# IKEv2 com Windows 7 IKEv2 Agile VPN Client e Autenticação de Certificado em FlexVPN

## Contents



## Introduction

FlexVPN é a nova infraestrutura de VPN baseada em IKEv2 (Internet Key Exchange versão 2) no Cisco IOS® e deve ser uma solução de VPN unificada. Este documento descreve como configurar o cliente IKEv2 que é incorporado ao Windows 7 para conectar um headend do Cisco IOS com a utilização de uma autoridade de certificação (CA).

> **Note**: O Adaptive Security Appliance (ASA) agora oferece suporte a conexões IKEv2 com o cliente integrado Windows 7 a partir da versão 9.3(2).

> **Note**: Os protocolos SUITE-B não funcionam porque o headend do IOS não suporta SUITE-B com IKEv1 ou o cliente Windows 7 IKEv2 Agile VPN não suporta atualmente SUITE-B com IKEv2.

## Prerequisites

### Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- cliente VPN incorporado do Windows 7
- Software Cisco IOS versão 15.2(2)T
- Autoridade de certificação - OpenSSL CA

### Componentes Utilizados

As informações neste documento são baseadas nas seguintes versões de hardware e software:

- cliente VPN incorporado do Windows 7
- Software Cisco IOS versão 15.2(2)T
- Autoridade de certificação - 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.

### Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter informações sobre convenções de documentos.

## Configurar

### Overview

Há quatro etapas principais na configuração do cliente IKEv2 integrado do Windows 7 para conectar um headend do Cisco IOS com a utilização de uma CA:

1. Configurar CA

   A AC deve permitir que você incorpore a EKU (Extended Key Usage, uso de chave estendida) necessária no certificado. Por exemplo, no servidor IKEv2, 'Server Auth EKU' é necessário, enquanto o certificado do cliente precisa de 'Client Auth EKU'. As implantações locais podem usar:Servidor CA do Cisco IOS - Os certificados autoassinados não podem ser usados devido ao bug CSCuc82575.servidor de CA OpenSSLMicrosoft CA server - Em geral, essa é a opção preferida porque pode ser configurada para assinar o certificado exatamente como desejado.

2. Configurar o headend do Cisco IOS

   Obter um certificadoConfigurar IKEv2

3. Configurar o cliente incorporado do Windows 7
4. Obter certificado de cliente

Cada uma dessas etapas principais é explicada em detalhes nas seções subsequentes.

> **Note**: Use a Command Lookup Tool ( somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

## Configurar autoridade de certificado

Este documento não fornece etapas detalhadas sobre como configurar uma CA. No entanto, as etapas nesta seção mostram como configurar a CA para que ela possa emitir certificados para esse tipo de implantação.

### OpenSSL

O OpenSSL CA é baseado no arquivo 'config'. O arquivo 'config' para o servidor OpenSSL deve ter:

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

### Cisco IOS CA Server

Se você usa um servidor de CA do Cisco IOS, certifique-se de usar a versão mais recente do Cisco IOS Software, que atribui a 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
```

## Configurar Headend do Cisco IOS

### Obter um certificado

O certificado deve ter os campos EKU definidos como 'Autenticação de servidor' para o Cisco IOS e 'Autenticação de cliente' para o cliente. Geralmente, a mesma CA é usada para assinar os certificados do cliente e do servidor. Nesse caso, a 'Autenticação do servidor' e a 'Autenticação do cliente' são vistas no certificado do servidor e no certificado do cliente, respectivamente, o que é aceitável.

Se a autoridade de certificação emitir os certificados no formato PKCS (Public-Key Cryptography Standards) #12 no servidor IKEv2 para os clientes e o servidor, e se a CRL (Certificate Revision List, lista de revogação de certificados) não estiver acessível ou disponível, ela deverá ser configurada:

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

Insira este comando para importar o 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.
```

Se um servidor de CA do Cisco IOS conceder automaticamente certificados, o servidor IKEv2 deve ser configurado com a URL do servidor de CA para receber um certificado como mostrado neste exemplo:

```
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 o ponto de confiança é configurado, você precisa:

1. Autentique a CA com este comando:

```
crypto pki authenticate FlexRootCA
```

2. Inscreva o servidor IKEv2 com a CA com este comando:

```
crypto pki enroll FlexRootCA
```

Para ver se o certificado contém todas as opções necessárias, use 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
```

## Configurar IKEv2

Este é um exemplo de configuração de 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
```

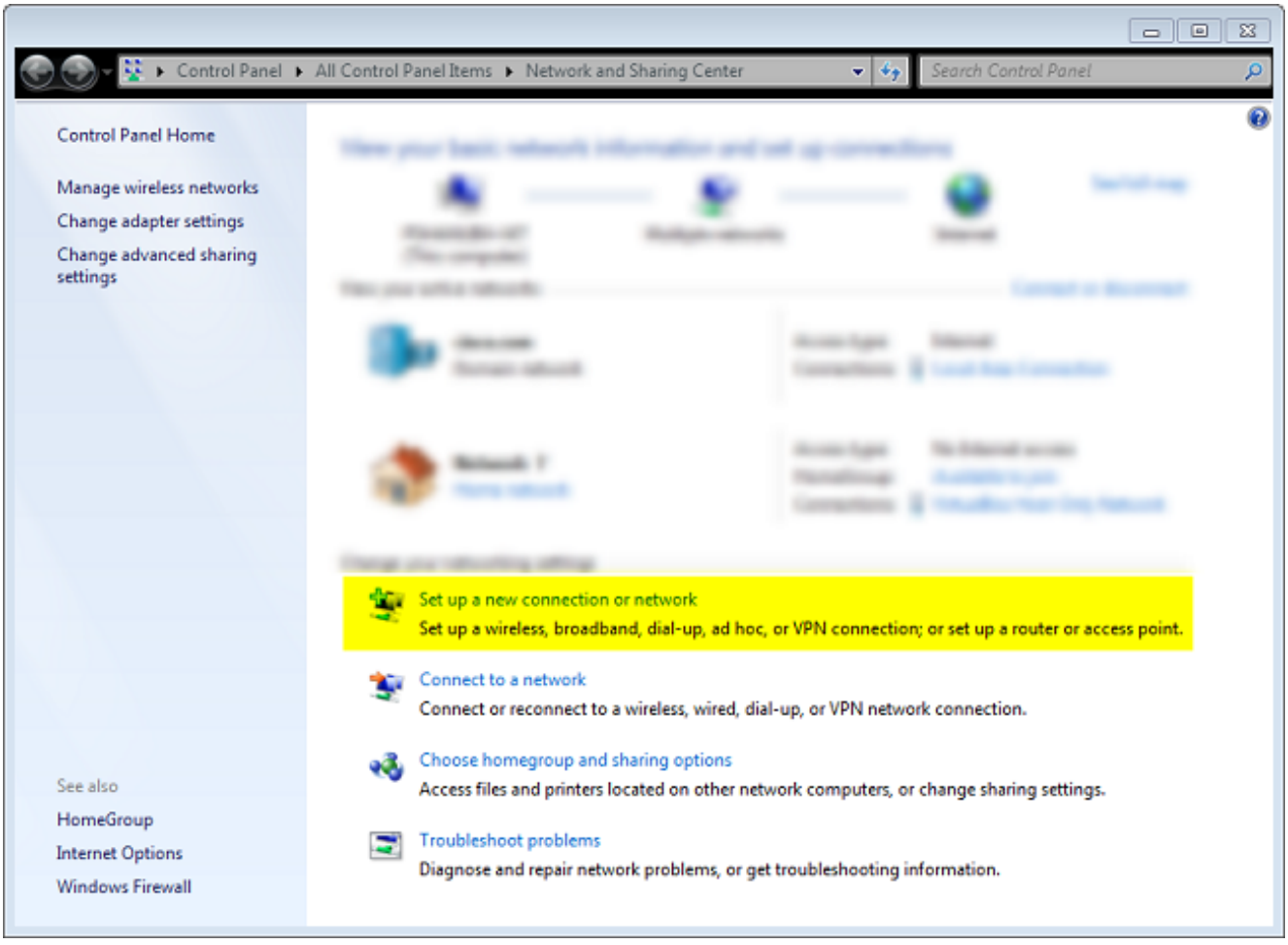
```
!! dVTI interface - A termination point for IKEv2 Clients

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

O IP não numerado do modelo virtual deve ser qualquer coisa, exceto o endereço local usado para a conexão IPsec.  [Se você usar um cliente de hardware, trocaria informações de roteamento por meio do nó de configuração IKEv2 e criaria um problema de roteamento recursivo no cliente de hardware.]

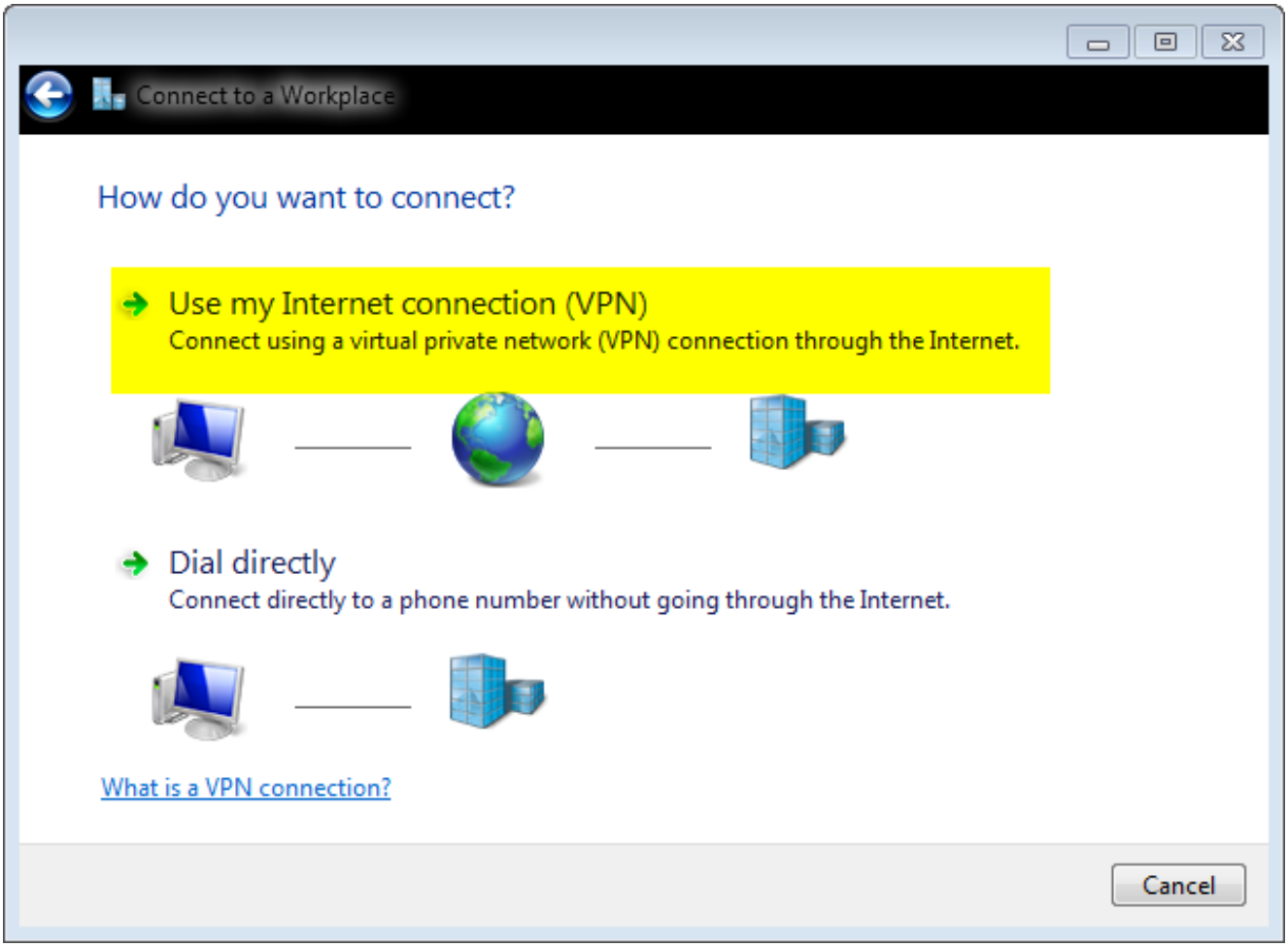
## Configurar o cliente interno do Windows 7

Este procedimento descreve como configurar o cliente interno do Windows 7.

1. Navegue até a **Central de Rede e Compartilhamento** e clique em **Configurar uma nova conexão ou rede**.

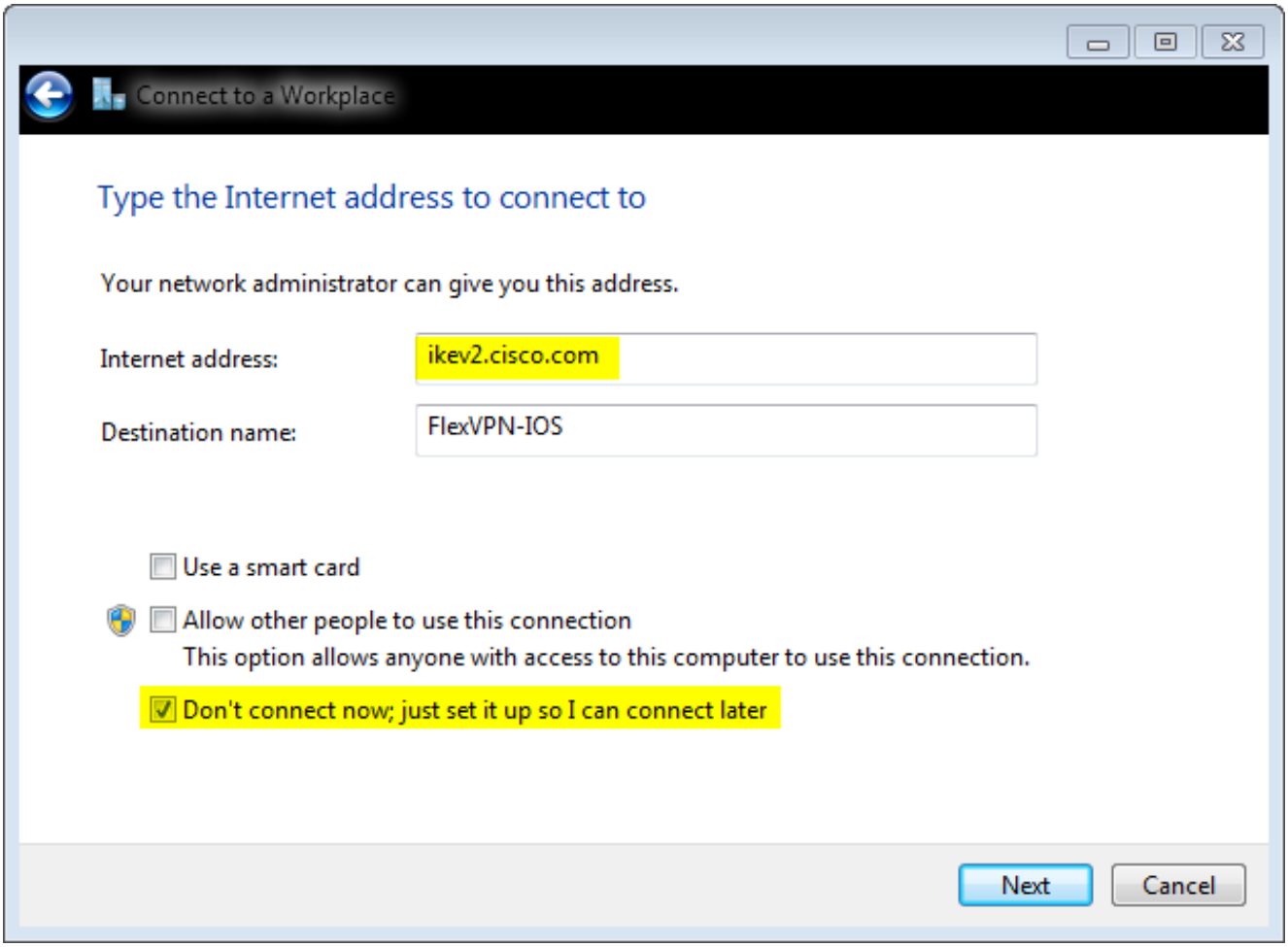



2. Clique em **Usar minha conexão com a Internet (VNP)**. Isso permite configurar uma conexão VPN negociada em uma conexão atual com a Internet.

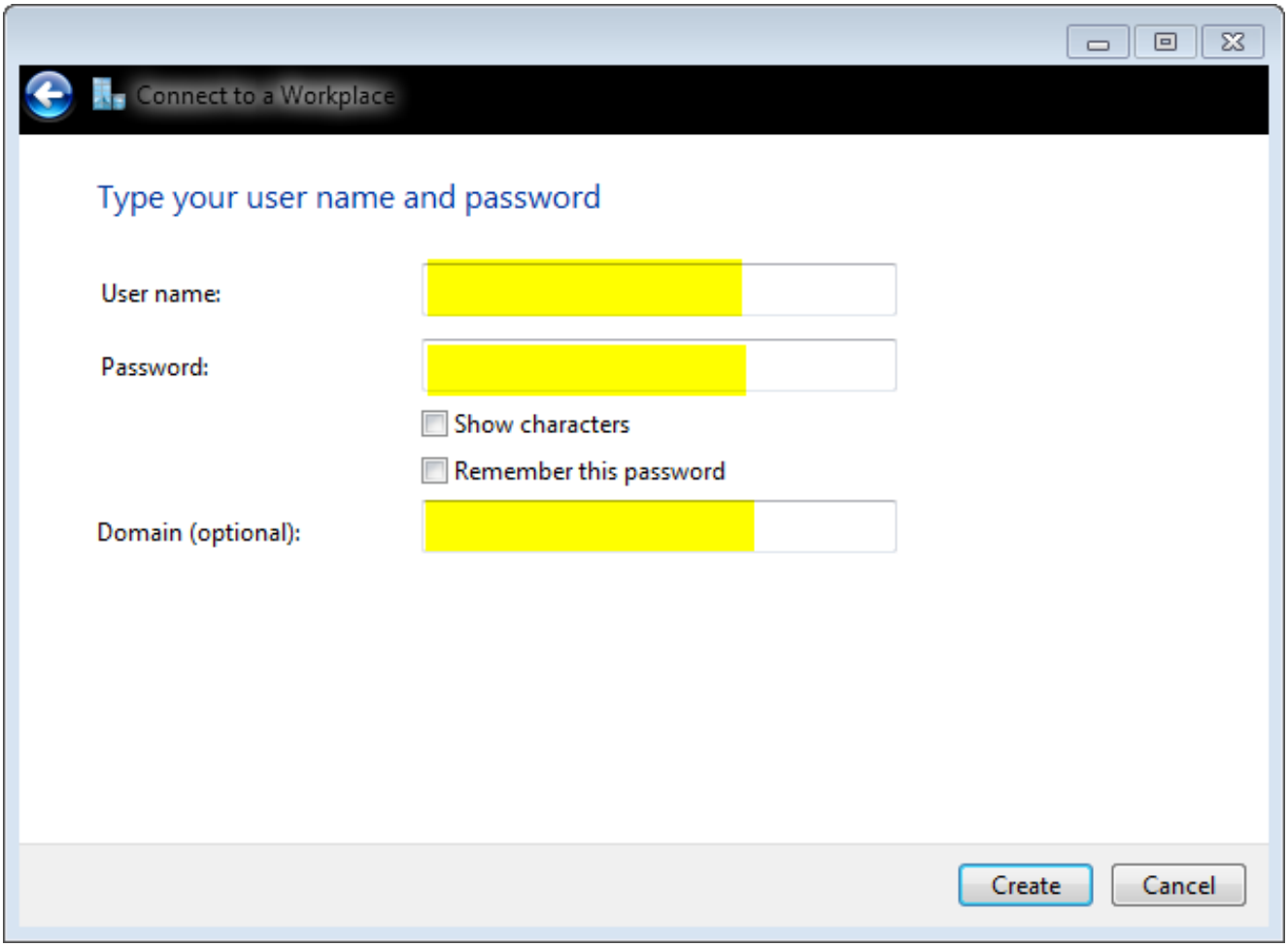



3. Insira o nome de domínio totalmente qualificado (FQDN) ou o endereço IP do servidor IKEv2 e atribua a ele um nome de destino para identificá-lo localmente.

   **Note**: O FQDN deve corresponder ao Common Name (CN) do certificado de identidade do roteador. O Windows 7 descarta a conexão com um erro 13801 se detectar uma incompatibilidade.
   Como parâmetros adicionais precisam ser definidos, marque **Não conectar agora; basta configurá-lo para que eu possa conectar mais tarde** e clicar em **Avançar**:

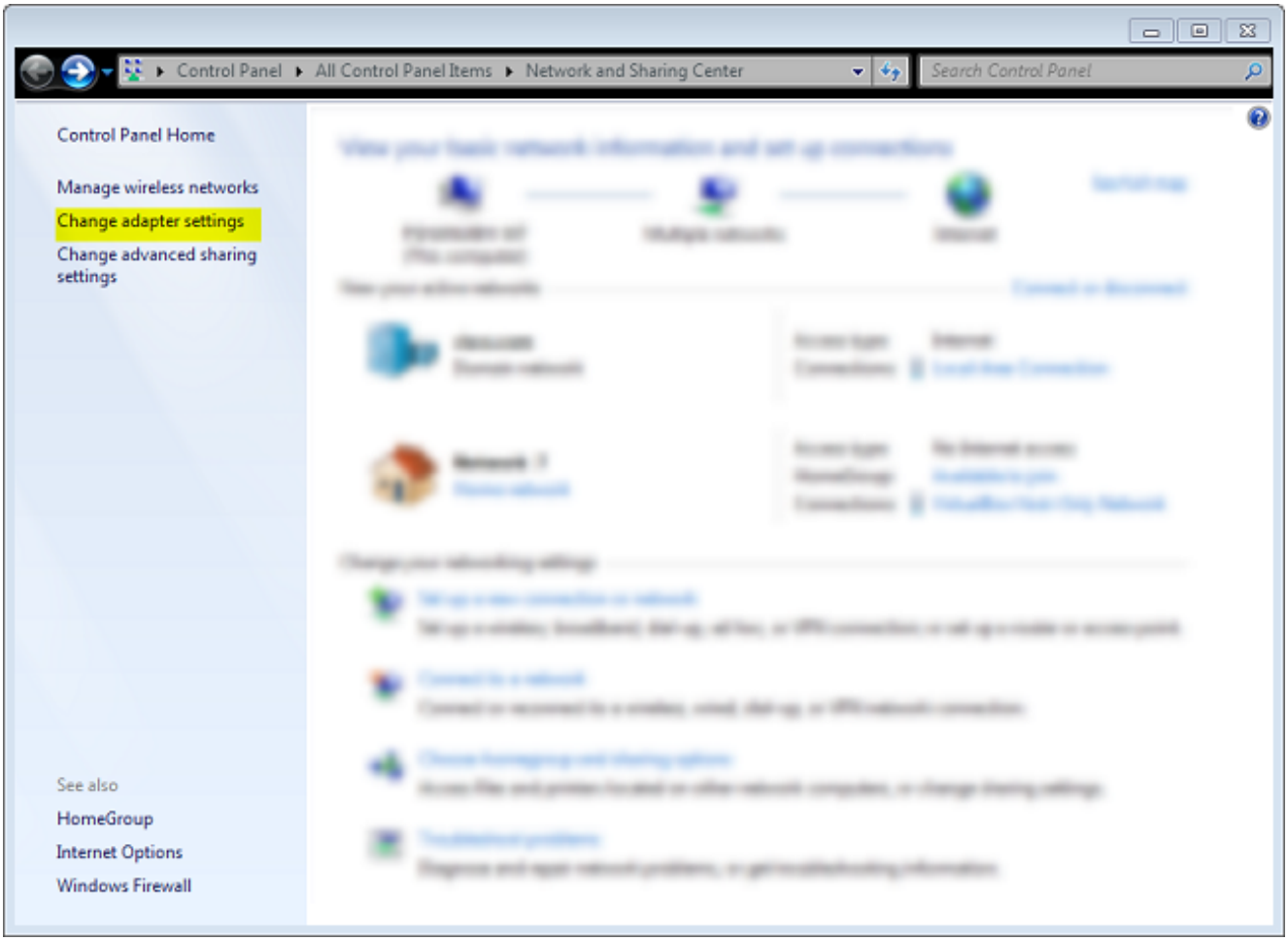



4. Não preencha os campos **Nome de usuário**, **Senha** e **Domínio (opcional)** porque a Autenticação de certificado deve ser usada. Clique em **Criar**.



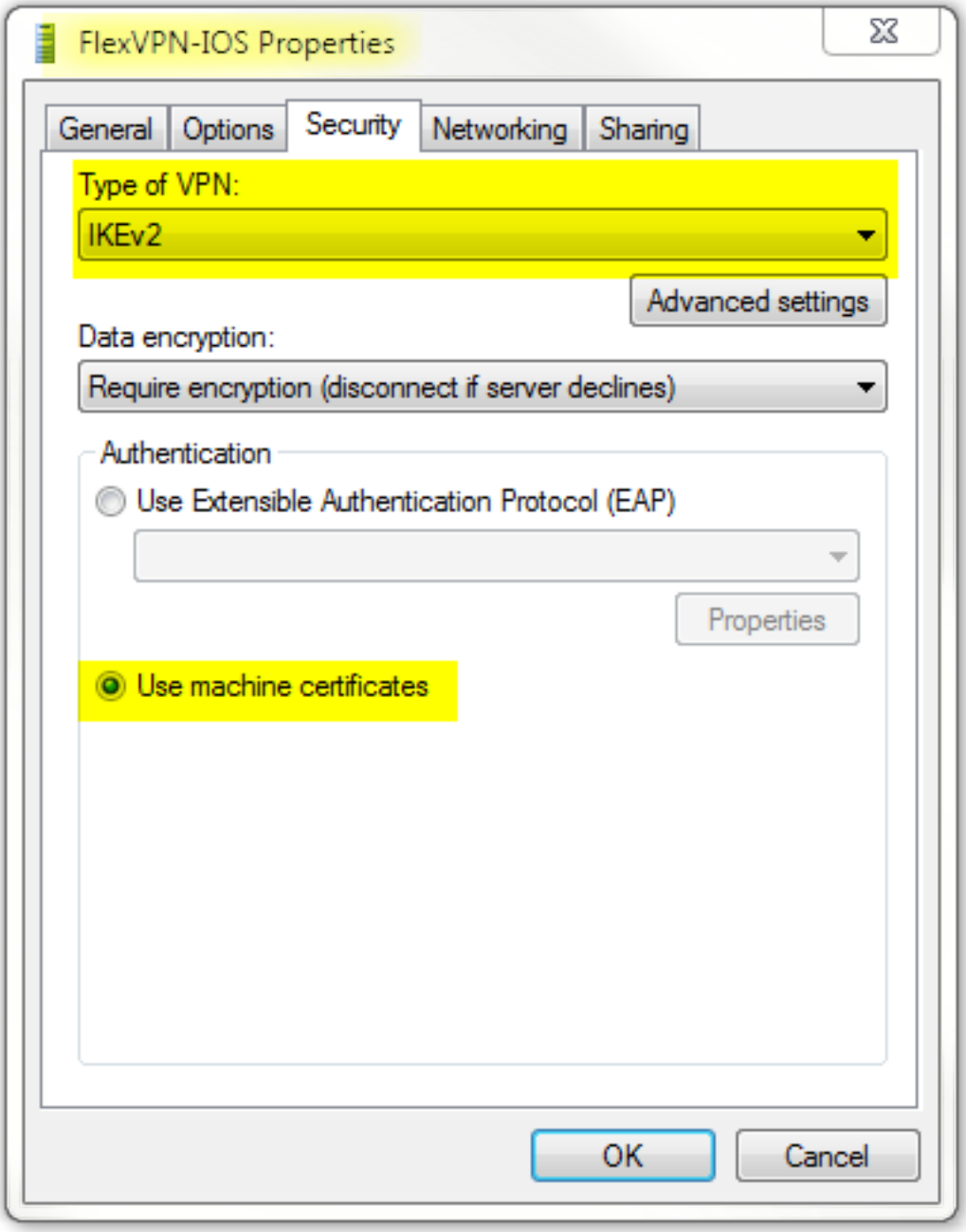

**Note**: Feche a janela resultante. **Não tente se conectar.**

5. Volte para a **Central de Rede e Compartilhamento** e clique em **Alterar configurações do adaptador**.




6. Escolha o Adaptador lógico FlexVPN-IOS, que é o resultado de todas as etapas realizadas até este ponto. Clique em suas propriedades. Estas são as propriedades do perfil de conexão recém-criado chamado FlexVPN-IOS:

   Na guia Security (Segurança), o tipo de VPN deve ser IKEv2.Na seção Autenticação, escolha **Usar certificados da máquina**.




O perfil FlexVPN-IOS agora está pronto para ser conectado depois que você importar um certificado para o repositório de certificados da máquina.

## Obter certificado do cliente

O certificado do cliente requer estes fatores:

- O certificado do cliente tem um EKU de 'Autenticação do cliente'. Além disso, a CA fornece um 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
```

## Detalhes importantes

- 'Intermediário IKE IPSec' (OID = 1.3.6.1.5.5.8.2.2) deve ser usado como EKU se ambas as afirmações se aplicarem:

  O servidor IKEv2 é um servidor Windows 2008.Há mais de um Certificado de Autenticação de Servidor em uso para conexões IKEv2. Se isso for verdade, coloque EKU 'Autenticação de servidor' e EKU 'IKE intermediário IPSec' em um certificado ou distribua esses EKUs entre os certificados. Certifique-se de que pelo menos um certificado contenha EKU 'IKE Intermediário IPSec'.

  Consulte Troubleshooting de Conexões VPN IKEv2 para obter mais informações.

- Em uma implantação FlexVPN, não use 'IPSec IKE Intermediate' em EKU. Se você fizer isso, o cliente IKEv2 não recolherá o certificado do servidor IKEv2. Como resultado, eles não podem responder ao CERTREQ do IOS na mensagem de resposta IKE_SA_INIT e, portanto, não conseguem se conectar com um ID de erro 13806.

- Embora o nome alternativo do assunto (SAN) não seja necessário, é aceitável que os certificados tenham um.

- No Windows 7 Client Certificate Store, certifique-se de que o Machine-Trusted Root Certificate Authority Store tenha o menor número possível de certificados. Se tiver mais de 50 ou mais, o Cisco IOS pode não conseguir ler a carga do Cert_Req inteira, que contém o Nome distinto do certificado (DN) de todas as CAs conhecidas da caixa do Windows 7. Como resultado, a negociação falha e você vê o tempo limite da conexão no cliente.

# Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A ferramenta Output Interpreter (exclusiva para clientes registrados) é compatível com alguns comandos de exibição.. Use a ferramenta Output Interpreter para visualizar uma análise do resultado gerado pelo 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

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

# Informações Relacionadas

- Depurações do ASA IKEv2 para VPN site a site com PSKs TechNote
- ASA IPsec e IKE debugs (modo principal IKEv1) - Nota técnica de solução de problemas
- IOS IPSec e depurações IKE - IKEv1 Main Mode Troubleshooting TechNote
- IPSec ASA e depurações de IKE - modo agressivo IKEv1 TechNote
- Dispositivos de segurança adaptáveis Cisco ASA 5500 Series
- Downloads de software dos dispositivos de segurança adaptável Cisco ASA 5500 Series
- Cisco IOS Firewall
- Cisco IOS Software
- Secure Shell (SSH)
- Negociação IPsec/Protocolos IKE
- Suporte Técnico e Documentação - Cisco Systems