

# IKEv2 con cliente VPN ágil IKEv2 de Windows 7 y autenticación de certificado en FlexVPN

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configurar](#)

[Overview](#)

[Configurar autoridad de certificados](#)

[Configuración de la cabecera de Cisco IOS](#)

[Configurar cliente integrado de Windows 7](#)

[Obtener certificado de cliente](#)

[Detalles importantes](#)

[Verificación](#)

[Troubleshoot](#)

[Información Relacionada](#)

## Introducción

FlexVPN es la nueva infraestructura de VPN basada en Internet Key Exchange versión 2 (IKEv2) en Cisco IOS<sup>®</sup> y está diseñada para ser una solución de VPN unificada. Este documento describe cómo configurar el cliente IKEv2 integrado en Windows 7 para conectar una cabecera de Cisco IOS con la utilización de una Autoridad de Certificación (CA).

**Nota:** El dispositivo de seguridad adaptable (ASA) ahora admite conexiones IKEv2 con el cliente integrado de Windows 7 a partir de la versión 9.3(2).

**Nota:** Los protocolos SUITE-B no funcionan porque la cabecera del IOS no admite SUITE-B con IKEv1, o el cliente VPN ágil IKEv2 de Windows 7 no soporta actualmente SUITE-B con IKEv2.

## Prerequisites

## Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cliente VPN incorporado de Windows 7
- Versión 15.2(2)T del software del IOS de Cisco
- Autoridad de certificados - OpenSSL CA

## Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software y hardware.

- Cliente VPN incorporado de Windows 7
- Versión 15.2(2)T del software del IOS de Cisco
- Autoridad de certificados - 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.

## Convenciones

Consulte [Convenciones de Consejos Técnicos de Cisco para obtener información sobre las convenciones sobre documentos.](#)

## Configurar

### Overview

Hay cuatro pasos principales en la configuración del cliente IKEv2 integrado de Windows 7 para conectar una cabecera de Cisco IOS con la utilización de una CA:

#### 1. Configurar CA

La CA debe permitirle incrustar el uso de clave extendida (EKU) requerido en el certificado. Por ejemplo, en el servidor IKEv2, se requiere 'Server Auth EKU', mientras que el certificado del cliente necesita 'Client Auth EKU'. Las implementaciones locales pueden hacer uso de: Servidor CA de Cisco IOS - Los certificados autofirmados no se pueden utilizar debido al error [CSCuc82575](#). Servidor OpenSSLCAServidor CA de Microsoft: en general, esta es la opción preferida porque se puede configurar para firmar el certificado exactamente como se desee.

#### 2. Configuración de cabecera de Cisco IOS

Obtener un certificadoConfiguración de IKEv2

3. Configurar cliente integrado de Windows 7
4. Obtener certificado de cliente

Cada uno de estos pasos principales se explica en detalle en las secciones siguientes.

**Nota:** Use la [Command Lookup Tool \(clientes registrados solamente\) para obtener más información sobre los comandos usados en esta sección.](#)

## Configurar autoridad de certificados

Este documento no proporciona pasos detallados sobre cómo configurar una CA. Sin embargo, los pasos de esta sección muestran cómo configurar la CA para que pueda emitir certificados para este tipo de implementación.

### OpenSSL

La CA OpenSSL se basa en el archivo 'config'. El archivo 'config' para el servidor OpenSSL debe tener:

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

### Servidor CA de Cisco IOS

Si utiliza un servidor CA de Cisco IOS, asegúrese de utilizar la versión más reciente del software Cisco IOS, que asigna la ECU.

```
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
```

## Configuración de la cabecera de Cisco IOS

### Obtener un certificado

El certificado debe tener los campos ECU establecidos en 'Autenticación de servidor' para Cisco IOS y 'Autenticación de cliente' para el cliente. Normalmente, la misma CA se utiliza para firmar los certificados de cliente y de servidor. En este caso, tanto la 'autenticación del servidor' como la 'autenticación del cliente' se ven en el certificado del servidor y el certificado del cliente respectivamente, lo que es aceptable.

Si la CA emite los certificados en formato PKCS (Public-Key Cryptography Standards) n.º 12 en el servidor IKEv2 a los clientes y al servidor, y si la lista de revocación de certificados (CRL) no es accesible o no está disponible, debe configurarse:

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

Ingrese este comando para importar el certificado 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 servidor CA de Cisco IOS otorga certificados automáticamente, el servidor IKEv2 debe configurarse con la URL del servidor CA para recibir un certificado como se muestra en este ejemplo:

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

Cuando se configura el punto de confianza, debe:

1. Autentique la CA con este comando:

```
crypto pki authenticate FlexRootCA
```

2. Inscriba el servidor IKEv2 con la CA con este comando:

```
crypto pki enroll FlexRootCA
```

Para ver si el certificado contiene todas las opciones requeridas, utilice este comando 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

## Configuración de IKEv2

Este es un ejemplo de configuración 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

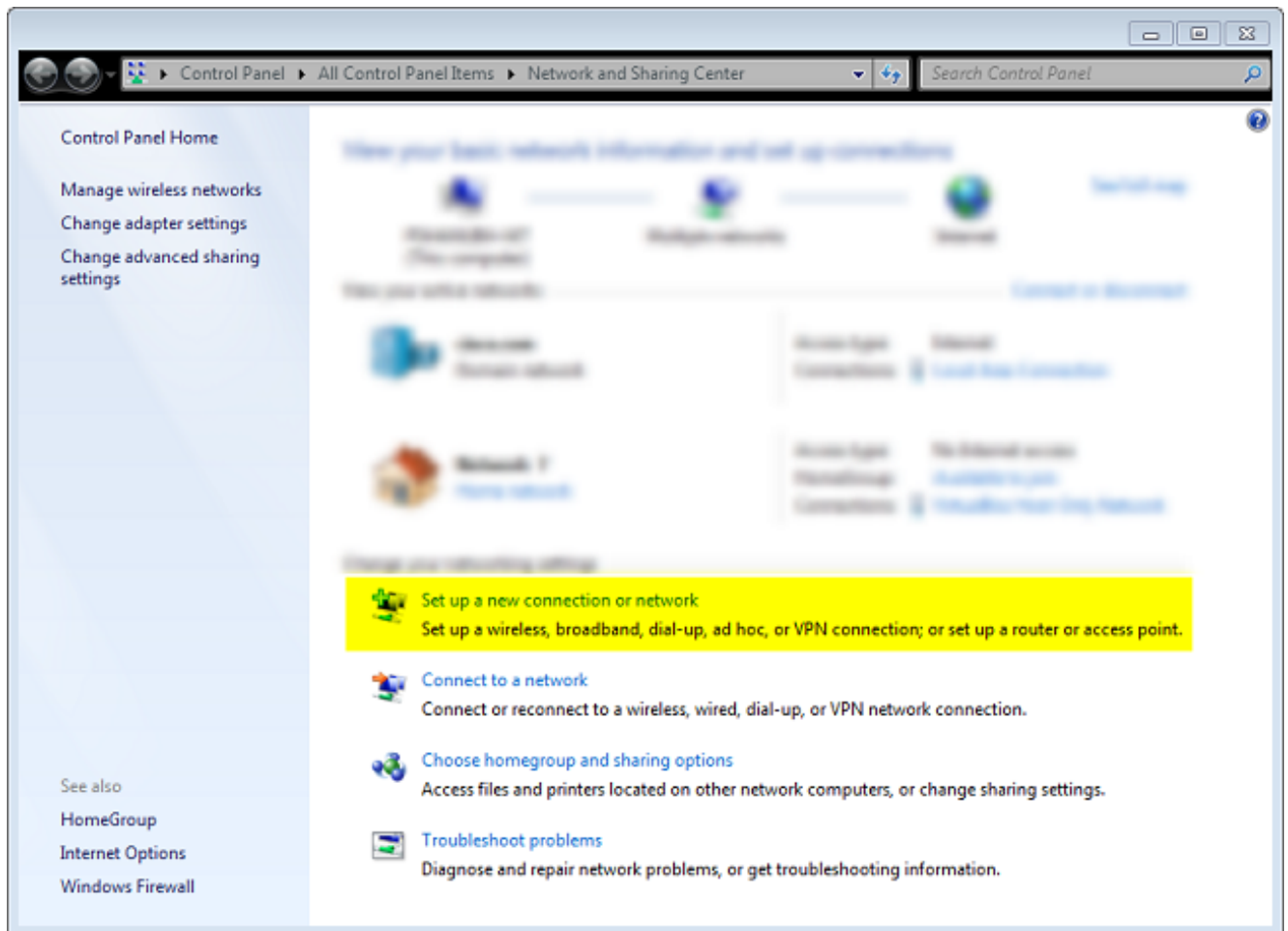
```
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile win7_ikev2
```

La IP sin numerar de la plantilla virtual debe ser cualquier cosa excepto la dirección local utilizada para la conexión IPsec. [Si utiliza un cliente de hardware, intercambiaría información de routing a través del nodo de configuración IKEv2 y crearía un problema de routing recursivo en el cliente de hardware.]

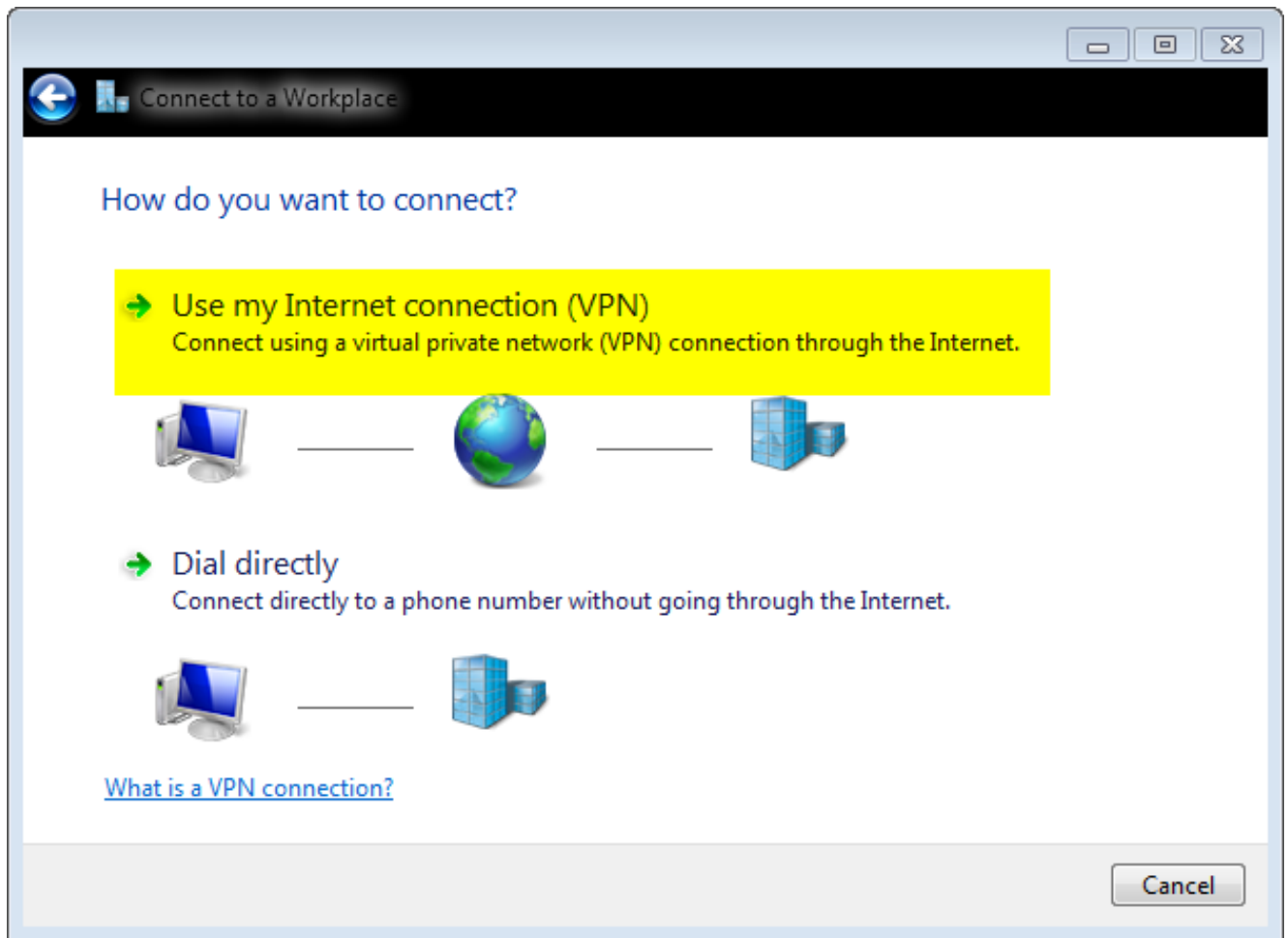
## Configurar cliente integrado de Windows 7

Este procedimiento describe cómo configurar el cliente integrado de Windows 7.

1. Navegue hasta el **Centro de Red y Compartir** y haga clic en **Configurar una nueva conexión o red**.

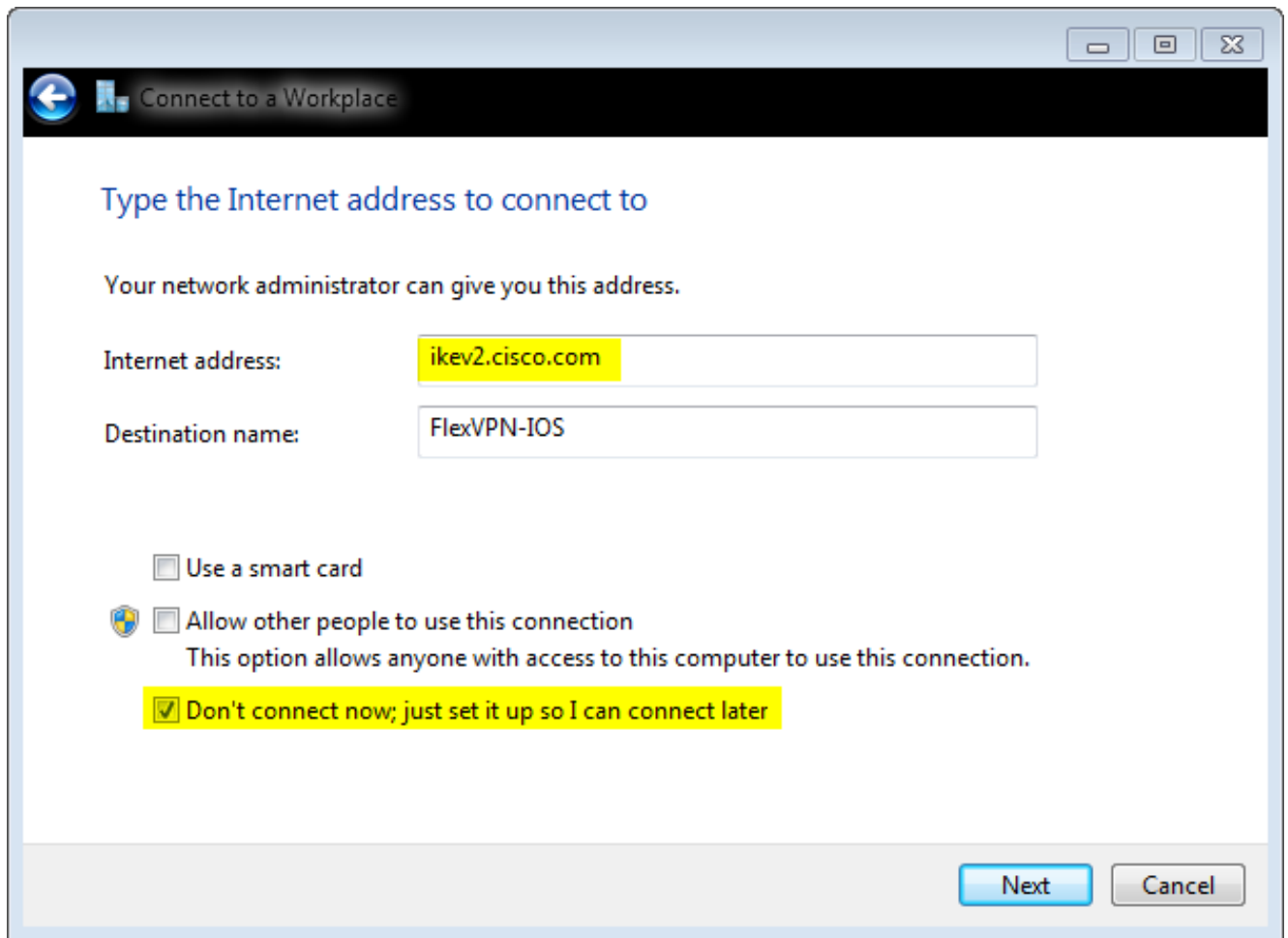


2. Haga clic en **Usar mi conexión a Internet (VPN)**. Esto le permite configurar una conexión VPN negociada a través de una conexión a Internet actual.



3. Introduzca el nombre de dominio completo (FQDN) o la dirección IP del servidor IKEv2 y asígnele un nombre de destino para identificarlo localmente.

**Nota:** El FQDN debe coincidir con el nombre común (CN) del certificado de identidad del router. Windows 7 descarta la conexión con un error 13801 si detecta una discordancia. Dado que es necesario establecer parámetros adicionales, marque **No conectar ahora; sólo debe configurarlo para poder conectarme más tarde** y hacer clic en **Siguiente**:



Connect to a Workplace

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address:

Destination name:

Use a smart card

Allow other people to use this connection  
This option allows anyone with access to this computer to use this connection.

Don't connect now; just set it up so I can connect later

Next Cancel

4. No rellene los campos **Nombre de usuario**, **Contraseña** y **Dominio (opcional)** porque se utilizará la autenticación de certificado. Haga clic en **Crear**.



Connect to a Workplace

Type your user name and password

User name:

Password:

Show characters

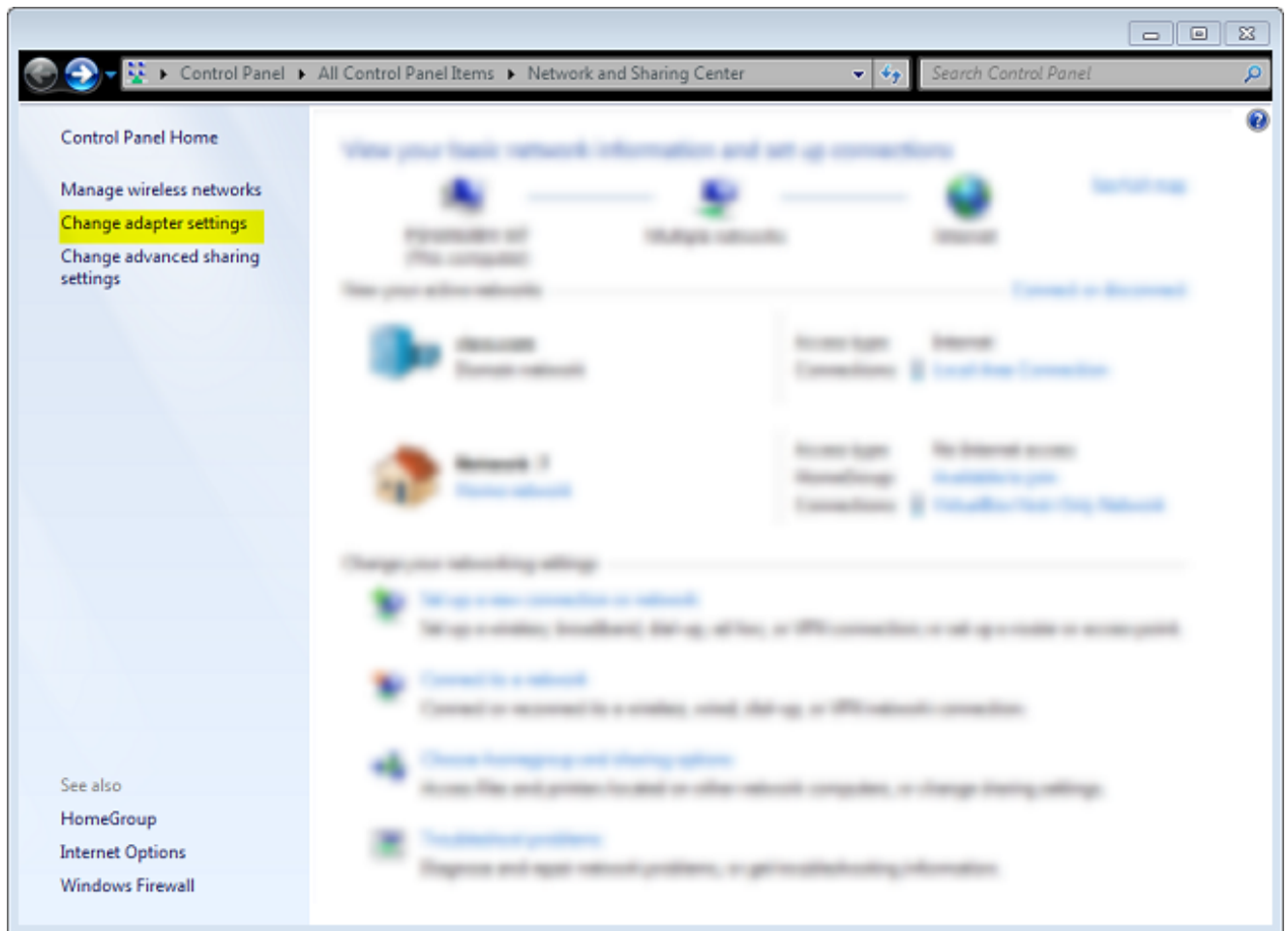
Remember this password

Domain (optional):

Create Cancel

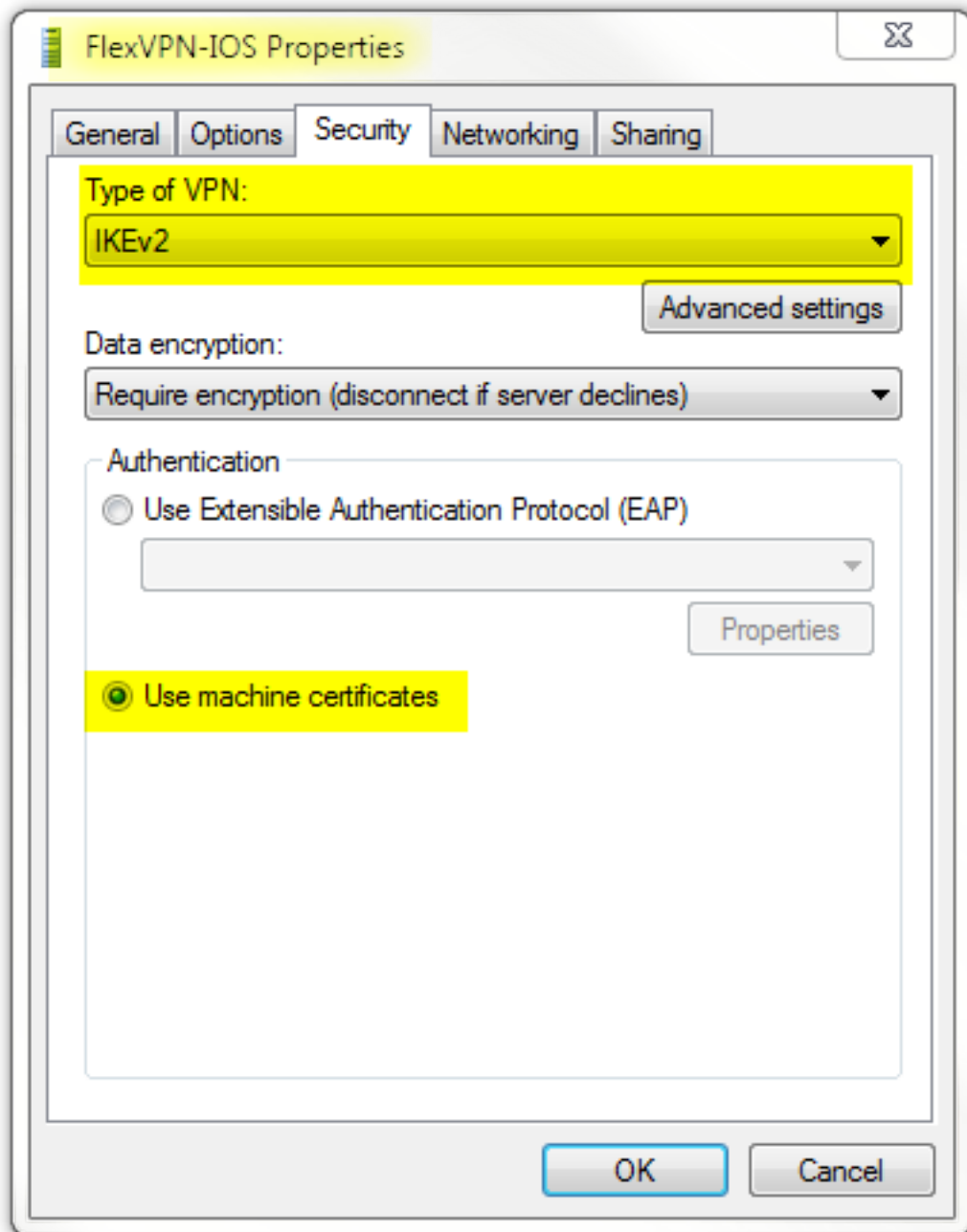
**Nota:** Cierre la ventana resultante. **No intente conectarse.**

5. Vuelva al **Centro de Red y Uso Compartido** y haga clic en **Cambiar la configuración del adaptador**.



6. Elija el adaptador lógico FlexVPN-IOS, que es el resultado de todos los pasos realizados hasta este punto. Haga clic en sus propiedades. Estas son las propiedades del perfil de conexión recién creado llamado FlexVPN-IOS:

En la ficha Seguridad, el tipo de VPN debe ser IKEv2. En la sección Autenticación, elija **Usar certificados de máquina**.



El perfil FlexVPN-IOS ya está listo para conectarse después de importar un certificado al almacén de certificados de la máquina.

## Obtener certificado de cliente

El certificado de cliente requiere estos factores:

- El certificado de cliente tiene un EKU de 'Autenticación de cliente'. Además, la CA proporciona un certificado PKCS#12:

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

- Certificado CA:

CA Certificate goes into Local Machine Trusted Root Certificate Authorities Store

## Detalles importantes

- 'IPSec IKE intermedio' (OID = 1.3.6.1.5.5.8.2.2) debe utilizarse como EKU si se aplican ambas afirmaciones:

El servidor IKEv2 es un servidor Windows 2008. Hay más de un certificado de autenticación de servidor en uso para conexiones IKEv2. Si esto es cierto, coloque EKU de 'autenticación de servidor' y EKU 'IPSec IKE intermedio' en un certificado o distribuya estos EKU entre los certificados. Asegúrese de que al menos un certificado contiene EKU 'IPSec IKE intermedio'.

Consulte [Resolución de Problemas de Conexiones VPN IKEv2](#) para obtener más información.

- En una implementación de FlexVPN, no utilice 'IPSec IKE intermedio' en EKU. Si lo hace, el cliente IKEv2 no recoge el certificado de servidor IKEv2. Como resultado, no pueden responder a CERTREQ de IOS en el mensaje de respuesta IKE\_SA\_INIT y, por lo tanto, no pueden conectarse con una ID de error 13806.
- Aunque no se requiere el nombre alternativo del sujeto (SAN), es aceptable si los certificados tienen uno.
- En el almacén de certificados de cliente de Windows 7, asegúrese de que el almacén de autoridades de certificados raíz de confianza de equipo tiene el menor número posible de certificados. Si tiene más de 50, es posible que Cisco IOS no pueda leer la carga útil Cert\_Req completa, que contiene el Nombre distinguido de certificado (DN) de todas las CA conocidas del cuadro Windows 7. Como resultado, la negociación falla y se ve el tiempo de espera de la conexión en el cliente.

## Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

La herramienta de interpretación de información de salida (disponible para clientes registrados únicamente) admite ciertos comandos show. Utilice la herramienta para ver un análisis de información de salida del comando 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
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:

## Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

## Información Relacionada

- [Depuraciones ASA IKEv2 para VPN de sitio a sitio con PSK TechNote](#)
- [Diagnóstico de problemas de depuración de IPsec e IKE \(modo principal IKEv1\) de ASA](#)
- [Depuraciones de IOS IPsec e IKE - Nota técnica de resolución de problemas del modo principal IKEv1](#)
- [Depuraciones de ASA IPsec e IKE - IKEv1 Modo agresivo TechNote](#)
- [Cisco ASA 5500 Series Adaptive Security Appliances](#)
- [Descargas de software de dispositivos de seguridad adaptable Cisco ASA serie 5500](#)
- [Cisco IOS Firewall](#)
- [Cisco IOS Software](#)
- [Secure Shell \(SSH\)](#)
- [Negociación IPsec/Protocolos IKE](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)