在FlexVPN上使用Windows 7 IKEv2灵活VPN客户端和证书身份验证的IKEv2

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[规则](#)
[配置](#)
[概述](#)
[配置证书颁发机构](#)
[配置Cisco IOS头端](#)
[配置Windows 7内置客户端](#)
[获取客户端证书](#)
[重要详细信息](#)
[验证](#)
[故障排除](#)
[相关信息](#)

简介

FlexVPN是Cisco IOS®上基于Internet密钥交换第2版(IKEv2)的新VPN基础设施，是统一VPN解决方案。本文档介绍如何配置内置到Windows 7中的IKEv2客户端，以便使用证书颁发机构(CA)连接Cisco IOS头端。

> **注意**：自适应安全设备(ASA)现在支持从版本9.3(2)起与Windows 7内置客户端建立IKEv2连接。

> **注意**：SUITE-B协议不起作用，因为IOS头端不支持SUITE-B与IKEv1，或者Windows 7 IKEv2 Agile VPN客户端当前不支持SUITE-B与IKEv2。

先决条件

要求

Cisco 建议您了解以下主题：

- Windows 7内置VPN客户端
- 思科IOS软件版本15.2(2)T
- 证书颁发机构 — OpenSSL CA

使用的组件

本文档中的信息基于下列硬件和软件版本：

- Windows 7内置VPN客户端
- 思科IOS软件版本15.2(2)T
- 证书颁发机构 — OpenSSL CA

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的信息，请参阅 Cisco 技术提示规则。

配置

概述

配置Windows 7内置IKEv2客户端有四个主要步骤，以便使用CA连接Cisco IOS头端：

1. 配置CA

   CA应允许您在证书中嵌入所需的扩展密钥使用(EKU)。例如，在IKEv2服务器上，需要“Server Auth EKU”，而客户端证书需要“Client Auth EKU”。 本地部署可以利用：Cisco IOS CA服务器 — 由于Bug CSCuc82575，无法使用自签名证书。OpenSSL CA服务器Microsoft CA服务器 — 通常，这是首选选项，因为它可以配置为完全按照需要签署证书。

2. 配置Cisco IOS头端

   获取证书配置IKEv2

3. 配置Windows 7内置客户端
4. 获取客户端证书

以下各节将详细介绍这些主要步骤。

注意：使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

配置证书颁发机构

本文档不提供有关如何设置CA的详细步骤。但是，本节中的步骤将向您展示如何配置CA，以便它可以为此类部署颁发证书。

OpenSSL

OpenSSL CA基于“config”文件。OpenSSL服务器的“config”文件应具有：

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

思科IOS CA服务器

如果使用Cisco IOS CA服务器，请确保使用最新的Cisco IOS软件版本，该版本分配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
```

配置Cisco IOS头端

获取证书

证书的EKU字段必须设置为Cisco IOS的“服务器身份验证”，客户端的“客户端身份验证”。通常，同一CA用于签署客户端证书和服务器证书。在这种情况下，服务器证书和客户端证书上分别显示“服务器身份验证”和“客户端身份验证”，这是可接受的。

如果CA在IKEv2服务器上向客户端和服务器颁发公钥加密标准(PKCS)#12格式的证书，并且如果证书撤销列表(CRL)不可访问或不可用，则必须配置：

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

输入以下命令以导入PKCS#12证书：

```
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服务器自动授予证书，则必须使用CA服务器URL配置IKEv2服务器，以便接收证书，如本例所示：

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

配置信任点时，您需要：

1. 使用此命令对CA进行身份验证：

```
crypto pki authenticate FlexRootCA
```

2. 使用以下命令向CA注册IKEv2服务器：

```
crypto pki enroll FlexRootCA
```

要查看证书是否包含所有必需选项，请使用以下**show**命令：

```
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
```

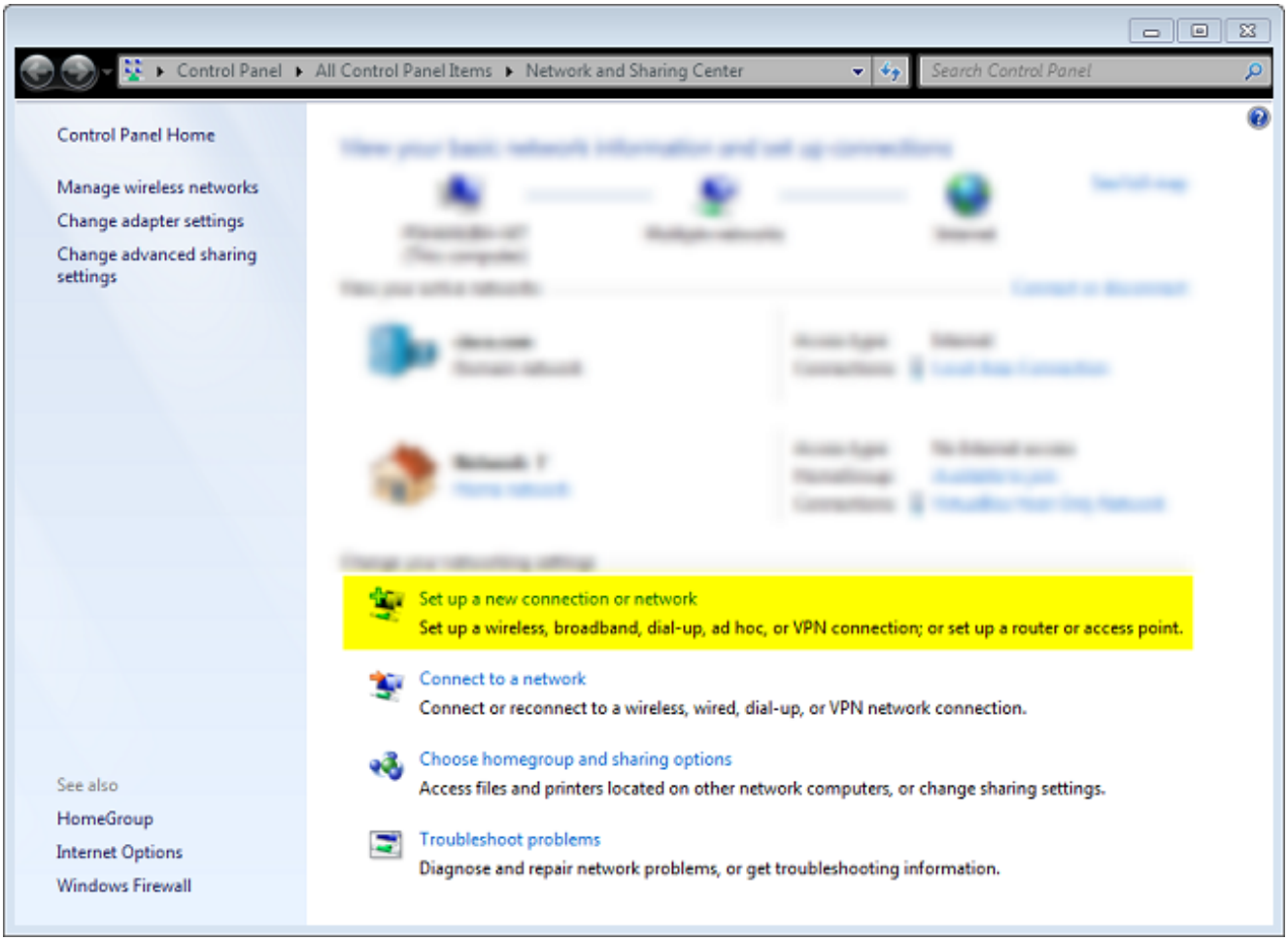
```
!! One of the proposals that Windows 7 Built-In Client Likes

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
```

除用于IPsec连接的本地地址外，虚拟模板的未编号IP应为任何值。 [如果使用硬件客户端，您将通过IKEv2配置节点交换路由信息并在硬件客户端上创建递归路由问题。]

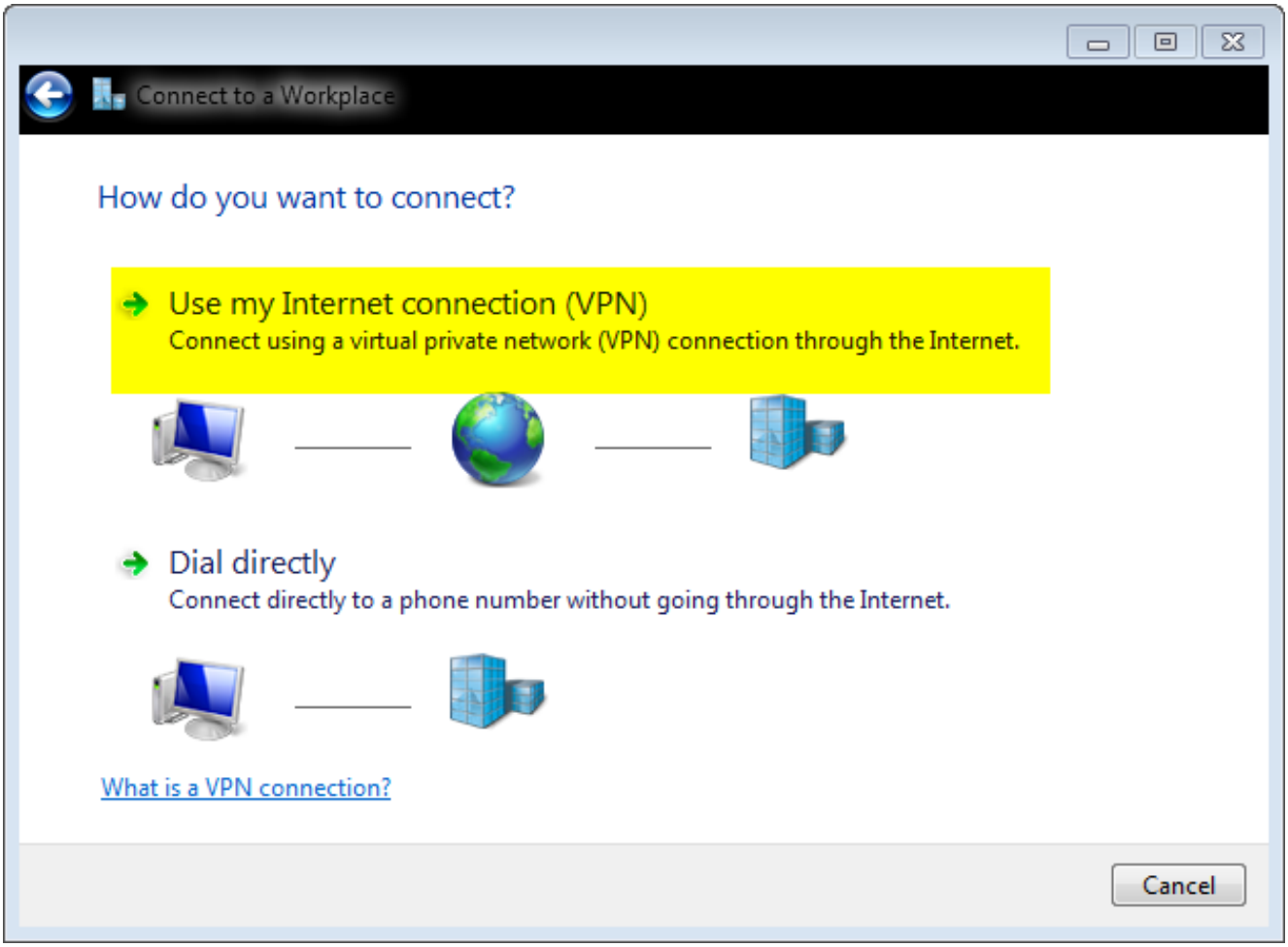
配置Windows 7内置客户端

此过程介绍如何配置Windows 7内置客户端。

1. 导航至网**络和共享中**心，然**后单击“设置新连接或网络”**。

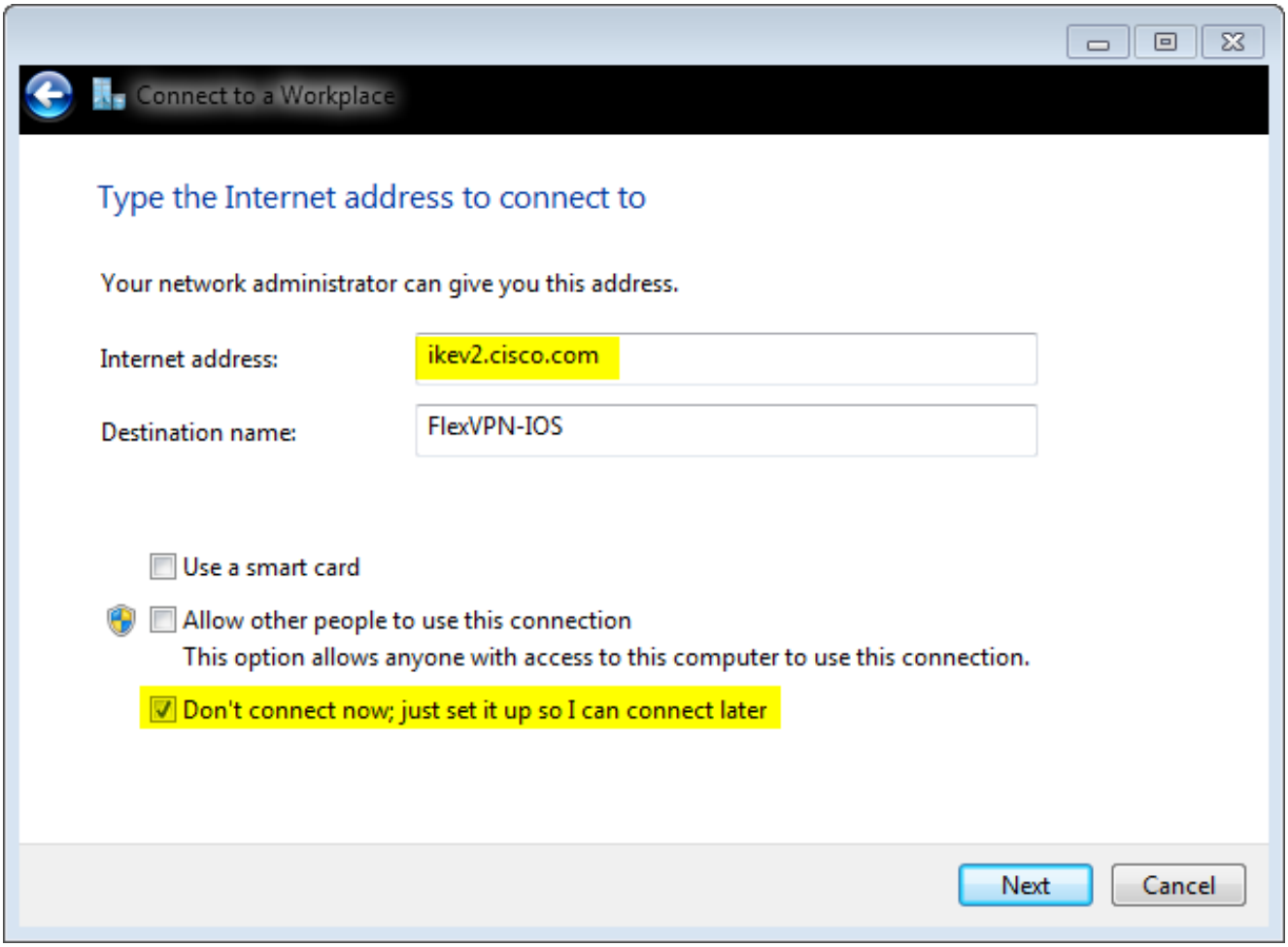


2. 单击**Use my Internet connection(VNP)(使用我的互联网连接(VNP))**。 这允许您设置通过当前Internet连接协商的VPN连接。

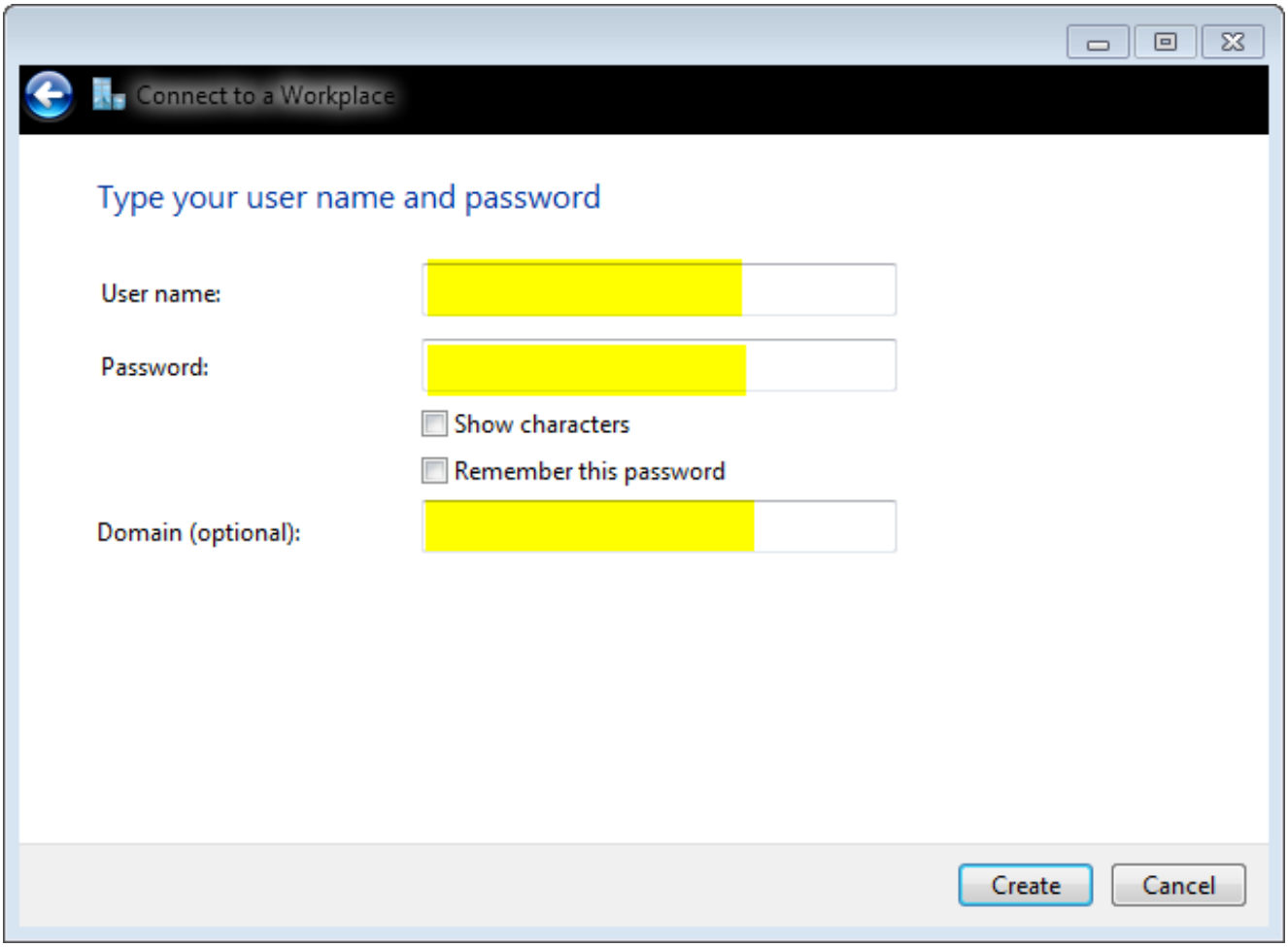


3. 输入IKEv2服务器的完全限定域名(FQDN)或IP地址，并为其指定目标名称以在本地标识它。

注意：FQDN必须与路由器身份证书中的公用名称(CN)匹配。如果Windows 7检测到不匹配，则会断开连接，出现13801错误。
由于需要设置其他参数，请选**中Do not connect now;只需设置它，以便我以后可以连接**，然后单击“下**一步**:

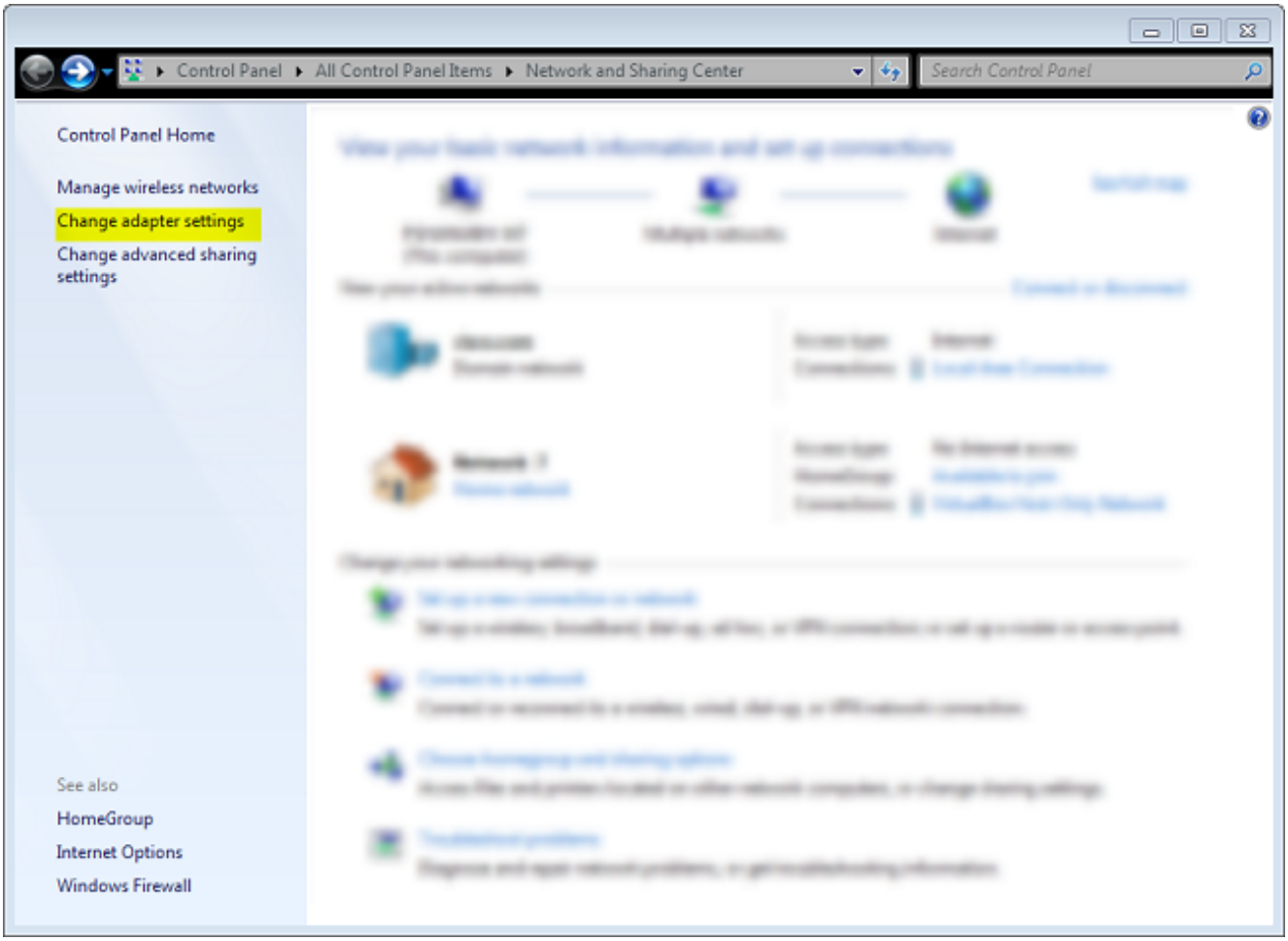


4. 请勿填写“**用户名、密码**和**域（可选）**”字段，因为要使用“证书身份验证”。Click **Create**.



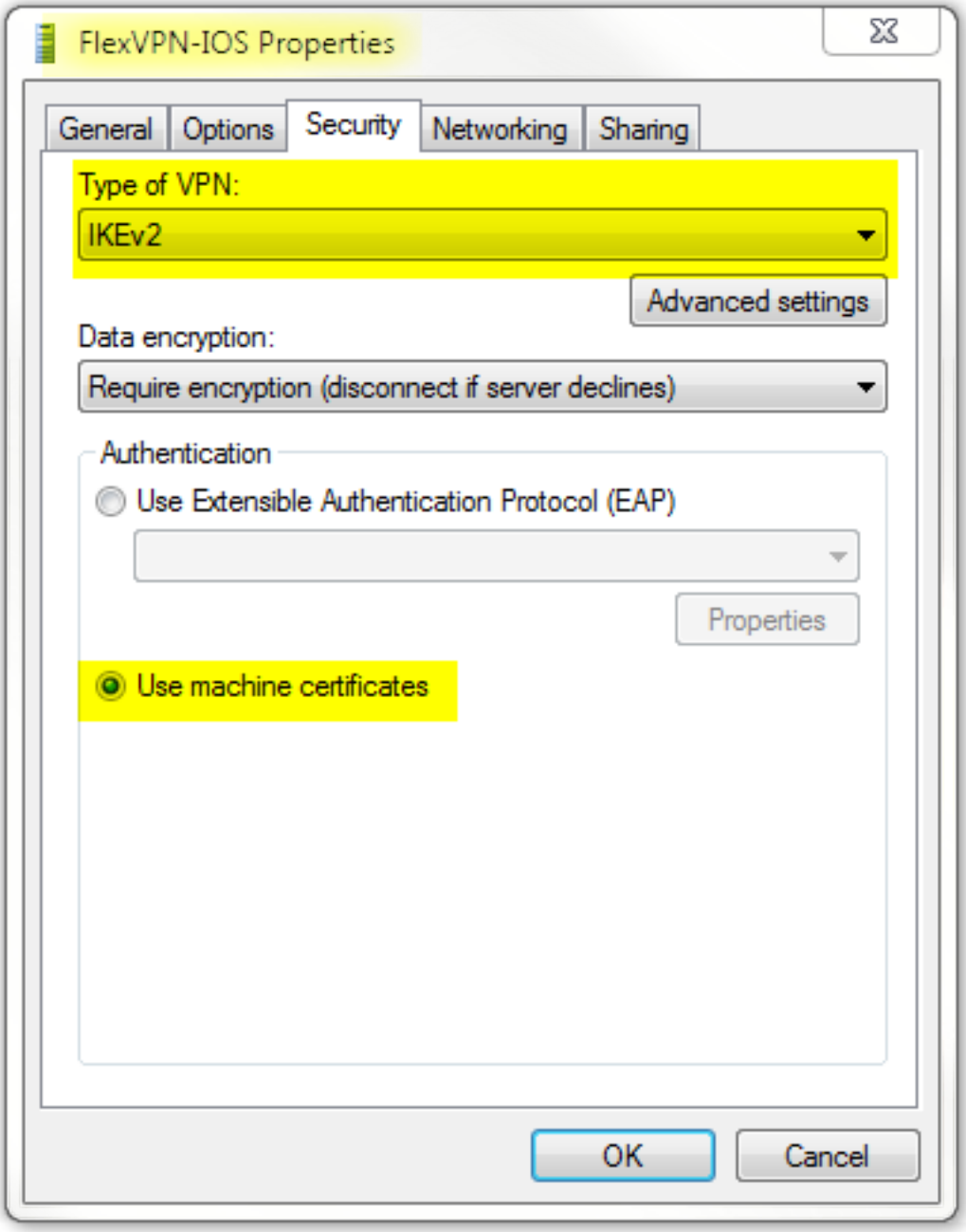
注意：关闭生成的窗口。**请勿尝试连接。**

5. 导航回网络和共**享中心，然**后单击“更**改适配器设置**”。



6. 选择逻辑适配器FlexVPN-IOS，这是到目前为止所采取的所有步骤的结果。单击其属性。以下是新创建的连接配置文件（称为FlexVPN-IOS）的属性：

   在Security选项卡上，VPN的类型应为IKEv2。在“身份验证”部分，选择**使用计算机证书**。



在您将证书导入计算机证书存储后，FlexVPN-IOS配置文件现已准备好连接。

获取客户端证书

客户端证书需要以下因素：

- 客户端证书的EKU为“客户端身份验证”。 此外，CA会提供PKCS#12证书：

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

- CA 证书:

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

重要详细信息

- 如果以下两种语句均适用，应将“IPSec IKE中间”(OID = 1.3.6.1.5.5.8.2.2)用作EKU:

IKEv2服务器是Windows 2008服务器。IKEv2连接使用多个服务器身份验证证书。如果为真，请将“服务器身份验证”EKU和“IPSec IKE中间”EKU都放在一个证书上，或在证书之间分发这些EKU。确保至少一个证书包含“IPSec IKE Intermediate”EKU。

有关详细信息，请参阅排除IKEv2 VPN连接故障。

- 在FlexVPN部署中，请勿在EKU中使用“IPSec IKE中间”。如果您这样做，IKEv2客户端将不会拾取IKEv2服务器证书。因此，它们无法从IKE_SA_INIT响应消息中的IOS响应CERTREQ，因此无法连接13806错误ID。
- 虽然不需要主题备用名称(SAN)，但如果证书有，则可接受。
- 在Windows 7客户端证书存储区上，确保计算机受信任根证书颁发机构存储区具有尽可能少的证书数。如果超过50个，Cisco IOS可能无法读取整个Cert_Req负载，该负载包含Windows 7框中所有已知CA的证书可分辨名称(DN)。因此，协商失败，您在客户端上看到连接超时。

验证

使用本部分可确认配置能否正常运行。

命令输出解释程序工具（仅限注册用户）支持某些 **show 命令。**使用输出解释器工具来查看 show 命令输出的分析。

```
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:
```

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- 使用PSK的站点到站点VPN的ASA IKEv2调试技术说明
- ASA IPsec和IKE调试（IKEv1主模式）故障排除技术说明
- IOS IPSec和IKE调试 — IKEv1主模式故障排除技术说明
- ASA IPSec和IKE调试 — IKEv1主动模式技术说明
- Cisco ASA 5500 系列自适应安全设备
- Cisco ASA 5500系列自适应安全设备软件下载
- Cisco IOS 防火墙

- Cisco IOS 软件
- Secure Shell (SSH)
- IPsec 协商/IKE 协议
- 技术支持和文档 - Cisco Systems