IKEv2 met Windows 7 IKEv2 mobiele VPN-client en certificaatverificatie op FlexVPN

Inhoud

Inleiding

FlexVPN is de nieuwe op internet Key Exchange versie 2 (IKEv2) gebaseerde VPN-infrastructuur op Cisco IOS® en is bedoeld om een verenigde VPN-oplossing te zijn. Dit document beschrijft hoe u de IKEv2-client moet configureren die in Windows 7 is ingebouwd om een Cisco IOS-head-end te verbinden met het gebruik van een certificaatinstantie (CA).

> Opmerking: De adaptieve security applicatie (ASA) ondersteunt IKEv2 verbindingen met de ingebouwde Windows 7 client vanaf release 9.3(2).

> Opmerking: SUITE-B-protocollen werken niet omdat het IOS-head-end SUITE-B niet ondersteunt met IKEv1, of de Windows 7 IKEv2 Google VPN-client momenteel geen SUITE-B met IKEv2 ondersteunt.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Windows 7 ingebouwde VPN-client
- Cisco IOS-softwarerelease 15.2(2)T
- certificaatautoriteit - OpenSSL CA

Gebruikte componenten

De informatie in dit document is gebaseerd op deze hardware- en softwareversies:

- Windows 7 ingebouwde VPN-client
- Cisco IOS-softwarerelease 15.2(2)T
- certificaatautoriteit - OpenSSL CA

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg Cisco Technical Tips Convention voor informatie over documentconventies.

Configureren

Overzicht

Er zijn vier belangrijke stappen in de configuratie van de ingebouwde Windows 7 IKEv2-client om een Cisco IOS head-end te verbinden met het gebruik van een CA:

1. CA instellen

   CA dient u in staat te stellen het vereiste Extended Key Use (EKU) in het certificaat te stoppen. Bijvoorbeeld, op de IKEv2 server is "Server Auth EKU" vereist, terwijl het client certificaat "Client Auth EKU" nodig heeft. Plaatselijke implementaties kunnen gebruik maken van:Cisco IOS CA server - zelfgetekende certificaten kunnen niet worden gebruikt vanwege bug CSCuc82575.OpenSSL CA-serverMicrosoft CA-server - In het algemeen is dit de gewenste optie, omdat deze kan worden ingesteld om het certificaat precies naar wens te ondertekenen.

2. Cisco IOS-head-end configureren

   Een certificaat verkrijgenIKEv2 configureren

3. Ingebouwde Windows 7-client configureren
4. Verkrijg klantcertificaat

Elk van deze belangrijke stappen wordt in de volgende paragrafen uitvoerig toegelicht.

> Opmerking: Gebruik de Command Lookup Tool (alleen voor geregistreerde gebruikers) voor meer informatie over de opdrachten die in deze sectie worden gebruikt.

Certificaat-instantie instellen

Dit document bevat geen gedetailleerde stappen over het instellen van een CA. De stappen in deze sectie tonen u echter hoe u CA kunt configureren zodat het certificaten voor dit soort plaatsing kan uitgeven.

OpenSSL

OpenSSL CA is gebaseerd op het "configuratie" bestand. Het 'configuratie'-bestand voor de OpenSSL-server moet:

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

Cisco IOS CA-server

Als u een Cisco IOS CA server gebruikt, zorg er dan voor dat u de meest recente Cisco IOS softwarerelease gebruikt, die EKU toegewezen heeft.

```
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
```

Cisco IOS-head-end configureren

Een certificaat verkrijgen

Het certificaat moet de EKU velden hebben ingesteld op 'Server Authentication' voor Cisco IOS en 'Client Authentication' voor de client. Meestal wordt dezelfde CA gebruikt om zowel de client- als servercertificaten te tekenen. In dit geval worden zowel 'serververificatie' als 'Clientverificatie' op het servercertificaat en het client-certificaat vermeld, wat aanvaardbaar is.

Als de CA de certificaten in het PKCS #12-formaat (Public-Key Cryptography Standards) op de IKEv2-server afgeeft aan de klanten en de server, en als de lijst van certificeringsintrekkingen (CRL) niet bereikbaar of beschikbaar is, moet deze worden geconfigureerd:

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

Typ deze opdracht om het PKCS#12-certificaat te importeren:

```
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.
```

Als een Cisco IOS CA server auto's garandeert, moet de IKEv2 server worden geconfigureerd met de CA server URL om een certificaat te ontvangen zoals in dit voorbeeld:

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

Als het vertrouwde punt is ingesteld, moet u:

1. Verifieer CA met deze opdracht:

```
crypto pki authenticate FlexRootCA
```

2. Geef de IKEv2-server op met de CA onder deze opdracht:

```
crypto pki enroll FlexRootCA
```

Om te zien of het certificaat alle gewenste opties bevat, gebruikt u deze opdracht **tonen**:

```
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
```

IKEv2 configureren

Dit is een voorbeeld van de IKEv2-configuratie:

```
!! 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
```

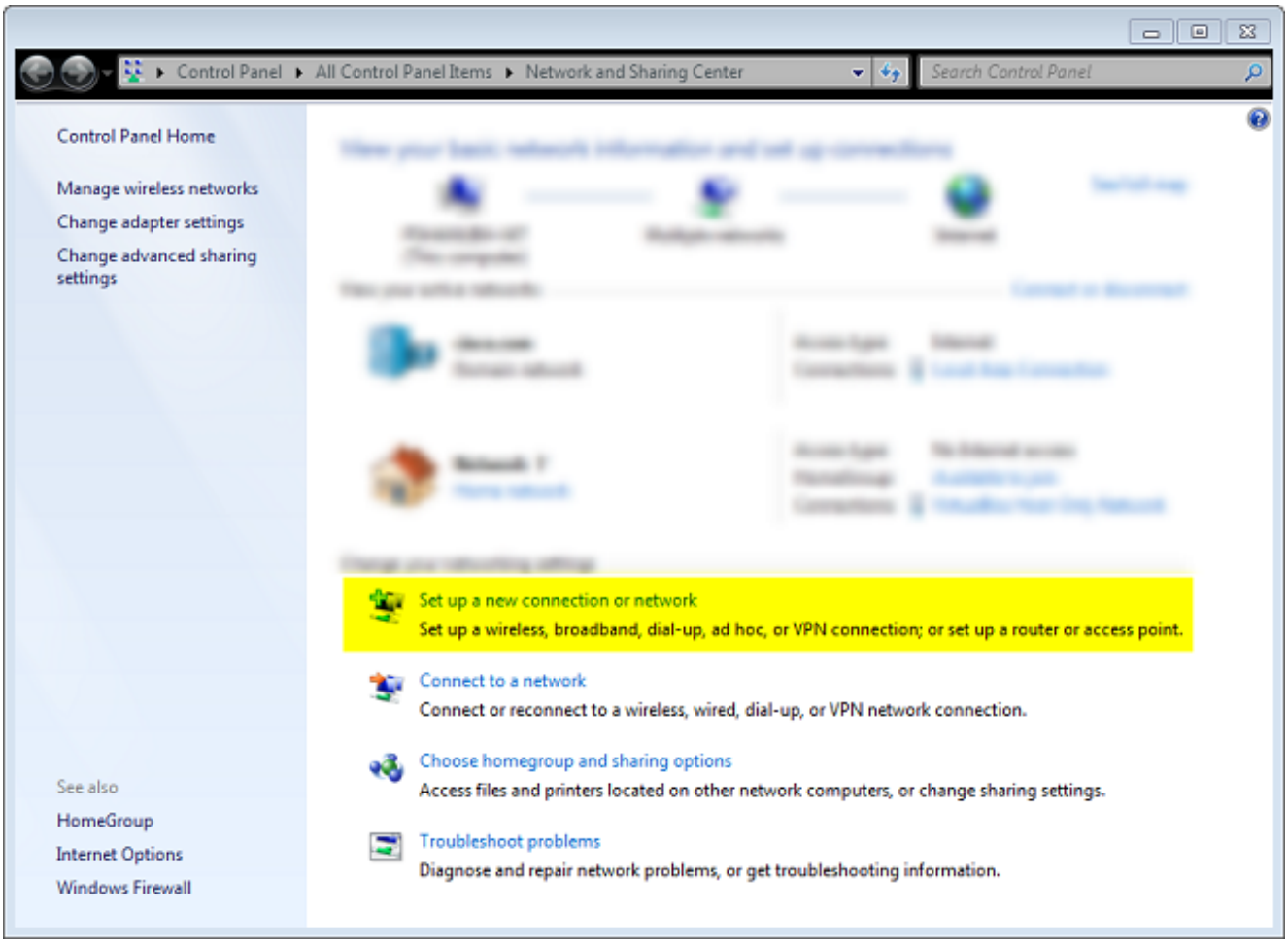
```
interface Virtual-Template1 type tunnel
  ip unnumbered Loopback0
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile win7_ikev2
```

Het IP-nummer dat niet van de virtuele-sjabloon is, is gelijk aan of gelijk aan het lokale adres dat wordt gebruikt voor de IPsec-verbinding. [Als u een hardwareclient gebruikt, zou u routinginformatie uitwisselen via IKEv2-configuratieknooppunt en een recursief routingprobleem op de hardwareclient maken.]

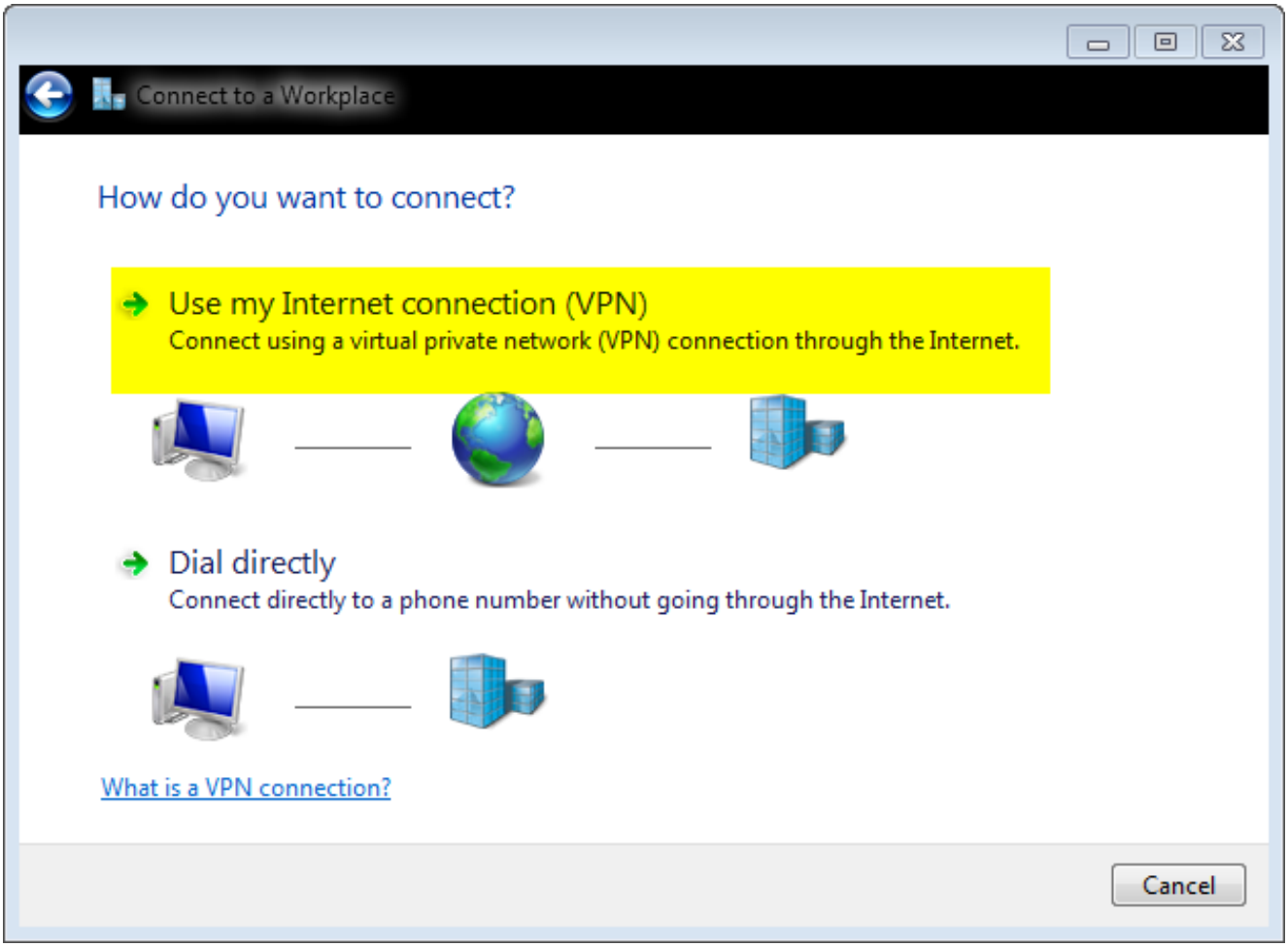
Ingebouwde client voor Windows 7 configureren

Deze procedure beschrijft hoe u de ingebouwde client van Windows 7 kunt configureren.

1. Navigeer naar het **Netwerk en het deelt Centrum**, en klik **Instellen een nieuwe verbinding of een netwerk**.

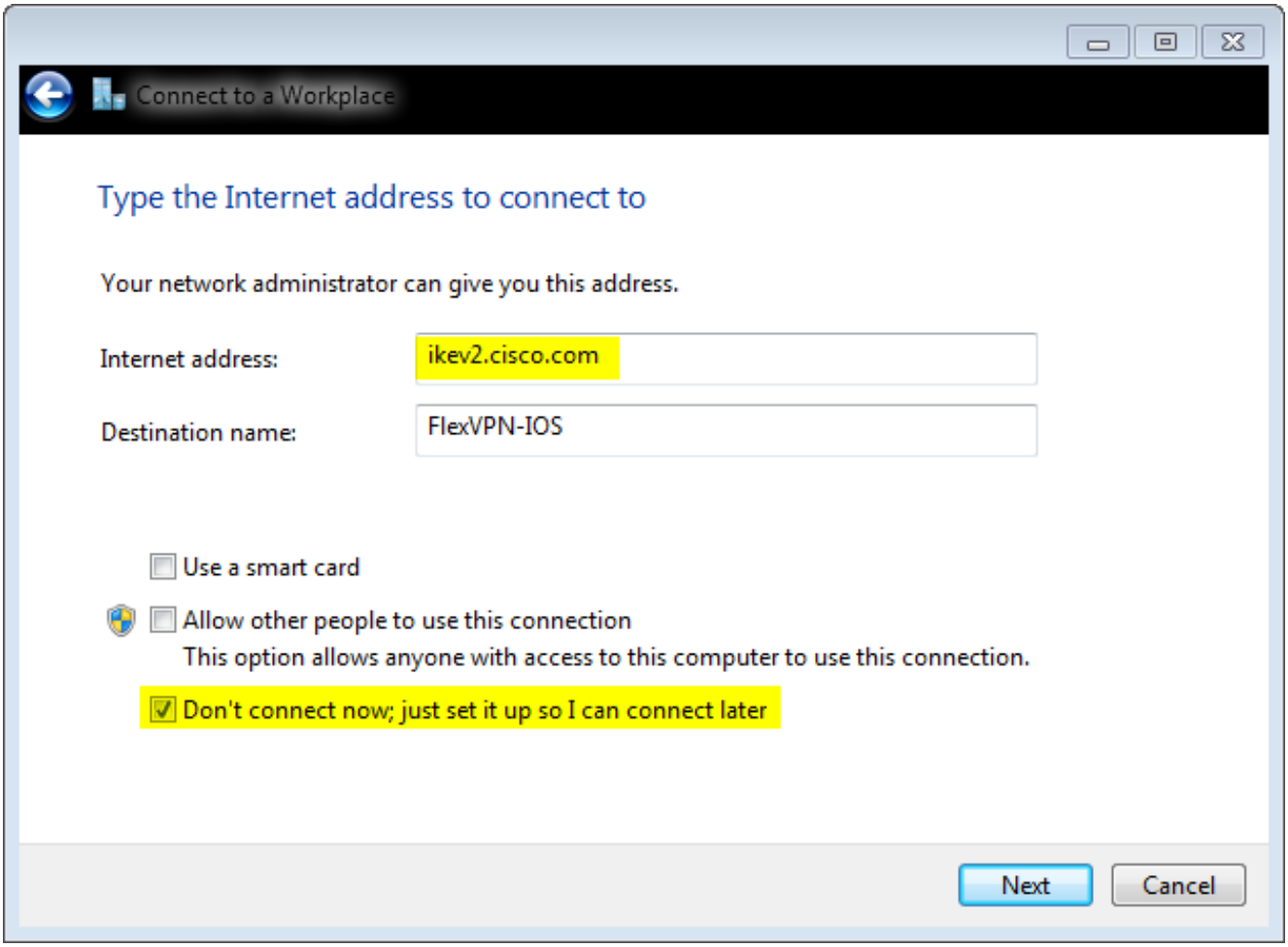


2. Klik op **VPN (Internet Connection)**. Hier kunt u een VPN-verbinding instellen die via een huidige internetverbinding is onderhandeld.

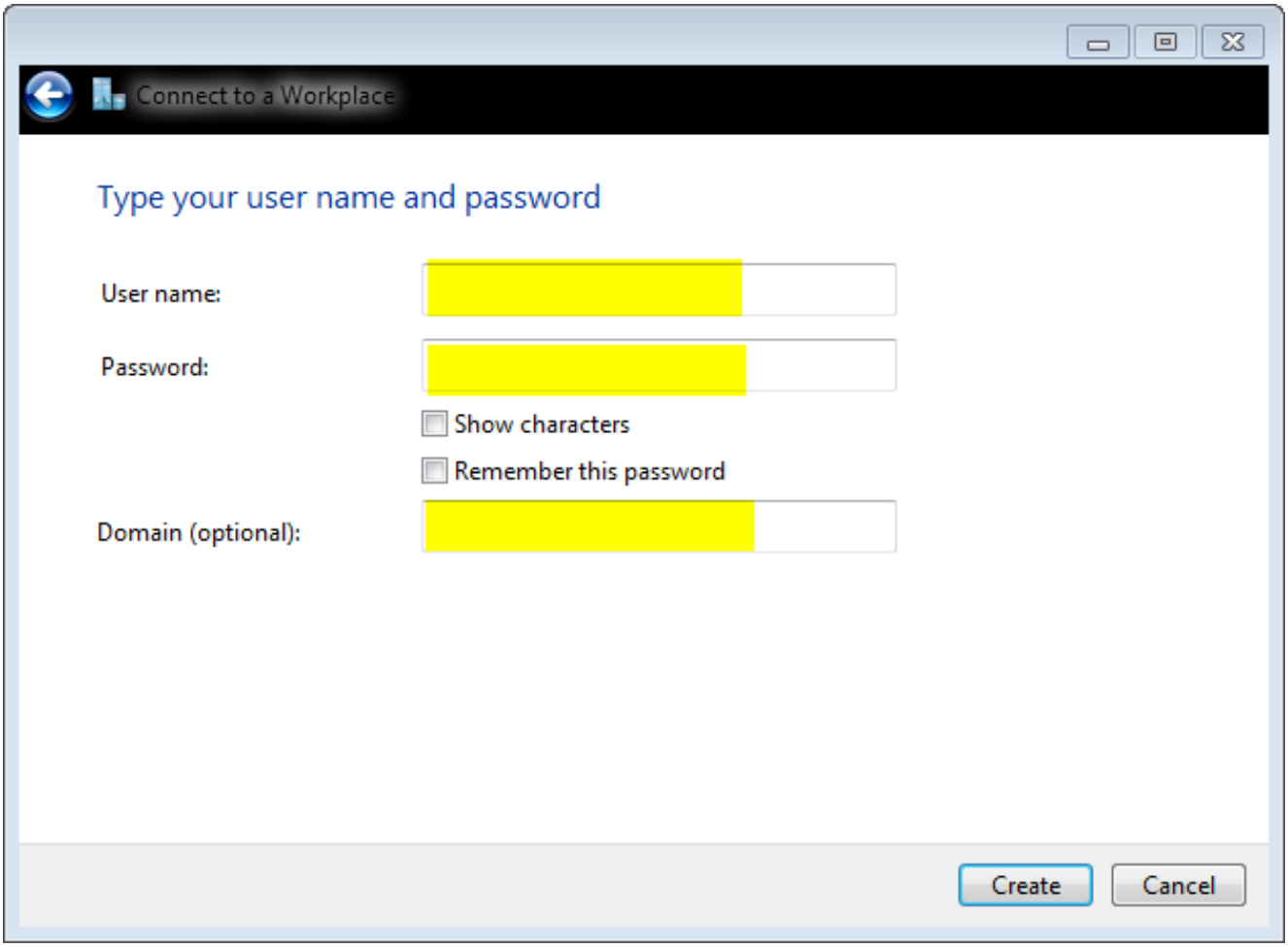


3. Voer de volledig gekwalificeerde domeinnaam (FQDN) of het IP-adres van de IKEv2-server in en geef deze een doelnaam om het lokaal te identificeren.

   Opmerking: De FQDN moet overeenkomen met de Common Name (CN) van het certificaat van de router-identiteit. Windows 7 laat de verbinding met een fout 13801 vallen als er een fout wordt gedetecteerd.
   Omdat extra parameters moeten worden ingesteld, controleer **of u nu geen verbinding maakt. Stel het item in zodat ik er later verbinding mee kan maken** en klik op **Volgende**:

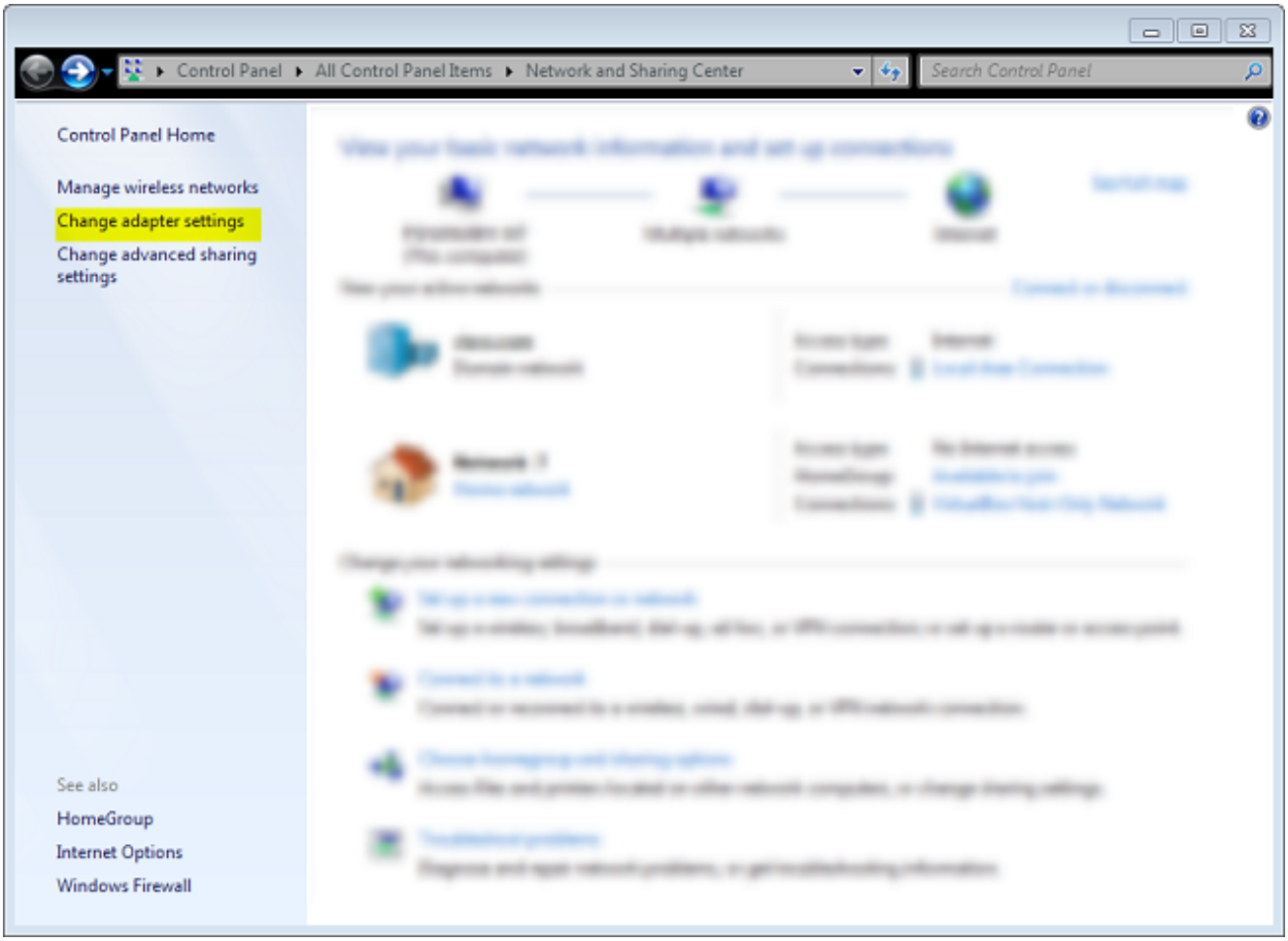


4. Vul de velden **Gebruikersnaam**, **Wachtwoord** en **Domein (optioneel)** niet in omdat certificaatverificatie moet worden gebruikt. Klik op **Maken**.



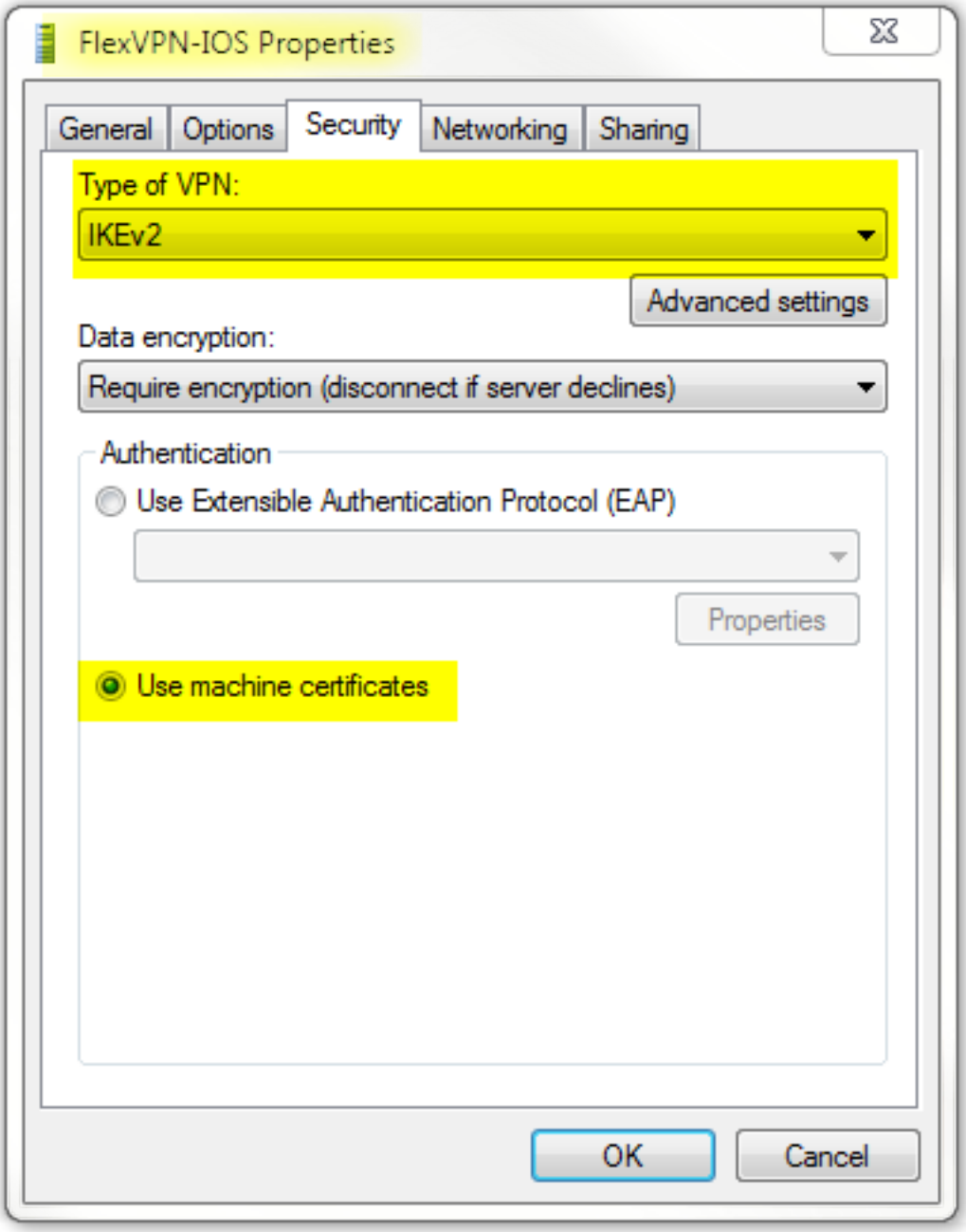
Opmerking: Sluit het resulterende venster. **Probeer geen verbinding te maken.**

5. Navigeer terug naar het **Netwerk en het delen Centrum**, en klik op **Wijzig adapterinstellingen**.



6. Kies de Logische Adapter FlexVPN-IOS, die het resultaat is van alle stappen die naar dit punt zijn ondernomen. Klik op de eigenschappen ervan. Dit zijn de eigenschappen van het nieuwe verbindingsprofiel FlexVPN-IOS:

   Op het tabblad Beveiliging moet het type VPN IKEv2 zijn.Selecteer in het gedeelte Verificatie de optie **Machinecertificaten gebruiken**.



Het FlexVPN-IOS-profiel kan nu worden aangesloten nadat u een certificaat hebt geïmporteerd naar de winkel met machinecertificaat.

Verkrijg een clientcertificaat

Het certificaat van de cliënt vereist deze factoren:

- Het clientcertificaat heeft een EKU van 'Clientverificatie'. Bovendien geeft de CA een PKCS#12-certificaat:

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

- CA-certificaat:

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

Belangrijke details

- "IPSec IKE intermediair" (OID = 1.3.6.1.5.5.8.2.2) dient als EKU te worden gebruikt indien beide van deze verklaringen van toepassing zijn:

  De IKEv2-server is een Windows 2008-server.Er is meer dan één serververificatiecertificaat in gebruik voor IKEv2-verbindingen. Als dit waar is, zet zowel de EKU voor serververificatie als de EKU voor 'IPSec IKE Intermediate'-EKU op één certificaat, of verdeel deze EKU's onder de certificaten. Zorg ervoor dat ten minste één certificaat de "IPSec IKE Intermediate" EKU bevat.

  Raadpleeg de verbindingen voor probleemoplossing van IKEv2 VPN voor meer informatie.

- Gebruik in een FlexVPN-toepassing 'IPSec IKE Intermediate' niet in EKU. Als u dit wel doet, haalt de IKEv2-client het IKEv2-servercertificaat niet op. Als resultaat hiervan kunnen ze niet reageren op CERTREQ van IOS in het IKE_SA_INIT antwoordbericht en dus niet in verbinding staan met een 13806 Error ID.

- Hoewel de Onderwerp Alternative Name (SAN) niet vereist is, is deze aanvaardbaar als de certificaten één hebben.

- Zorg ervoor dat in de Windows 7 Client Certificate Store op de machine-Trusted Root-certificeringsinstantie het minste aantal certificaten heeft. Als deze meer dan 50 heeft, kan Cisco IOS er niet in slagen de volledige lading Cert_Req te lezen, die het certificaatonderscheidde Naam (DN) van alle bekende CAs van het vakje van Windows 7 bevat. Als resultaat hiervan faalt de onderhandeling en u ziet de verbindingstijd op de cliënt.

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

De Output Interpreter Tool (alleen voor geregistreerde klanten) ondersteunt bepaalde opdrachten met show. Gebruik de Output Interpreter Tool om een analyse te bekijken van de output van de opdracht **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:
```

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- ASA IKEv2-debugs voor Site-to-Site VPN met PSKs TechNotes
- ASA IPsec- en IKE-debugs (IKEv1 hoofdmodus) voor probleemoplossing bij technische opmerking
- IOS IPSec- en IKE-implementaties - IKEv1 hoofdmodus voor probleemoplossing
- ASA IPSec and IKE-implementaties - IKEv1 aggregation mode TechNotes
- Cisco ASA 5500 Series adaptieve security applicaties
- Cisco ASA 5500 Series softwaredownloads voor adaptieve security applicaties
- Cisco IOS Firewall
- Cisco IOS-software
- Secure Shell (SSH)
- IPsec-onderhandeling/IKE-protocollen
- Technische ondersteuning en documentatie – Cisco Systems