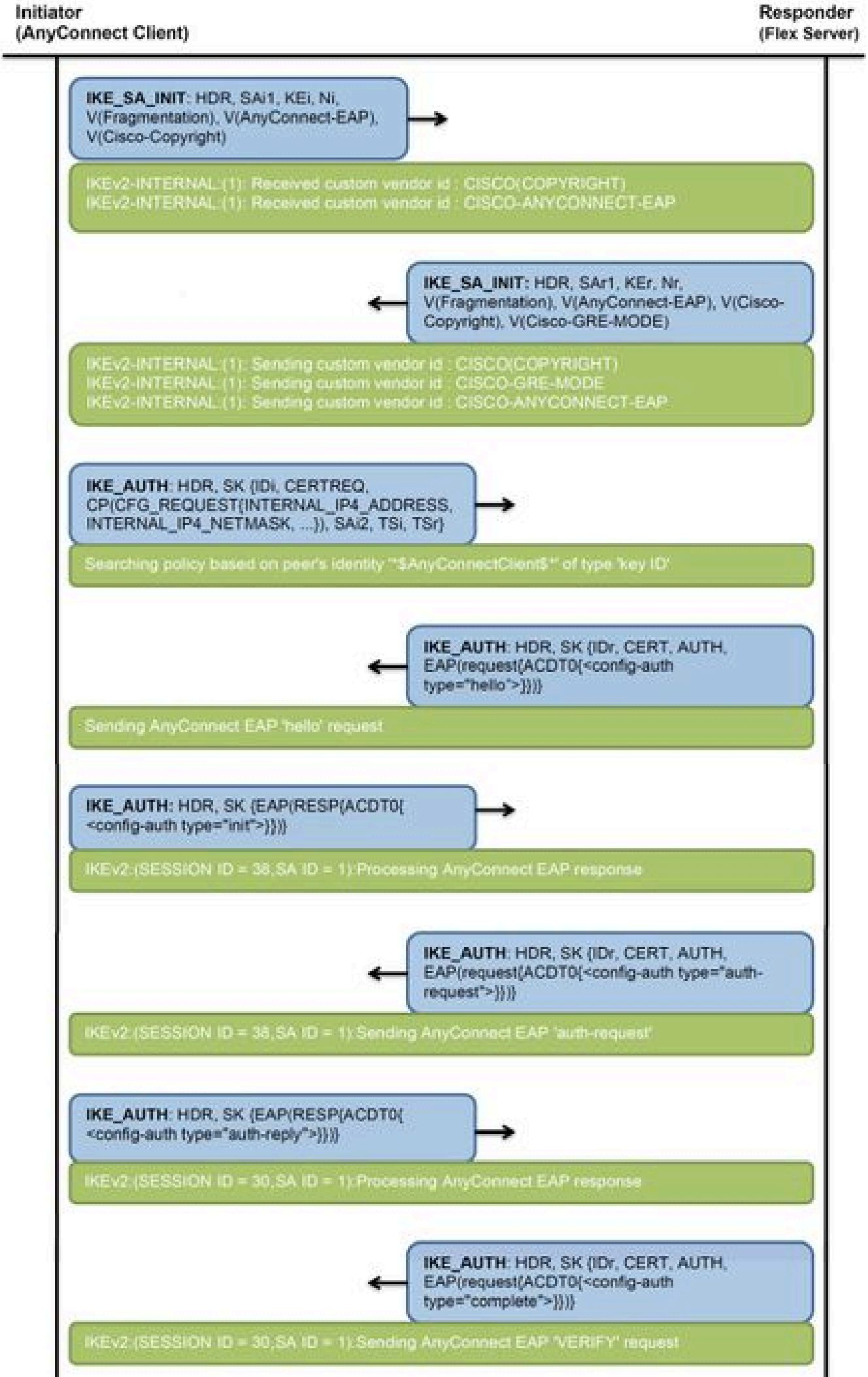
يلزم إعادة تشغيل عميل AnyConnect حتى يصبح ملف التعريف مرئيا في واجهة المستخدم الرسومية (GUI). الا يكفي إغلاق نافذة AnyConnect. يمكن إعادة تشغيل العملية بالنقر بزر الماوس الأيمن على أيقونة AnyConnect في درج Windows وحدد خيار إنهاء:



تدفق الاتصالات

انقر هنا

تبادل IKEv2 و 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
```

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

1. تصحيح أخطاء IKEv2 للتجميع من وحدة الاستقبال والبث:

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

2. تصحيح أخطاء المصادقة والتفويض والمحاسبة (AAA) للاطلاع على تعيين السمات المحلية و/أو البعيدة:

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

3. أداة التشخيص وإعداد التقارير (DART) لعميل AnyConnect.
لتجميع حزمة DART، قم بتنفيذ الخطوات الموضحة في دليل مسؤول Cisco Secure Client (بما في ذلك AnyConnect)، الإصدار 5، الفصل: الفصل: أستكشاف أخطاء Cisco Secure ClientDocument وإصلاحها.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).