

# ل دعب نع لوصول FlexVPN: نيوكت تانايب ةدعاق مادختساب AnyConnect IKEv2 يلحمل مدختسمل

## تايوتحمل

[ةمدقملا](#)

[ةيساسألا تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسمل تانوكملا](#)

[ةيساسأ تامولعم](#)

[ةكبش ليل يطيطختلا مسرلا](#)

[نيوكتلا](#)

[ةيلحمل تانايبلا ةدعاق مادختساب ني مدختسمل لضيوفتلا ةقداصملا](#)

[\(يرايخ\) AnyConnect ليزنت ةيناكملا ليطعت](#)

[AnyConnect XML فيرعت فلم ميلاست](#)

[تالاصتالاق فدت](#)

[EAP و IKEv2 لدابت](#)

[ةحصللا نم ققحتلا](#)

[اهخالص او اعاطخألا فاشكتسا](#)

## ةمدقملا

Cisco IOS®/ XE زارطلل ثبل او لابق تسالا ةدحو نيوكت ةيفيك دن تسمل اذه حضوي مدختسمل تانايب ةدعاق مادختساب AnyConnect IKEv2 / EAP ةقداصم ربع اهيل لوصول يلحمل.

## ةيساسألا تابلطتملا

### تابلطتملا

ةيلاتلا عيضاوملاب ةفرعم كيدل نوكت نأ Cisco ي صوت:

- IKEv2 لوكوتورب

### ةمدختسمل تانوكملا

ةيلاتلا ةيدامل تانوكملا او جماربلا تارادصا يل دن تسمل اذه في ةدراولا تامولعمل دن تست:

- Cisco IOS® XE 16.9.2 لغشي يذلا Cisco نم ةباحسلا تامدخ هجوم
- AnyConnect Client رادصا ال 4.6.03049 يذلا Windows 10 ل معي يذلا

ةصاخ ةي لمعم ةئي ب ي ف ةدوجوملا ةزهجالا نم دنتسملا اذه ي ف ةدراوللا تامولعمللا ءاشنإ م ت تناك اذا .(يضا رتفا) حوسمم نيوك تب دنتسملا اذه ي ف ةمدختسُملا ةزهجالا عيمج ت ادب رما يأل لمحتحمللا ريثأتلل كمهف نم دكأتف ،ليغشتلا دي ق ك تكبش

## ةيساسأ تامولعم

ةيناكمإ Flex مداخل ،ةي عيمجتلا ةقداصملا مساب اضيأ فورعمللا ،AnyConnect-EAP حيتي Cisco نم ةصاخلا AnyConnect-EAP ةقيرط ربع AnyConnect ليمع ةقداصم

ةقاطب لثم ىلإ ةدنتسملا ةيسايقلا (EAP) عسوتملا ةقداصملا لوكوتورب قرطك سيل لمعي ال ،كلذ ىلإ امو EAP- Message Digest 5 (EAP-MD5) و EAP (EAP-GTC) ماعال زيمملا زمرا EAP ريرمت عضو ي ف Flex مداخل

مدختسملا بولطملا ةسلجلا حاتفمو Flex Server ىلع ليمعلا عم EAP تالاصتإ عيمج يهتني Flex Server ةطساوب اي لحم هباسح متي ةقداصملا ةلومح ءاشنإل

بولطم وه امك تاداهشلا م ادختساب ليمعلا ىدل هسفن ةقداصمب نرملا مداخل موقوي نأ بجي IKEv2 RFC ةطساوب

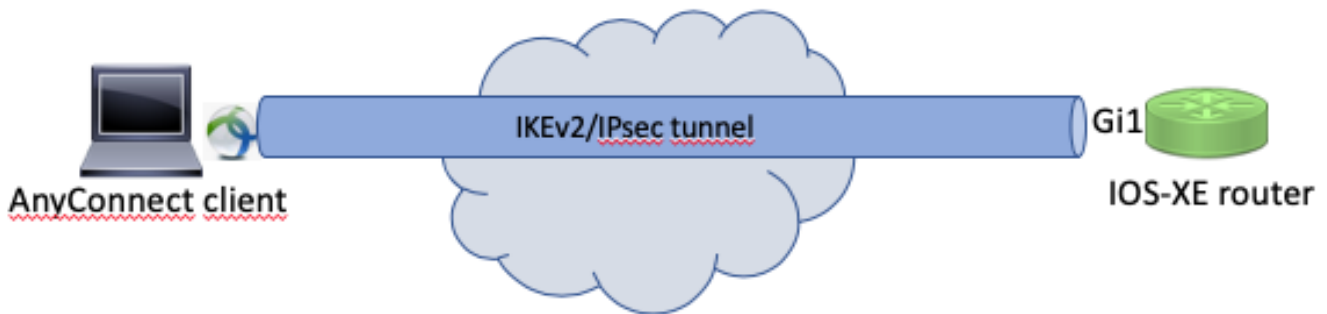
ةيرايخإ دع ب نع ةقداصملا او Flex Server ىلع نأل ةم و عدم يلحملا مدختسملا ةقداصم

نع لوصوللا يمدختسم ددع اهيف لقي يتلا ريغص قاطن ىلع رشنلا تاي لمعل يلاثم اذهو ضيوفتلا ةقداصملا مداخل لوصوللا ةيناكمإ اهيف رفوتت ال يتلا تائيبللا يفو دع ب ي ج راخلا (AAA) ةب س احملا و

اهيف نوكت يتلا تاهوي رانيسيلا يفو قاطنلا ةعساو رشنلا تاي لمعل ةب سننلابف ،كلذ عمو ةقداصملا ي ج راخ AAA مداخل م ادختساب ىصوي لازي ال ،ةبولطم مدختسم لك تامس ضيوفتلا و


ةب س احملا و لي وختلا و دع ب نع ةقداصملا ل RADIUS م ادختسا AnyConnect-EAP ذي فن ت حيتي

## ةكبش ل ل يطي طختلا مسرلا



## نيوكتلا

## ةي ل ح م ل ا ت ا ن ا ي ب ل ا ة د ع ا ق م ا د خ ت س ا ب ن ي م د خ ت س م ل ل ض ي و ف ت ل ا و ة ق د ا ص م ل ا

 مزل ي ، ه ج و م ل ا ي ل ع ة ي ل ح م ل ا ت ا ن ا ي ب ل ا ة د ع ا ق ي ل ع ن ي م د خ ت س م ل ا ة ق د ا ص م ل : ة ط ح ا ل م  
R S A - ي ل ح م ل ا ة ق د ا ص م ل ا ب و ل س ا ن و ك ي ن ا ب ج ي ، E A P م ا د خ ت س ا ل ، ك ل ذ ع و م و . E A P م ا د خ ت س ا  
ة د ا ه ش ن و ك ي ن ا ن ك م ي ا ل و ، ه ي ل ع ة ت ب ث م ة ب س ا ن م ة د ا ه ش ي ل ا ه ج و م ل ا ج ا ت ح ي ك ل ذ ل ، S i g ،  
ا ي ت ا ذ ة ع ق و م .

د ي ع ب ل ا م د خ ت س م ل ا ل ي و خ ت و ي ل ح م ل ا م د خ ت س م ل ا ة ق د ا ص م م د خ ت س ي ي ذ ل ا ن ي و ك ت ل ا ج ذ و م ن  
د ع ب ن ع ة ب س ا ح م ل ا و ة و م ج م ل ا و .

ة ق د ا ص م ل ا م ئ ا و ق ن ي و ك ت و ( A A A ) ة ب س ا ح م ل ا و ض ي و ف ت ل ا و ة ق د ا ص م ل ا ن ي ك م ت . 1 ة و ط خ ل ل  
ة ي ل ح م ل ا ت ا ن ا ي ب ل ا ة د ع ا ق ي ل ا م د خ ت س م م س ا ة ف ا ض ا و ة ب س ا ح م ل ا و ض ي و ف ت ل ا و :

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

د ا ر ي ت س ا م ا د خ ت س ا م ت ي . ه ج و م ل ا ة د ا ه ش ب ط ا ف ت ح ا ل ل ة ص ص خ م ة ق ث ة ط ق ن ن ي و ك ت . 2 ة و ط خ ل ل  
P K I ن ي و ك ت ل ي ل د ة ع ج ا ر م ي ج ر ي ، ي ر خ ا ت ا ر ا ي خ ي ل ع ل و ص ح ل ل . ل ا ث م ل ا ا ذ ه ي ف P K C S 1 2 ف ل م  
( م ا ع ا ل ح ا ت ف م ل ل ة ي س ا س ا ل ا ة ي ن ب ل ) :

[https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec\\_conn\\_pki/configuration/xr-3s/sec-pki-xr-3s-book/sec-cert-enroll-pki.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/xr-3s/sec-pki-xr-3s-book/sec-cert-enroll-pki.html)

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

A n y C o n n e c t V P N : ء ا ل م ع ي ل ا ن ي و ا ن ع ل ا ن ي ي ع ت ل ي ل ح م ل ا I P ع م ج ت د د ح . 3 ة و ط خ ل ل

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

I K E v 2 : ي ل ح م ل ي و خ ت ج ه ن ء ا ش ن ا . 4 ة و ط خ ل ل


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

اذه نيوكت مدع ةلاح ي ف .نېبولطم ال IKEv2 ةسايس و حرتقم ءاشن اب مق .(ةيرايتخا) 5 ةوطخال  
ة: كذلا تايضارت فالال مادختسا متي ،رايخال

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

AnyConnect في صوت ءاشن | 6. ةوطخال

---

 لىل عوجرلا ىجرى .لېمعال زاھ ىل | AnyConnect في رعت فلم مېلست مزلي :ةظالم  
تامولعملال نم ديزم ىلع لوصحلل يلاتال مسقلا

---

في حضورم وه امك AnyConnect في رعت فلم ررحم مادختساب لېمعال في رعت فلم نيوكتب مق  
ةروصل:

VPN

- Preferences (Part 1)
- Preferences (Part 2)
- Backup Servers
- Certificate Pinning
- Certificate Matching
- Certificate Enrollment
- Mobile Policy
- Server List

### Server List

Profile: Untitled

Hostname	Host Address	User Group	Backup Server List	SCEP	Mobile Settings	Certificate Pins

Note: it is highly recommended that at least one server be defined in a profile.

Add... Delete

Edit... Details

Help

دېدحت نم دكأت (VPN) ډېره اظلاله صاخلا ډكېشل ل ډاوبل ل اځد اءاشن اءل "ډفاضا" قوف رونا ډرابع "ASA" راځل دېدحت اءاغل اء م ق. "ډساسا لوكوټورب" ك "IPsec".

Server **Load Balancing Servers** SCEP Mobile Certificate Pinning

**Primary Server**

Display Name (required)

FQDN or IP Address  /

User Group

Group URL

**Connection Information**

Primary Protocol

ASA gateway

Auth Method During IKE Negotiation

IKE Identity (IOS gateway only)

**Backup Servers**

Host Address	
	<input type="button" value="Add"/>  <input type="button" value="Move Up"/> <input type="button" value="Move Down"/> <input type="button" value="Delete"/>


في رعتال فل مل XML فدارم .م س اب ظ فح -> File :ص ي ص خ ت ال فل م ظ فح


```
<?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>

```

 عون للية ضارته الة IKE ةوهك "\$AnyConnectClient\$" AnyConnect مدختسي :ةظالم ةقباطم ل AnyConnect فيرت فلم في ايودي ةوهال هذه ريرغت نكمي ،كلذ عمو .key-id رشنللا تاجايتح

 Cisco IOS® XE 16.9.1 رادصل رفوت مزلي ،هجوم الة الة XML فيرت فلم ليمحتل :ةظالم ليطعت مزلي ، Cisco IOS® XE جم انرب نم مدق الة رادصل الامدختسل لاج في .ثدح رادصل وة ينالمة ليطعت "مسق الة الة عوجرل ايجري .ليمعل الة فيرتل فلم ليزنت ةردق .تامولعمل نم ديزم الة لوصحلل "AnyConnect" ليزنت


ددو هجوم لل (ةتقؤم الة الة) Flash ةركاذ الة الة ؤاشنل مة ذل الة XML فيرت فلم ليمحتب مق فيرتل فلم:


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

 acvpn.xml وه AnyConnect XML فيرت فلم لمدختسي يذال فلمل مسال :ةظالم

ليمعل الة ةقداصل ل AnyConnect-EAP بولسل الة IKEv2 فيصوت ؤاشنل .7 ةوطخل


```
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
```

 ةقداصملا ةقيرط لبق دعب نع ةقداصملا ةقيرط نيوكت CLI لبق ي: ةظالم ني سحتل بلطب صاخلا حالصإلإ يلع يوتحت ال يتل تارادصلإ يلع رثوي ال هنكلو EAP دعب نع ةقداصملا بولسأ ناك اذا، [CSCvb29701](#) Cisco نم ءاطخأل احيحصت فرعم نيوكت نم دكأت، دعب نع ةقداصم ةقيرطك EAP نيوكت دنع، تارادصلإ هذهل ةبس نلاب رخأ لكش يأ عم ةلكشملا هذه رهظت ال. الوأ rsa-sig ةقيرطك ةقداصملا ةقيرط دعب نع ةقداصملا قرط نم.

 ةقداصملا ةقيرط نيوكت نم دكأت، دعب نع ةقداصملا بولسأ ناك اذا، [CSCvb24236](#) Cisco نم ءاطخأل احيحصت فرعمب ةرثأت ملام زمرلا تارادصلإ ي: ةظالم ةقيرط نيوكت نم دكأت، دعب نع ةقداصملا بولسأ ناك اذا، [CSCvb24236](#) Cisco نم ءاطخأل احيحصت فرعمب ةرثأت ملام زمرلا تارادصلإ ي: ةظالم ةقيرط نيوكت نم دكأت، دعب نع ةقداصملا بولسأ ناك اذا، [CSCvb24236](#) Cisco نم ءاطخأل احيحصت فرعمب ةرثأت ملام زمرلا تارادصلإ ي: ةظالم ةقيرط نيوكت نم دكأت، دعب نع ةقداصملا بولسأ ناك اذا، [CSCvb24236](#) Cisco نم ءاطخأل احيحصت فرعمب ةرثأت ملام زمرلا تارادصلإ ي: ةظالم

هجوم ال يلع HTTP مداخل و HTTP-URL ال ةدنتسملا ةداهش ال نع ثحبل ليطعت. 8 ةوطخلا

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

 تاي مزراوخ معدت كيدل هجوملا ةزهجأ تناك اذا ام ديكأتل [دنتسملا اذه يلا](#) عجرا: ةظالم IPsec SA تيبثت نإف ال او، (NGE تاي مزراوخ نمضت ي قباسل لاثملا) NGE ريفشت ضوافتلا نم ةقيرط ال ءاطخأل ءاطخأل لشف ي زاهج ال يلع.

تانايب ال ةمامحل ةمدختسملا ةئزجتلا تاي مزراوخ و ريفشتلا فيرعت. 9 ةوطخلا

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

IPsec فيرعت فلم ءاشن. 10 ةوطخلا

```
crypto ipsec profile AnyConnect-EAP
```



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

لوصول تاهجاو ريعتست .يمهو IP ناونع مادختساب عاجرتسا ةهجاو نيوكتب مق 11 ةوطخال  
اهنم IP ناونع يرهاظال

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

IKEv2 فيرعت فلم في بلالال نارقال يرهاظ بلال نيوكت 12 ةوطخال

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

ليعمل نم تانايا بلال رورم تاكرح عيجم لاسرا متي، يضارتفا لكش ب (ياري تخا) STEAP 13  
طقف ةددمال رورمال ةكرحل حمسي يذلاو، ماسقنا قف ننيوكت كنكمي .قفنل ربح  
قفنل ربح لاقتنالاب

```
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
```

NAT in order تلكش، قفنل لالال نم بهذي نأ رورم ةكرح لك بلطتي نا (ةياري تخا) 14 ةوطخال  
ديعب نوبزل ةي لوصولم تنرتنل تحتمس to

```
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
```

## (ياري تإخ) AnyConnect لي زنت ةي ناك مإ لي طعت

نم مدق أال Cisco IOS® XE جمانرب رادصإ مادختسإ ةلاحي ف طقف ةيرورص ةوطخلال هذه نوكت هجومل إلى XML فيرعت فلم لي محت ةي ناك مإ نكت مل Cisco IOS® XE 16.9.1 لبق 16.9.1 حجانل لوخدل لي جست دعب XML فيرعت فلم لي زنت ةارجإ AnyConnect لي مع لواحي. ةرفوت نم كل ممل نم، لي دب لحك. لي صوتل لش في احاتم في صوتل نكي مل اذا. يضا رتفا لك شب نكمي، كلذب مايق لل. هس فن لي عمل إلى AnyConnect فيرعت فلم لي زنت ةردق لي طعت فل مل اذه لي دعته:

For Windows:

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

For MAC OS:

/opt/cisco/anyconnect/AnyConnectLocalPolicy.xml

لاثمل لي بس إلى ع، "true" إلى ع "BypassDownloader" ياري ناي عت متي:

```
<?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>
```

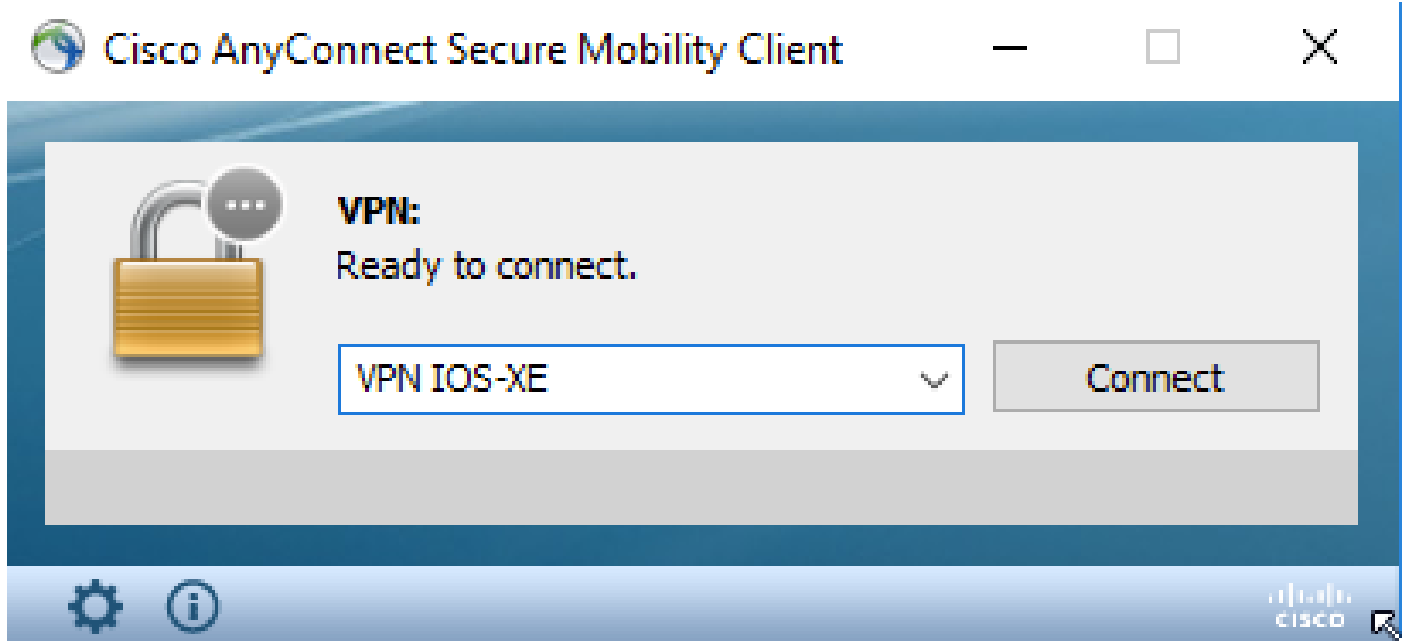
AnyConnect لي مع لي غشت ةداعإ مزلي، لي دعته ل دعب.

## AnyConnect XML فيرعت فلم مي لسنت

مدختس مل ل نكمي، (ةفاضم XML فيرعت تا فلم نودب) AnyConnect ل دي دجلال تي بثت لا عم لاصتا كل ذنع جتن ي. AnyConnect لي مع ني وانع طيرش ي ف ايودي VPN ةرابعل FQDN لإخدا تالوكوتورب مادختساب VPN ق فن عاشن AnyConnect لي مع لواحي ال. ةابواب ل SSL لي عمل إلى ع XML فيرعت فلم تي بثت ي ف ببسلا وه اذه. يضا رتفا لك شب IKEv2/IPsec لي عمل إلى ع XML فيرعت فلم تي بثت ي ف ببسلا وه اذه. يضا رتفا لك شب IKEv2/IPsec ق فن عاشن إلى ي مازلإ VPN Cisco IOS® XE ةابواب مادختساب IKEv2/IPsec ق فن عاشن إلى ي مازلإ

AnyConnect نڤوانع طڤر شڤ ةلدس نمل ةمئاقلا نم هدي دحت دنع فڤصوتلا مدختسڤ

فڤرعت فلم ررحم فڤ "ضرعلا مسا" ف ددحملا مسالا سفن وه رهظي يذلا مسالا AnyConnect.



للدلا اذف فڤ اڤوڤي XML فڤرعت فلم عضو نكمڤ

For Windows:

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

For MAC OS:

/opt/cisco/anyconnect/profile

مدختسمل ةهجاو فڤ اڤررم فڤرعتلا فلم حبصڤ ىتح AnyConnect لڤمع لڤغشت ةداعا مزلف رقنلاب ةڤلمعلا لڤغشت ةداعا نكمڤ. AnyConnect ةذفان قالاغ ا فڤكڤ ال. (GUI) ةڤموسرلا "ءاهن" راڤلا دڤدحتو Windows جرد فڤ AnyConnect زمر ىلع نمڤال سواملا رزب

Open AnyConnect



Show Connection Notices

VPN

Connect

About

Quit



ENG

11:16 AM

PLP

12/14/2018



تالاصتالاقفدت

EAP و IKEv2 لدابت

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
```

اه حال صإو ءاطخأل فاشك تسإ

اهال صاوا نيوكتلا اءاطخأ فاشكتسال اهم ادختسا كنكمي تامولعم مسقلا اذه رفوي

1. ثبلاو لابقتسال اءءوو نم عيمجتلل IKEv2 اءاطخأ حيحصت

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

2. تامسال نييعت ىلع عالطالل (AAA) ةبسالامل او ضيوفتلاو ةقداصلما اءاطخأ حيحصت  
ءءيعبلا و/او ةيحمللا:

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

3. DART نمل AnyConnect.



ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت  
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او  
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب  
Cisco ةللخت. فرتمة مچرت مء دقء ةللأل ةل فارتحال ةمچرتل عم لاعل او  
ىل إلمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco  
Systems (رفوتم طبارل) ةل صأل ةل ءل ءن إل دن تسمل