IKEv2 con autenticazione client VPN Agile IKEv2 di Windows 7 e certificato su FlexVPN

Sommario

Introduzione

FlexVPN è la nuova infrastruttura VPN basata su Internet Key Exchange versione 2 (IKEv2) su Cisco IOS® ed è progettata per essere una soluzione VPN unificata. In questo documento viene descritto come configurare il client IKEv2 incorporato in Windows 7 per connettere un headend Cisco IOS con l'utilizzo di un'Autorità di certificazione (CA).

> **Nota:** A partire dalla versione 9.3(2), Adaptive Security Appliance (ASA) supporta ora le connessioni IKEv2 con il client incorporato di Windows 7.

> **Nota:** I protocolli SUITE-B non funzionano perché l'headend IOS non supporta SUITE-B con IKEv1 o il client VPN Agile Windows 7 IKEv2 non supporta attualmente SUITE-B con IKEv2.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Client VPN incorporato di Windows 7
- Software Cisco IOS release 15.2(2)T
- Autorità di certificazione - CA OpenSSL

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni hardware e software:

- Client VPN incorporato di Windows 7
- Software Cisco IOS release 15.2(2)T
- Autorità di certificazione - CA OpenSSL

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Configurazione

Panoramica

Per connettere un headend Cisco IOS all'utilizzo di una CA, è necessario configurare il client IKEv2 incorporato di Windows 7 in quattro passaggi principali:

1. Configura CA

   La CA deve consentire di incorporare l'utilizzo chiavi avanzato (EKU) richiesto nel certificato. Nel server IKEv2, ad esempio, è richiesto l'utilizzo chiavi avanzato di autenticazione server, mentre per il certificato client è necessario l'utilizzo chiavi avanzato di autenticazione client. Le distribuzioni locali possono utilizzare:Server CA Cisco IOS - Impossibile utilizzare certificati autofirmati a causa del bug CSCuc82575.Server CA OpenSSLServer CA Microsoft - In generale, questa è l'opzione preferita perché può essere configurato per firmare il certificato esattamente come desiderato.

2. Configurazione headend Cisco IOS

Ottenere un certificatoConfigurare IKEv2

3. Configura client predefinito di Windows 7
4. Ottieni certificato client

Ognuno di questi passaggi principali viene descritto in dettaglio nelle sezioni successive.

> **Nota:** per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Configura Autorità di certificazione

In questo documento non vengono fornite istruzioni dettagliate su come configurare una CA. Tuttavia, la procedura descritta in questa sezione illustra come configurare la CA in modo che possa rilasciare certificati per questo tipo di distribuzione.

OpenSSL

La CA OpenSSL è basata sul file 'config'. Il file 'config' per il server OpenSSL deve avere:

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

Cisco IOS CA Server

Se si usa un server CA Cisco IOS, verificare di usare la versione software Cisco IOS più recente, a cui è stato assegnato 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
```

Configurazione headend Cisco IOS

Ottieni un certificato

I campi EKU del certificato devono essere impostati su 'Autenticazione server' per Cisco IOS e su 'Autenticazione client' per il client. In genere, la stessa CA viene utilizzata per firmare i certificati sia del client che del server. In questo caso, sia 'Autenticazione server' che 'Autenticazione client' vengono visualizzati rispettivamente nel certificato server e nel certificato client, il che è accettabile.

Se la CA rilascia i certificati nel formato PKCS (Public-Key Cryptography Standards) #12 sul server IKEv2 ai client e al server e se l'elenco di revoche di certificati (CRL) non è raggiungibile o disponibile, è necessario configurarlo:

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

Immettere questo comando per importare il certificato 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.
```

Se un server CA Cisco IOS concede automaticamente i certificati, per poter ricevere un certificato, il server IKEv2 deve essere configurato con l'URL del server CA, come mostrato nell'esempio seguente:

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

Quando il trust point è configurato, è necessario:

1. Autenticare la CA con questo comando:

   ```
   crypto pki authenticate FlexRootCA
   ```

2. Registrare il server IKEv2 con la CA con questo comando:

   ```
   crypto pki enroll FlexRootCA
   ```

Per verificare se il certificato contiene tutte le opzioni richieste, utilizzare questo 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
```

Configurare IKEv2

Questo è un esempio di configurazione di 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
```

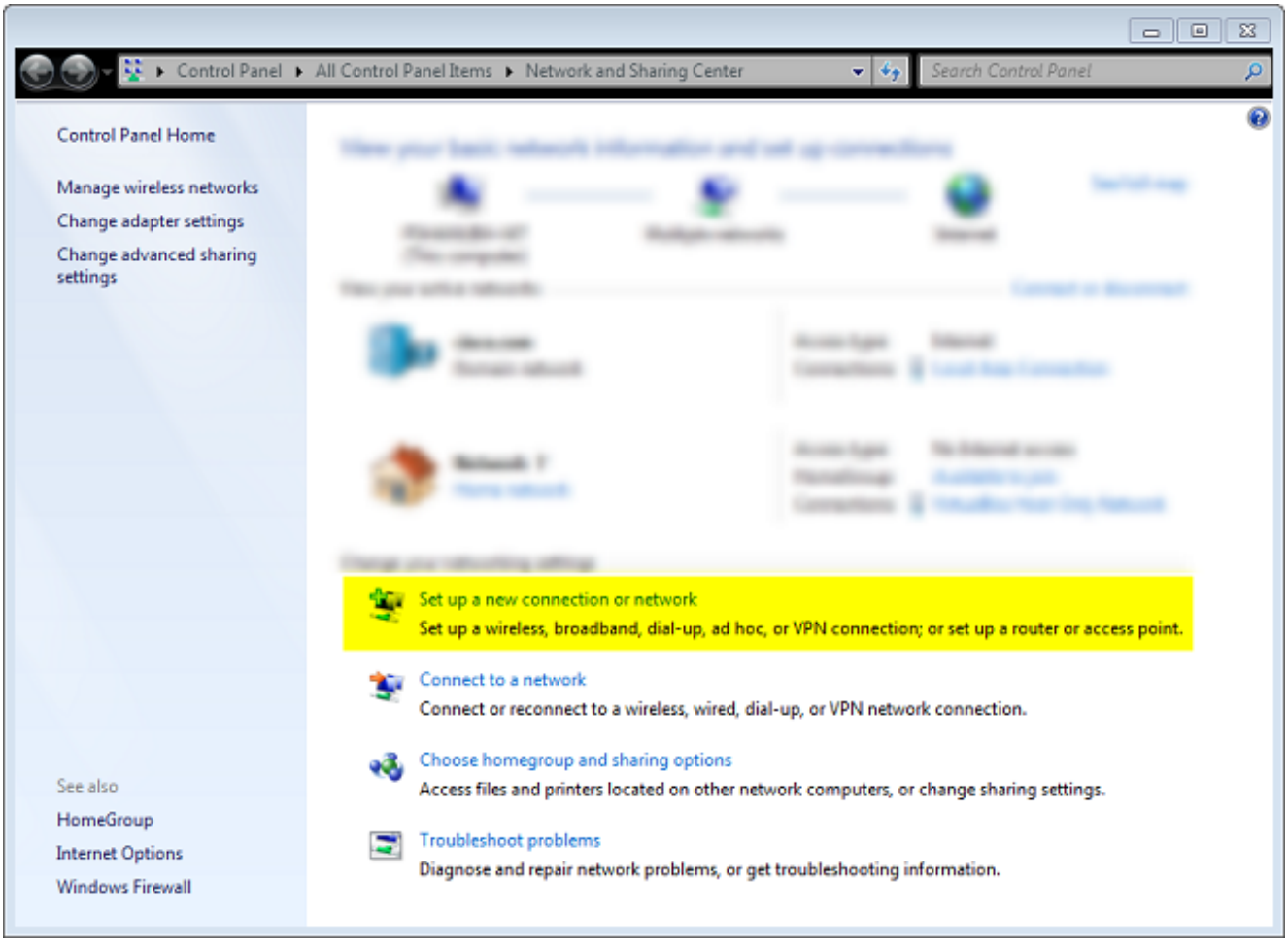
```
!! dVTI interface - A termination point for IKEv2 Clients

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

Il valore IP senza numero del modello virtuale deve essere diverso dall'indirizzo locale utilizzato per la connessione IPSec. [Se si utilizza un client hardware, scambiare le informazioni di routing tramite il nodo di configurazione IKEv2 e creare un problema di routing ricorsivo sul client hardware.]

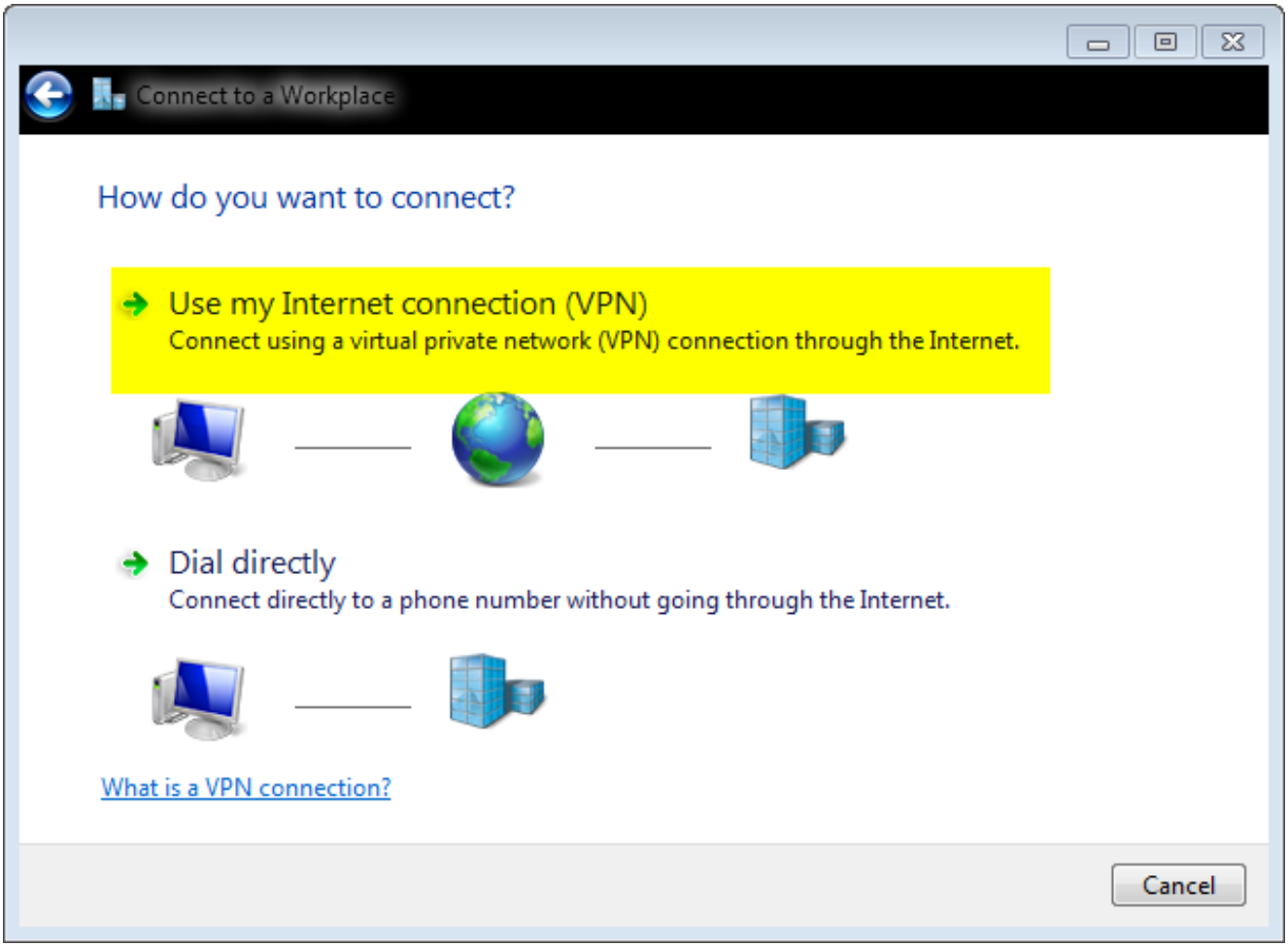
Configura client predefinito di Windows 7

In questa procedura viene descritto come configurare il client predefinito di Windows 7.

1. Passare al **Centro connessioni di rete e condivisione** e fare clic su **Configura nuova connessione o rete**.

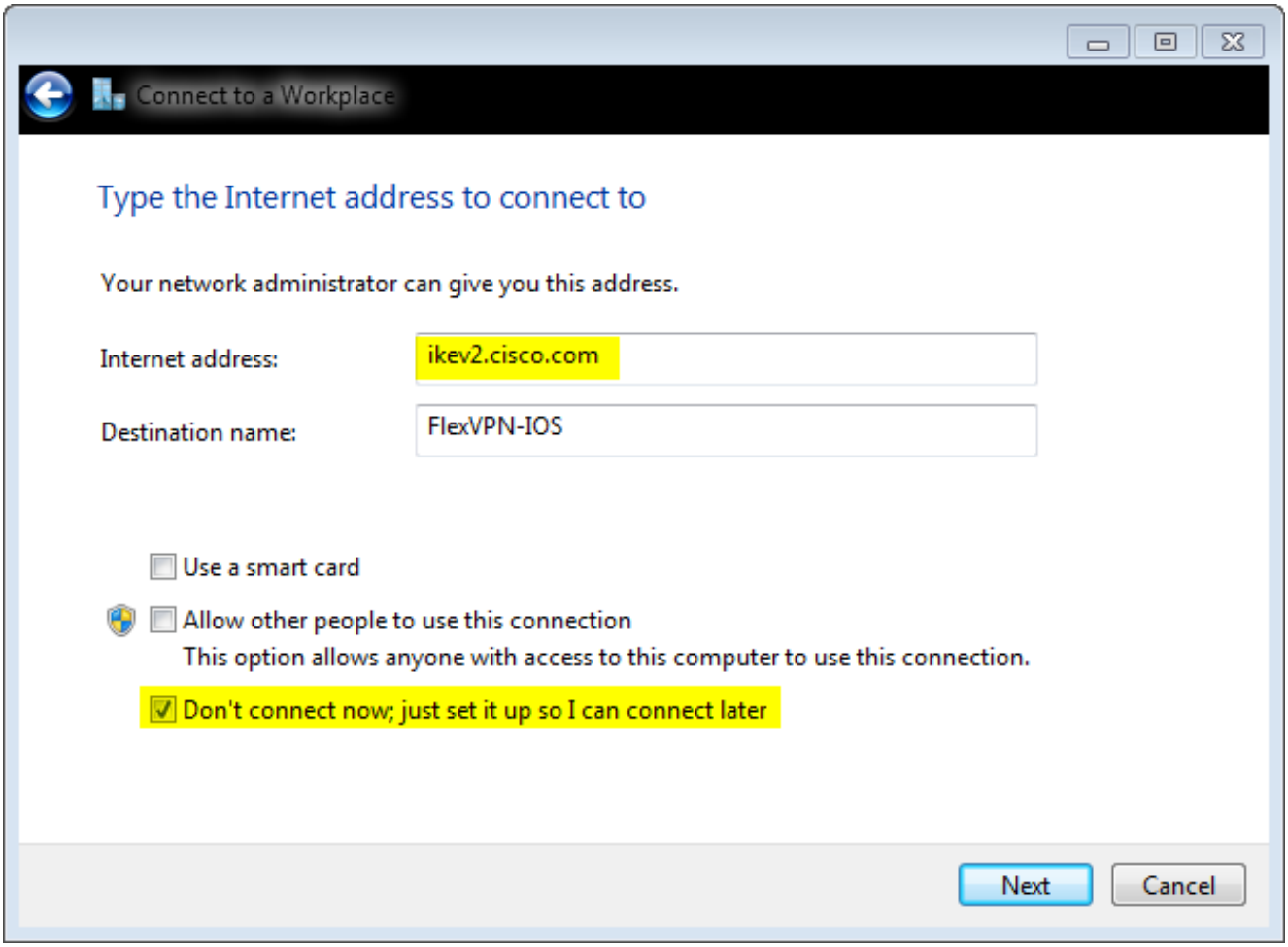


2. Fare clic su **Utilizza connessione Internet (VPN)**. Ciò consente di configurare una connessione VPN negoziata su una connessione Internet corrente.

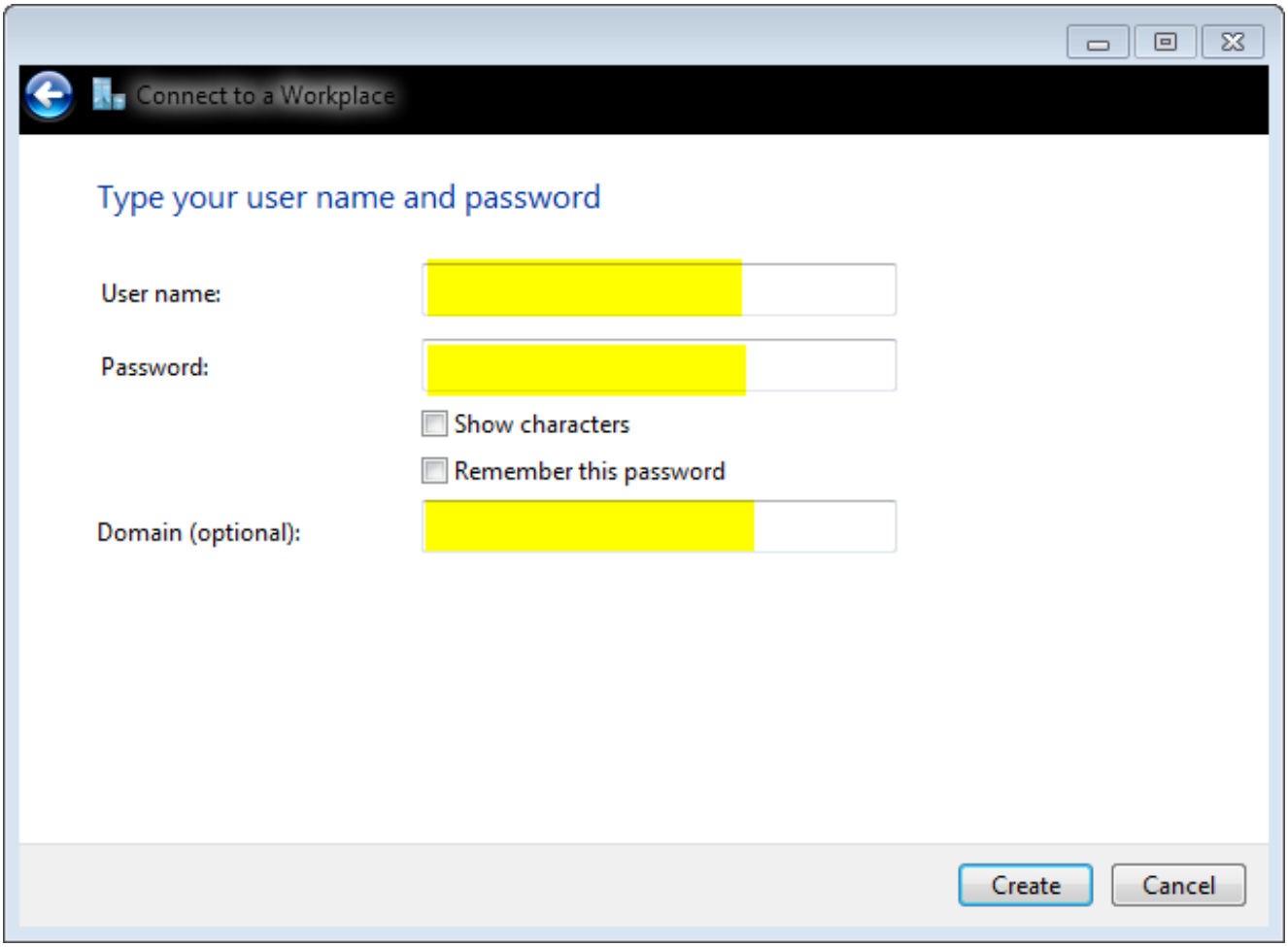


3. Immettere il nome di dominio completo (FQDN) o l'indirizzo IP del server IKEv2 e assegnargli un nome di destinazione per identificarlo localmente.

   Nota: Il nome di dominio completo (FQDN) deve corrispondere al nome comune (CN) del certificato di identità del router. Windows 7 interrompe la connessione con un errore 13801 se rileva una mancata corrispondenza.
   Poiché è necessario impostare parametri aggiuntivi, selezionare **Non connettere ora. configuralo in modo da potermi connettere in seguito**, quindi fai clic su **Avanti**:

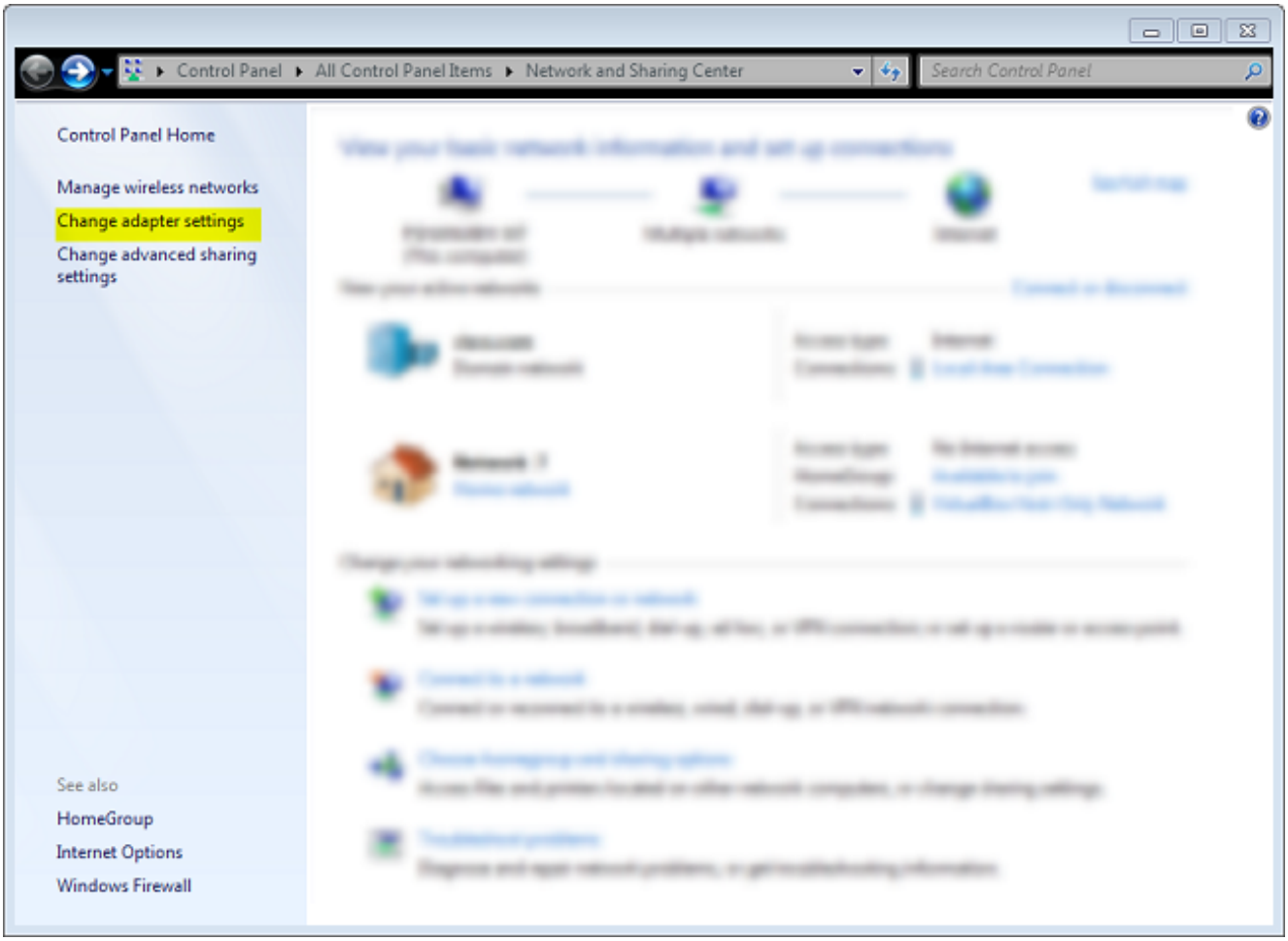


4. Non compilare i campi **Nome utente**, **Password** e **Dominio (facoltativo)** perché deve essere utilizzata l'autenticazione del certificato. Fare clic su **Crea**.



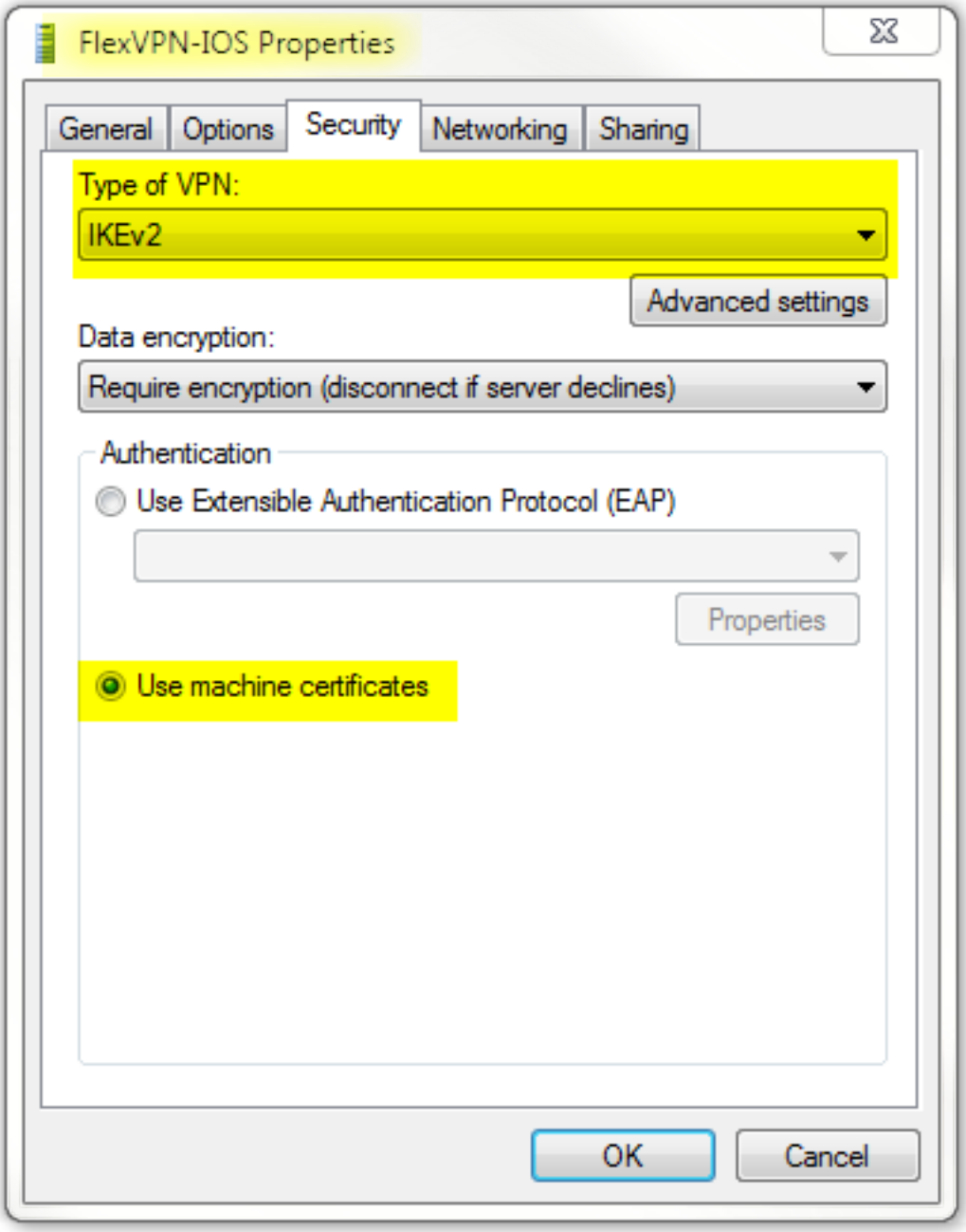
Nota: Chiudete la finestra risultante. **Non provare a connettersi.**

5. Tornare al **Centro connessioni di rete e condivisione** e fare clic su **Cambia impostazioni scheda**.



6. Scegliere la scheda logica FlexVPN-IOS, che è il risultato di tutti i passi compiuti fino a questo punto. Fare clic sulle relative proprietà. Queste sono le proprietà del profilo di connessione appena creato chiamato FlexVPN-IOS:

   Nella scheda Sicurezza il tipo di VPN deve essere IKEv2.Nella sezione Autenticazione scegliere **Usa certificati computer**.



Il profilo FlexVPN-IOS è pronto per la connessione dopo l'importazione di un certificato nell'archivio certificati del computer.

Ottieni certificato client

Il certificato client richiede i fattori seguenti:

- Il certificato client dispone di un utilizzo chiavi avanzato (EKU) di 'Autenticazione client'. La CA fornisce inoltre un certificato PKCS#12:

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

- Certificato CA:

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

Dettagli importanti

- Utilizzare 'Intermedio IPSec IKE' (OID = 1.3.6.1.5.5.8.2.2) come EKU se si applicano entrambe le istruzioni seguenti:

  Il server IKEv2 è un server Windows 2008.Più certificati di autenticazione server in uso per le connessioni IKEv2. In questo caso, inserire entrambi gli EKU di autenticazione server e di intermediazione IPSec IKE in un unico certificato oppure distribuirli tra i certificati. Verificare che almeno un certificato contenga l'utilizzo chiavi avanzato 'IPSec IKE Intermediate'.

  Per ulteriori informazioni, fare riferimento a Risoluzione dei problemi delle connessioni VPN IKEv2.

- In una distribuzione FlexVPN, non utilizzare 'IPSec IKE Intermediate' in EKU. In caso contrario, il client IKEv2 non acquisisce il certificato server IKEv2. Di conseguenza, non sono in grado di rispondere a CERTREQ da IOS nel messaggio di risposta IKE_SA_INIT e pertanto non riescono a connettersi con un ID errore 13806.

- Sebbene non sia richiesto il nome alternativo del soggetto (SAN), è accettabile che i certificati ne abbiano uno.

- Nell'archivio certificati client di Windows 7 verificare che nell'archivio Autorità di certificazione radice attendibili per il computer sia presente il minor numero di certificati possibile. Se il payload Cert_Req è più di 50, Cisco IOS potrebbe non essere in grado di leggere l'intero payload Cert_Req, che contiene il nome distinto (DN) del certificato di tutte le CA conosciute nella casella Windows 7. Di conseguenza, la negoziazione non riesce e sul client viene visualizzato il timeout della connessione.

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Lo strumento Output Interpreter (solo utenti registrati) supporta alcuni comandi show. Usare lo strumento Output Interpreter per visualizzare un'analisi dell'output 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:
```

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- Nota tecnica sui debug ASA IKEv2 per la VPN da sito a sito con PSK
- Nota tecnica sulla risoluzione dei problemi relativi ai debug ASA IPsec e IKE (modalità principale IKEv1)
- Note tecniche sulla risoluzione dei problemi relativi alla modalità principale IOS IPSec e IKE
- Debug ASA IPSec e IKE - Nota tecnica sulla modalità aggressiva IKEv1
- Cisco ASA serie 5500 Adaptive Security Appliance
- Download di software per appliance Cisco ASA serie 5500 Adaptive Security
- Cisco IOS Firewall
- Software Cisco IOS
- SSH (Secure Shell)
- Negoziazione IPSec/protocolli IKE
- Documentazione e supporto tecnico – Cisco Systems