IKEv2 con el cliente VPN ágil de Windows 7 IKEv2 y autenticación certificada en FlexVPN

Contenido

Introducción

FlexVPN es el nuevo intercambio de claves de Internet versión 2 (infraestructura IKEv2)-based el VPN en el ® del Cisco IOS y se significa para ser una solución de VPN unificada. Este documento describe cómo configurar al cliente IKEv2 que se incorpora a Windows 7 para conectar un headend del Cisco IOS con la utilización de un Certificate Authority (CA).

> Nota: El dispositivo de seguridad adaptante (ASA) ahora soporta las conexiones IKEv2 con el cliente incorporado de Windows 7 a partir de la versión 9.3(2).

> Nota: Los protocolos SUITE-B no trabajan porque el headend IOS no soporta SUITE-B con IKEv1, o el cliente VPN ágil de Windows 7 IKEv2 no soporta actualmente SUITE-B con IKEv2.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cliente VPN del accesorio de Windows 7
- Cisco IOS Software Release 15.2(2)T
- Certificate Authority - OpenSSL CA

Componentes Utilizados

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

- Cliente VPN del accesorio de Windows 7
- Cisco IOS Software Release15.2(2)T
- Certificate Authority - OpenSSL CA

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener información sobre las convenciones sobre documentos.

Configurar

Información general

Hay cuatro pasos principales en configuración del cliente incorporado IKEv2 de Windows 7 para conectar un headend del Cisco IOS con la utilización de CA:

1. Configuración CA

   CA debe permitir que usted integre el uso dominante extendido requerido (EKU) en el certificado. Por ejemplo, en el servidor IKEv2, “se requiere el EKU del auth del servidor”, mientras que el certificado del cliente necesita “el EKU del auth del cliente.” Las implementaciones locales pueden hacer uso:Servidor de CA del Cisco IOS - Los certificados autofirmados no se pueden utilizar debido al bug CSCuc82575.Servidor de CA del OpenSSLMicrosoft CA server - Ésta es generalmente la opción preferida porque puede ser configurada para firmar el certificado exactamente según lo deseado.

2. Headend del Cisco IOS de la configuración

Obtenga un certificadoConfigure IKEv2

3. Configure al cliente del accesorio de Windows 7
4. Obtenga el certificado del cliente

Cada uno de estos pasos principales se explica detalladamente en las secciones posteriores.

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

Configure el Certificate Authority

Este documento no proporciona los pasos detallados en cómo configurar CA. Sin embargo, los pasos en esta sección le muestran cómo configurar CA así que puede publicar los Certificados para esta clase de despliegue.

OpenSSL

El OpenSSL CA se basa en el archivo de los “config”. El archivo de los “config” para el servidor del OpenSSL debe tener:

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

Servidor de CA del Cisco IOS

Si usted utiliza un servidor de CA del Cisco IOS, aseegurese le utilizar la versión de Cisco IOS Software más reciente, que asigna el 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
```

Configure el headend del Cisco IOS

Obtenga un certificado

El certificado debe tener los campos del EKU fijados a la “autenticación de servidor” para el Cisco IOS y la “autenticación de cliente” para el cliente. Típicamente, mismo CA se utiliza para firmar ambos los Certificados de cliente y servidor. En este caso, la “autenticación de servidor” y la “autenticación de cliente” se consideran en el certificado de servidor y el certificado del cliente respectivamente, que es aceptable.

Si CA publica los Certificados en los estándares del Cifrado de clave pública (PKCS) #12 formatan en el servidor IKEv2 a los clientes y el servidor, y si el Listas de revocación de certificados (CRL) no está accesible o disponible, deben ser configurados:

```
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
```

Ingrese este comando para importar el certificado del 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 auto del servidor de CA del Cisco IOS concede los Certificados, el servidor IKEv2 se debe configurar con el servidor URL de CA para recibir un certificado tal y como se muestra en de este ejemplo:

```
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.
```

Cuando se configura el trustpoint, usted necesita:

1. Autentique CA con este comando:

   ```
   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.
   ```

2. Aliste el servidor IKEv2 con CA con este comando:

   ```
   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.
   ```

Para ver si el certificado contiene todas las opciones obligatorias, utilice este comando show:

```
ikev2#show crypto pki cert verbose
Certificate
  <snip>
 Issuer:
   <snip>
 Subject:
   Name: ikev2.cisco.com
   ou=TAC
   o=Cisco
   c=BE
   cn=ikev2.cisco.com
<snip>
 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
```

Configure IKEv2

Éste es un ejemplo de la configuración IKEv2:

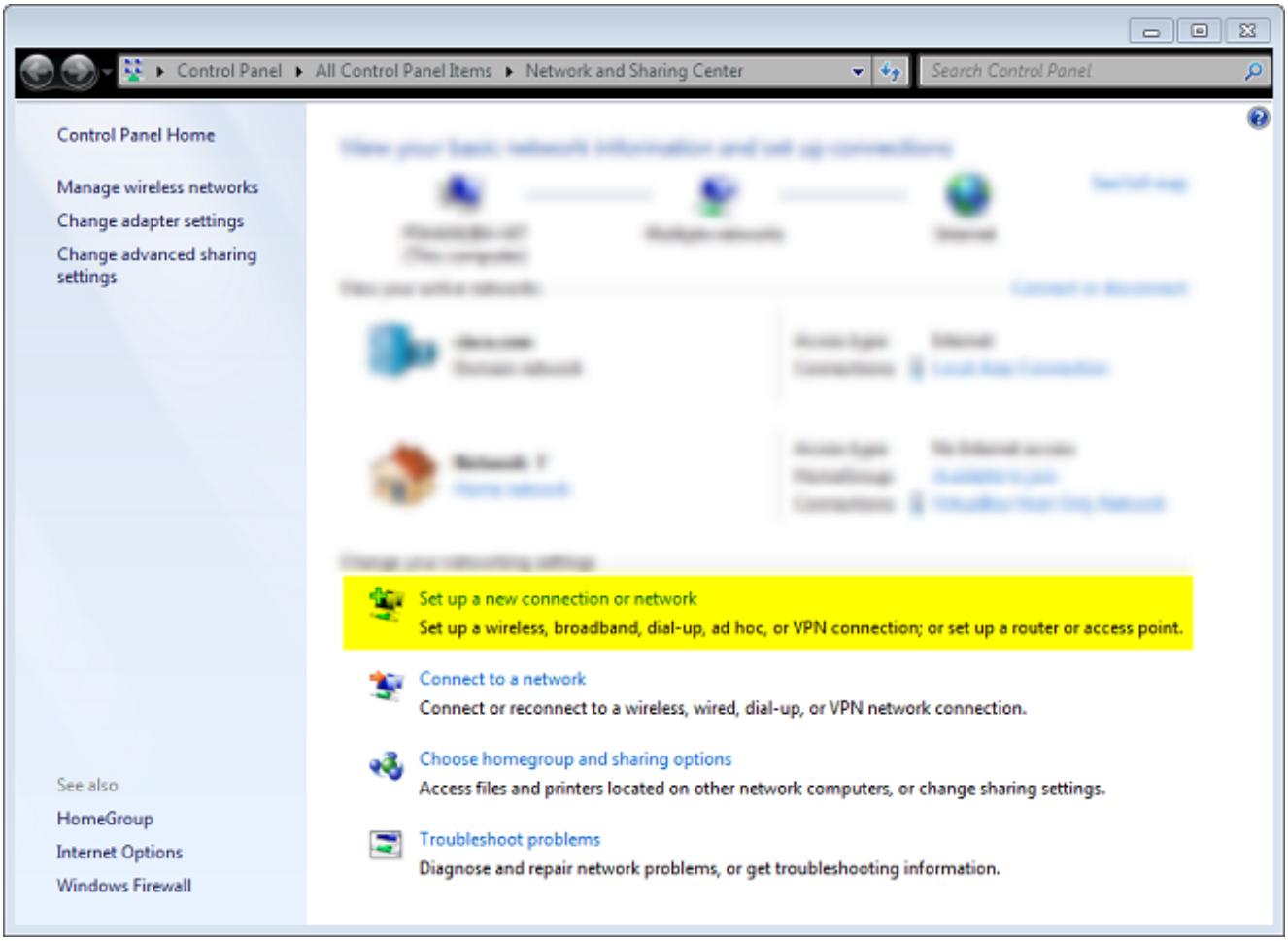
```
ikev2#show crypto pki cert verbose
Certificate
  <snip>
 Issuer:
   <snip>
 Subject:
   Name: ikev2.cisco.com
   ou=TAC
   o=Cisco
   c=BE
   cn=ikev2.cisco.com
<snip>
 Subject Key Info:
   Public Key Algorithm: rsaEncryption
   RSA Public Key: (1024 bit)
 Signature Algorithm: MD5 with RSA Encryption
 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
```

El IP innumerable de la virtual-plantilla debe ser cualquier cosa dirección local del exceptthe usada para conexión IPSec. [If you use a hardware client, you would exchange routing information via IKEv2 configuration node and create a recursive routing issue on the hardware client.]

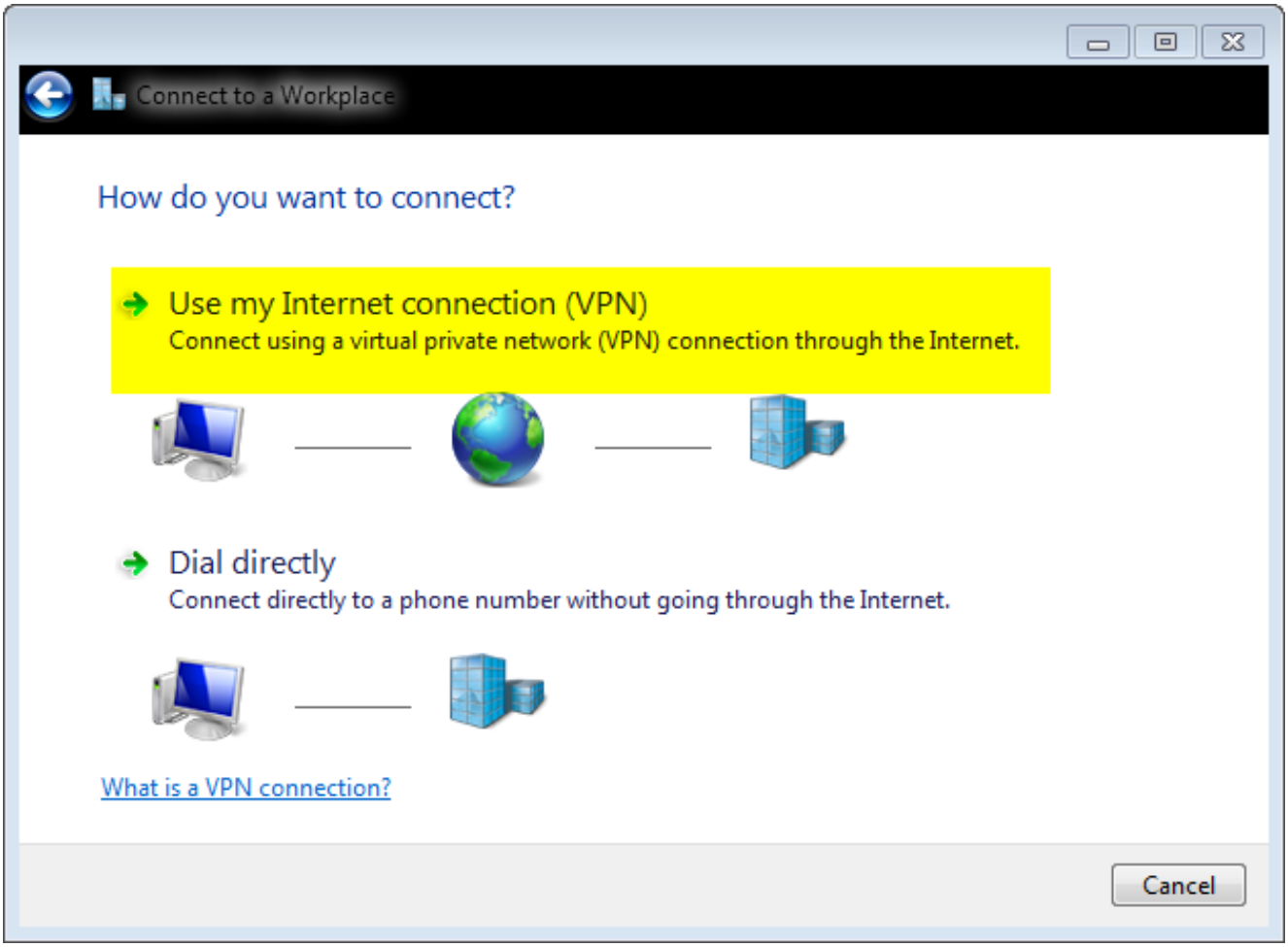
Cliente del accesorio de Windows 7 de la configuración

Este procedimiento describe cómo configurar al cliente del accesorio de Windows 7.

1. Navegue a la **red y centro de la distribución**, y haga clic **configura una nueva conexión o una red**.

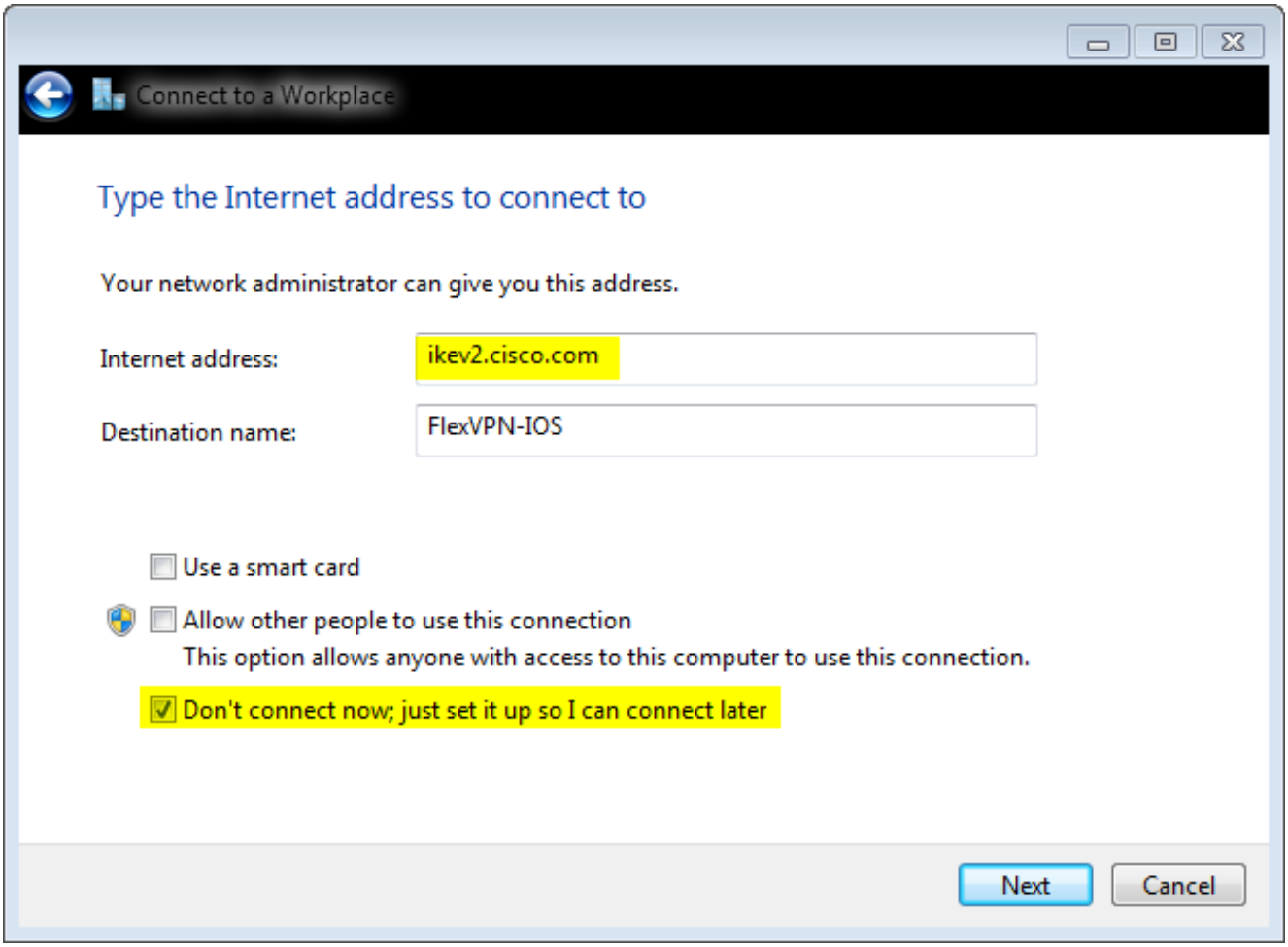


2. Haga clic el **uso mi conexión de Internet (VNP)**. Esto permite que usted ponga una conexión VPN negociada sobre una conexión de Internet actual.

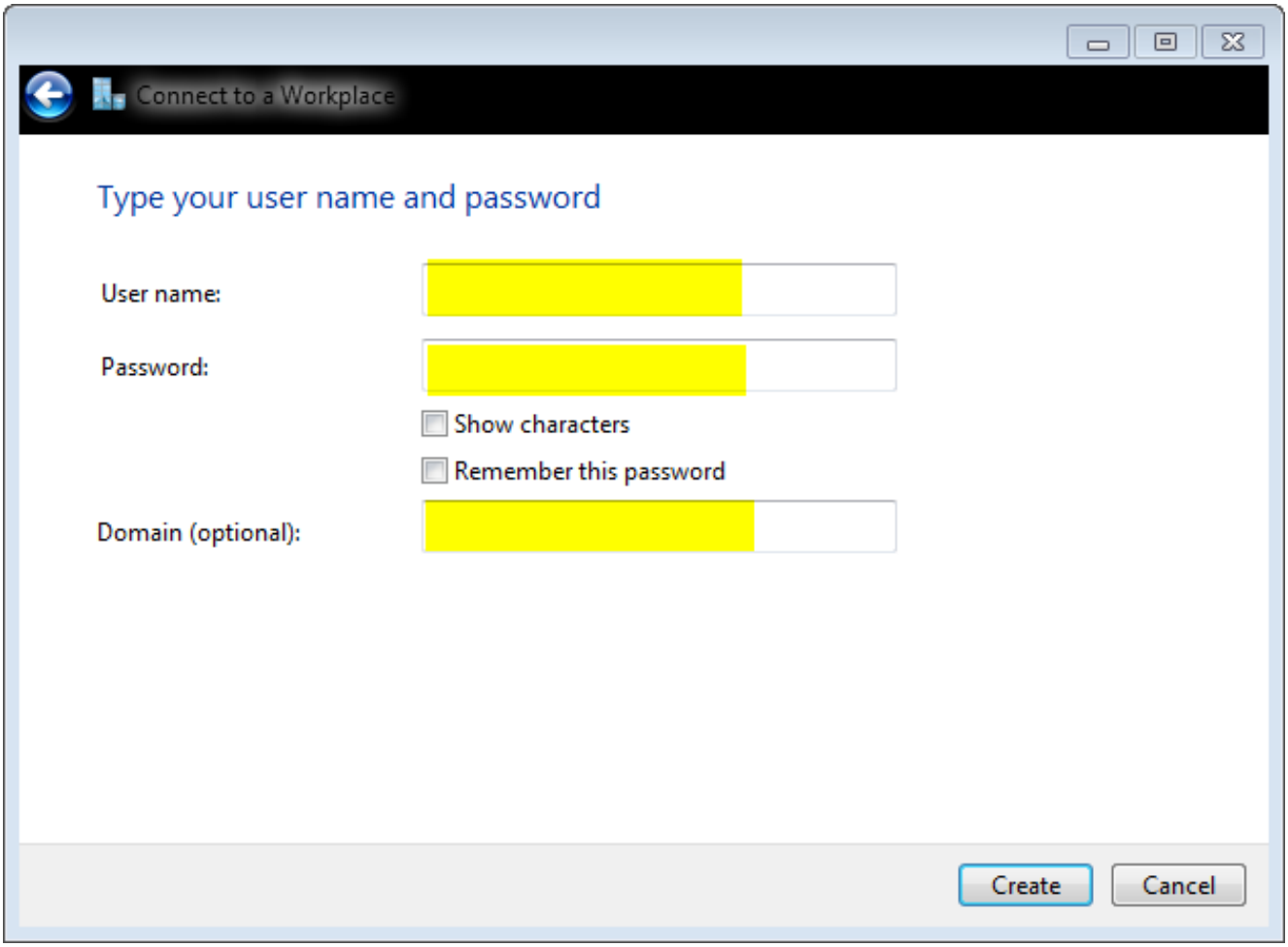


3. Ingrese el Nombre de dominio totalmente calificado (FQDN) (FQDN) o el IP Address del servidor IKEv2, y déle un nombre del destino para identificarlo localmente.

   Nota: El FQDN debe hacer juego el Common Name (CN) del certificado de identidad del router. Windows 7 cae la conexión con un error 13801 si detecta una discordancía.
   Porque los parámetros adicionales necesitan ser fijados, el control **ahora no conecta; apenas fijado lo para arriba puedo conectar tan más adelante**, y hago clic **después**:

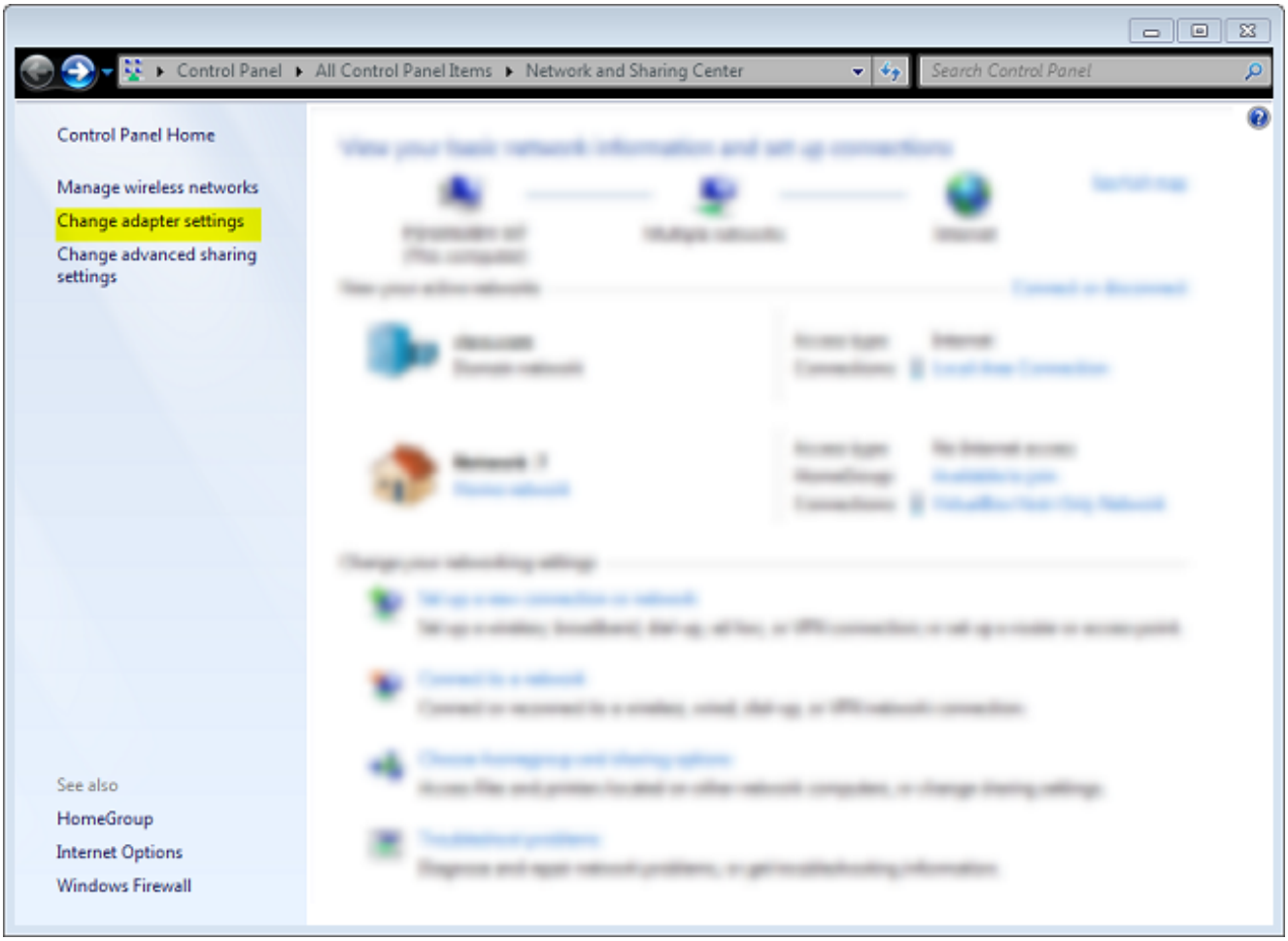


4. No complete los campos **(opcionales) del Nombre de usuario**, de la **contraseña** y del **dominio** porque la autenticación certificada debe ser utilizada. El tecleo **crea**.



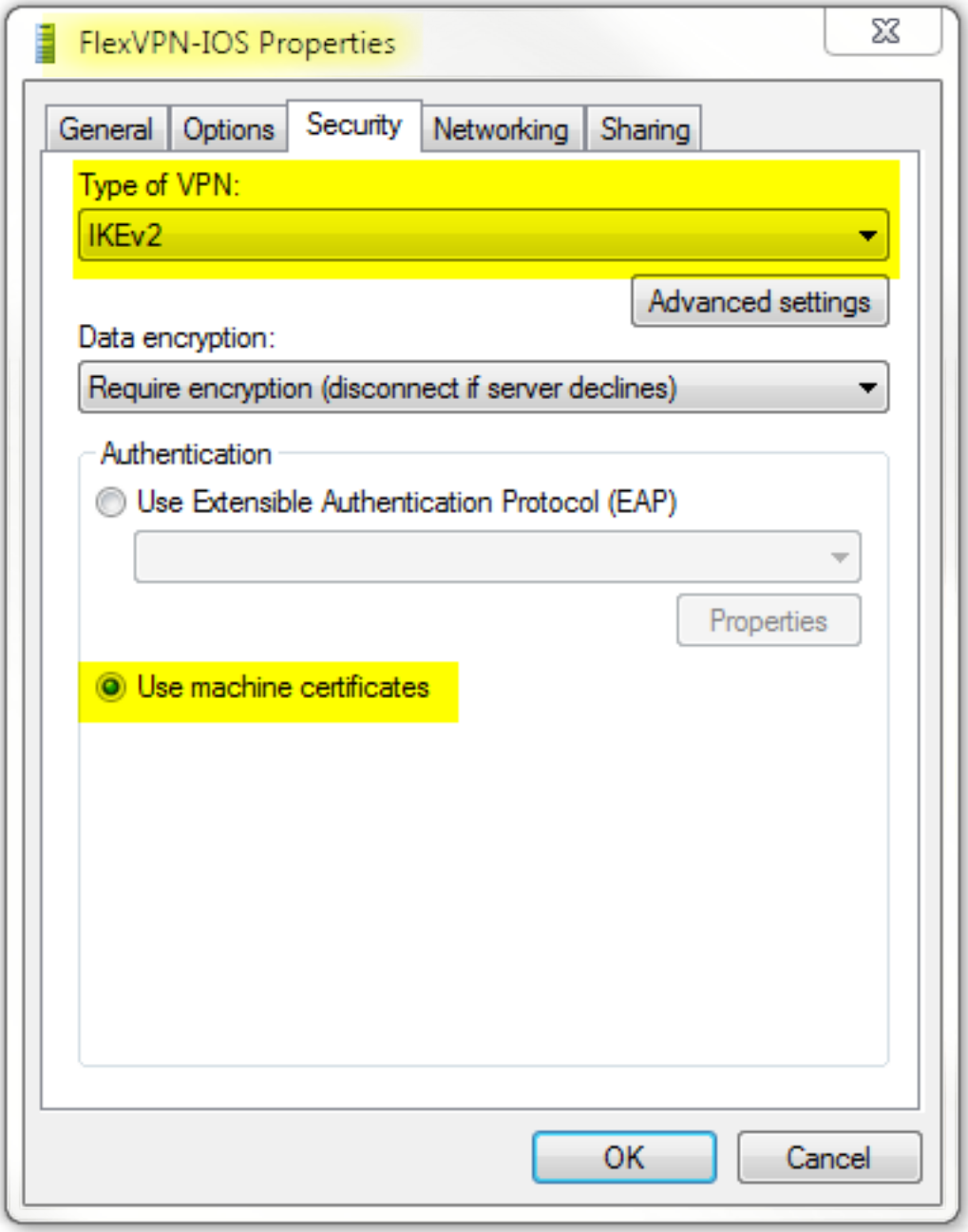
Nota: Cierre la ventana resultante. **No intente conectar.**

5. Navegue de nuevo a la **red y centro de la distribución**, y haga clic las **configuraciones del adaptador del cambio**.



6. Elija el FlexVPN-IOS lógico del adaptador, que es el resultado de todas las medidas llevadas esta punta. Haga clic sus propiedades. Éstas son las propiedades del perfil de la conexión creado recientemente llamado FlexVPN-IOS:

   En la ficha de seguridad, el tipo de VPN debe ser IKEv2.En la sección de la autenticación, elija los **certificados de la máquina del uso**.



El perfil FlexVPN-IOS está listo ahora para ser conectado después de que usted haya importado un certifcate al almacén del certificado de la máquina.

Obtenga el certificado del cliente

El certificado del cliente requiere estos factores:

- El certificado del cliente tiene un EKU de la “autenticación de cliente”. También, CA da un certificado del PKCS-12:

```
ikev2#show crypto pki cert verbose
Certificate
  <snip>
 Issuer:
   <snip>
 Subject:
   Name: ikev2.cisco.com
   ou=TAC
   o=Cisco
```

```
   c=BE
   cn=ikev2.cisco.com
<snip>
 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
```

- Certificado de CA:

```
ikev2#show crypto pki cert verbose
Certificate
  <snip>
 Issuer:
   <snip>
 Subject:
   Name: ikev2.cisco.com
   ou=TAC
   o=Cisco
   c=BE
   cn=ikev2.cisco.com
<snip>
 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
```

Detalles importantes

- El “intermedio del IPSec IKE” (OID = 1.3.6.1.5.5.8.2.2) se debe utilizar como EKU si ambas

declaraciones se aplican:

El servidor IKEv2 es un servidor de Windows 2008.Hay más de un Certificado de autenticación de servidor funcionando para las conexiones IKEv2. Si esto es verdad, cualquier EKU de la “autenticación de servidor” del lugar y el EKU intermedio del “IPSec IKE” en un certificado, o distribuyen este EKUs entre los Certificados. Aseegurese por lo menos un certificado contiene “el EKU del intermedio del IPSec IKE”.

Refiera a resolver problemas IKEv2 VPN Connectionsfor más información.

- En un despliegue de FlexVPN, no utilice el “intermedio del IPSec IKE” en el EKU. Si usted hace, el cliente IKEv2 no coge el certificado de servidor IKEv2. Como consecuencia, no pueden responder a CERTREQ del IOS en el mensaje de respuesta IKE_SA_INIT y no poder así conectar con 13806 un error ID.

- Mientras que el nombre alternativo sujeto (SAN) no se requiere, es aceptable si los Certificados tienen uno.

- En el almacén del certificado del cliente de Windows 7, aseegurese que el almacén Máquina- de confianza de las autoridades del certificado raíz tiene el menos número de Certificados posibles. Si tiene más de 50 o así pues, el Cisco IOS pudo no poder leer el payload entero de Cert_Req, que contiene el Nombre distintivo (DN) del certificado de todos los CA sabidos del cuadro de Windows 7. Como consecuencia, la negociación falla y usted ve el descanso de conexión en el cliente.

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

La herramienta del Output Interpreter (clientes registrados solamente) apoya los ciertos comandos show. Utilice la herramienta del Output Interpreter para ver una análisis de la 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:
```

Troubleshooting

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

Información Relacionada

- Debugs ASA IKEv2 para el VPN de sitio a sitio con la Nota Técnica de PSKs
- IPSec ASA y debugs IKE (modo principal IKEv1) que resuelven problemas la Nota Técnica
- IPSec IOS y debugs IKE - Modo principal IKEv1 que resuelve problemas la Nota Técnica
- IPSec ASA y debugs IKE - Nota Técnica del modo agresivo IKEv1
- Cisco ASA 5500 Series Adaptive Security Appliances
- Descargas del software del Dispositivos de seguridad adaptable Cisco ASA de la serie 5500
- Cisco IOS Firewall
- Cisco IOS Software
- Secure Shell (SSH)
- Negociación IPSec/Protocolos IKE
- Soporte Técnico y Documentación - Cisco Systems