IKEv2 mit Windows 7 IKEv2 Agile VPN-Client und Zertifikatauthentifizierung auf FlexVPN

Inhalt

Einführung

FlexVPN ist die neue VPN-Infrastruktur auf Basis von IKEv2 (Internet Key Exchange Version 2) auf Cisco IOS® und soll eine einheitliche VPN-Lösung sein. In diesem Dokument wird beschrieben, wie der in Windows 7 integrierte IKEv2-Client konfiguriert wird, um ein Cisco IOS-Headend mit der Verwendung einer Zertifizierungsstelle (Certificate Authority, CA) zu verbinden.

> **Hinweis**: Die Adaptive Security Appliance (ASA) unterstützt ab Version 9.3(2) jetzt IKEv2-Verbindungen mit dem integrierten Windows 7-Client.

> **Hinweis**: SUITE-B-Protokolle funktionieren nicht, da das IOS-Headend SUITE-B mit IKEv1 nicht unterstützt oder der Windows 7 IKEv2 Agile VPN-Client derzeit SUITE-B mit IKEv2 nicht unterstützt.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Integrierter Windows 7-VPN-Client
- Cisco IOS Softwareversion 15.2(2)T
- Zertifizierungsstelle - OpenSSL CA

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Hardware- und Softwareversionen:

- Integrierter Windows 7-VPN-Client
- Cisco IOS Software Release 15.2(2)T
- Zertifizierungsstelle - OpenSSL CA

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Konfigurieren

Übersicht

Der in Windows 7 integrierte IKEv2-Client muss in vier Hauptschritten konfiguriert werden, um ein Cisco IOS-Headend mit der Verwendung einer CA zu verbinden:

1. Konfiguration der CA

   Die CA sollte es Ihnen ermöglichen, die erforderliche Extended Key Usage (EKU) in das Zertifikat einzubetten. Beispielsweise ist auf dem IKEv2-Server "Server Auth EKU" erforderlich, während das Client-Zertifikat "Client Auth EKU" benötigt. Lokale Bereitstellungen können von folgenden Vorteilen profitieren:Cisco IOS CA-Server - Selbstsignierte Zertifikate können wegen des Bugs CSCuc82575 nicht verwendet werden.OpenSSL CA-ServerMicrosoft CA-Server - Im Allgemeinen ist dies die bevorzugte Option, da sie so konfiguriert werden kann, dass das Zertifikat genau wie gewünscht signiert wird.

2. Konfigurieren des Cisco IOS-Headend

   Zertifikat erhaltenKonfigurieren von IKEv2

3. Integrierten Windows 7-Client konfigurieren
4. Kundenzertifikat abrufen

Jeder dieser Hauptschritte wird in den nachfolgenden Abschnitten ausführlich erläutert.

> **Hinweis**: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Zertifizierungsstelle konfigurieren

Dieses Dokument enthält keine detaillierten Schritte zum Einrichten einer Zertifizierungsstelle. Die Schritte in diesem Abschnitt zeigen jedoch, wie die Zertifizierungsstelle konfiguriert wird, damit sie Zertifikate für diese Art von Bereitstellung ausstellen kann.

OpenSSL

OpenSSL CA basiert auf der Konfigurationsdatei. Die 'config'-Datei für den OpenSSL-Server sollte folgende Eigenschaften aufweisen:

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

Cisco IOS CA-Server

Wenn Sie einen Cisco IOS CA-Server verwenden, stellen Sie sicher, dass Sie die neueste Cisco IOS Software-Version verwenden, die der EKU zugewiesen ist.

```
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
```

Konfigurieren des Cisco IOS-Headend

Zertifikat abrufen

Für das Zertifikat müssen die EKU-Felder auf "Server Authentication" (Serverauthentifizierung) für Cisco IOS und "Client Authentication" (Client-Authentifizierung) für den Client eingestellt sein. In der Regel wird dieselbe CA zum Signieren von Client- und Serverzertifikaten verwendet. In diesem Fall werden sowohl "Server Authentication" (Serverauthentifizierung) als auch "Client Authentication" (Client-Authentifizierung) auf dem Serverzertifikat bzw. dem Clientzertifikat angezeigt, was akzeptabel ist.

Wenn die Zertifizierungsstelle die Zertifikate im PKCS-Nr. 12-Format (Public-Key Cryptography Standards) auf dem IKEv2-Server an die Clients und den Server ausgibt und die Zertifikatswiderrufliste (Certificate Revocation List, CRL) nicht erreichbar oder verfügbar ist, muss sie konfiguriert werden:

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

Geben Sie diesen Befehl ein, um das PKCS#12-Zertifikat zu importieren:

```
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.
```

Wenn ein Cisco IOS CA-Server automatisch Zertifikate zulässt, muss der IKEv2-Server mit der CA-Server-URL konfiguriert werden, um ein Zertifikat zu erhalten, wie in diesem Beispiel gezeigt:

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

Wenn der Trustpoint konfiguriert ist, müssen Sie:

1. Authentifizierung der CA mit folgendem Befehl:

   ```
   crypto pki authenticate FlexRootCA
   ```

2. Registrieren Sie den IKEv2-Server mit der CA mithilfe des folgenden Befehls:

   ```
   crypto pki enroll FlexRootCA
   ```

Um zu sehen, ob das Zertifikat alle erforderlichen Optionen enthält, verwenden Sie den folgenden Befehl 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
```

Konfigurieren von IKEv2

Dies ist ein Beispiel für die IKEv2-Konfiguration:

```
!! 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
```

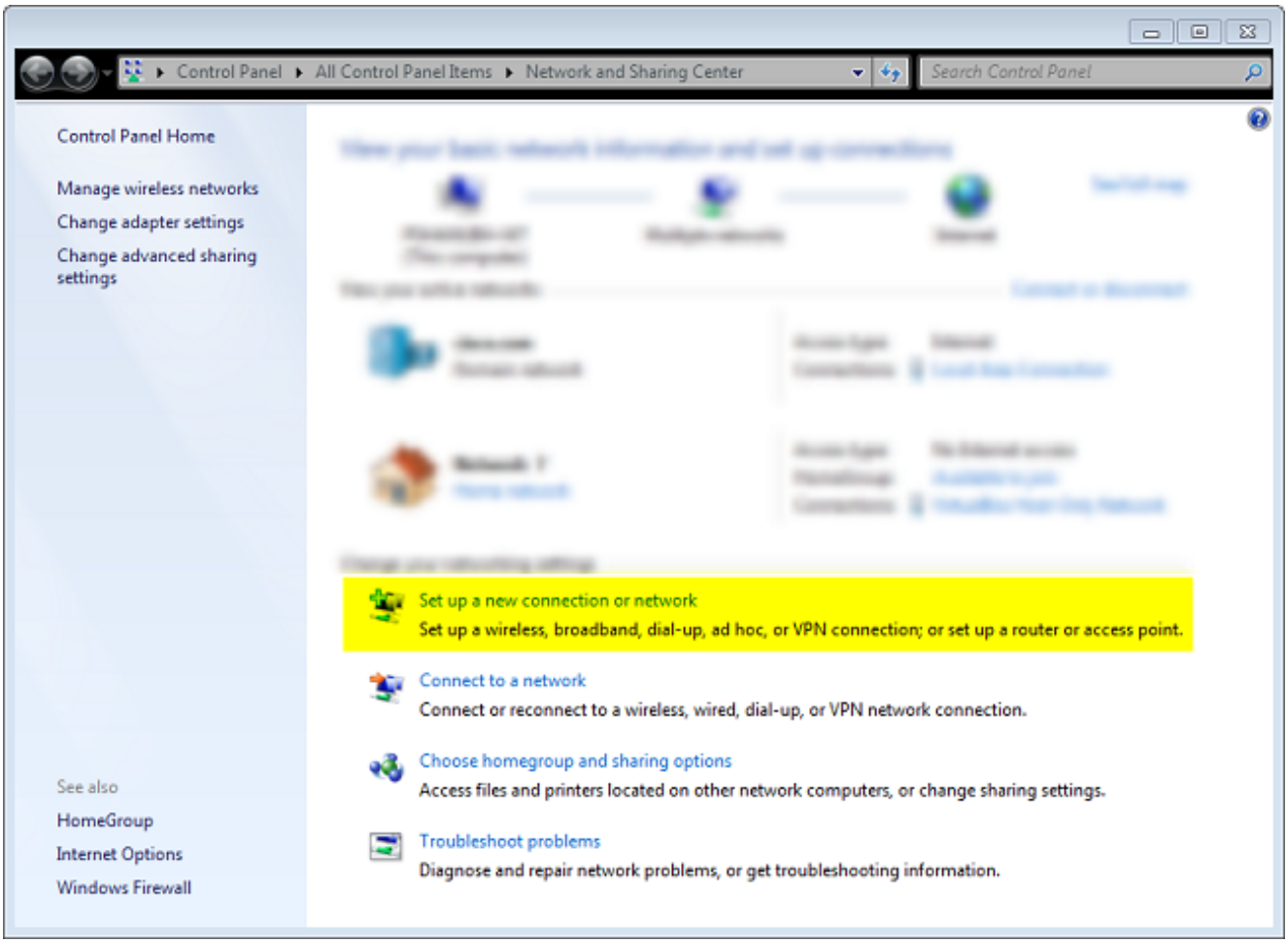
```
!! IPSec Profile that calls IKEv2 Profile

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
```

Die nicht nummerierte IP-Adresse der virtuellen Vorlage sollte alles andere sein als die für die IPsec-Verbindung verwendete lokale Adresse. [Wenn Sie einen Hardware-Client verwenden, würden Sie Routing-Informationen über den IKEv2-Konfigurationsknoten austauschen und auf dem Hardware-Client ein rekursives Routing-Problem erstellen.]

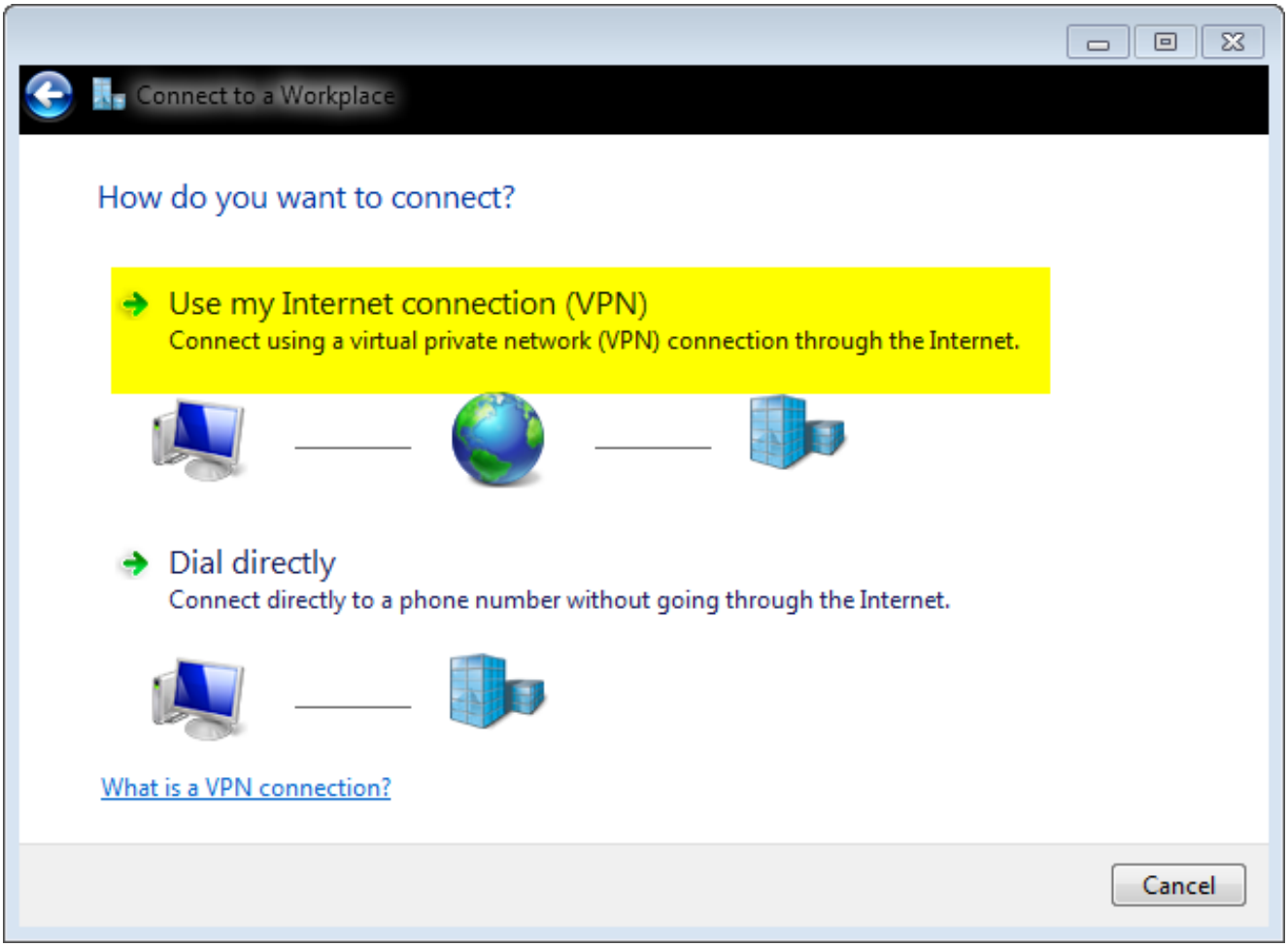
Integrierten Windows 7-Client konfigurieren

In diesem Verfahren wird beschrieben, wie der integrierte Client von Windows 7 konfiguriert wird.

1. Navigieren Sie zum **Netzwerk- und Freigabecenter**, und klicken Sie auf **Neue Verbindung oder neues Netzwerk einrichten**.

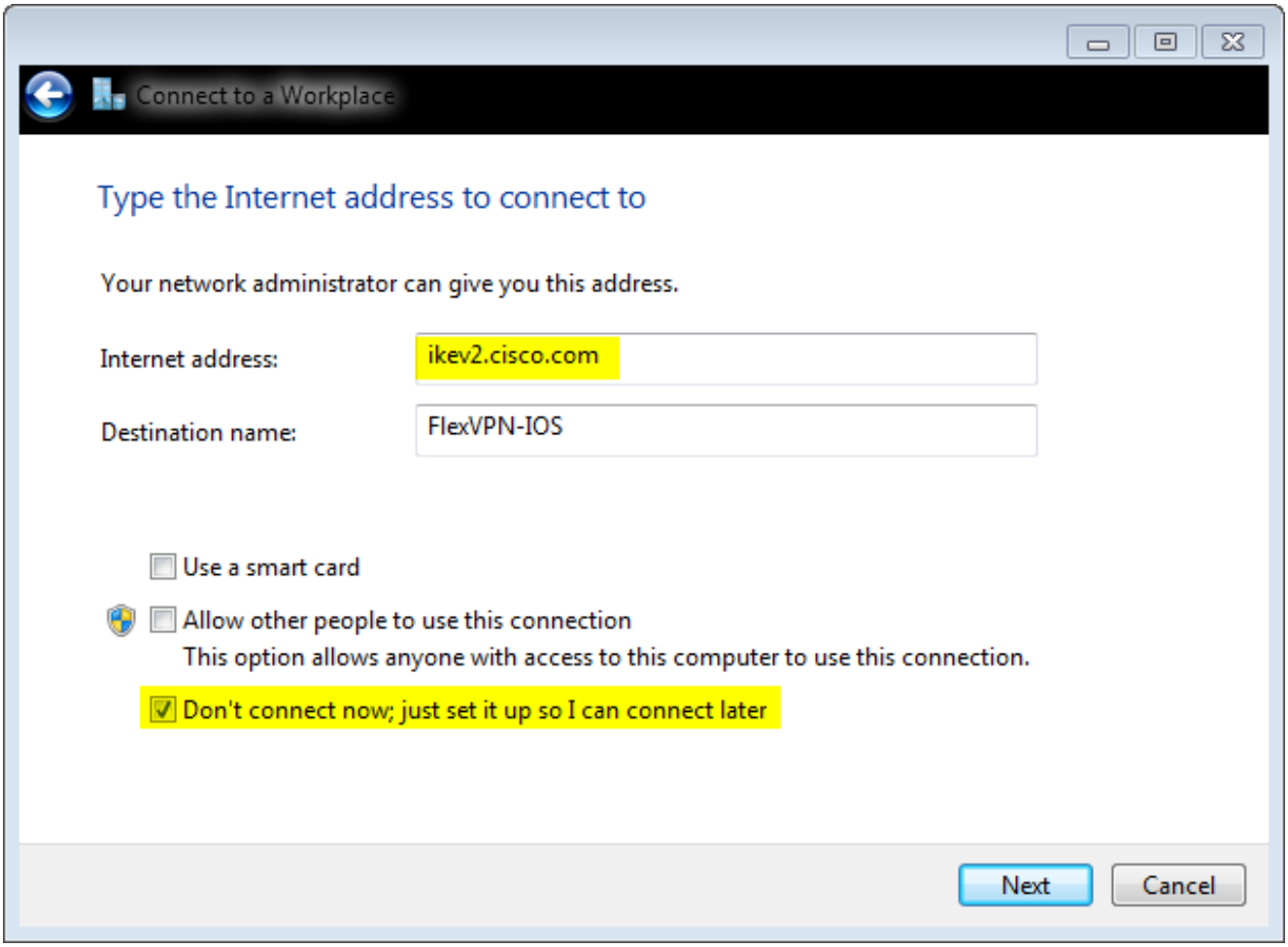


2. Klicken Sie auf **Meine Internetverbindung verwenden**. Dadurch können Sie eine VPN-Verbindung einrichten, die über eine aktuelle Internetverbindung ausgehandelt wird.

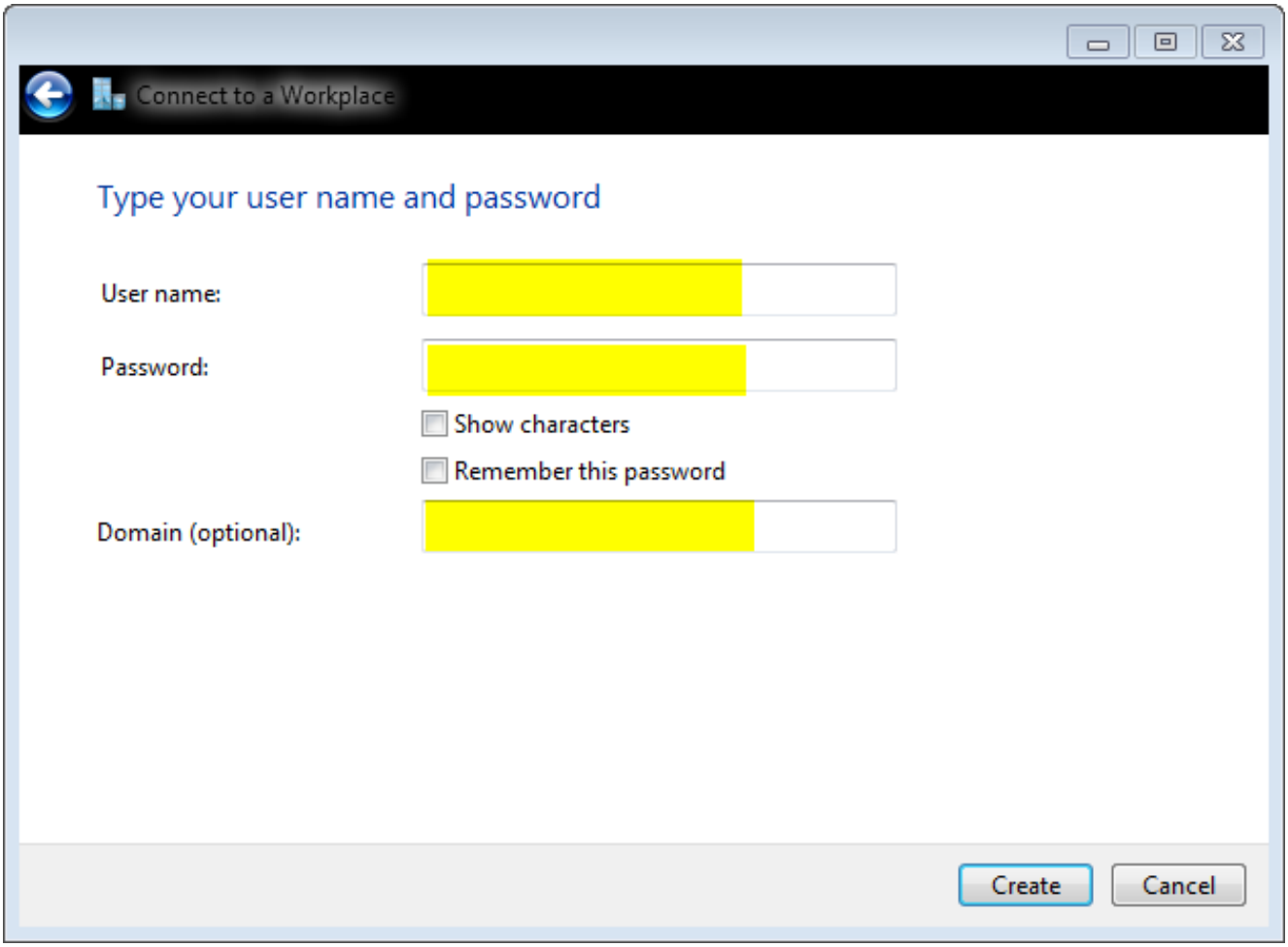


3. Geben Sie den vollqualifizierten Domänennamen (FQDN) oder die IP-Adresse des IKEv2-Servers ein, und geben Sie diesem einen Zielnamen für die lokale Identifizierung ein.

   Hinweis: Der FQDN muss mit dem Common Name (CN) aus dem Router-Identitätszertifikat übereinstimmen. Windows 7 verwirft die Verbindung mit dem Fehler 13801, wenn eine Diskrepanz festgestellt wird.
   Da zusätzliche Parameter festgelegt werden müssen, aktivieren Sie **Jetzt nicht verbinden. richten Sie die Verbindung einfach ein, damit ich später eine Verbindung herstellen kann**, und klicken Sie auf **Weiter**:

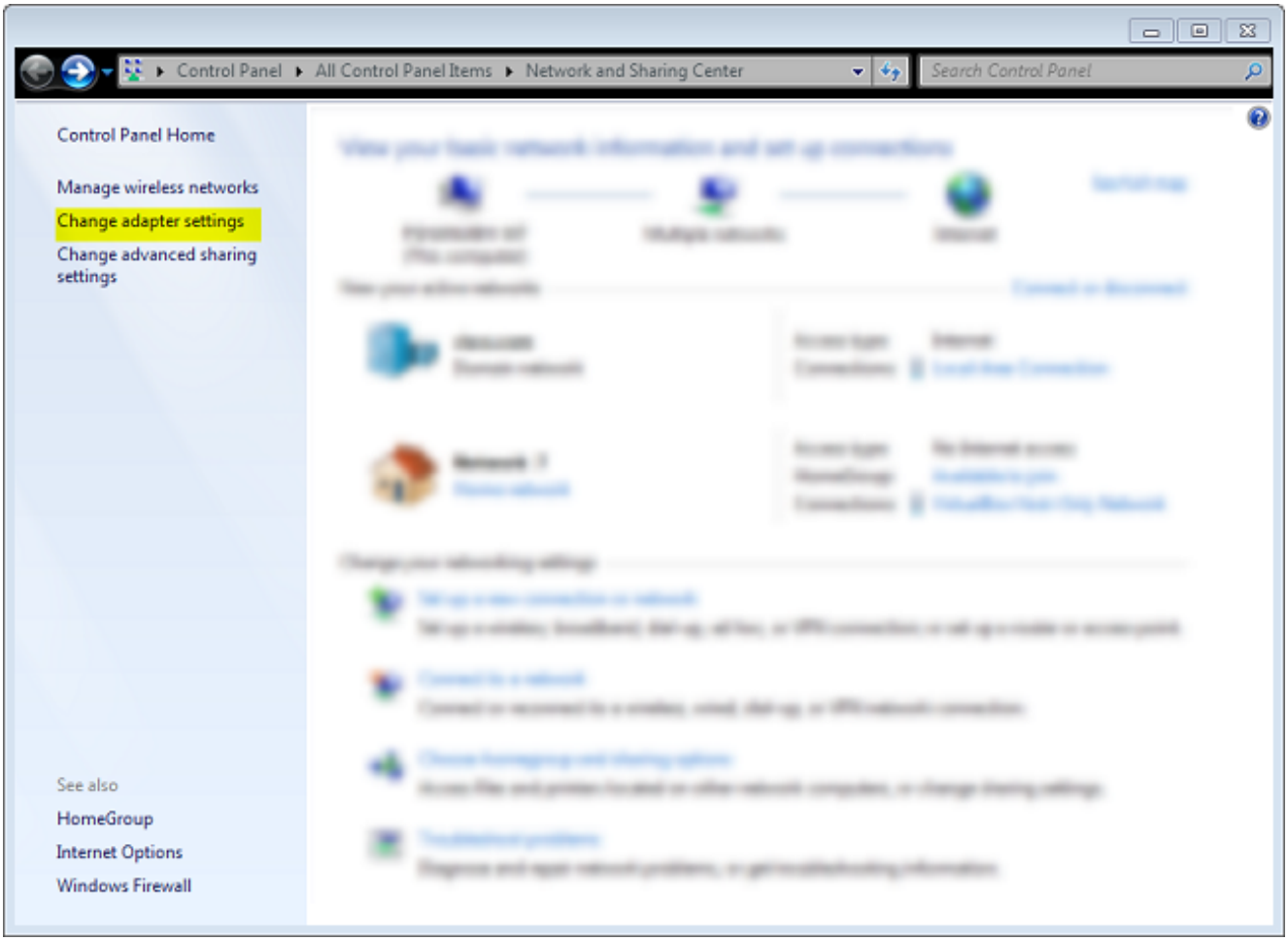


4. Füllen Sie die Felder **Benutzername**, **Kennwort** und **Domäne (optional)** nicht aus, da die Zertifikatauthentifizierung verwendet werden soll. Klicken Sie auf **Erstellen**.



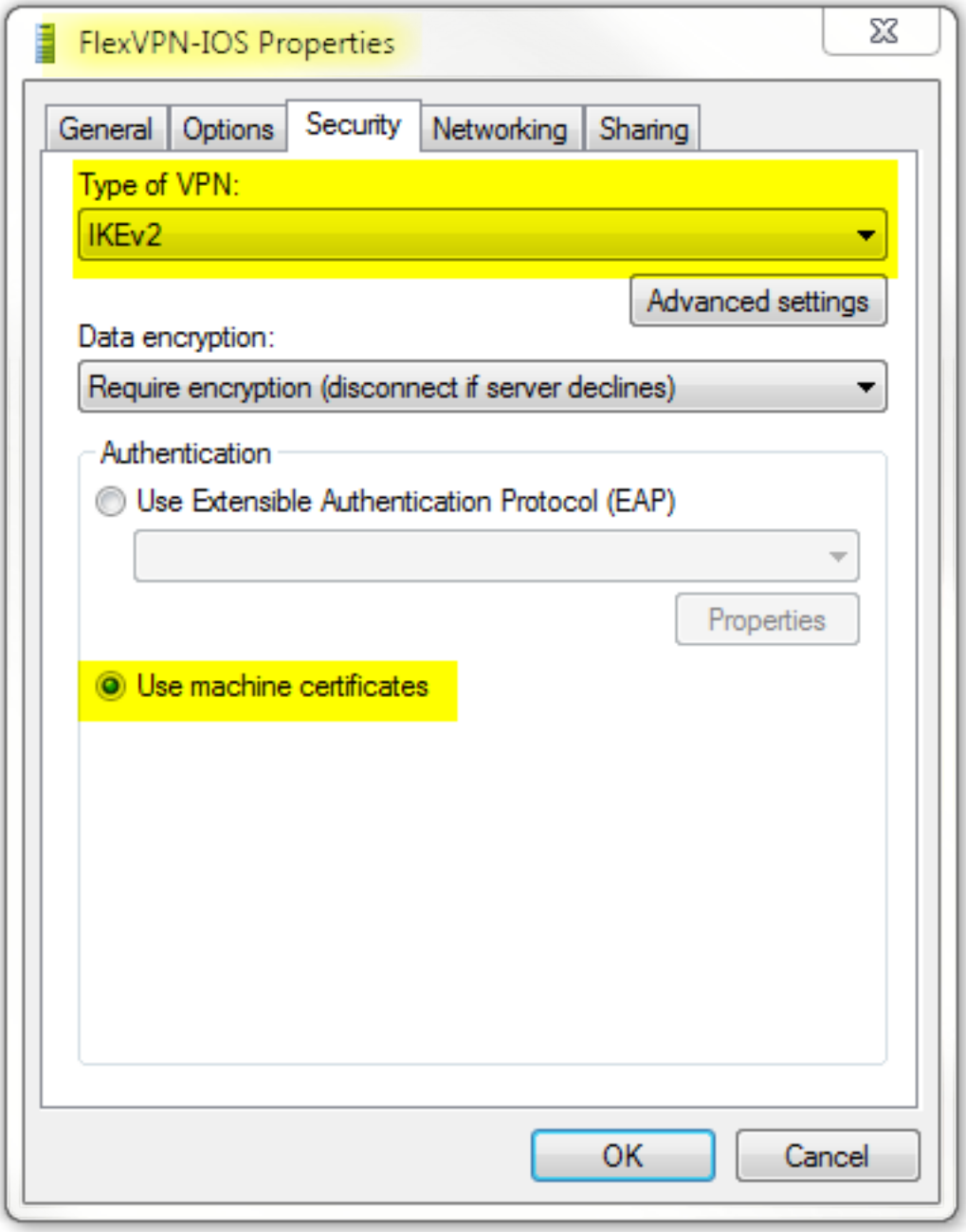
Hinweis: Schließen Sie das resultierende Fenster. **Versuchen Sie nicht, eine Verbindung herzustellen.**

5. Navigieren Sie zurück zum **Netzwerk- und Freigabecenter**, und klicken Sie auf **Adaptereinstellungen ändern**.



6. Wählen Sie den logischen Adapter FlexVPN-IOS aus. Dies ist das Ergebnis aller Schritte, die bis zu diesem Zeitpunkt unternommen wurden. Klicken Sie auf die entsprechenden Eigenschaften. Dies sind die Eigenschaften des neu erstellten Verbindungsprofils FlexVPN-IOS:

   Auf der Registerkarte Sicherheit sollte der VPN-Typ IKEv2 sein.Wählen Sie im Abschnitt Authentifizierung die Option **Computerzertifikate verwenden aus**.



Das FlexVPN-IOS-Profil kann jetzt angeschlossen werden, nachdem Sie ein Zertifikat in den Zertifikatsspeicher des Computers importiert haben.

Clientzertifikat abrufen

Das Clientzertifikat erfordert folgende Faktoren:

- Das Client-Zertifikat hat die EKU 'Client Authentication'. Darüber hinaus gibt die CA ein PKCS#12-Zertifikat aus:

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

- Zertifizierungsstellenzertifikat:

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

Wichtige Details

- 'IPSec IKE Intermediate' (OID = 1.3.6.1.5.5.8.2.2) sollte als EKU verwendet werden, wenn beide Aussagen zutreffen:

  Der IKEv2-Server ist ein Windows 2008-Server.Für IKEv2-Verbindungen wird mehr als ein Server-Authentifizierungszertifikat verwendet. Wenn dies zutrifft, platzieren Sie entweder "Server Authentication" EKU und "IPSec IKE Intermediate" EKU auf einem Zertifikat, oder verteilen Sie diese EKUs unter den Zertifikaten. Stellen Sie sicher, dass mindestens ein Zertifikat "IPSec IKE Intermediate" EKU enthält.

  Weitere Informationen finden Sie unter Problembehandlung bei IKEv2-VPN-Verbindungen.

- Verwenden Sie in einer FlexVPN-Bereitstellung nicht "IPSec IKE Intermediate" in EKU. Wenn ja, übernimmt der IKEv2-Client das IKEv2-Serverzertifikat nicht. Daher können sie in der IKE_SA_INIT-Antwortmeldung nicht auf CERTREQ von IOS reagieren und können daher keine Verbindung mit einer Fehler-ID 13806 herstellen.

- Obwohl der Subject Alternative Name (SAN) nicht erforderlich ist, ist er akzeptabel, wenn die Zertifikate über einen Namen verfügen.

- Stellen Sie im Windows 7-Client-Zertifikatspeicher sicher, dass der Store für Machine-Trusted Root Certificate Authorities Store über die geringstmögliche Anzahl von Zertifikaten verfügt. Wenn es über mehr als 50 Datensätze verfügt, kann Cisco IOS die gesamte Payload "Cert_Req", die den DN (Certificate Distinguished Name) aller bekannten CAs enthält, aus dem Feld "Windows 7" nicht lesen. Als Ergebnis schlägt die Verhandlung fehl, und Sie sehen das Timeout für die Verbindung auf dem Client.

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das Output Interpreter Tool (nur registrierte Kunden) unterstützt bestimmte **show**-Befehle. Verwenden Sie das Output Interpreter Tool, um eine Analyse der **Ausgabe des** Befehls **show** anzuzeigen.

```
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:
```

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- ASA IKEv2-Debugger für Site-to-Site-VPN mit PSKs - Technische Anmerkung
- ASA IPsec- und IKE-Debug (IKEv1-Hauptmodus) Fehlerbehebung TechHinweis
- IOS IPSec- und IKE-Debug - IKEv1 Main Mode Troubleshooting TechNote
- ASA IPSec- und IKE-Debug - IKEv1 Aggressive Mode TechNote
- Cisco Adaptive Security Appliances der Serie ASA 5500
- Software-Downloads für Cisco Adaptive Security Appliances der Serie ASA 5500
- Cisco IOS-Firewall
- Cisco IOS-Software
- Secure Shell (SSH)
- IPsec-Aushandlung/IKE-Protokolle
- Technischer Support und Dokumentation - Cisco Systems