IKEv2 مع عميل IKEv2 AGILE VPN من Windows 7 ومصادقة الشهادة على FlexVPN

المحتويات

المقدمة

FlexVPN هو البنية الأساسية الجديدة لشبكة VPN المستندة إلى مفتاح الإنترنت الإصدار 2 (IKEv2) على Cisco IOS® والمقصود منه أن يكون حل شبكة VPN موحد. يصف هذا المستند كيفية تكوين عميل IKEv2 المدمج في Windows 7 لتوصيل وحدة الاستقبال والبث من Cisco IOS باستخدام مرجع مصدق (CA).

ملاحظة: يدعم جهاز الأمان القابل للتكيف (ASA) الآن إتصالات IKEv2 مع العميل المضمن لنظام التشغيل Windows 7 اعتبارا من الإصدار 9.3(2).

ملاحظة: لا تعمل بروتوكولات Suite-B لأن وحدة الاستقبال والبث IOS لا تدعم Suite-B مع IKEv1، أو أن عميل Windows 7 IKEv2 Agile VPN لا يدعم حاليا Suite-B مع IKEv2.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- عميل شبكة VPN مدمج يعمل بنظام التشغيل Windows 7
- برنامج Cisco IOS، الإصدار 15.2(2)T
- جهة منح الشهادة - المرجع المصدق OpenSSL

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات المكونات المادية والبرامج التالية:

- عميل شبكة VPN مدمج يعمل بنظام التشغيل Windows 7
- برنامج Cisco IOS، الإصدار 15.2(2)T
- جهة منح الشهادة - المرجع المصدق OpenSSL

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

الاصطلاحات

أحلت cisco فني طرف إتفاق لمعلومة على وثيقة إتفاق.

التكوين

نظرة عامة

هناك أربع خطوات رئيسية في تكوين عميل IKEv2 المدمج لنظام التشغيل Windows 7 من أجل توصيل وحدة الاستقبال والبث من Cisco IOS باستخدام CA:

1. تكوين CA

   يجب أن يسمح لك المرجع المصدق بتضمين إستخدام المفتاح الموسع (EKU) المطلوب في الشهادة. على سبيل المثال، في خادم IKEv2، يلزم 'EKU لمصادقة الخادم'، بينما تحتاج شهادة العميل إلى 'EKU لمصادقة العميل.' يمكن لعمليات النشر المحلية الاستفادة من:خادم Cisco IOS CA - لا يمكن إستخدام الشهادات الموقعة ذاتيا بسبب الخطأ CSCuc82575.خادم OpenSSL CAخادم Microsoft CA - بشكل عام، هذا هو الخيار المفضل لأنه يمكن تكوينه لتوقيع الشهادة تماما كما هو مطلوب.

2. تكوين جهاز الاستقبال والبث من Cisco IOS

   الحصول على شهادةتكوين IKEv2

3. تكوين العميل المدمج لنظام التشغيل Windows 7
4. الحصول على شهادة عميل

وكل خطوة من هذه الخطوات الرئيسية يجري شرحها بالتفصيل في الفروع التالية.

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

تكوين مرجع الشهادة

لا يقدم هذا المستند خطوات تفصيلية حول كيفية إعداد مرجع مصدق. ومع ذلك، تظهر لك الخطوات الواردة في هذا القسم كيفية تكوين CA حتى يمكنه إصدار شهادات لهذا النوع من النشر.

OpenSSL

يعتمد المرجع المصدق OpenSSL على ملف 'config'. يجب أن يحتوي ملف 'config' لخادم OpenSSL على:

```
[ extCSR ]
keyUsage            = nonRepudiation, digitalSignature, keyEncipherment, dataEncipherment
                                    extendedKeyUsage    = serverAuth, clientAuth
```

خادم IOS CA من Cisco

إذا كنت تستخدم خادم Cisco IOS CA، فتأكد من إستخدام أحدث إصدار من برنامج Cisco IOS Software، الذي يعين وحدة المعالجة المركزية (EKU).

```
IOS-CA# show run | section crypto pki
                                    crypto pki server IOS-CA
                issuer-name cn=IOS-CA.cisco.com,ou=TAC,o=cisco
                                                  grant auto
                              eku server-auth client-auth
```

تكوين وحدة الاستقبال والبث عبر نظام IOS من Cisco

الحصول على شهادة

يجب أن تحتوي الشهادة على حقلي EKU معينين على "مصادقة الخادم" ل Cisco IOS و"مصادقة العميل" للعميل. وعادة ما يتم إستخدام المرجع المصدق نفسه لتوقيع كل من شهادات العميل والخادم. في هذه الحالة، تظهر كل من "مصادقة الخادم" و"مصادقة العميل" على شهادة الخادم وشهادة العميل على التوالي، وهذا مقبول.

إذا أصدر المرجع المصدق الشهادات بتنسيق #12 في خادم IKEv2 لمعايير التشفير للمفتاح العام (PKCS) للعملاء والخادم، وإذا كانت قائمة إلغاء الشهادة (CRL) غير قابلة للوصول أو متوفرة، فيجب تكوينها:

```
crypto pki trustpoint FlexRootCA
                                    revocation-check none
```

دخلت هذا أمر in order to استوردت ال PKCS#12 شهادة:

```
/:copy ftp://user:***@OpenSSLServer/p12/ikev2.p12*  flash
<crypto pki import FlexRootCA pkcs12 flash:/ikev2.p12 password <password
.Note: ikev2.p12 is a pkcs12 format certificate that has CA Certificate bundled in it !!
```

إذا قام خادم Cisco IOS CA بمنح الشهادات تلقائيا، فيجب تكوين خادم IKEv2 باستخدام عنوان URL لخادم CA لتلقي الشهادة كما هو موضح في هذا المثال:

```
crypto pki trustpoint IKEv2
enrollment url http://<CA_Sever_IP>:80
subject-name cn=ikev2.cisco.com,ou=TAC,o=cisco
revocation-check none
```

عند تكوين TrustPoint، يجب:

1. مصادقة المرجع المصدق باستخدام هذا الأمر:

```
crypto pki authenticate FlexRootCA
```

2. قم بتسجيل خادم IKEv2 باستخدام CA باستخدام هذا الأمر:

```
crypto pki enroll FlexRootCA
```

لترى إذا كانت الشهادة تحتوي على كل الخيارات المطلوبة، أستخدم أمر **show** هذا:

```
ikev2#show crypto pki cert verbose
Certificate

:Issuer

:Subject
Name: ikev2.cisco.com
ou=TAC
o=Cisco
c=BE
cn=ikev2.cisco.com

:Subject Key Info
Public Key Algorithm: rsaEncryption
(RSA Public Key: (1024 bit
Signature Algorithm: MD5 with RSA Encryption
Fingerprint MD5: 3FB01AE4 E36DF9D8 47F3C206 05F287C6

Fingerprint SHA1: DEE6C4D1 00CDD2D5 C0976274 203D2E74 2BC49BE8
:X509v3 extensions
X509v3 Key Usage: F0000000
Digital Signature
Non Repudiation
Key Encipherment
Data Encipherment
X509v3 Subject Key ID: CBCE6E9F F508927C E97040FD F49B52D1 D5919D45
X509v3 Authority Key ID: 4B86A079 A5738694 85721D0D 7A75892F 0CDAC723
:Authority Info Access
:Extended Key Usage
Client Auth
Server Auth
Associated Trustpoints: FlexRootCA
Key Label: FlexRootCA
```

تكوين IKEv2

هذا مثال على تكوين IKEv2:

```
IP Pool for IKEv2 Clients !!
```

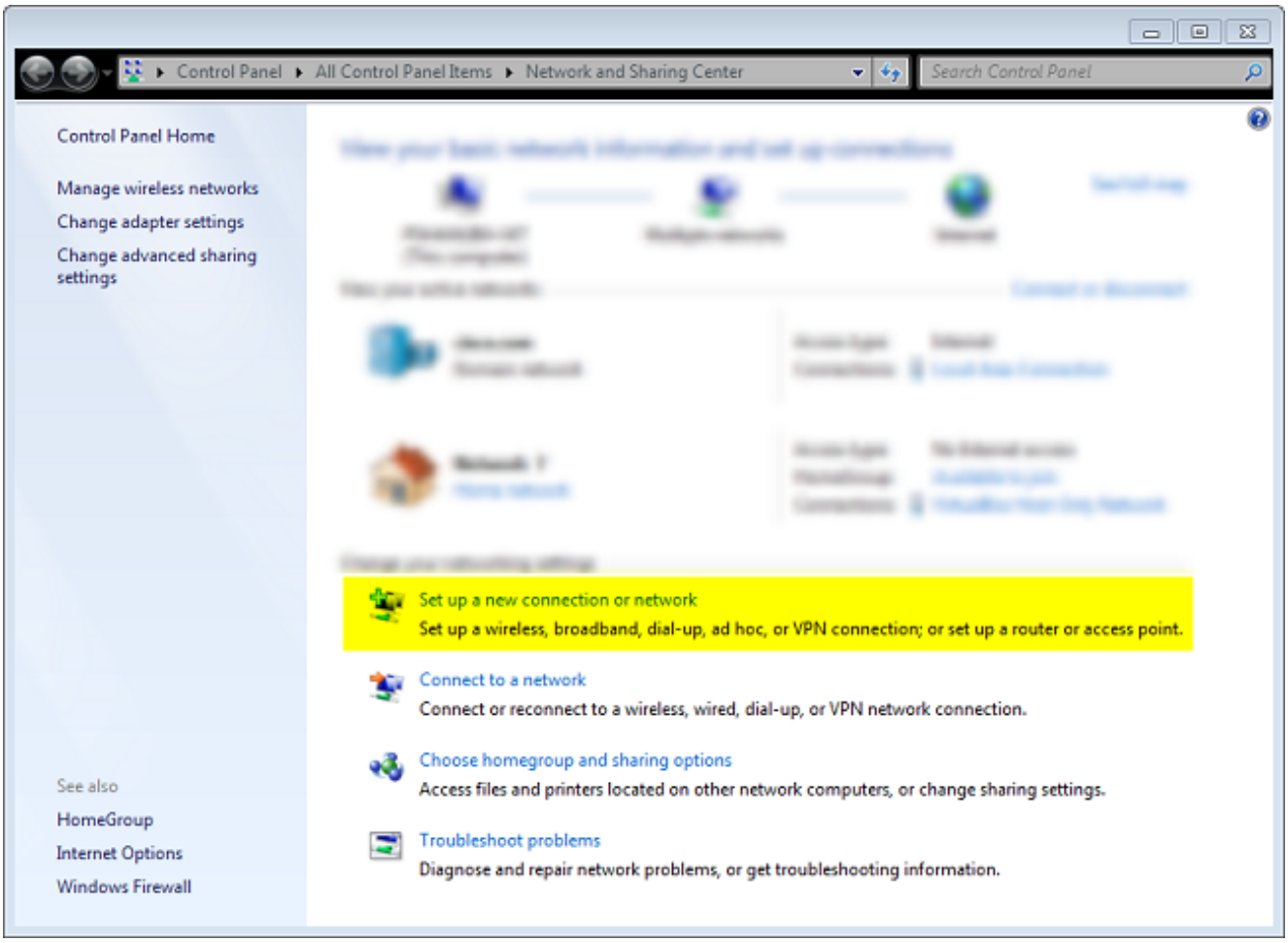
```
ip local pool mypool 172.16.0.101 172.16.0.250


Certificate MAP to match Remote Certificates, in our case the Windows 7 Clients !!

crypto pki certificate map win7_map 10
subject-name co ou = tac

One of the proposals that Windows 7 Built-In Client Likes !!

crypto ikev2 proposal win7
encryption aes-cbc-256
integrity sha1
group 2

IKEv2 policy to store a proposal !!

crypto ikev2 policy win7
proposal win7

IKEv2 Local Authorization Policy. Split-Tunneling does not work, as was !!
.the case in good old l2tp over IPSec !!

crypto ikev2 authorization policy win7_author
pool mypool

IKEv2 Profile !!

crypto ikev2 profile win7-rsa
match certificate win7_map
identity local fqdn ikev2.cisco.com
authentication local rsa-sig
authentication remote rsa-sig
pki trustpoint FlexRootCA
aaa authorization group cert list win7 win7_author
virtual-template 1


One of the IPSec Transform Sets that Windows 7 likes !!

crypto ipsec transform-set aes256-sha1 esp-aes 256 esp-sha-hmac


IPSec Profile that calls IKEv2 Profile !!

crypto ipsec profile win7_ikev2
set transform-set aes256-sha1
set ikev2-profile win7-rsa


dVTI interface - A termination point for IKEv2 Clients !!

interface Virtual-Template1 type tunnel
ip unnumbered Loopback0
tunnel mode ipsec ipv4
tunnel protection ipsec profile win7_ikev2
```

يجب أن يكون IP غير المرقم الخاص بالقالب الظاهري أي شيء باستثناء العنوان المحلي المستخدم لاتصال IPsec.
[إذا كنت تستخدم عميل أجهزة، فسوف تتبادل معلومات التوجيه عبر عقدة تكوين IKEv2 وتنشئ مشكلة توجيه متكررة على عميل الأجهزة.]

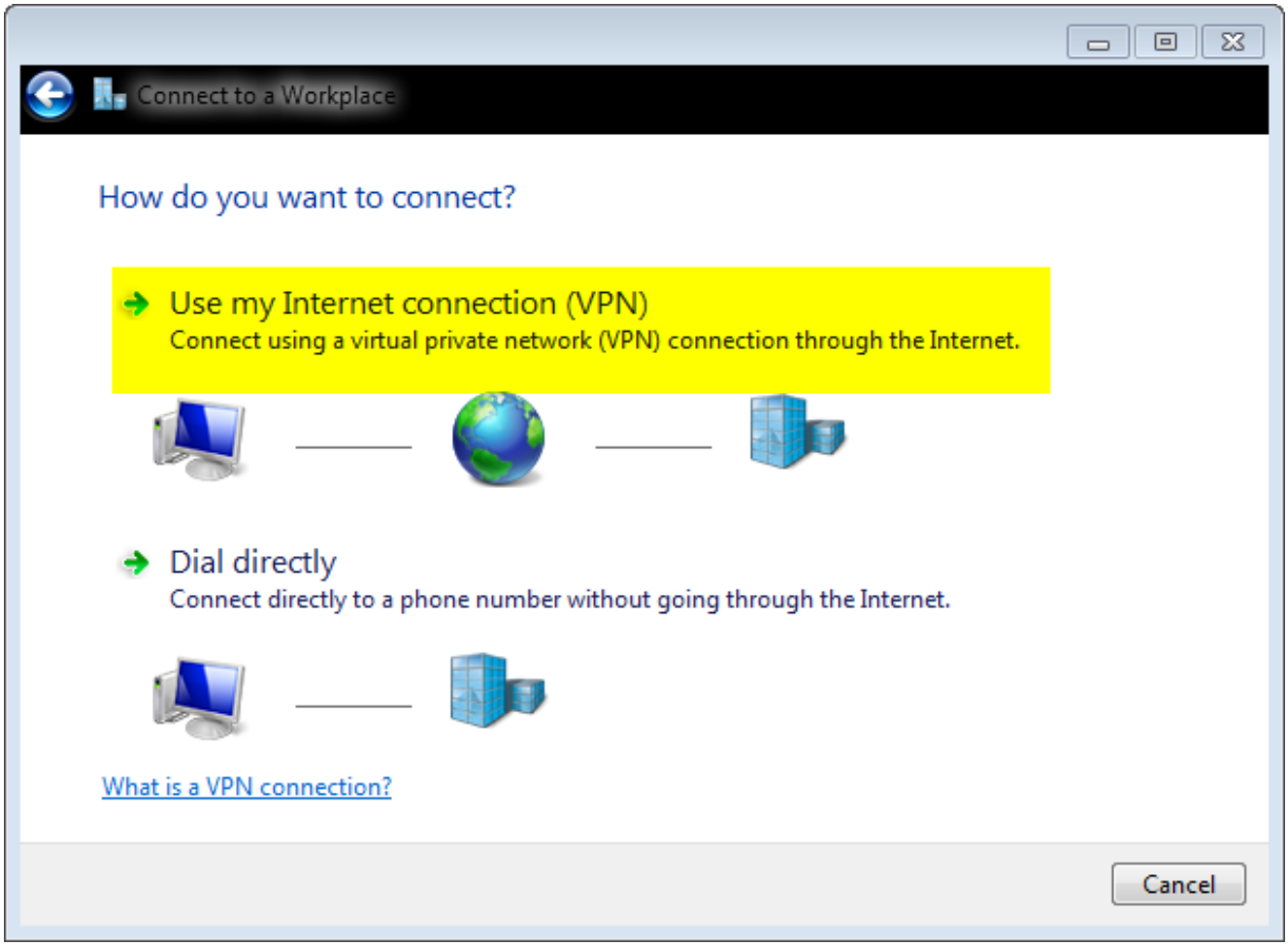
تكوين العميل المدمج لنظام التشغيل Windows 7

يوضح هذا الإجراء كيفية تكوين العميل المضمن لنظام التشغيل Windows 7.

1. انتقل إلى **مركز الشبكات والمشاركة**، وانقر فوق **إعداد اتصال أو شبكة جديدة**.

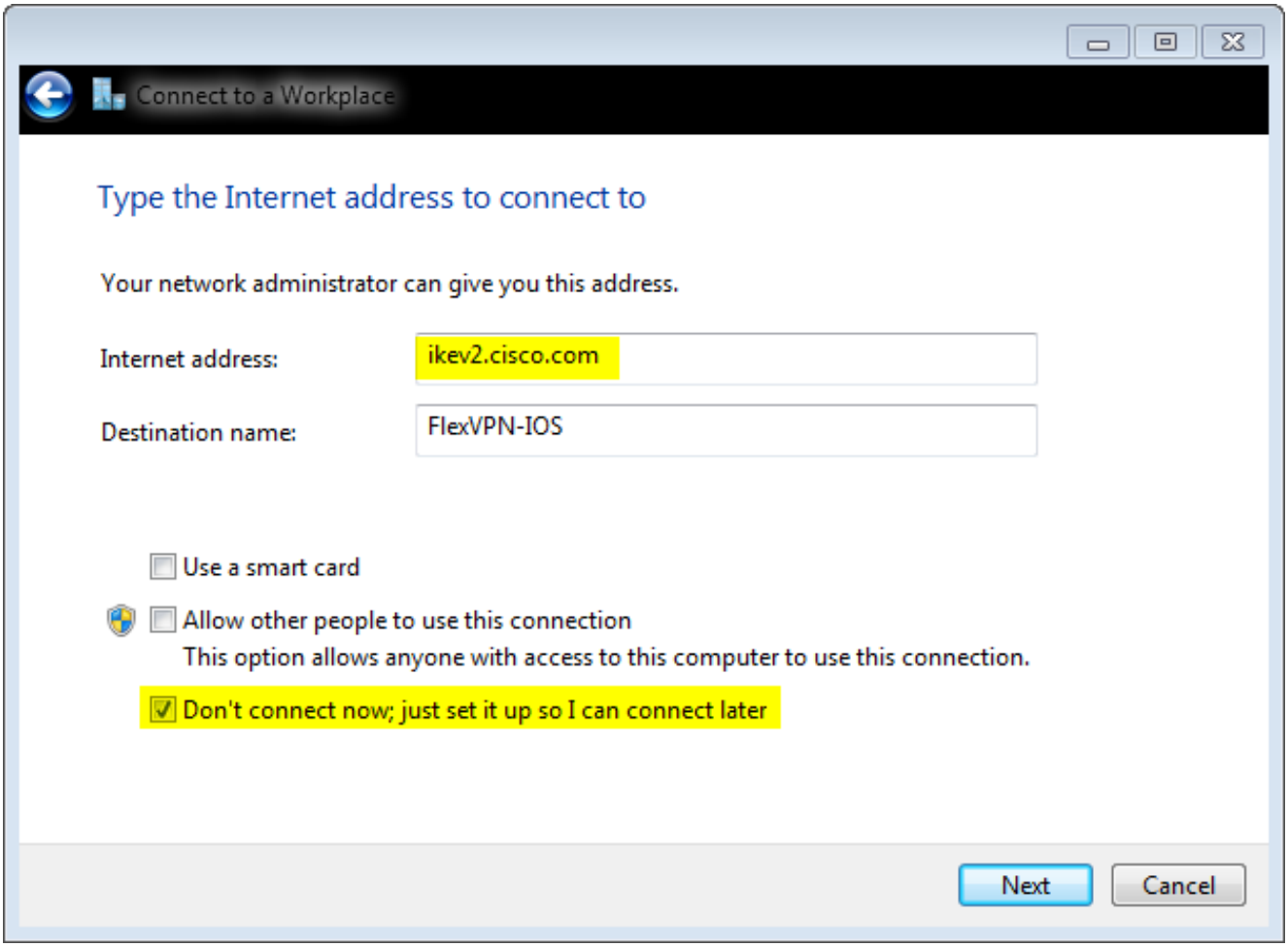


2. انقر على **إستخدام اتصال الإنترنت (VNP)**. وهذا يتيح لك إعداد اتصال VPN يخضع للتفاوض عبر اتصال إنترنت حالي.

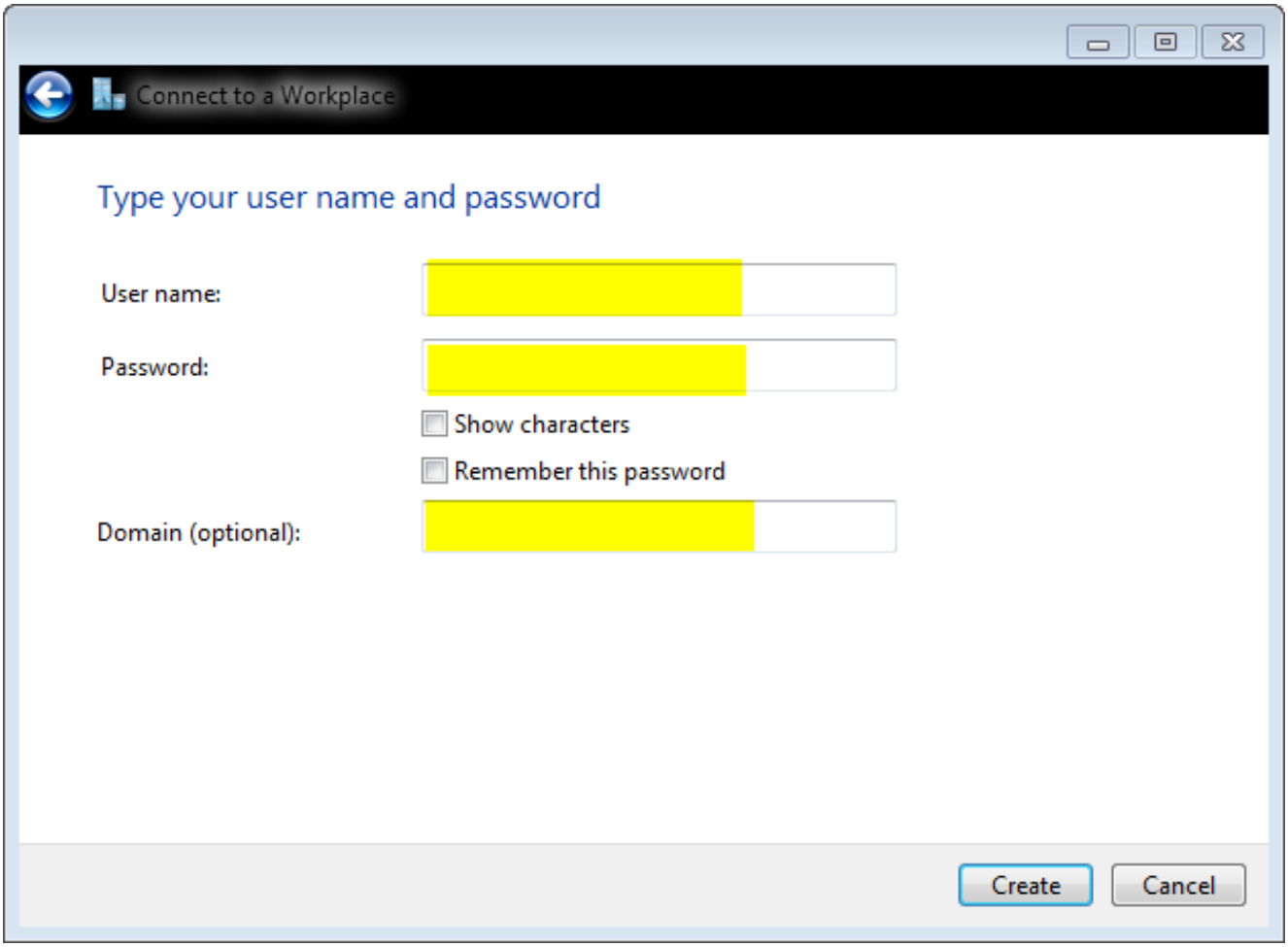


أدخل اسم المجال المؤهل بالكامل (FQDN) أو عنوان IP الخاص بخادم IKEv2، وأعطه اسم وجهة لتحديد3.
محليا.

ملاحظة: يجب أن تطابق FQDN الاسم الشائع (CN) من شهادة هوية الموجه. يقوم Windows 7 بإسقاط الاتصال بخطأ 13801 إذا اكتشف عدم تطابق.
نظرا لأنه يلزم تعيين معلمات إضافية، **تأكد من عدم الاتصال الآن؛ قم فقط بإعداده بحيث يمكنني الاتصال لاحقا،** وانقر فوق **التالي**:

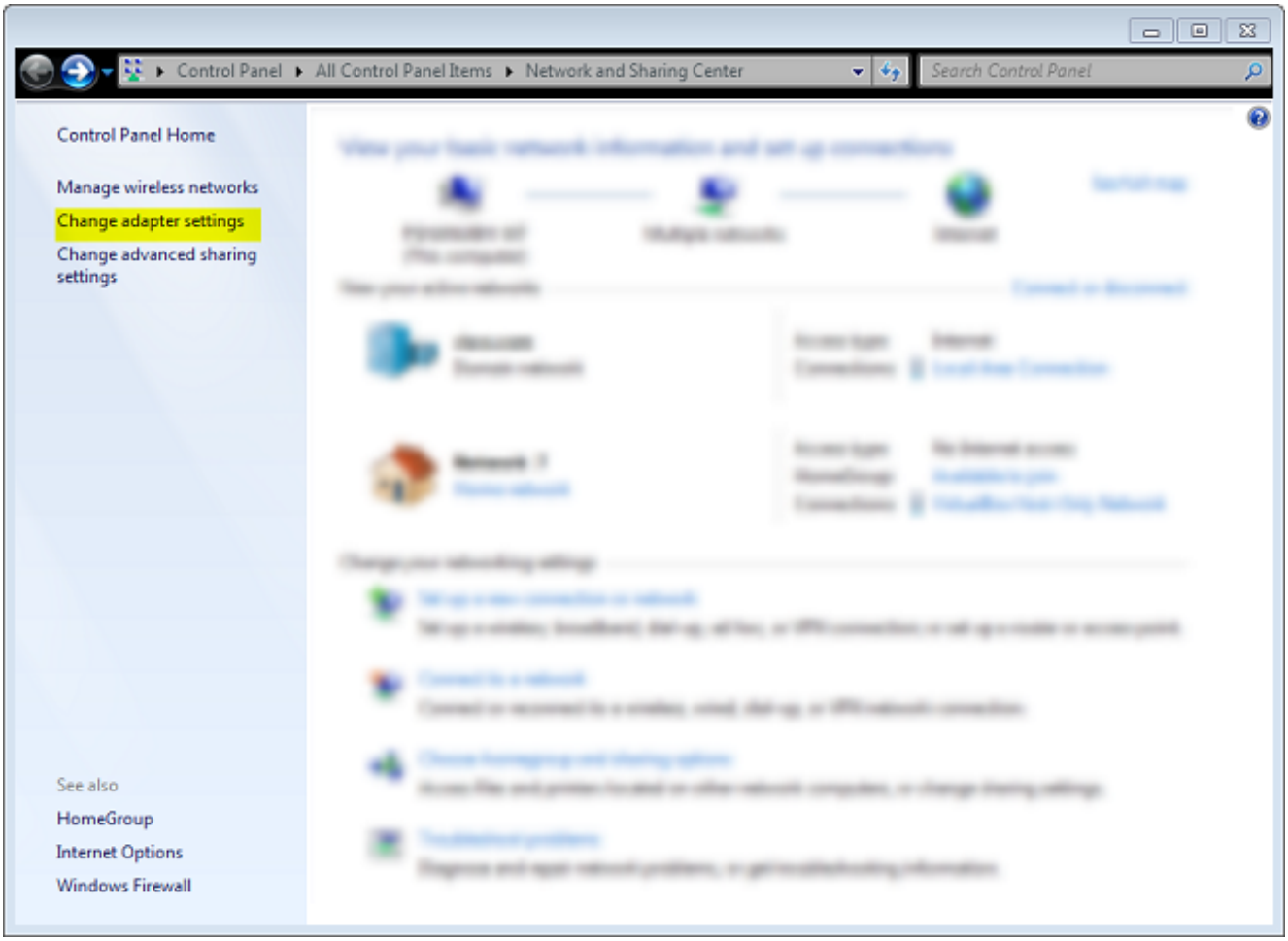


4. لا تقم بتعبئة الحقول **اسم المستخدم** و**كلمة المرور** و**المجال (إختياري)** لأن مصادقة الشهادة سيتم إستخدامها. طقطقة **يخلق**.



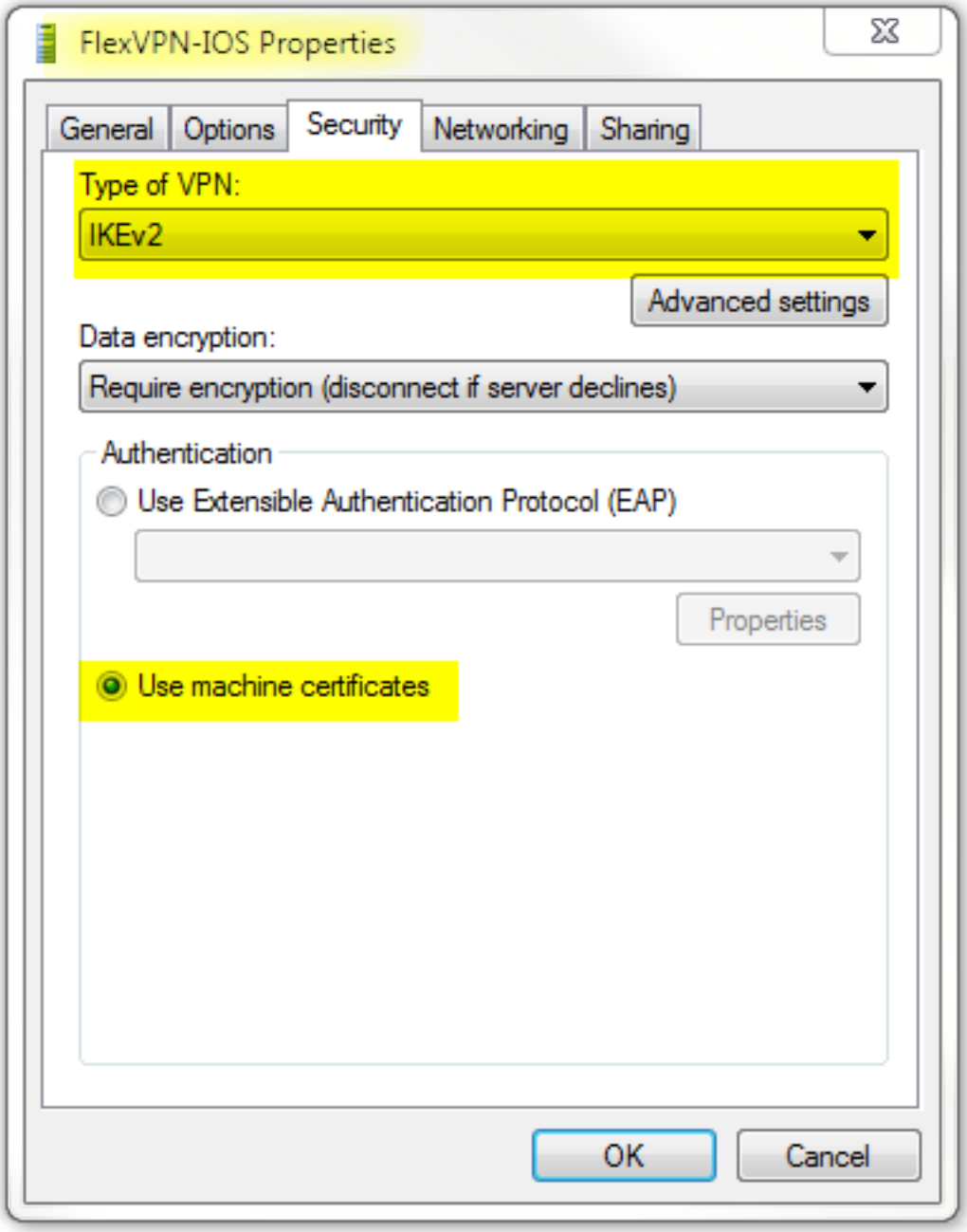
ملاحظة: إغلاق النافذة الناتجة. **لا تحاول الاتصال.**

5. انتقل مرة أخرى إلى **مركز الشبكات والمشاركة**، وانقر فوق **تغيير إعدادات المحول**.



6. أختر FlexVPN-IOS الخاص بالمهايئ المنطقي، والذي يكون نتيجة لجميع الخطوات المتخذة إلى هذه النقطة. انقر فوق خصائصه. هذه هي خصائص ملف تعريف الاتصال الذي تم إنشاؤه حديثا والمسمى FlexVPN-IOS:

على علامة التبويب "الأمان"، يجب أن يكون نوع شبكة VPN هو IKEv2.في قسم المصادقة، أختر **إستخدام شهادات الجهاز**.



أصبح ملف تعريف FlexVPN-IOS الآن جاهزا للتوصيل بعد إستيراد شهادة إلى مخزن شهادات الجهاز.

الحصول على شهادة العميل

تتطلب شهادة العميل هذه العوامل:

- تحتوي شهادة العميل على EKU من "مصادقة العميل". كما أن المرجع المصدق يعطي شهادة PKCS#12:

```
Client's PKCS12 Certificate will go into Local Machine Personal Certificate Store
```

- شهادة المرجع المصدق:

```
CA Certificate goes into Local Machine Trusted Root Certificate Authorities Store
```

تفاصيل هامة

- يجب إستخدام 'IPSec IKE intermediate' (OID = 1.3.6.1.5.5.8.2.2) ك EKU إذا تم تطبيق كلا العبارتين التاليتين:

خادم IKEv2 هو خادم Windows 2008.يوجد أكثر من شهادة مصادقة خادم قيد الاستخدام لاتصالات IKEv2. إذا كان هذا صحيحا، قم بوضع كل من "مصادقة الخادم" EKU و"EKU "IPSec IKE Intermediate على شهادة واحدة، أو قم بتوزيع وحدات EKU هذه بين الشهادات. تأكد من أن شهادة واحدة على الأقل تحتوي على 'EKU 'IPSec IKE Intermediate.

راجع أستكشاف أخطاء إتصالات IKEv2 VPN وإصلاحها للحصول على مزيد من المعلومات.

- في نشر FlexVPN، لا تستخدم 'IPSec IKE Intermediate' في EKU. وإذا قمت بذلك، فإن عميل IKEv2 لا يلتقط شهادة خادم IKEv2. ونتيجة لذلك، لا يمكنهم الاستجابة إلى CERTREQ من IOS في رسالة الاستجابة IKE_SA_INIT، وبالتالي فإنهم يفشلون في الاتصال بمعرف الخطأ 13806.

- في حين أن الاسم البديل للموضوع (SAN) غير مطلوب، فإنه مقبول إذا كانت الشهادات تحتوي على واحد.

- في "مخزن شهادات العملاء" الخاص بنظام التشغيل Windows 7، تأكد من أن "مخزن مراجع الشهادات الجذر" الموثوق به على الجهاز يحتوي على أقل عدد ممكن من الشهادات. إذا كان لديه أكثر من 50 جهازا أو نحو ذلك، فقد يفشل برنامج Cisco IOS في قراءة حمولة CERT_REQ بالكامل، والتي تحتوي على الاسم المميز للشهادة (DN) لجميع الشهادات المصدقة المعروفة من المربع Windows 7. ونتيجة لذلك، يفشل التفاوض وترى مهلة الاتصال على العميل.

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر show. استخدم "أداة مترجم الإخراج" لعرض تحليل لمُخرج الأمر **show**.

```
ikev2#show crypto ikev2 session detail
IPv4 Crypto IKEv2 Session

Session-id:4, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local Remote fvrf/ivrf Status
none/none READY 192.168.56.1/4500 10.0.3.1/4500 1
,Encr: AES-CBC, keysize: 256, Hash: SHA96, DH Grp:2, Auth sign: RSA
Auth verify: RSA
Life/Active Time: 86400/17 sec
CE id: 1004, Session-id: 4
Status Description: Negotiation done
Local spi: A40828A826160328 Remote spi: C004B7103936B430
Local id: ikev2.cisco.com
Remote id: ou=TAC,o=Cisco,c=BE,cn=Win7
Local req msg id: 0 Remote req msg id: 2
Local next msg id: 0 Remote next msg id: 2
Local req queued: 0 Remote req queued: 2
,Local window: 5 Remote window: 1 DPD configured for 0 seconds
retry 0
NAT-T is not detected
Cisco Trust Security SGT is disabled

ikev2#show crypto ipsec sa peer 192.168.56.1
```

```
interface: Virtual-Access1

Crypto map tag: Virtual-Access1-head-0, local addr 10.0.3.1
(protected vrf: (none
(local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0
(remote ident (addr/mask/prot/port): (172.16.0.104/255.255.255.255/0/0
current_peer 192.168.56.1 port 4500
{,PERMIT, flags={origin_is_acl
pkts encaps:5, #pkts encaps:5, #pkts encrypt: 5, #pkts digest: 5#
pkts decaps: 55, #pkts decrypt: 55, #pkts verify: 55#
pkts compressed: 0, #pkts decompressed: 0#
pkts not compressed: 0, #pkts compr. failed: 0#
pkts not decompressed: 0, #pkts decompress failed: 0#
send errors 0, #recv errors 0#

local crypto endpt.: 10.0.3.1, remote crypto endpt.: 192.168.56.1
path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
(current outbound spi: 0x3C3D299(63165081
PFS (Y/N): N, DH group: none

:inbound esp sas
(spi: 0xE461ED10(3831622928
, transform: esp-256-aes esp-sha-hmac
{ ,in use settings ={Tunnel
conn id: 7, flow_id: SW:7, sibling_flags 80000040, crypto map: Virtual-Access1-head-0
(sa timing: remaining key lifetime (k/sec): (4257423/0
IV size: 16 bytes
replay detection support: Y
(Status: ACTIVE(ACTIVE

:inbound ah sas

:inbound pcp sas

:outbound esp sas

(spi: 0x3C3D299(63165081
, transform: esp-256-aes esp-sha-hmac
{ ,in use settings ={Tunnel
conn id: 8, flow_id: SW:8, sibling_flags 80000040, crypto map: Virtual-Access1-head-0
(sa timing: remaining key lifetime (k/sec): (4257431/0
IV size: 16 bytes
replay detection support: Y
(Status: ACTIVE(ACTIVE

:outbound ah sas

:outbound pcp sas
```

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

معلومات ذات صلة

- تصحيح أخطاء ASA IKEv2 لشبكة VPN من موقع إلى موقع مع PSKs TechNote
- تصحيح أخطاء ASA IPsec و IKE (الوضع الرئيسي IKEv1) أستكشاف أخطاء TechNote وإصلاحها

- تصحيح أخطاء الوضع الرئيسي لـ IPSec و IKE - IKEv1 Main Mode Troubleshooting TechNote
- تصحيح أخطاء ASA IPSec و IKE - IKEv1 Aggressive Mode TechNote
- أجهزة الأمان المعدلة Cisco ASA 5500 Series Adaptive Security Appliances
- تنزيلات برامج أجهزة الأمان القابلة للتكيف ASA 5500 Series من Cisco
- جدار حماية Cisco IOS
- برنامج IOS من Cisco
- القشرة الآمنة (SSH)
- مفاوضة IPSec/بروتوكولات IKE
- الدعم التقني والمستندات - Cisco Systems

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).