

# ىلإ دعب نع لوصول ا FlexVPN: رشن AnyConnect IKEv2 EAP-MD5 م ادختساب

## المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [الرسم التخطيطي للشبكة](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [الاصطلاحات](#)
- [الخلفية](#)
- [التكوين الأولي IOS](#)
- [IOS - CA](#)
- [IOS - شهادة الهوية](#)
- [تكوين IOS - AAA و RADIUS](#)
- [التهيئة الأولية ل ACS](#)
- [تكوين IOS FlexVPN](#)
- [تكوين Windows](#)
- [إستيراد CA إلى Windows Trust](#)
- [تكوين توصيف AnyConnect XML](#)
- [الاختبارات](#)
- [التحقق](#)
- [موجه IOS](#)
- [ويندوز](#)
- [المحاذير والمشكلات المعروفة](#)
- [تشفير الجيل التالي](#)
- [معلومات ذات صلة](#)

## المقدمة

يقدم هذا المستند نموذجاً لتكوين كيفية إعداد الوصول عن بعد على IOS باستخدام مجموعة أدوات FlexVPN.

تتيح الشبكة الخاصة الظاهرية (VPN) للوصول عن بعد للعملاء النهائيين الذين يستخدمون أنظمة تشغيل مختلفة إمكانية الاتصال على نحو آمن بشبكاتهم المؤسسية أو المنزلية من خلال وسط غير آمن مثل الإنترنت. في السيناريو المقدم، يتم إنهاء نفق VPN على موجه Cisco IOS باستخدام بروتوكول IKEv2.

يوضح هذا المستند كيفية مصادقة المستخدمين وتحويلهم باستخدام خادم التحكم في الوصول (ACS) من خلال طريقة EAP-MD5.

## المتطلبات الأساسية

## الرسم التخطيطي للشبكة

يحتوي موجه IOS من Cisco على واجهتين - واحدة نحو ACS 5.3:



## المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

## المكونات المستخدمة

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

- ACS 5.3 مع حزمة 6
- موجه IOS مع برنامج M(4)15.2
- جهاز الكمبيوتر الذي يعمل بنظام التشغيل Windows 7 مع AnyConnect 3.1.01065

## الاصطلاحات

راجع [اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.](#)

## الخلفية

في IKEv1 Xauth الذي يتم استخدامه في المرحلة 1.5، يمكنك مصادقة المستخدمين محليا على موجه IOS واستخدام +RADIUS/TACACS عن بعد. لا يدعم IKEv2 Xauth ولا يدعم المرحلة 1.5 بعد ذلك. وهو يحتوي على دعم EAP مضمن، والذي يتم في المرحلة IKE\_AUTH. وتتمثل الميزة الكبرى لهذا الطراز في تصميم الإصدار الثاني من بروتوكول IKEv2، وبعد الطراز EAP معيارا معروفا.

يدعم EAP وضعين:

- الاتصال النفقي—EAP-TLS و EAP/PSK و EAP-PEAP، إلخ.
  - غير الاتصال النفقي—EAP-MD5، EAP-GTC، EAP-MSCHAPv2، وما إلى ذلك.
- في هذا المثال، يتم استخدام EAP-MD5 في وضع عدم الاتصال النفقي لأنه أسلوب المصادقة الخارجية EAP المدعوم حاليا في ACS 5.3.

لا يمكن استخدام EAP إلا لمصادقة بادئ (العميل) المستجيب (IOS في هذه الحالة).

## التكوين الأولي IOS

أولاً، أنت تحتاج إلى إنشاء مرجع مصدق (CA) وإنشاء شهادة هوية لموجه IOS. سيقوم العميل بالتحقق من هوية الموجه استناداً إلى هذه الشهادة.

يبدو تكوين CA على IOS كما يلي:

```
crypto pki server CA
grant auto
hash sha1
eku server-auth client-auth
```

تحتاج إلى تذكّر استخدام المفتاح الموسع (مصادقة الخادم مطلوبة ل EAP، و RSA-SIG تحتاج أيضاً إلى مصادقة العميل).

قم بتمكين CA باستخدام الأمر `no shutdown` في خادم PKI للتشغيل.

## IOS - شهادة الهوية

بعد ذلك، قم بتمكين بروتوكول تسجيل الشهادة البسيط (SCEP) للشهادة وتكوين TrustPoint.

```
ip http server
crypto pki trustpoint CA-self
enrollment url http://10.1.1.2:80
fqdn 10.1.1.2
ip-address 10.1.1.2
subject-name cn=10.1.1.2,ou=TAC
revocation-check none
eku request server-auth client-auth
```

ثم قم بمصادقة الشهادة وتسجيلها:

```
config)#crypto pki authenticate CA-self)
:Certificate has the following attributes
Fingerprint MD5: 741C671C 3202B3AE 6E05161C 694CA53E
Fingerprint SHA1: 8C99513C 2198470F 7CB58FA2 32D8AA8D FC31D1ED
Do you accept this certificate? [yes/no]: yes %
.Trustpoint CA certificate accepted

R1(config)#crypto pki enroll CA-self
%
.. Start certificate enrollment %
Create a challenge password. You will need to verbally provide this %
.password to the CA Administrator in order to revoke your certificate
.For security reasons your password will not be saved in the configuration
.Please make a note of it
:Password
:Re-enter password
The subject name in the certificate will include: cn=10.1.1.2,ou=TAC %
The subject name in the certificate will include: 10.1.1.2 %
Include the router serial number in the subject name? [yes/no]: no %
The IP address in the certificate is 10.1.1.2 %
Request certificate from CA? [yes/no]: yes
Certificate request sent to Certificate Authority %
The 'show crypto pki certificate verbose CA-self' command %
.will show the fingerprint
#(R1(config)
:Dec 2 10:57:44.141: CRYPTO_PKI: Certificate Request Fingerprint MD5*
BF8EF4B6 87FA8162 9079F917 698A5F36
:Dec 2 10:57:44.141: CRYPTO_PKI: Certificate Request Fingerprint SHA1*
```

AC13FEA3 295F7AE6 7014EF60 784E33AF FD94C41D

#(R1(config

Dec 2 10:57:44.198: %PKI-6-CERTRET: Certificate received from\*  
Certificate Authority

إذا لم تكن ترغب في الحصول على رسائل مطالبة في AnyConnect، فتذكر أنه يجب أن يكون CN مساويا لعناوين IP/hostname التي تم تكوينها في ملف تعريف AnyConnect.

في هذا المثال، cn=10.1.1.2. لذلك، يتم إدخال 10.1.1.2 كعنوان IP للخادم في ملف تعريف AnyConnect xml.

## تكوين AAA - IOS و RADIUS

تحتاج إلى تكوين مصادقة مصادقة مصادقة AAA والتفويض:

```
aaa new-model
radius-server host 192.168.56.202 key cisco
aaa group server radius SERV
server 192.168.56.202
aaa authentication login eap-list group SERV
aaa authorization network eap-list group SERV
```

## التهيئة الأولية ل ACS

أولا، أضف جهاز الشبكة الجديد في ACS (موارد الشبكة < أجهزة الشبكة وعملاء AAA < إنشاء):

The screenshot shows the configuration page for a new device in ACS. The 'Name' field is 'R1'. The 'Description' field is empty. Under 'Network Device Groups', 'Location' is 'All Locations' and 'Device Type' is 'All Device Types'. The 'IP Address' section has 'Single IP Address' selected, with the IP '192.168.56.2'. The 'Authentication Options' section has 'TACACS+' and 'RADIUS' tabs. Under 'RADIUS', 'Shared Secret' is 'cisco', 'CoA port' is '1700', 'Enable Keyvector' is unchecked, 'Key Encryption Key' is empty, 'Message Authentication Code Key' is empty, and 'Key Input Format' is 'HEXADECIMAL'. A legend at the bottom left indicates that orange dots represent required fields. The 'Submit' and 'Cancel' buttons are at the bottom.

إضافة مستخدم (المستخدمون ومخازن الهوية < مخازن الهوية الداخلية < المستخدمون < إنشاء):

Users and Identity Stores > Internal Identity Stores > Users > Create

**General**

Name: user3 Status: Enabled

Description:

Identity Group: All Groups

**Password Information**

Password must:

- Contain 4 - 32 characters

Password Type: Internal Users

Password: ●●●●●●

Confirm Password: ●●●●●●

Change password on next login

**User Information**

There are no additional identity attributes defined for user records

● = Pola wymagane

**Enable Password Information**

Password must:

- Contain 4 - 32 characters

Enable Password:

Confirm Password:

إضافة مستخدم للتحويل. في هذا المثال، إنها إيكست. يجب أن تكون كلمة المرور "cisco" لأنها الافتراضية التي يتم إرسالها بواسطة IOS.

**General**

Name: IKETEST Status: Enabled

Description:

Identity Group: All Groups

**Password Information**

Password must:

- Contain 4 - 32 characters

Password Type: Internal Users

Password: ●●●●●●●●

Confirm Password: ●●●●●●●●

Change password on next login

**User Information**

There are no additional identity attributes defined for user records

● = Pola wymagane

بعد ذلك، قم بإنشاء ملف تخصيص تحويل للمستخدمين (عناصر النهج < التحويل والأذونات < الوصول إلى الشبكة < ملفات تخصيص التحويل < إنشاء).

في هذا المثال، تسمى البركة. في هذا المثال، يتم إدخال زوج AV للنفق المنقسم (كبادئة) وإطار عنوان IP كعنوان IP سيتم تعيينه للعميل المتصل. يمكن العثور على قائمة بجميع أزواج الصوت والفيديو المدعومة هنا:

[http://www.cisco.com/en/US/docs/ios-xml/ios/sec\\_conn\\_ike2vpn/configuration/15-2mt/sec-apx-flex-rad.html](http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/15-2mt/sec-apx-flex-rad.html)

General Common Tasks **RADIUS Attributes**

Common Tasks Attributes

Attribute	Type	Value
-----------	------	-------

Manually Entered

Attribute	Type	Value
Framed-IP-Address	IPv4 Address	192.168.100.200
isco-sw-pair	String	isco:route-set=prefix 10.1.1.0/24

Add A... Edit V... Replace A... Delete

Dictionary Type: RADIUS-ITE

RADIUS Attribute:  Search

Attribute Type:

Attribute Value: Static

= Pola wymagane

Submit Cancel

بعد ذلك، يلزمك تشغيل دعم EAP-MD5 (للمصادقة) و PAP/ASCII (للتحويل) في سياسة الوصول. يتم استخدام الافتراضي في هذا المثال (سياسات الوصول < الوصول الافتراضي للشبكة):

General **Allowed Protocols**

Process Host Lookup

**Authentication Protocols**

▶  Allow PAP/ASCII

▶  Allow CHAP

▶  Allow MS-CHAPv1

▶  Allow MS-CHAPv2

▶  Allow EAP-MD5

▶  Allow EAP-TLS

▶  Allow LEAP


▶  Allow PEAP


▶  Allow EAP-FAST

Preferred EAP protocol

Submit Cancel

قم بإنشاء شرط لنهج الوصول وتعيين ملف تعريف التحويل الذي تم إنشاؤه. في هذه الحالة يتم إنشاء شرط ل  
NDG:Location في كل المواقع، لذلك لكل طلب تراخيص RADIUS سيزود ملف تعريف تحويل التجمع (سياسات  
الوصول < خدمات الوصول < الوصول الافتراضي إلى الشبكة):

**General**  
Name: Rule-1 Status: Enabled 

 The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.

**Conditions**  
 NDG:Location: in All Locations   
 Time And Date: -ANY-

**Results**  
Authorization Profiles:

POOL

You may select multiple authorization profiles. Attributes defined in multiple profiles will use the value from the first profile defined.

يجب أن تكون قادرا على الاختبار على موجه IOS إذا كان المستخدم قادرا على المصادقة بشكل صحيح:

```
R1#test aaa group SERV user3 Cisco123 new-code
User successfully authenticated

USER ATTRIBUTES
"username          0 "user3
addr               0 192.168.100.200
"route-set         0 "prefix 10.1.1.0/24
```

## تكوين IOS FlexVPN

أنت تحتاج أن يخلق IKEv2 اقتراح ونهج (قد لا تحتاج أن، راجع CSCtn59317). يتم إنشاء السياسة فقط لعنوان IP واحد (10.1.1.2) في هذا المثال.

```
crypto ikev2 proposal PROP
  encryption 3des
  integrity sha1
  group 2
```

```
crypto ikev2 policy 5
  match address local 10.1.1.2
  proposal PROP
```

ثم قم بإنشاء ملف تعريف IKEv2 وملف تعريف IPsec الذي سيتم ربطه بالقالب الظاهري.

تأكد من إيقاف تشغيل شهادة http-url، كما هو موصى به في دليل التكوين.

```
crypto ikev2 profile PROF
```



```
match identity remote address 0.0.0.0
match identity remote key-id IKETEST
authentication remote eap query-identity
authentication local rsa-sig
pki trustpoint CA-self
aaa authentication eap eap-list
aaa authorization user eap list eap-list IKETEST
virtual-template 1
```

```
no crypto ikev2 http-url cert
crypto ipsec transform-set transform1 esp-3des esp-sha-hmac
crypto ipsec profile PROF
set transform-set transform1
set ikev2-profile PROF
interface Virtual-Template1 type tunnel
ip unnumbered Ethernet0/0
tunnel mode ipsec ipv4
tunnel protection ipsec profile PROF
```

في هذا المثال، يتم إعداد التفويض استنادا إلى IKETEST للمستخدم، والذي تم إنشاؤه في تكوين ACS.

## تكوين Windows

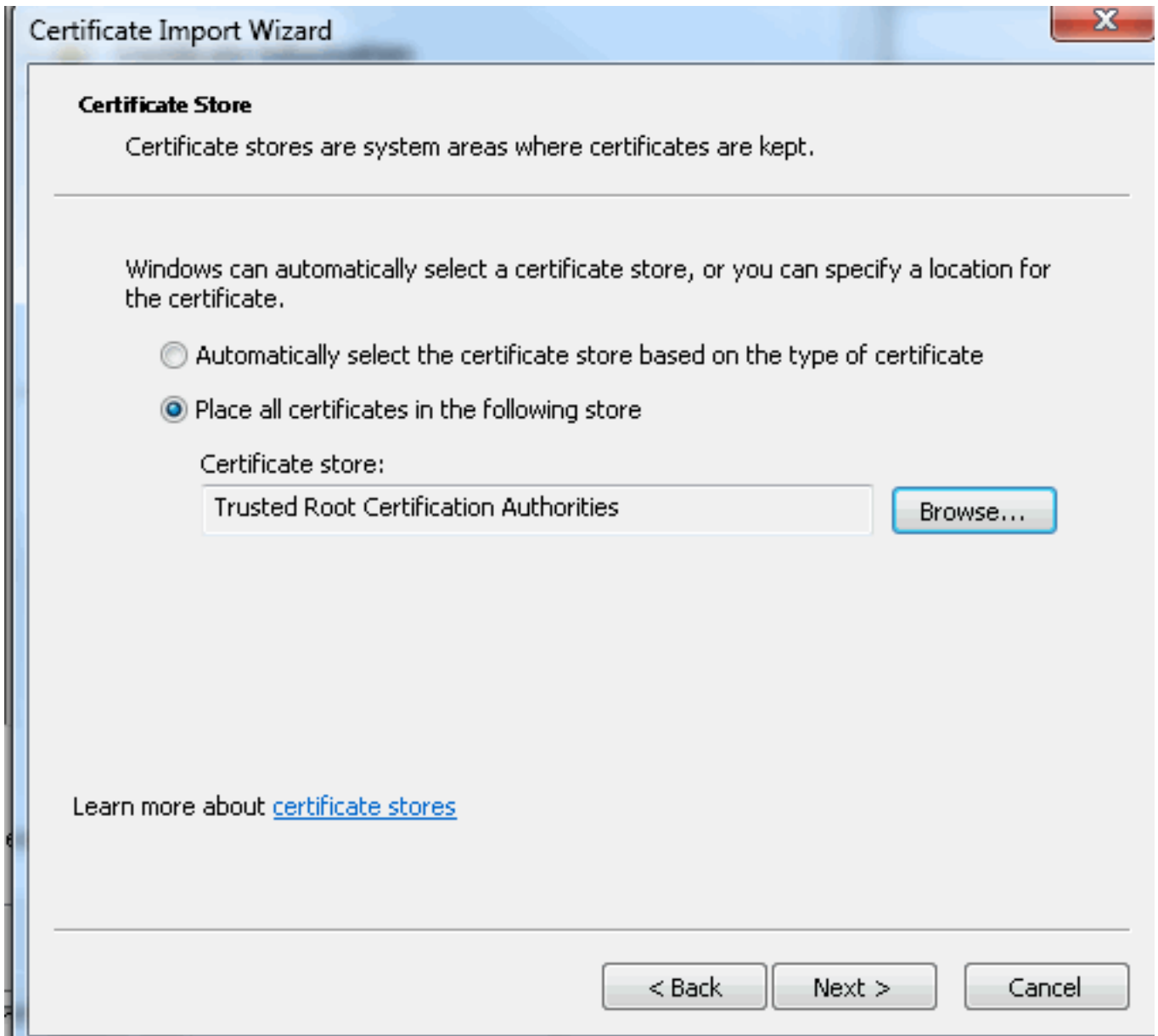
### إستيراد CA إلى Windows Trust

تصدير شهادة المرجع المصدق على IOS (تأكد من تصدير شهادة الهوية وأخذ الجزء الأول فقط):

```
R1(config)#crypto pki export CA-self pem terminal
:CA certificate %
-----BEGIN CERTIFICATE-----
MIIB8zCCAVygAwIBAgIBATANBgkqhkiG9w0BAQUFADANMQswCQYDVQQDEwJDQTAE
Fw0xMjExMjYxNzZmZmZlFw0xNTEyMjYxNzZmZmZlMA0xMzZAJBgNVBAMTAKNBMIGf
MA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCvDR4lH0crj42QfHpRuNu4EyFrLR8H
TbPanXYV+GdCBmu53pDILE00ASEHByD6DYBx01EZuDsio1J7t2MPTguB+YZe6V40
JbtayyxtZGmF7+eDqRegQHHC394adQQWl2oJgQiuTheRDTqDJR8i5gN2Ee+K0sr3
OjnHjUmXb/I6QIDAQABo2MwYTAPBgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQE+
AwIBhjAfbgNVHSMEGDAWgBTH5Sdh69q4HAJulLQYLYbYH0Nk9zzAdBgNVHQ4EFgQU
x+UnYevauBwCbP50GC22B9DZPc8wDQYJKoZIhvcNAQEFBQADgYEADtBLiNXnl+LC
PIgJ0nl/jH5p2IwV1zwbPbZcOsZ9mn54QaqrhmhbHnmqKQJl/20+JPE6p+4noICq
VBrxoiX2KYQ1OwmEScPpQ2XJ9vhGqtQ4Xcx3g20HhxxFDfp2XuW7hwU0W8dTCmZw
=4vodj47qEXKI6pGuzauw9MN1xhkNarc
-----END CERTIFICATE-----
```

انسخ الجزء الموجود بين "شهادة البدء" و"شهادة النهاية" ولصقه في Notepad في Windows والحفظ كملف .ca.crt

تحتاج إلى تثبيته كما هو الحال في المراجع الجذر الموثوق بها (انقر نقرا مزدوجا على الملف < تثبيت الشهادة > وضع جميع الشهادات في المتجر التالي < مراجع التصديق الجذر الموثوق بها):



## تكوين توصيف AnyConnect XML

في C:\ProgramData\Cisco\Cisco يقوم بإنشاء ملف **"any.xml"** ولصق هذا:

```
<?xml version="1.0" encoding="UTF-8?>
  /AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance
  <"xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd
    <ClientInitialization>
  <UseStartBeforeLogon UserControllable="true">>false</UseStartBeforeLogon>
    <"AutomaticCertSelection UserControllable="true"
      <false</AutomaticCertSelection
    <ShowPreConnectMessage>>false</ShowPreConnectMessage>
      <CertificateStore>All</CertificateStore>
    <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>
```

```

<ClearSmartcardPin UserControllable="true">true</ClearSmartcardPin>
    <IPProtocolSupport>IPv4,IPv6</IPProtocolSupport>
        AutoReconnect UserControllable="false">true>
AutoReconnectBehavior UserControllable="false">DisconnectOnSuspend>
    <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/>
        <ClientInitialization/>
            <ServerList>
                <HostEntry>
                    <HostName>IOSEAP-MD5</HostName>
                    <HostAddress>10.1.1.2</HostAddress>
                    <PrimaryProtocol>IPsec>
                    <StandardAuthenticationOnly>true>
<AuthMethodDuringIKENegotiation>EAP-MD5</AuthMethodDuringIKENegotiation>
    <IKEIdentity>IKETEST</IKEIdentity>
        <StandardAuthenticationOnly/>
        <PrimaryProtocol/>
            <HostEntry/>
                <ServerList/>
                    <AnyConnectProfile/>

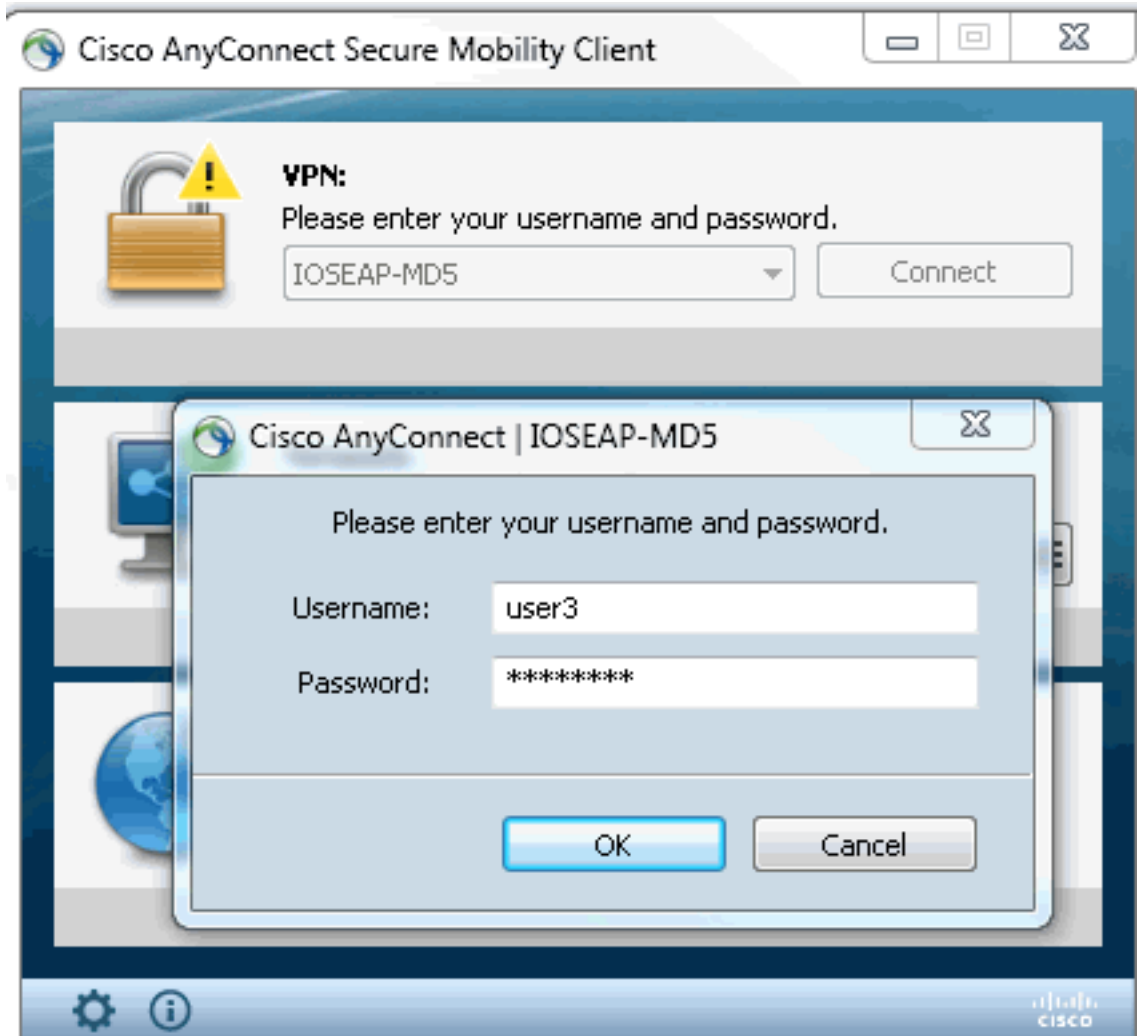
```

تأكد من أن إدخال 10.1.1.2 هو نفس إدخال CN=10.1.1.2 الذي تم إدخاله لشهادة الهوية.

## [الاختبارات](#)

في هذا السيناريو، لم يتم استخدام SSL VPN، لذلك تأكد من تعطيل خادم HTTP على IOS (لا يوجد خادم ip http). وإلا، فستلقى رسالة خطأ في AnyConnect تنص على، "إستخدام متصفح للحصول على الوصول".

عند الاتصال في AnyConnect، يجب مطالبتك بكلمة مرور. في هذا المثال، تم إنشاء User3



بعد ذلك، يتم توصيل المستخدم.

[التحقق](#)

[موجه IOS](#)

```

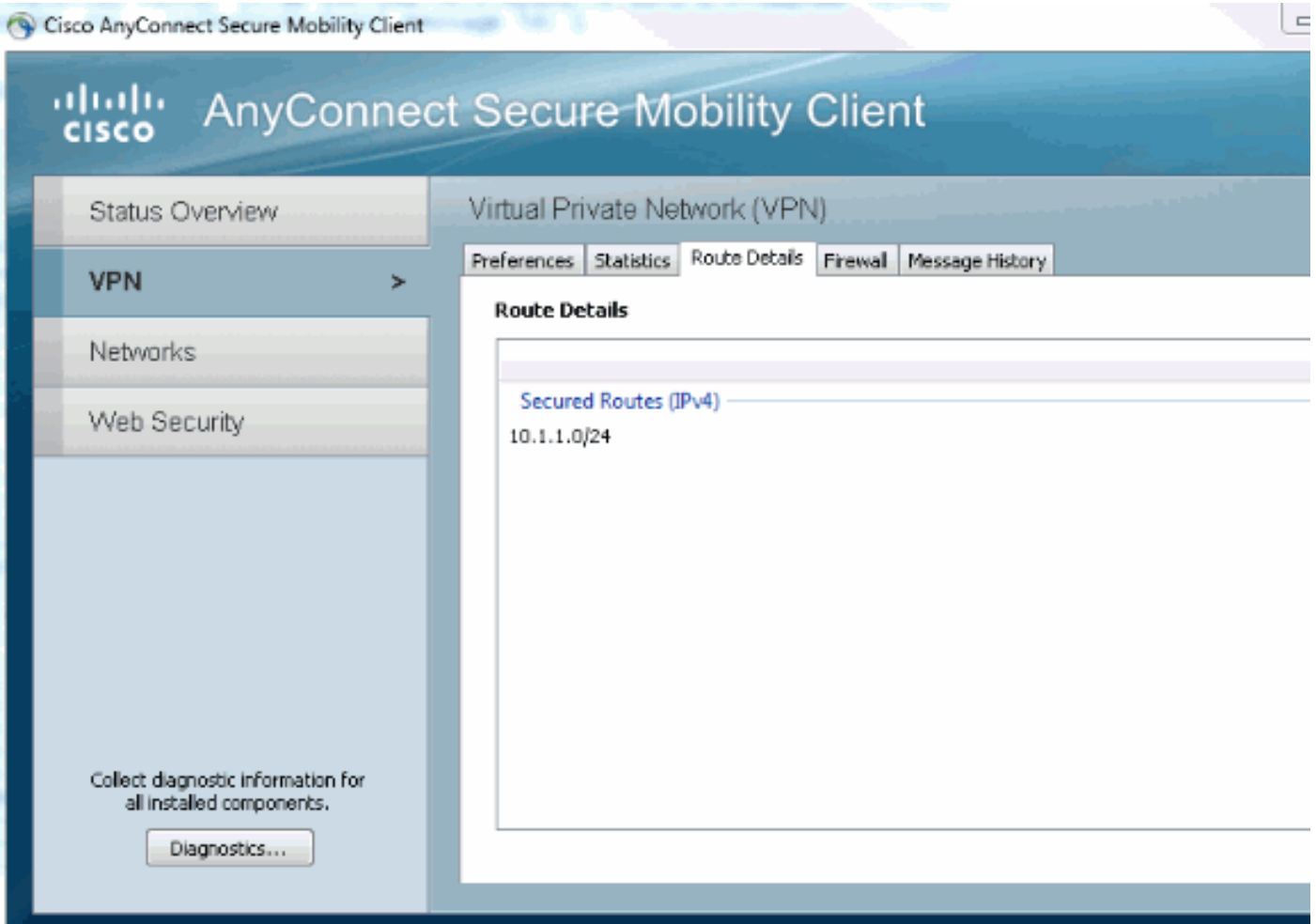
R1#show ip inter brief | i Virtual
Virtual-Access1  10.1.1.2  YES unset  up  up
Virtual-Templat1 10.1.1.2  YES unset  up  down
R1# show ip route 192.168.100.200
Routing entry for 192.168.100.200/32
(Known via "static", distance 1, metric 0 (connected
:Routing Descriptor Blocks
directly connected, via Virtual-Access1 *
Route metric is 0, traffic share count is 1
R1#show crypto ikev2 sa
IPv4 Crypto IKEv2 SA
Tunnel-id Local Remote fvrf/ivrf Status
none/none  READY 110.1.1.100/61021 10.1.1.2/4500 1
Encr: 3DES, Hash: SHA96, DH Grp:2, Auth sign: RSA, Auth verify: EAP
Life/Active Time: 86400/94 sec
IPv6 Crypto IKEv2 SA
R1#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
Interface: Virtual-Access1
Uptime: 00:04:06
Session status: UP-ACTIVE
(Peer: 192.168.56.1 port 61021 fvrf: (none) ivrf: (none)
Phase1_id: IKETEST
(Desc: (none)
IKEv2 SA: local 10.1.1.2/4500 remote 10.1.1.100/61021 Active
Capabilities:(none) connid:1 lifetime:23:55:54
IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 host 192.168.100.200
Active SAs: 2, origin: crypto map
Inbound: #pkts dec'ed 1 drop 0 life (KB/Sec) 4160122/3353
Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 4160123/3353
يمكنك تنفيذ تصحيح الأخطاء (debug crypto ikev2).
```

## ويندوز

في الخيارات المتقدمة من AnyConnect في شبكة VPN، يمكنك التحقق من تفاصيل المسار للاطلاع على شبكات الاتصال النفقي المنفصلة:



## المحاذير والمشكلات المعروفة

- تذكر عند وجود SHA1 في تجزئة التوقيع وفي نهج التكامل في IKEv2 (راجع معرف تصحيح الأخطاء من Cisco CSCtn59317 [العملاء المسجلون فقط](#)).
- يجب أن يكون CN في شهادة هوية IOS اسم مضيف متساو في ملف تعريف ACS XML.
- إذا أردت استخدام أزواج RADIUS AV التي تم تمريرها أثناء المصادقة وعدم استخدام تفويض المجموعة على

الإطلاق، يمكنك استخدام هذا في توصيف IKEv2:

```
aaa authorization user eap cached
```

- يستخدم التحويل دائما كلمة المرور "cisco" لتفويض المجموعة/المستخدمين. قد يكون هذا مربك أثناء الاستخدام لأنها ستحاول التفويض باستخدام المستخدم الذي تم تمريره في AnyConnect كمستخدم وكلمة مرور "cisco"، والتي قد لا تكون كلمة مرور المستخدم.
- في حالة أي مشاكل، هذه هي المخرجات التي يمكنك تحليلها وتقديمها إلى Cisco TAC: debug crypto ikev2debug crypto ikev2 داخل مخرجات DART
- إذا لم تكن تستخدم SSL VPN فتذكر تعطيل خادم ip http (لا يوجد خادم ip http). وإلا، فسيحاول AnyConnect الاتصال بخادم HTTP واستلام النتيجة، "إستخدام مستعرض للوصول".

## تشفير الجيل التالي

تم توفير التكوين المذكور أعلاه للمرجع لإظهار تكوين عمل محدود.

توصي Cisco باستخدام تشفير الجيل التالي (NGC) حيثما كان ذلك ممكنا.

يمكن الاطلاع على التوصيات الحالية المتعلقة بالهجرة هنا:

[http://www.cisco.com/web/about/security/intelligence/nextgen\\_crypto.html](http://www.cisco.com/web/about/security/intelligence/nextgen_crypto.html)

عند إختيار تكوين NGC، تأكد من أن كل من برنامج العميل وجهاز وحدة الاستقبال والبيث يدعمان هذا التكوين. يوصى بأن تكون موجهات ISR من الجيل 2 و ASR 1000 بمثابة محولات طرفية نظرا لدعم أجهزتها ل NGC.

وعلى جانب AnyConnect، واعتبارا من إصدار 3.1 AnyConnect، يتم دعم مجموعة الاتصال B من NSA.

## معلومات ذات صلة

- [Cisco ASA IKEv2 PKI Site-VPN](#)
- [تصحيح أخطاء الموقع IKEv2 على IOS](#)
- [FlexVPN / IKEv2: Windows 7 Building-Client وحدة الاستقبال والبيث IOS: الجزء 1 - مصادقة الشهادة](#)
- [دليل تكوين FlexVPN و Internet Key Exchange الإصدار 2، Cisco IOS، الإصدار 15.2M&T](#)
- [الدعم التقني والمستندات - Cisco Systems](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذہ Cisco تچرت  
ملاعلاء انءمچي فني مدختسمل معدى وتحم مي دقتل ةيرشبل او  
امك ةقيقد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچري. ةصاغل مهتغب  
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه  
ىلإ أمئاد عوچرلاب ي صؤتو تامچرتل هذه ةقدنع اهتيلوئسم Cisco  
Systems (رفوتم طبارل) ي لصلأل يزي لچنل دن تسمل