採用Windows 7的IKEv2 IKEv2 Agile VPN使用者端和FlexVPN上的憑證驗證

目錄

簡介

FlexVPN是Cisco IOS®上新的基於Internet金鑰交換版本2(IKEv2)的VPN基礎設施，旨在成為統一VPN解決方案。本文檔介紹如何配置Windows 7中內建的IKEv2客戶端，以便利用證書頒發機構(CA)連線Cisco IOS頭端。

> **附註**：自版本9.3(2)起，自適應安全裝置(ASA)現在支援與Windows 7內建客戶端的IKEv2連線。

> **附註**：SUITE-B協定不起作用，因為IOS頭端不支援使用IKEv1的SUITE-B，或者Windows 7 IKEv2 Agile VPN客戶端當前不支援使用IKEv2的SUITE-B。

必要條件

需求

思科建議您瞭解以下主題：

- Windows 7內建VPN客戶端
- Cisco IOS軟體版本15.2(2)T
- 憑證授權單位 — OpenSSL CA

採用元件

本檔案中的資訊是根據以下硬體和軟體版本：

- Windows 7內建VPN客戶端
- Cisco IOS軟體版本15.2(2)T
- 憑證授權單位 — OpenSSL CA

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需檔案慣例的相關資訊，請參閱思科技術提示慣例。

設定

概觀

配置Windows 7內建IKEv2客戶端時需要執行四個主要步驟，以便使用CA連線Cisco IOS頭端：

1. 配置CA

   CA應允許您在憑證中嵌入所需的延伸金鑰使用(EKU)。例如，在IKEv2伺服器上，需要「Server Auth EKU」，而客戶端證書需要「Client Auth EKU」。 本地部署可使用：Cisco IOS CA伺服器 — 由於CSCuc82575錯誤，無法使用自簽名證書。OpenSSL CA伺服器Microsoft CA伺服器 — 通常，這是首選選項，因為它可以配置為完全按照所需對證書進行簽名。

2. 配置Cisco IOS頭端

   取得憑證配置IKEv2

3. 配置Windows 7內建客戶端
4. 獲取客戶端證書

以下各節詳細說明了這些主要步驟中的每一步。

附註：使用命令查詢工具(僅供已註冊客戶使用)可獲取本節中使用的命令的更多資訊。

配置證書頒發機構

本文不提供如何設定CA的詳細步驟。但是，本節中的步驟說明如何配置CA，以便它可以為此類部署頒發證書。

OpenSSL

OpenSSL CA是根據「config」檔案。OpenSSL伺服器的「config」檔案應具有：

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

Cisco IOS CA伺服器

如果您使用Cisco IOS CA伺服器，請確保使用分配了EKU的最新Cisco IOS軟體版本。

```
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
```

配置Cisco IOS頭端

取得憑證

對於Cisco IOS，證書的EKU欄位必須設定為「伺服器身份驗證」，對於客戶端必須設定為「客戶端身份驗證」。通常，相同的CA用於對客戶端和伺服器證書進行簽名。在這種情況下，伺服器憑證和使用者端憑證上分別會看到「伺服器驗證」和「使用者端驗證」，這是可接受的。

如果CA在IKEv2伺服器上以公鑰加密標準(PKCS)#12格式向使用者端和伺服器頒發憑證，且憑證撤銷清單(CRL)無法存取或可用，則必須設定：

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

輸入以下命令以匯入PKCS#12證書：

```
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.
```

如果Cisco IOS CA伺服器自動授予證書，則必須使用CA伺服器URL配置IKEv2伺服器以接收證書，如以下示例所示：

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

配置信任點時，您需要：

1. 使用以下命令驗證CA:

```
crypto pki authenticate FlexRootCA
```

2. 使用以下命令使用CA註冊IKEv2伺服器：

```
crypto pki enroll FlexRootCA
```

若要檢視憑證是否包含所有所需的選項，請使用以下**show**指令：

```
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
```

配置IKEv2

以下是IKEv2配置的示例：

```
!! 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
```

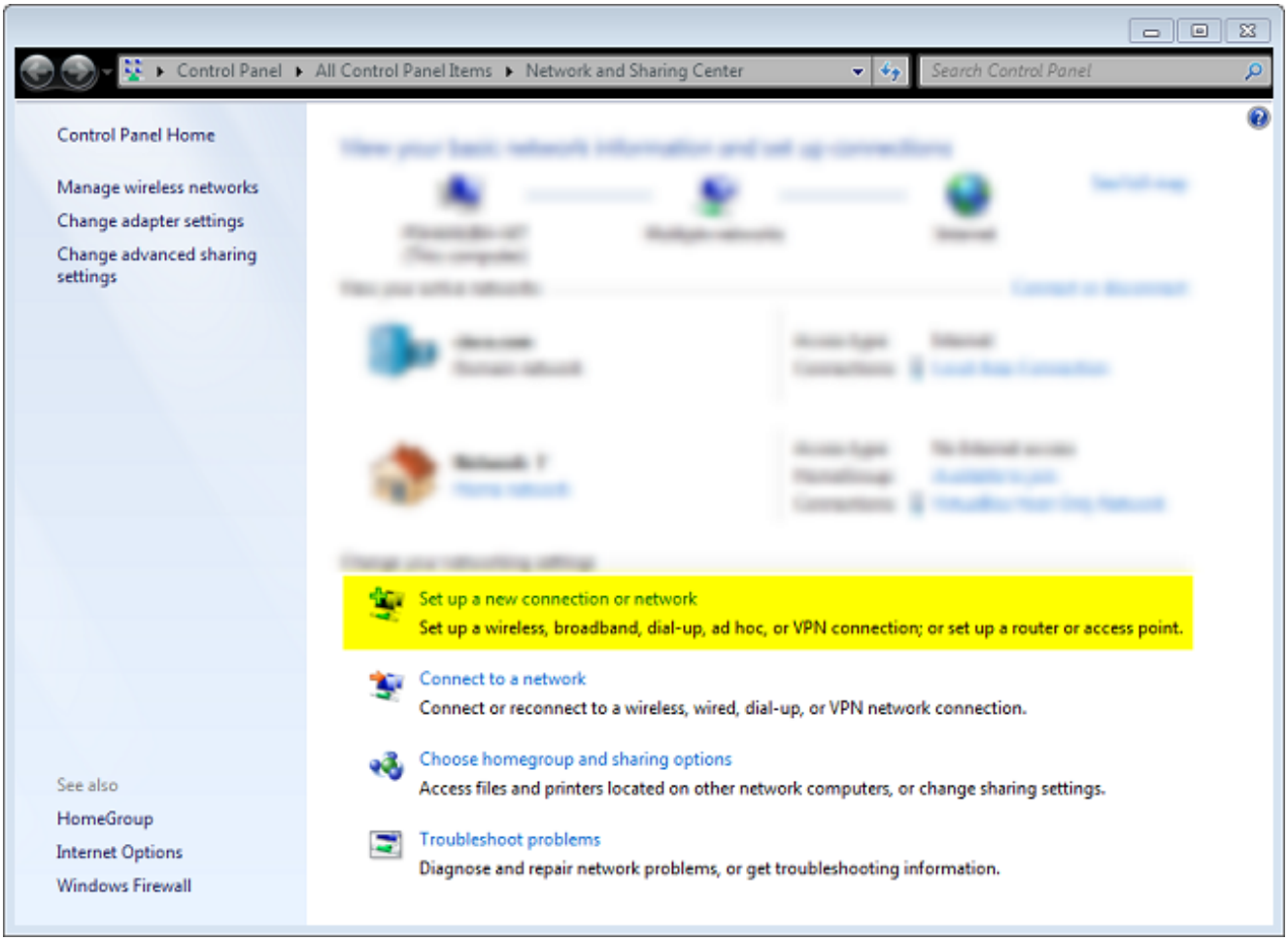
```
!! One of the proposals that Windows 7 Built-In Client Likes

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
```

虛擬模板未編號的IP應為除IPsec連線使用的本地地址以外的任何內容。 [如果使用硬體客戶端，您將通過IKEv2配置節點交換路由資訊，並在硬體客戶端上建立遞迴路由問題。]

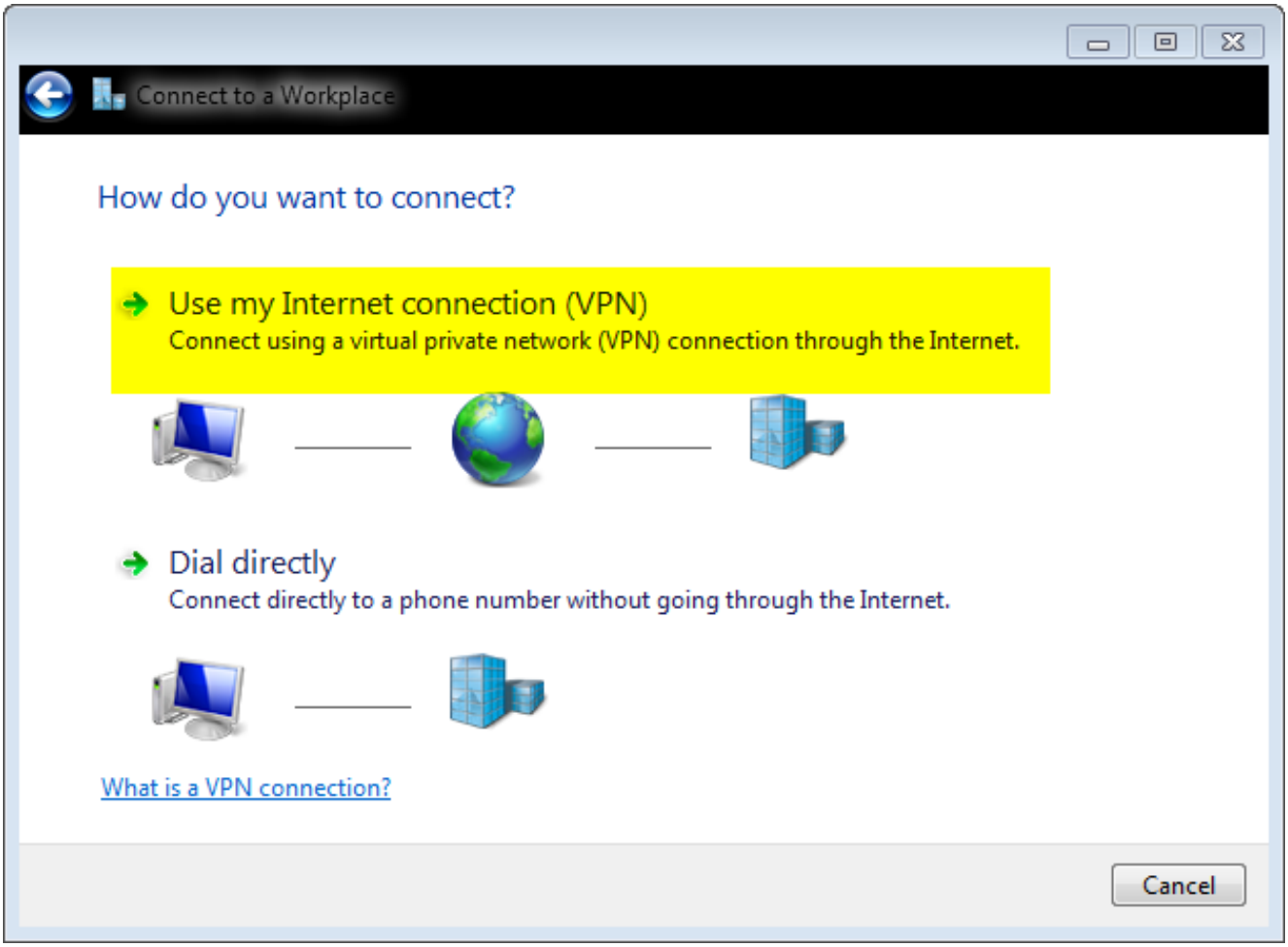
配置Windows 7內建客戶端

以下過程介紹了如何配置Windows 7內建客戶端。

1. 導航到**網路和共用中心**，然後按一下Set a new connection or network。

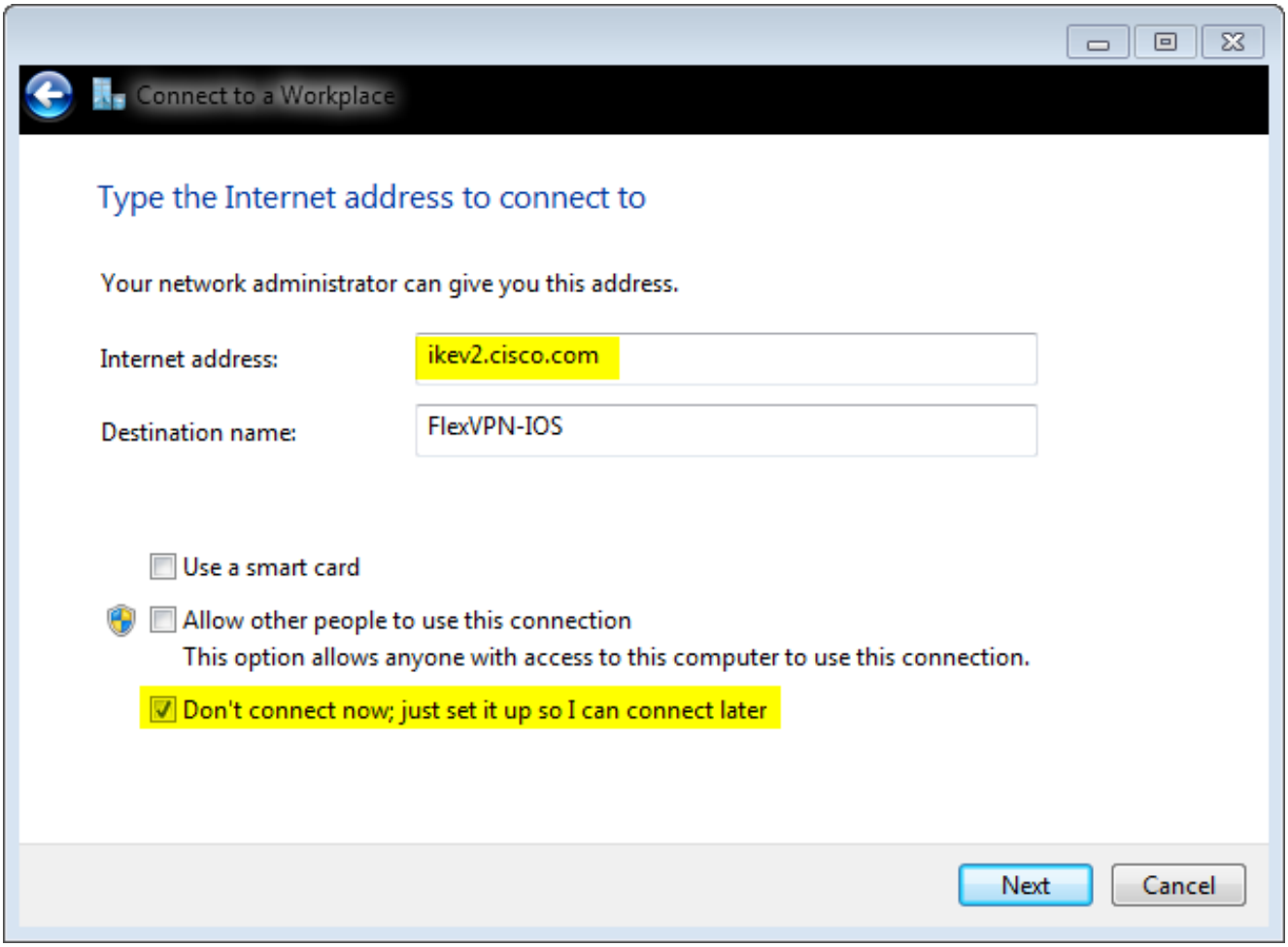


2. 按一下「Use my Internet connection(VNP)」。 這允許您設定通過當前網際網路連線協商的VPN連線。

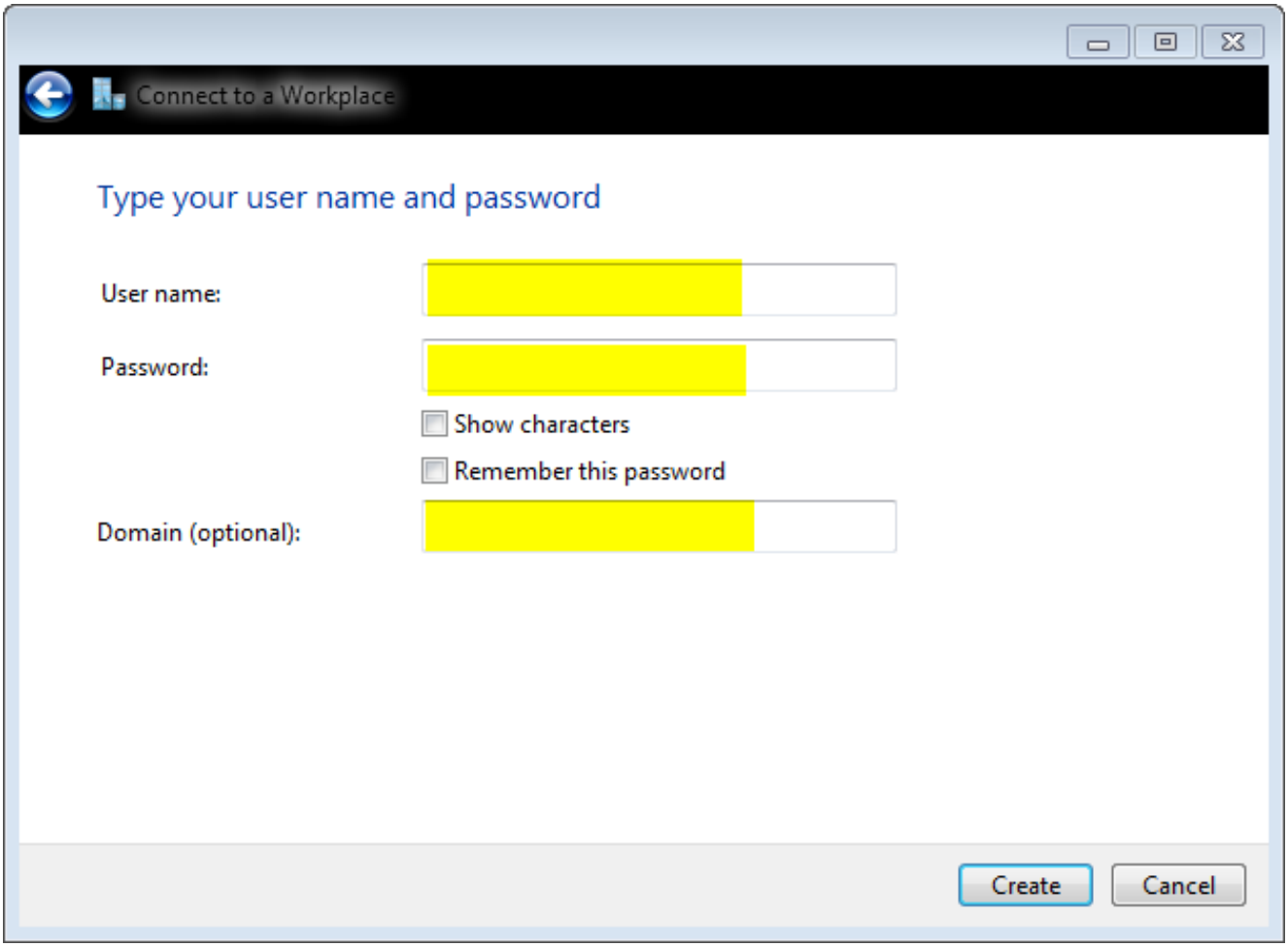


3. 輸入完全限定的域名(FQDN)或IKEv2伺服器的IP地址，並為其指定目標名稱以在本地標識該域名。

   附註：FQDN必須與路由器身份證書中的公用名(CN)匹配。如果檢測到不匹配，Windows 7將丟13801連線並出現錯誤。
   由於需要設定其他引數，請選中**Don't connect now;只需設定它以便稍後連線，然**後按一下**下一步**:

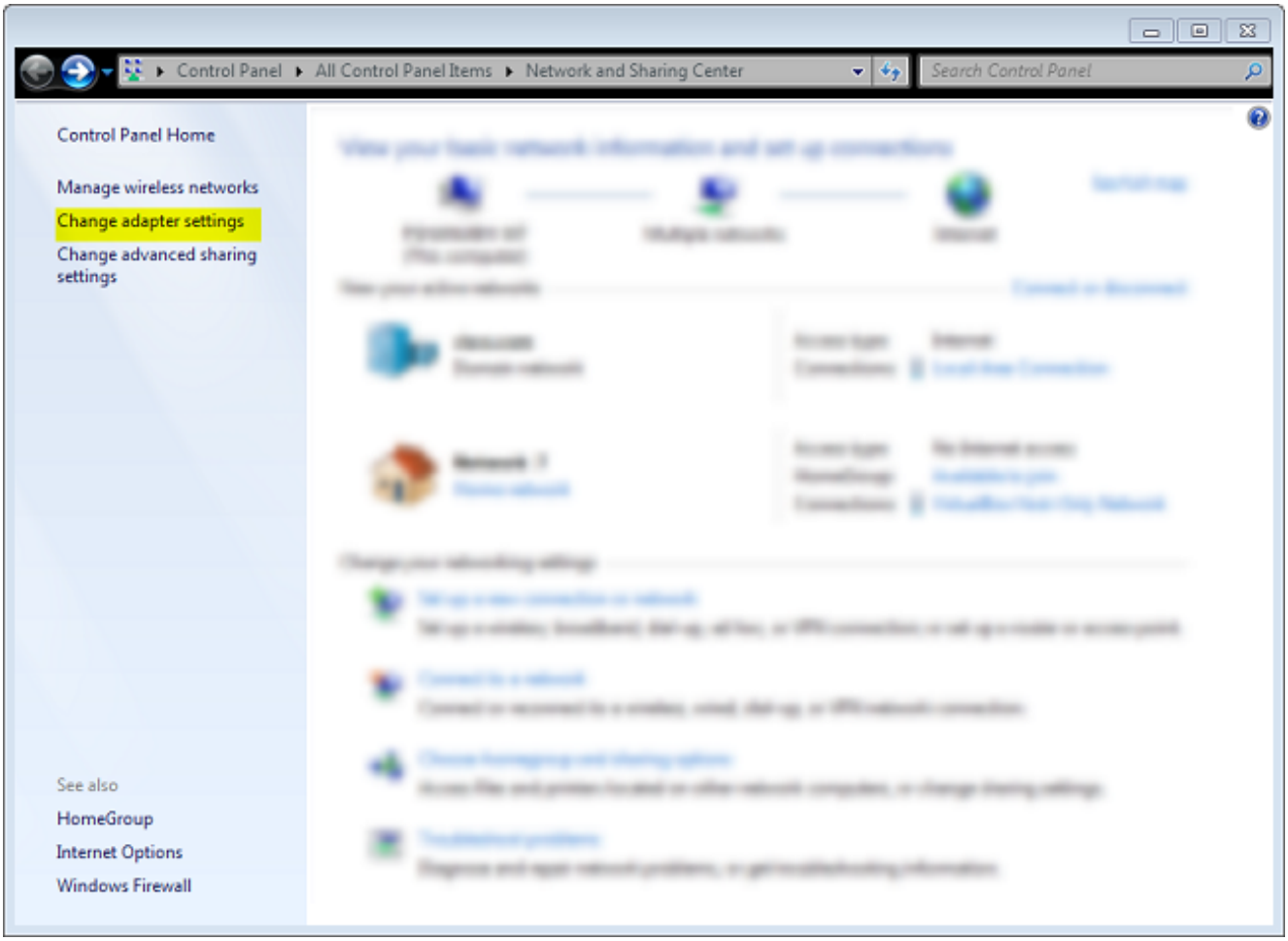


4. 請勿填寫User name、Password和Domain（可選）欄位，因為將使用證書身份驗證。按一下「Create」。



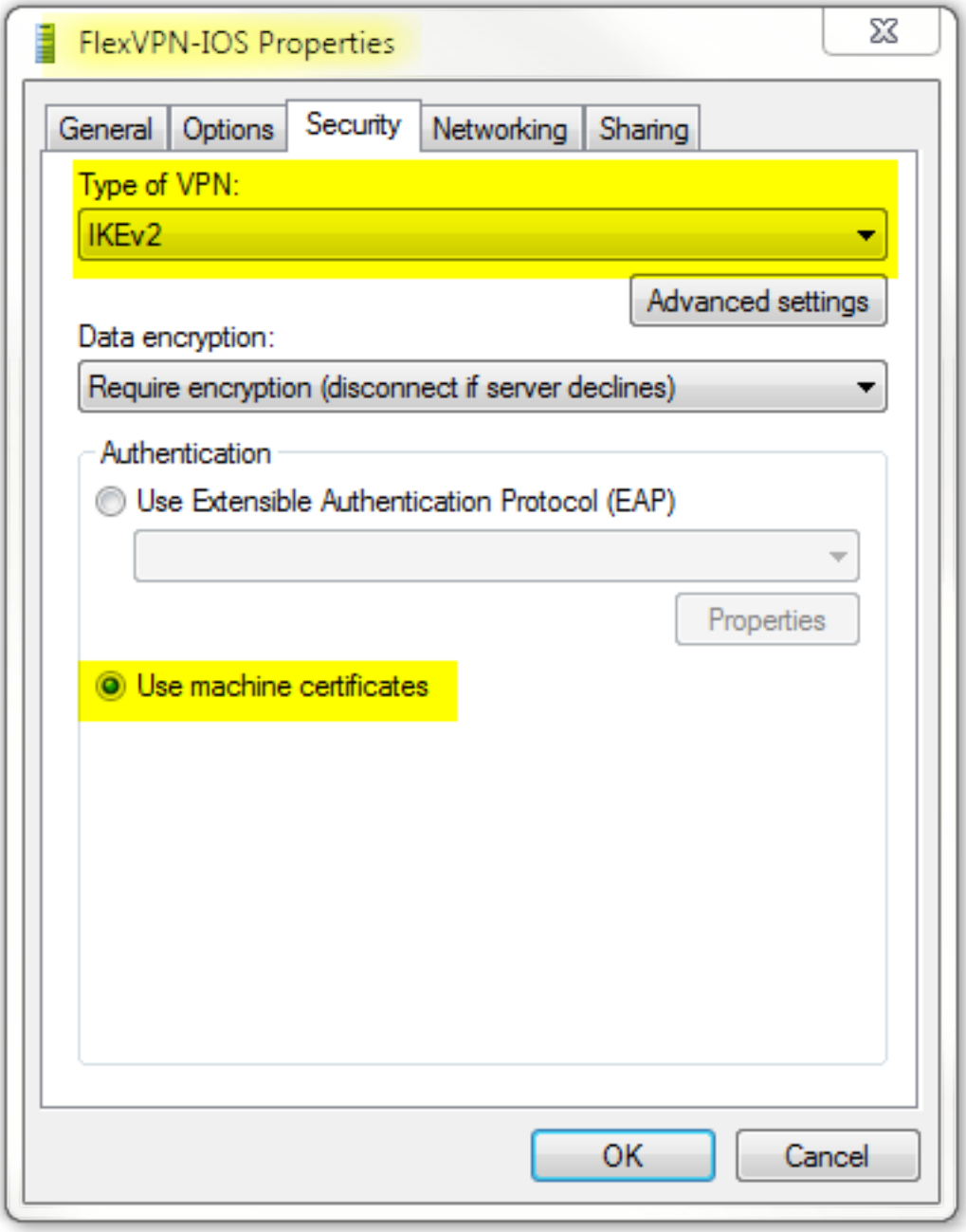
附註：關閉生成的視窗。**請勿嘗試連線。**

5. 導航回**網路和共用中心**，然後按一下**更改介面卡設定**。



6. 選擇Logical Adapter FlexVPN-IOS，這是到目前為止執行的所有步驟的結果。按一下其屬性。以下是新建立的名為FlexVPN-IOS的連線配置檔案的屬性：

   在Security頁籤上，VPN的型別應為IKEv2。在Authentication部分，選擇**Use machine certificates**。



在將證書匯入到電腦證書儲存後，FlexVPN-IOS配置檔案現在即可連線。

獲取客戶端證書

使用者端憑證需要以下因素：

- 客戶端證書的EKU為「客戶端身份驗證」。 此外，CA會提供PKCS#12憑證：

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

- CA證書：

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

重要詳細資訊

- 如果以下兩個語句都適用，則應將「IPSec IKE中繼」(OID = 1.3.6.1.5.5.8.2.2)用作EKU:

IKEv2伺服器是Windows 2008伺服器。有多個伺服器身份驗證證書用於IKEv2連線。如果為true，則將「伺服器身份驗證」EKU和「IPSec IKE中繼」EKU都放在一個證書上，或者在證書中分發這些EKU。請確保至少一個證書包含「IPSec IKE Intermediate」EKU。

有關詳細資訊，請參閱IKEv2 VPN連線故障排除。

- 在FlexVPN部署中，不要在EKU中使用「IPSec IKE Intermediate」。如果這樣做，IKEv2客戶端不會獲取IKEv2伺服器證書。因此，它們無法從IKE_SA_INIT響應消息中的IOS響應CERTREQ，因此無法使用13806 Error ID進行連線。
- 雖然不需要使用者替代名稱(SAN)，但如果憑證有此名稱，則可接受。
- 在Windows 7客戶端證書儲存區上，確保機器信任的根證書頒發機構儲存區具有儘可能少的證書。如果超過50個，Cisco IOS可能無法讀取整個Cert_Req負載，該負載包含Windows 7框中所有已知CA的證書可分辨名稱(DN)。因此，協商失敗，您會看到客戶端上的連線超時。

驗證

使用本節內容，確認您的組態是否正常運作。

輸出直譯器工具(僅供已註冊客戶使用)支援某些**show**命令。使用輸出直譯器工具來檢視**show**命令輸出的分析。

```
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
1 10.0.3.1/4500 192.168.56.1/4500 none/none READY
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:
```

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- 適用於採用PSK的站點到站點VPN的ASA IKEv2調試技術說明
- ASA IPsec和IKE調試（IKEv1主模式）故障排除技術說明
- IOS IPSec和IKE調試 — IKEv1主模式故障排除技術說明
- ASA IPSec和IKE調試 — IKEv1主動模式技術說明
- Cisco ASA 5500系列調適型安全裝置
- Cisco ASA 5500系列自適應安全裝置軟體下載
- Cisco IOS 防火牆

- Cisco IOS軟體
- 安全殼層 (SSH)
- IPSec 協商/IKE 通訊協定
- 技術支援與文件 - Cisco Systems