

IKEv2 avec client VPN agile IKEv2 Windows 7 et authentification de certificat sur FlexVPN

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Conventions](#)

[Configuration](#)

[Aperçu](#)

[Configurer l'autorité de certification](#)

[Configurer la tête de réseau Cisco IOS](#)

[Configurer le client intégré de Windows 7](#)

[Obtenir le certificat client](#)

[Détails importants](#)

[Vérification](#)

[Dépannage](#)

[Informations connexes](#)

Introduction

FlexVPN est la nouvelle infrastructure VPN basée sur Internet Key Exchange version 2 (IKEv2) sur Cisco IOS[®] et est conçue comme une solution VPN unifiée. Ce document décrit comment configurer le client IKEv2 intégré à Windows 7 afin de connecter une tête de réseau Cisco IOS à l'utilisation d'une autorité de certification (CA).

Note: L'ASA (Adaptive Security Appliance) prend désormais en charge les connexions IKEv2 avec le client intégré Windows 7 à partir de la version 9.3(2).

Note: Les protocoles SUITE-B ne fonctionnent pas, car la tête de réseau IOS ne prend pas en charge SUITE-B avec IKEv1 ou le client VPN agile Windows 7 IKEv2 ne prend pas en charge SUITE-B avec IKEv2.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Client VPN intégré Windows 7
- Logiciel Cisco IOS Version 15.2(2)T
- Autorité de certification - OpenSSL CA

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Client VPN intégré Windows 7
- Logiciel Cisco IOS Version 15.2(2)T
- Autorité de certification - OpenSSL CA

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

Configuration

Aperçu

La configuration du client IKEv2 intégré à Windows 7 comporte quatre étapes principales afin de connecter une tête de réseau Cisco IOS à l'utilisation d'une autorité de certification :

1. Configurer CA

L'autorité de certification doit vous permettre d'incorporer l'utilisation de clé étendue (EKU) requise dans le certificat. Par exemple, sur le serveur IKEv2, 'Server Auth EKU' est requis, tandis que le certificat client nécessite 'Client Auth EKU'. Les déploiements locaux peuvent utiliser : Serveur CA Cisco IOS - Les certificats auto-signés ne peuvent pas être utilisés en raison du bogue [CSCuc82575](#). Serveur OpenSSL CA Serveur Microsoft CA - En général, c'est l'option préférée car elle peut être configurée pour signer le certificat exactement comme vous le souhaitez.

2. Configurer la tête de réseau Cisco IOS

Obtenir un certificat Configurer IKEv2

3. Configurer le client intégré de Windows 7
4. Obtenir le certificat client

Chacune de ces étapes principales est expliquée en détail dans les sections suivantes.

Note: Utilisez l'[Outil de recherche de commande \(clients inscrits seulement\) pour obtenir plus d'informations sur les commandes utilisées dans cette section.](#)

Configurer l'autorité de certification

Ce document ne fournit pas d'étapes détaillées sur la façon de configurer une autorité de certification. Cependant, les étapes de cette section vous montrent comment configurer l'autorité de certification afin qu'elle puisse émettre des certificats pour ce type de déploiement.

OpenSSL

OpenSSL CA est basé sur le fichier 'config'. Le fichier 'config' du serveur OpenSSL doit avoir :

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

Serveur Cisco IOS CA

Si vous utilisez un serveur CA Cisco IOS, assurez-vous d'utiliser la version la plus récente du logiciel Cisco IOS, qui attribue l'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
```

Configurer la tête de réseau Cisco IOS

Obtenir un certificat

Les champs EKU du certificat doivent être définis sur 'Authentification du serveur' pour Cisco IOS et 'Authentification du client' pour le client. Généralement, la même autorité de certification est utilisée pour signer les certificats client et serveur. Dans ce cas, 'Authentification du serveur' et 'Authentification du client' sont affichés respectivement sur le certificat du serveur et le certificat du client, ce qui est acceptable.

Si l'autorité de certification émet les certificats au format PKCS (Public-Key Cryptography Standards) #12 sur le serveur IKEv2 aux clients et au serveur, et si la liste de révocation de certificats (CRL) n'est pas accessible ou disponible, elle doit être configurée :

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

Entrez cette commande afin d'importer le certificat PKCS#12 :

```
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.
```

Si un serveur d'autorité de certification Cisco IOS accorde automatiquement des certificats, le serveur IKEv2 doit être configuré avec l'URL du serveur d'autorité de certification afin de recevoir un certificat comme indiqué dans cet exemple :

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

Lorsque le point de confiance est configuré, vous devez :

1. Authentifier l'autorité de certification à l'aide de la commande suivante :

```
crypto pki authenticate FlexRootCA
```

2. Inscrivez le serveur IKEv2 avec l'autorité de certification avec la commande suivante :

```
crypto pki enroll FlexRootCA
```

Afin de voir si le certificat contient toutes les options requises, utilisez cette commande **show** :

```
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

Configurer IKEv2

Voici un exemple de configuration 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

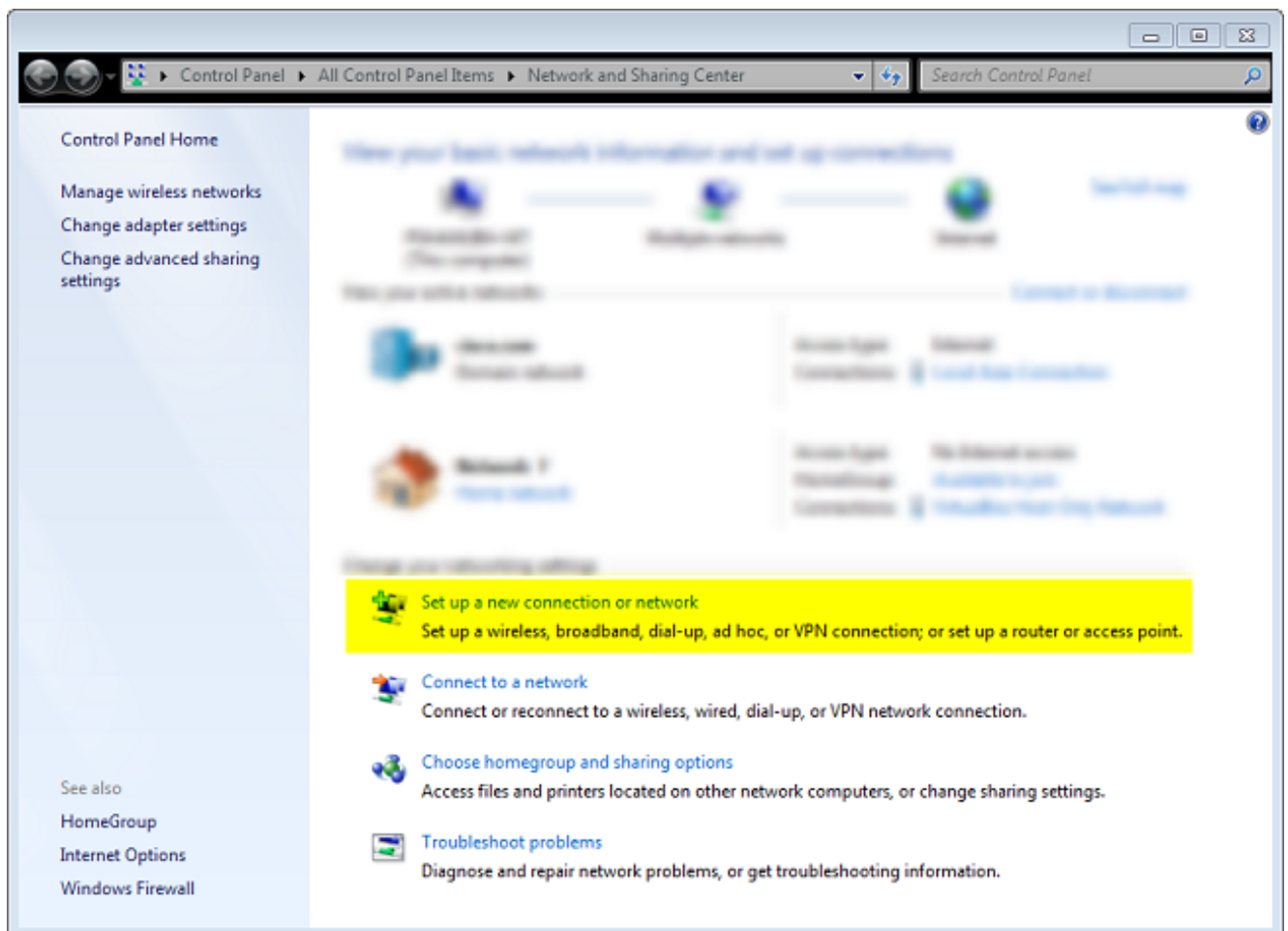
```
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile win7_ikev2
```

L'adresse IP non numérotée du modèle virtuel doit être tout sauf l'adresse locale utilisée pour la connexion IPsec. [Si vous utilisez un client matériel, vous échangeriez des informations de routage via le noeud de configuration IKEv2 et créeriez un problème de routage récursif sur le client matériel.]

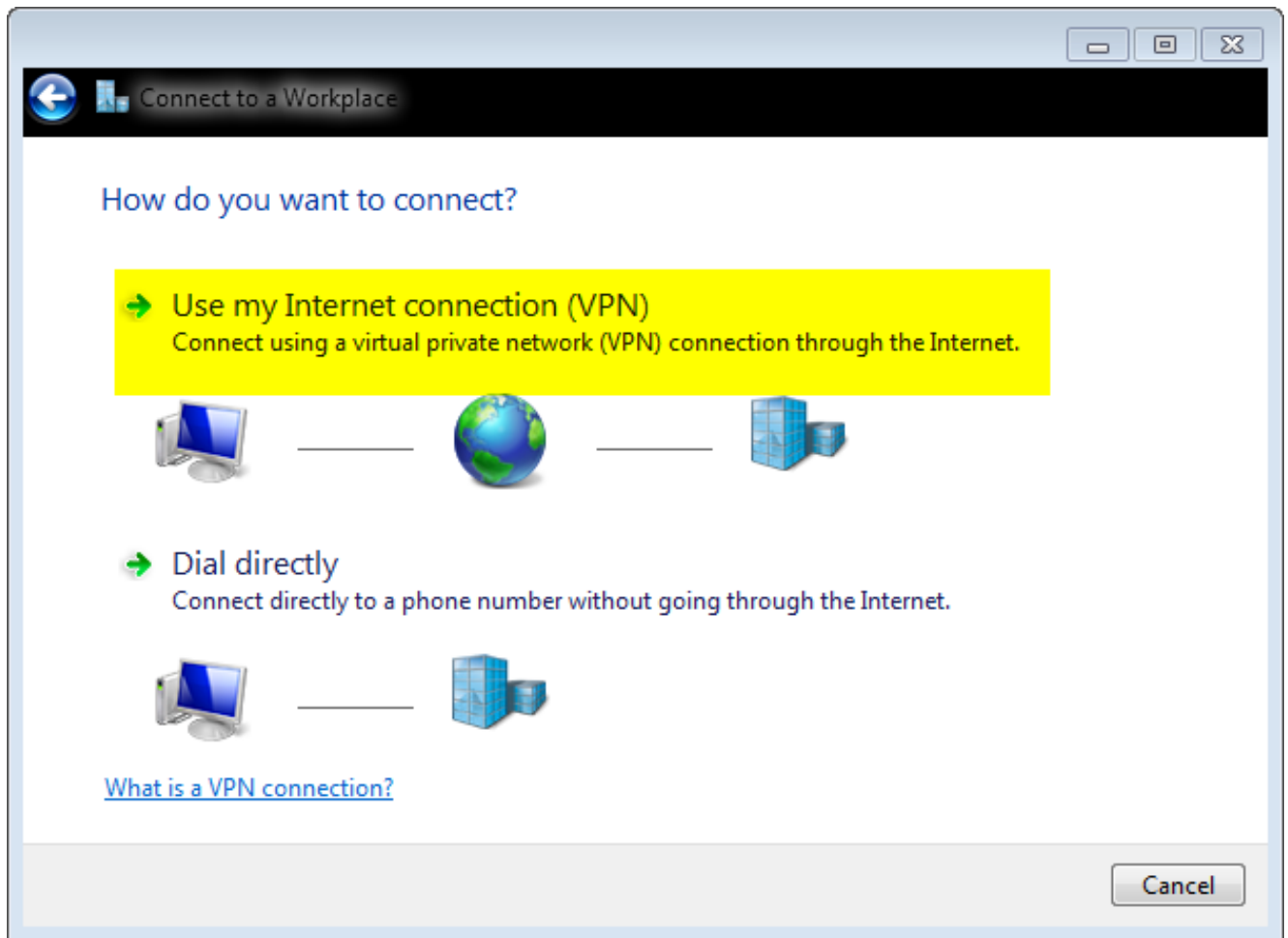
Configurer le client intégré de Windows 7

Cette procédure décrit comment configurer le client intégré de Windows 7.

1. Accédez au **Centre Réseau et partage**, puis cliquez sur **Configurer une nouvelle connexion ou un nouveau réseau**.



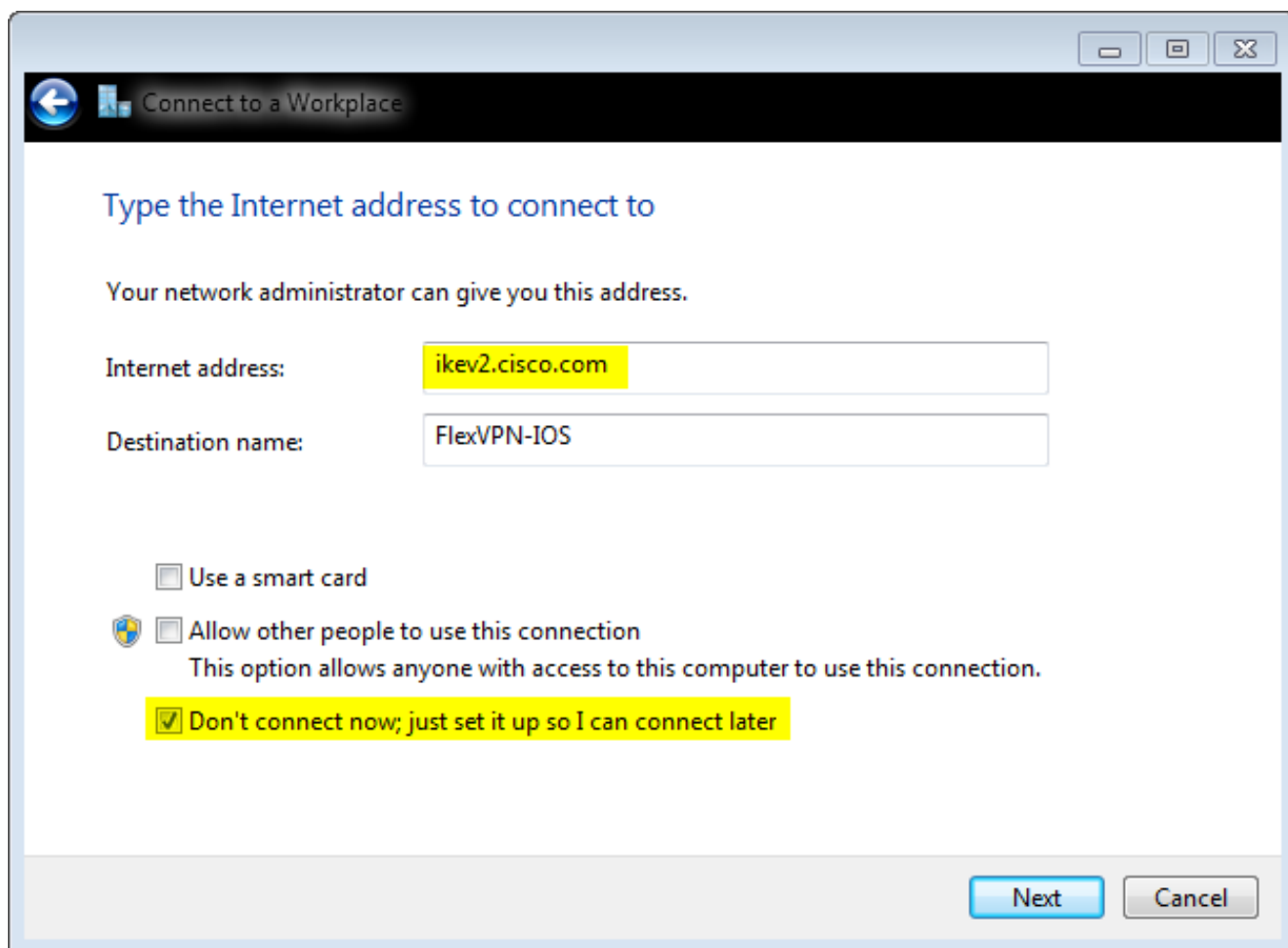
2. Cliquez sur **Utiliser ma connexion Internet (VPN)**. Cela vous permet de configurer une connexion VPN négociée via une connexion Internet en cours.



3. Saisissez le nom de domaine complet (FQDN) ou l'adresse IP du serveur IKEv2 et attribuez-lui un nom de destination pour l'identifier localement.

Note: Le nom de domaine complet (FQDN) doit correspondre au nom commun (CN) du certificat d'identité du routeur. Windows 7 supprime la connexion avec une erreur 13801 s'il détecte une non-correspondance.

Étant donné que des paramètres supplémentaires doivent être définis, cochez la case **Ne pas se connecter maintenant** ; il suffit de le configurer pour que je puisse me connecter plus tard, puis cliquez sur **Suivant** :



4. Ne renseignez pas les champs **Nom d'utilisateur**, **Mot de passe** et **Domaine (facultatif)**, car **l'authentification de certificat doit être utilisée**. Click **Create**.

Connect to a Workplace

Type your user name and password

User name:

Password:

Show characters

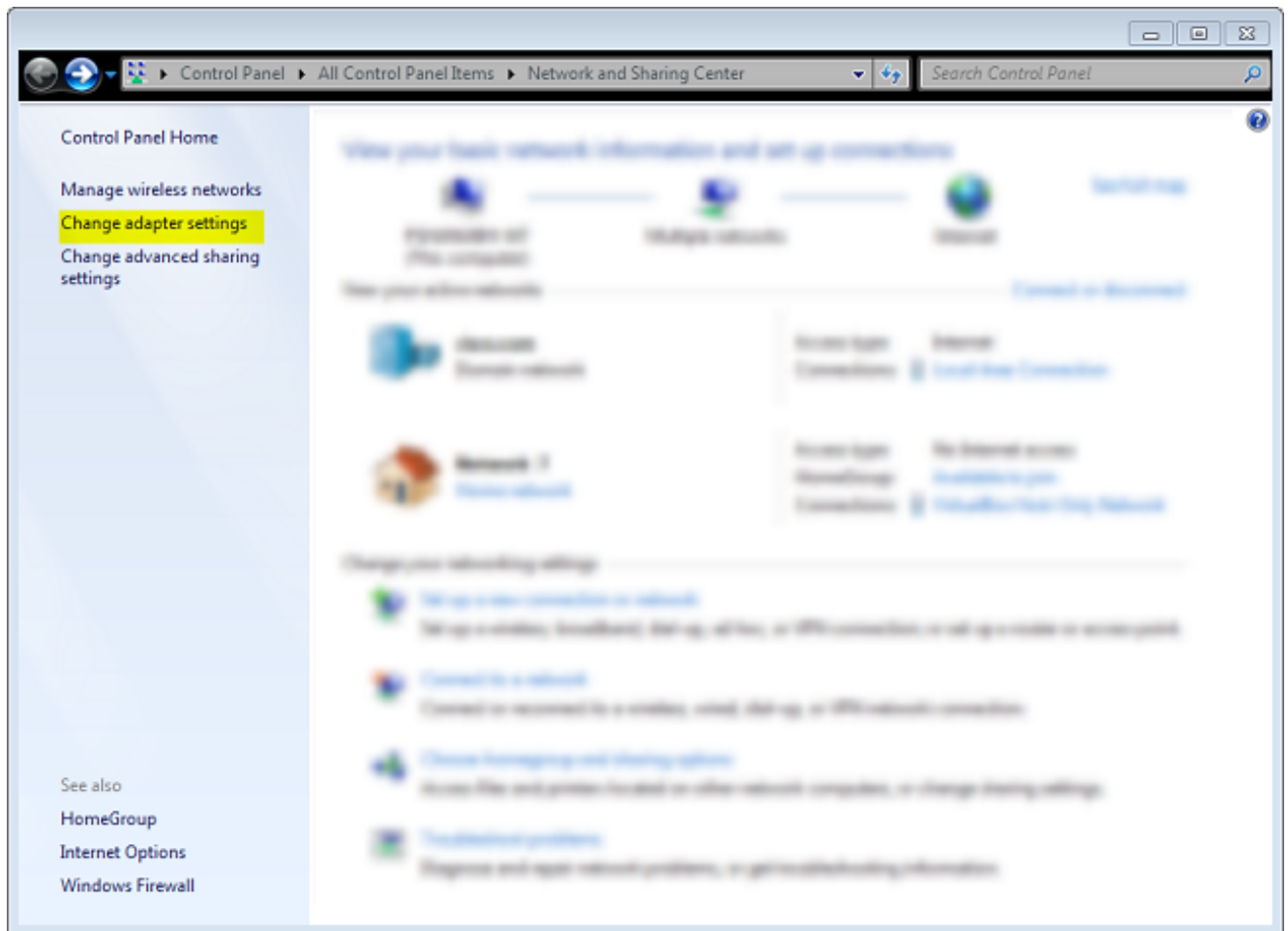
Remember this password

Domain (optional):

Create Cancel

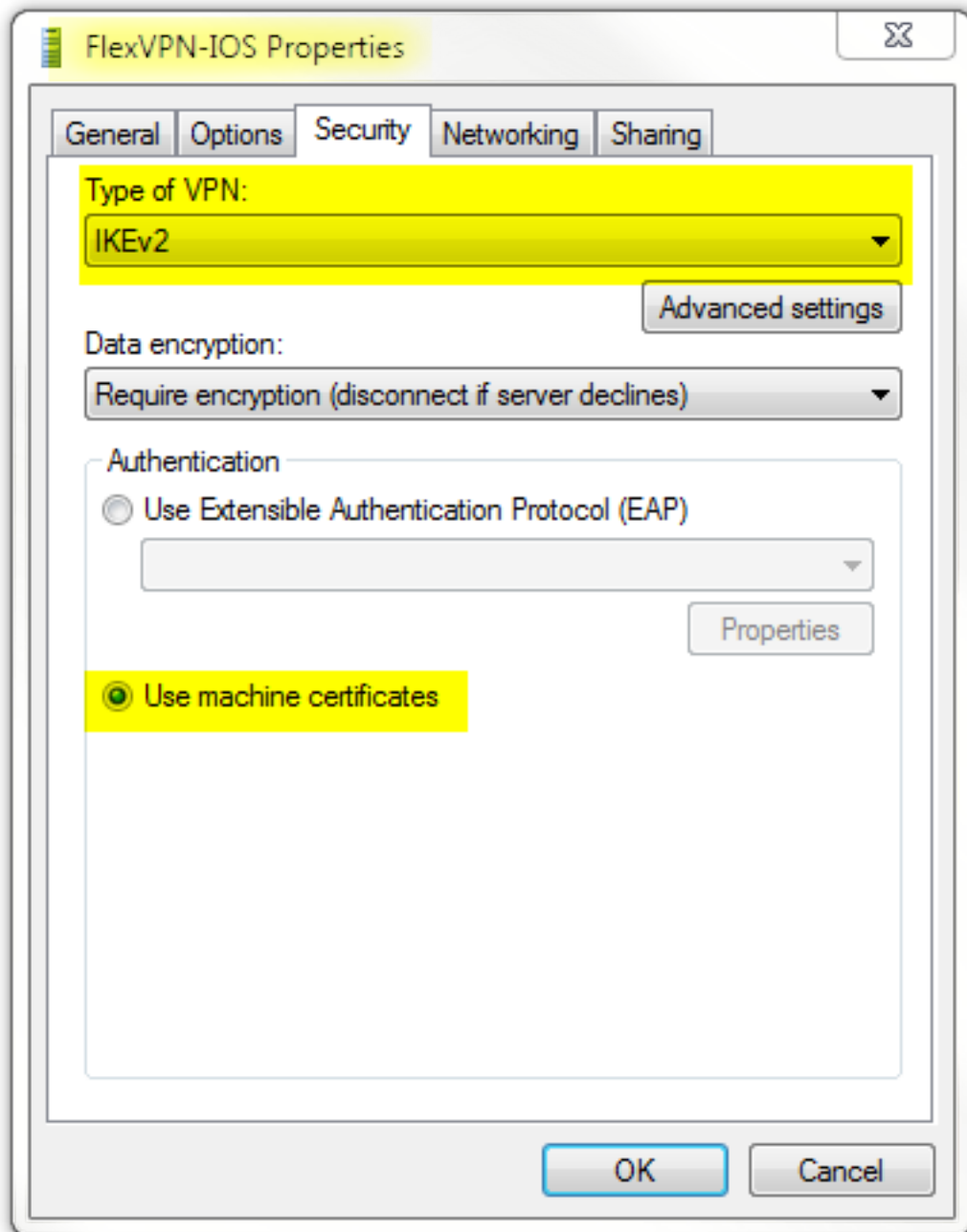
Note: Fermez la fenêtre résultante. **N'essayez pas de vous connecter.**

5. Revenez au **Centre Réseau et partage**, puis cliquez sur **Modifier les paramètres de la carte**.



6. Choisissez l'adaptateur logique FlexVPN-IOS, qui est le résultat de toutes les étapes effectuées à ce point. Cliquez sur ses propriétés. Voici les propriétés du profil de connexion récemment créé appelé FlexVPN-IOS :

Dans l'onglet Security, le type de VPN doit être IKEv2. Dans la section Authentification, sélectionnez **Utiliser les certificats de l'ordinateur**.



Le profil FlexVPN-IOS est maintenant prêt à être connecté après l'importation d'un certificat dans le magasin de certificats de l'ordinateur.

Obtenir le certificat client

Le certificat client requiert les facteurs suivants :

- Le certificat client a un EKU de 'Authentification du client'. En outre, l'autorité de certification fournit un certificat PKCS#12 :

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

- Certificat CA :

CA Certificate goes into Local Machine Trusted Root Certificate Authorities Store

Détails importants

- 'Intermédiaire IKE IPsec' (OID = 1.3.6.1.5.5.8.2.2) doit être utilisé comme EKU si ces deux instructions s'appliquent :

Le serveur IKEv2 est un serveur Windows 2008. Plusieurs certificats d'authentification de serveur sont utilisés pour les connexions IKEv2. Si cela est vrai, placez l'EKU 'Server Authentication' et l'EKU 'IPsec IKE Intermediate' sur un certificat, ou distribuez ces EKU parmi les certificats. Assurez-vous qu'au moins un certificat contient l'EKU 'IPsec IKE Intermediate'.

Référez-vous à [Dépannage des connexions VPN IKEv2](#) pour plus d'informations.

- Dans un déploiement FlexVPN, n'utilisez pas IPsec IKE Intermediate dans EKU. Si vous le faites, le client IKEv2 ne récupère pas le certificat de serveur IKEv2. Par conséquent, ils ne peuvent pas répondre à CERTREQ à partir de l'IOS dans le message de réponse IKE_SA_INIT et ne peuvent donc pas se connecter avec un ID d'erreur 13806.
- Bien que le nom de remplacement du sujet (SAN) ne soit pas requis, il est acceptable que les certificats en aient un.
- Dans le magasin de certificats client Windows 7, assurez-vous que le magasin d'autorités de certificats racine de confiance en ordinateur a le moins de certificats possible. S'il a plus de 50 caractères, Cisco IOS peut ne pas lire la charge utile Cert_Req entière, qui contient le nom distinctif de certificat (DN) de toutes les autorités de certification connues dans la zone Windows 7. Par conséquent, la négociation échoue et vous voyez le délai de connexion sur le client.

Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'Outil d'interprétation de sortie (clients enregistrés seulement) prend en charge certaines commandes d'affichage. Utilisez l'Outil d'interprétation de sortie afin de visualiser une analyse de commande d'affichage de sortie .

```
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:

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- [Débogues ASA IKEv2 pour VPN site à site avec PSKs TechNote](#)
- [Dépannage des débogages ASA IPsec et IKE \(IKEv1 Main Mode\) TechNote](#)
- [Débogues IOS IPsec et IKE - IKEv1 Main Mode Trouver TechNote](#)
- [Débogues ASA IPsec et IKE - IKEv1 Aggressive Mode TechNote](#)
- [Dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500](#)
- [Téléchargements de logiciels des appareils de sécurité adaptatifs de la gamme Cisco ASA 5500](#)
- [Cisco IOS Firewall](#)
- [Logiciel Cisco IOS](#)
- [Secure Shell \(SSH\)](#)
- [Négociation IPsec/Protocoles IKE](#)
- [Support et documentation techniques - Cisco Systems](#)