IKEv2 com o cliente VPN ágil de Windows 7 IKEv2 e certificado de autenticação em FlexVPN

Índice

Introdução

FlexVPN é a versão 2 nova do intercâmbio de chave de Internet (infraestrutura IKEv2)-based o VPN no ® do Cisco IOS e é significado ser uma solução de VPN unificada. Este documento descreve como configurar o cliente IKEv2 que é construído em Windows 7 a fim conectar um final do cabeçalho do Cisco IOS com a utilização de um Certificate Authority (CA).

> Nota: A ferramenta de segurança adaptável (ASA) apoia agora as conexões IKEv2 com o cliente incorporado de Windows 7 até à data da liberação 9.3(2).

> Nota: Os protocolos SUITE-B não trabalham porque o final do cabeçalho IO não apoia SUITE-B com IKEv1, ou o cliente VPN ágil de Windows 7 IKEv2 não apoia atualmente SUITE-B com IKEv2.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

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

Componentes Utilizados

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

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

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

Configurar

Visão geral

Há quatro etapas principal na configuração do cliente IKEv2 incorporado de Windows 7 a fim conectar um final do cabeçalho do Cisco IOS com a utilização de CA:

1. Configurar CA

   CA deve permitir que você encaixe o uso chave prolongado exigido (EKU) no certificado. Por exemplo, no server IKEv2, do “o AUTH EKU server” está exigido, quando o certificado de cliente precisar do “o AUTH EKU cliente.” As disposições locais podem utilizar:Server de CA do Cisco IOS - Os certificados auto-assinados não podem ser usados devido ao erro CSCuc82575.Server de CA do OpenSSLMicrosoft CA server - Geralmente, esta é a opção preferida porque pode ser configurado para assinar exatamente o certificado como desejado.

2. Configurar o final do cabeçalho do Cisco IOS

Obtenha um certificadoConfigurar IKEv2

3. Configurar o cliente do acessório de Windows 7
4. Obtenha o certificado de cliente

Cada um destas etapas principal é explicada em detalhe nas seções subsequente.

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

Configurar o Certificate Authority

Este documento não fornece etapas detalhadas em como estabelecer CA. Contudo, as etapas nesta seção mostram-lhe como configurar CA assim que pode emitir Certificados para este tipo do desenvolvimento.

OpenSSL

O OpenSSL CA é baseado no arquivo da “configuração”. O arquivo da “configuração” para o server do OpenSSL deve ter:

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

Server de CA do Cisco IOS

Se você usa um server de CA do Cisco IOS, certifique-se que você usa o Cisco IOS Software Release o mais recente, que atribui o 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 o final do cabeçalho do Cisco IOS

Obtenha um certificado

O certificado deve ter os campos EKU ajustados à “autenticação de servidor” para o Cisco IOS e a “authenticação do cliente” para o cliente. Tipicamente, mesmo CA é usado para assinar ambos os Certificados de cliente e servidor. Neste caso, a “autenticação de servidor” e a “authenticação do cliente” são consideradas no certificado de servidor e no certificado de cliente respectivamente, que é aceitável.

Se CA emite os Certificados nos padrões da criptografia de chave pública (PKCS) #12 formatam no server IKEv2 aos clientes e no server, e se o Certificate Revocation List (CRL) não está alcançável ou disponível, devem 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
```

Incorpore este comando a fim importar o certificado do 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 automóvel do server de CA do Cisco IOS concede Certificados, o server IKEv2 deve ser configurado com o server URL de CA a fim receber um certificado segundo as indicações deste exemplo:

```
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.
```

Quando o ponto confiável é configurado, você precisa:

1. Autentique CA com 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. Registre o server IKEv2 com CA com 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.
   ```

A fim ver se o certificado contém todas as opções requerida, use 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
```

Configurar IKEv2

Este é um exemplo da configuração IKEv2:

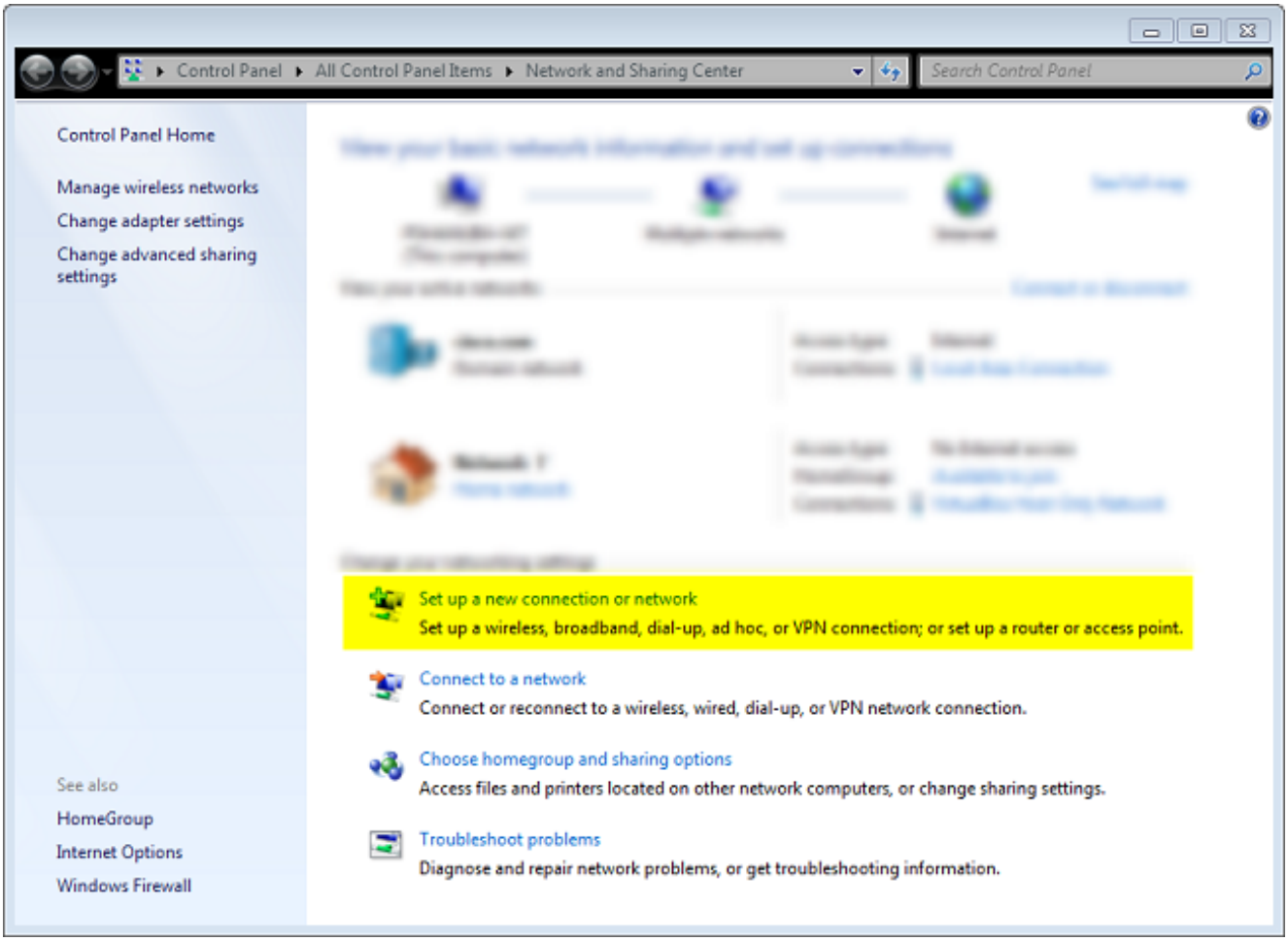
```
ikev2#show crypto pki cert verbose
Certificate
  <snip>
 Issuer:
   <snip>
 Subject:
   Name: ikev2.cisco.com
   ou=TAC
   o=Cisco
   c=BE
   cn=ikev2.cisco.com
<snip>
 Subject Key Info:
   Public Key Algorithm: rsaEncryption
   RSA Public Key: (1024 bit)
 Signature Algorithm: MD5 with RSA Encryption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

O IP unnumbered do virtual-molde deve ser qualquer coisa endereço local do exceptthe usado para a conexão 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.]

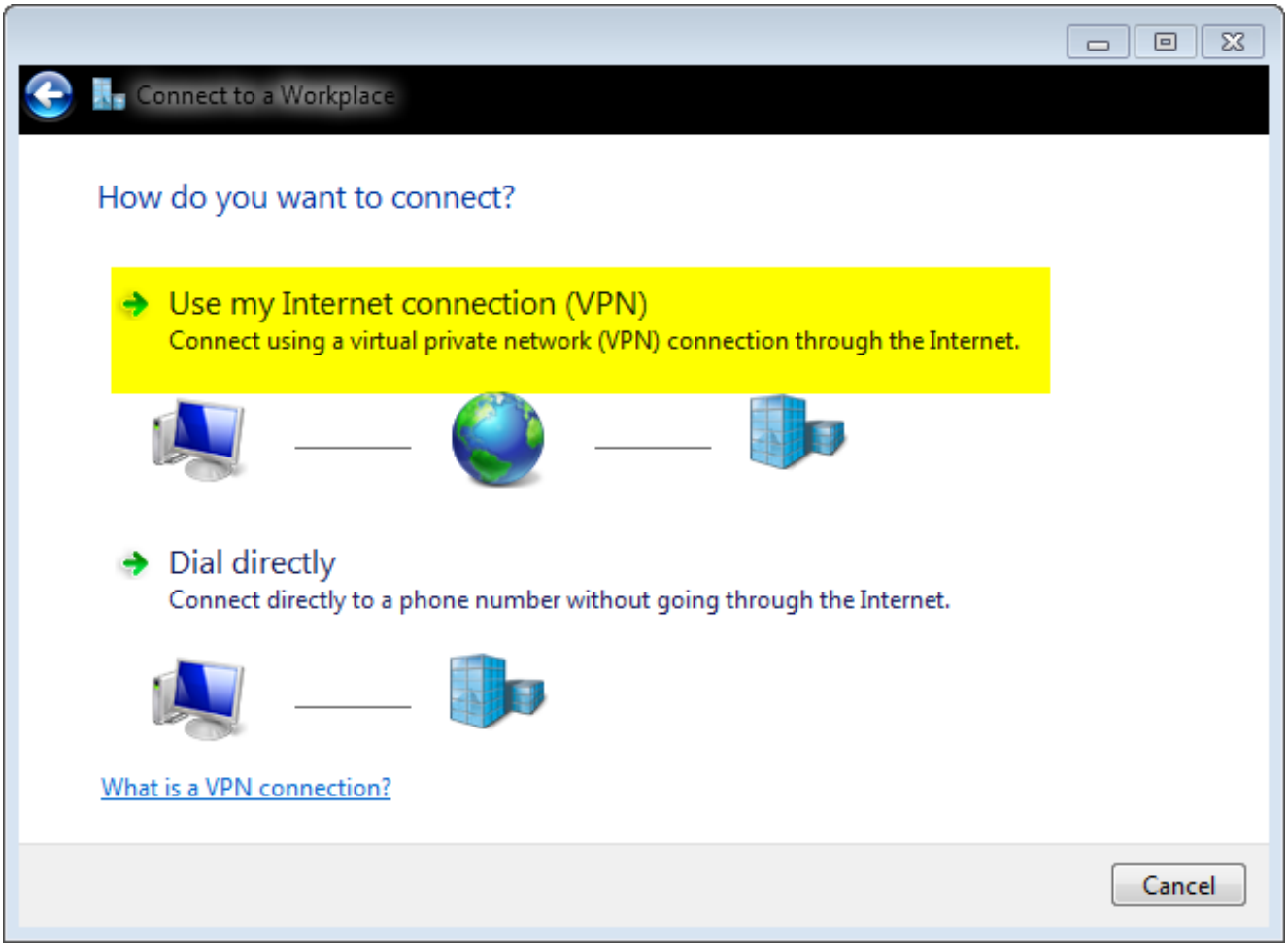
Configurar o cliente do acessório de Windows 7

Este procedimento descreve como configurar o cliente do acessório de Windows 7.

1. Navegue à **rede e centro da partilha**, e clique **estabelece uma nova conexão ou uma rede**.

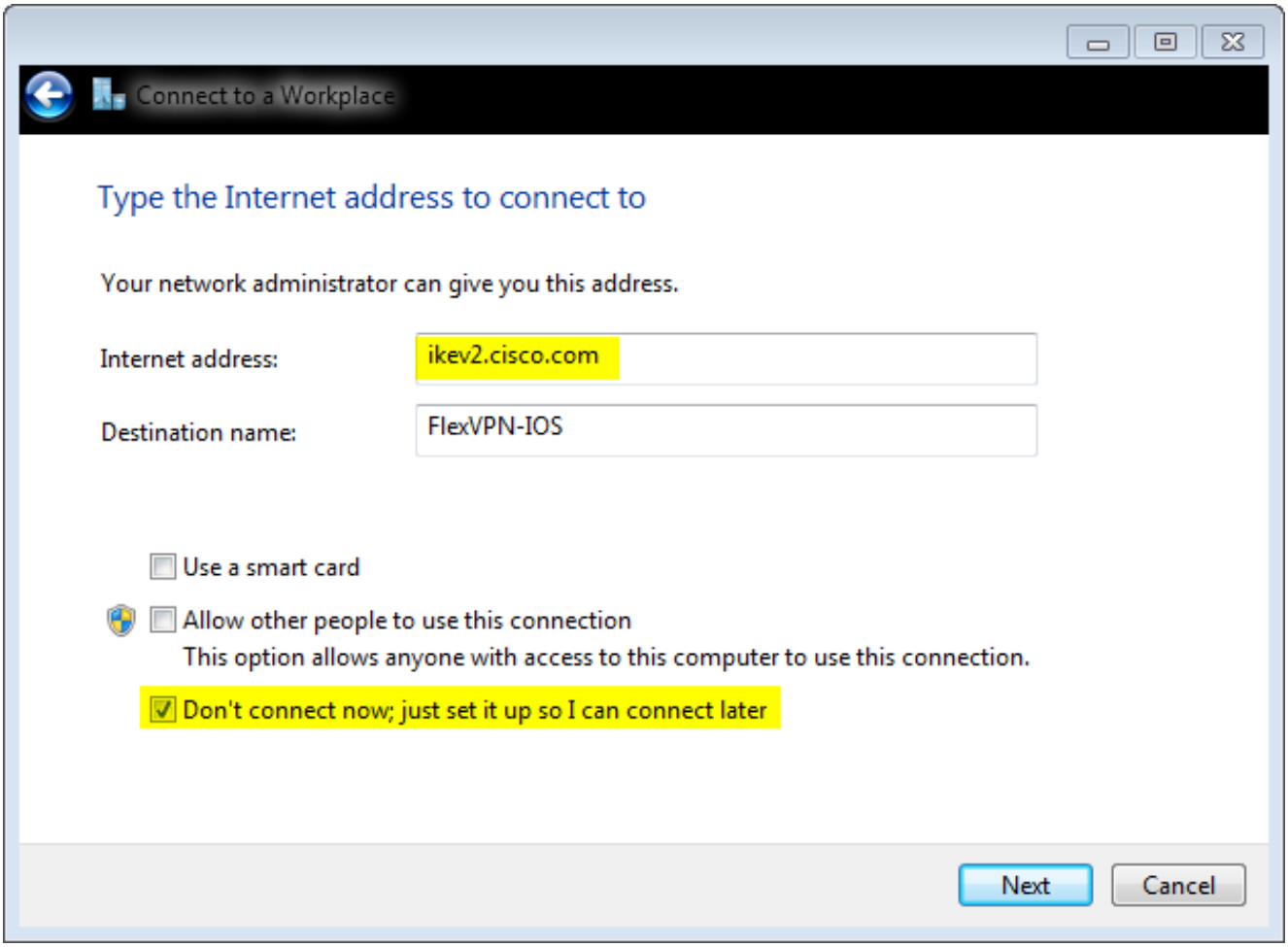


2. Clique o **uso minha conexão com o Internet (VNP)**. Isto permite que você setup uma conexão de VPN negociada sobre uma conexão com o Internet atual.

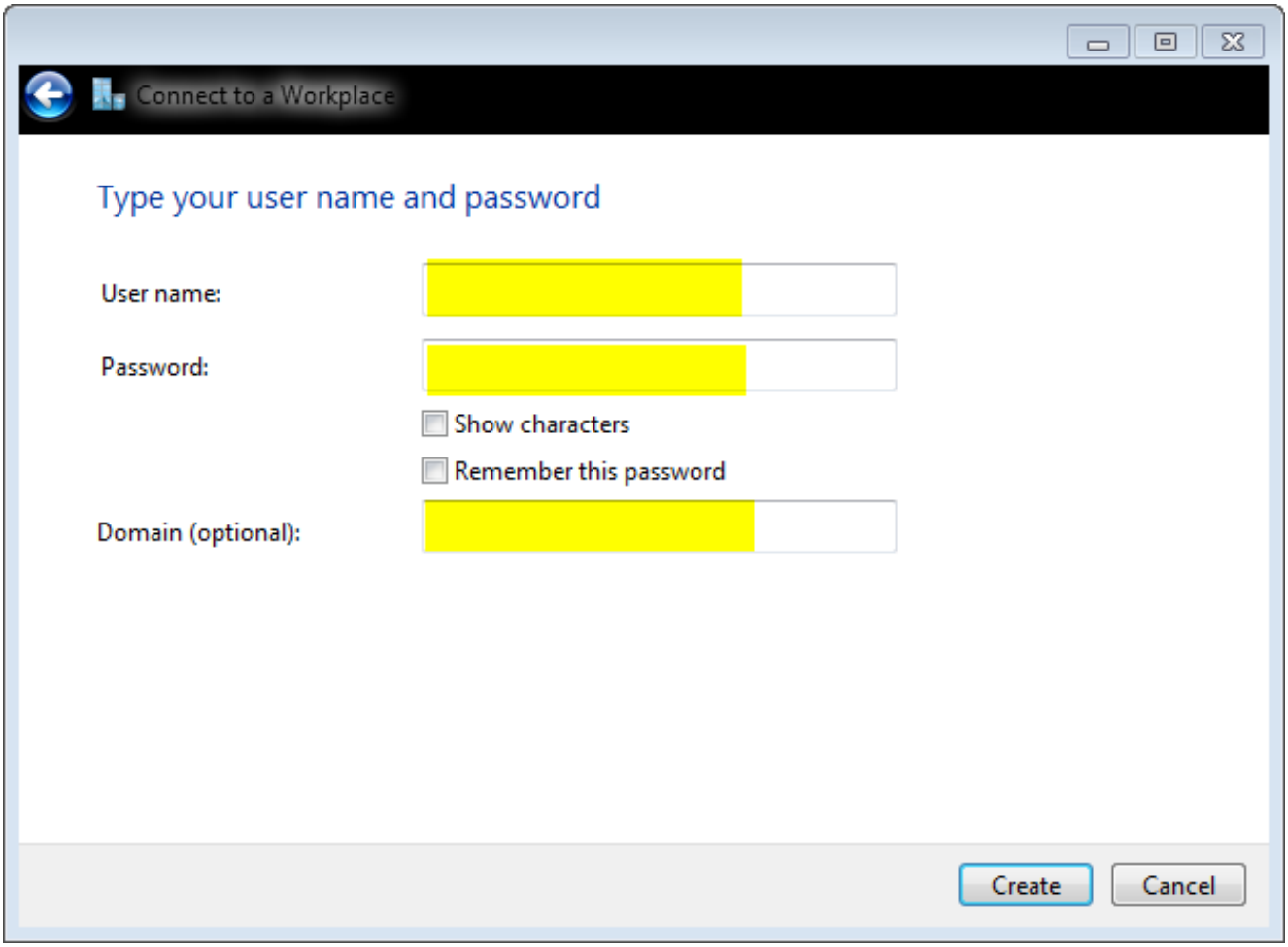


3. Incorpore o nome de domínio totalmente qualificado (FQDN) ou o endereço IP de Um ou Mais Servidores Cisco ICM NT do server IKEv2, e dê-lhe um nome do destino para identificá-lo localmente.

   Nota: O FQDN deve combinar o Common Name (CN) do certificado de identidade do roteador. Windows 7 deixa cair a conexão com um erro 13801 se detecta uma má combinação.
   Porque os parâmetros adicionais precisam de ser ajustados, a verificação **não conecta agora; apenas ajustado a acima assim eu posso conectar mais tarde**, e clico **em seguida**:

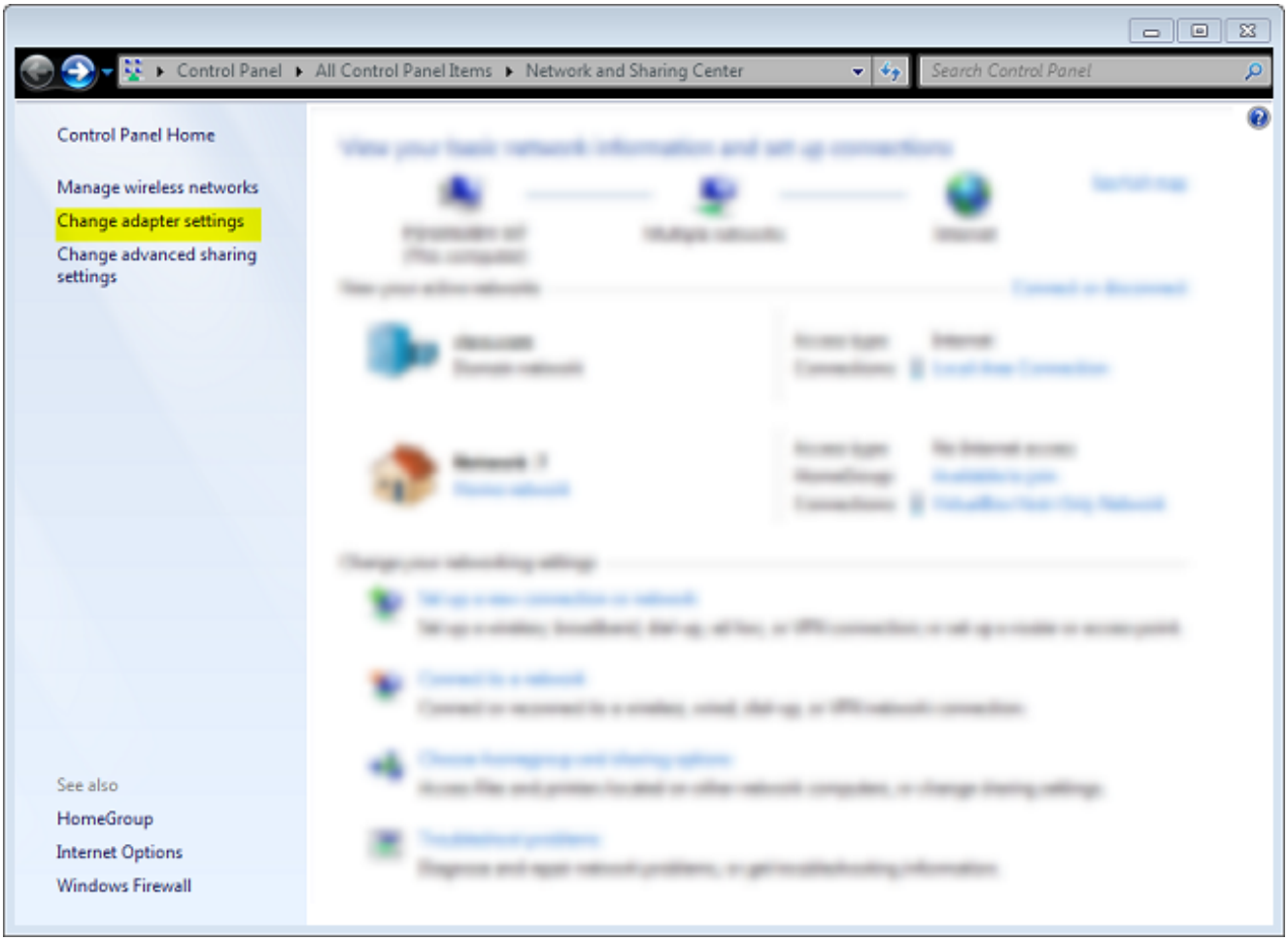


4. Não preencha os campos **(opcionais) do nome de usuário**, da **senha** e do **domínio** porque o certificado de autenticação deve ser usada. O clique **cria**.



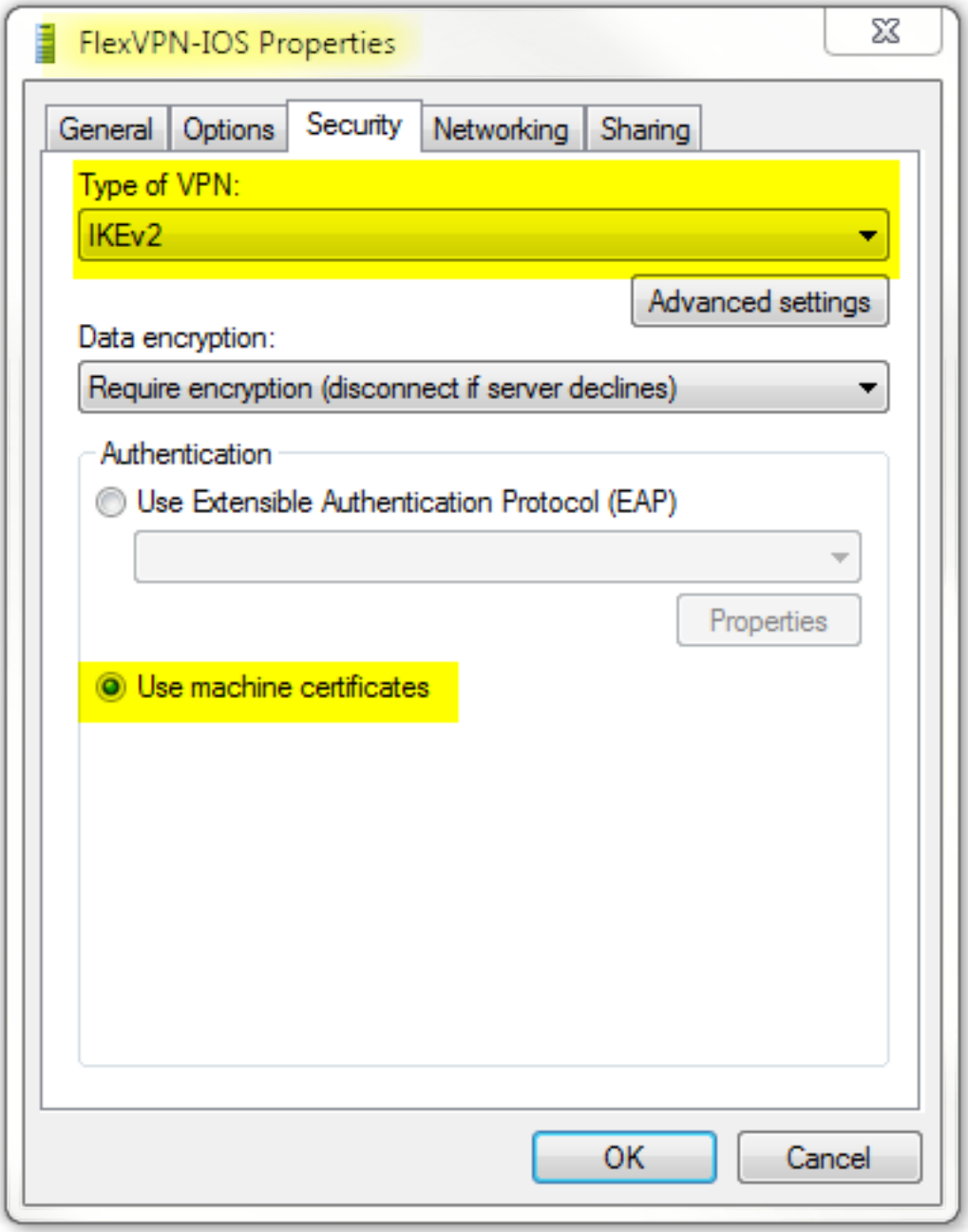
Nota: Feche o indicador resultante. **Não tente conectar.**

5. Navegue de volta à **rede e centro da partilha**, e clique **ajustes do adaptador da mudança**.



6. Escolha o adaptador lógico FlexVPN-IO, que é o resultado de todas as etapas tomadas a este ponto. Clique suas propriedades. Estas são as propriedades do perfil de conexão recém-criado chamado FlexVPN-IO:

   Na ABA de segurança, o tipo de VPN deve ser IKEv2.Na seção da autenticação, escolha **certificados da máquina do uso**.



O perfil FlexVPN-IO está agora pronto para ser conectado depois que você importou um certifcate à loja do certificado da máquina.

Obtenha o certificado de cliente

O certificado de cliente exige estes fatores:

- O certificado de cliente tem um EKU da “authenticação do cliente”. Também, CA dá um certificado do 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
```

Detalhes importantes

- Do “o intermediário IPsec IKE” (OID = 1.3.6.1.5.5.8.2.2) deve ser usado como o EKU se both

of these indicações se aplicam:

O server IKEv2 é um server de Windows 2008.Há mais de um certificado de autenticação de servidor no uso para as conexões IKEv2. Se isto é verdadeiro, um ou outro lugar "autenticação de servidor" EKU e o "IPsec IKE" EKU intermediário em um certificado, ou distribuem estes EKU entre os Certificados. Certifique-se que pelo menos um certificado contém o "IPsec IKE" EKU intermediário.

Refira a pesquisa de defeitos de IKEv2 VPN Connectionsfor mais informação.

- Em um desenvolvimento de FlexVPN, não use do "o intermediário IPsec IKE" no EKU. Se você faz, o cliente IKEv2 não pegara o certificado de servidor IKEv2. Em consequência, não podem responder a CERTREQ dos IO no mensagem de resposta IKE_SA_INIT e assim não conectam com 13806 um erro ID.

- Quando o nome alternativo sujeito (SAN) não for exigido, é aceitável se os Certificados têm um.

- Na loja do certificado de cliente de Windows 7, certifique-se de que a loja Máquina-confiada das autoridades do certificado de raiz tem menos número de Certificados possíveis. Se tem mais do que 50 pés ou assim, o Cisco IOS pôde não lê o payload inteiro de Cert_Req, que contém o nome destacado (DN) do certificado de todos os CA conhecidos da caixa de Windows 7. Em consequência, a negociação falha e você vê o intervalo de conexão no cliente.

Verificar

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

A ferramenta Output Interpreter (clientes registrados somente) apoia determinados comandos de exibição. Use a ferramenta Output Interpreter a fim ver uma análise do emissor de comando de execução.

```
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

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

Informações Relacionadas

- O ASA IKEv2 debuga para o VPN de Site-para-Site com PSK TechNote
- O IPsec ASA e o IKE debugam (modo principal IKEv1) pesquisar defeitos TechNote
- O IPsec IO e o IKE debugam - Modo principal IKEv1 que pesquisa defeitos TechNote
- O IPsec ASA e o IKE debugam - IKEv1 modo assertivo TechNote
- Cisco ASA 5500 Series Adaptive Security Appliances
- Downloads do software do Dispositivos de segurança adaptáveis Cisco ASA série 5500
- Cisco IOS Firewall
- Cisco IOS Software
- Secure Shell (SSH)
- Negociação IPsec/Protocolos IKE
- Suporte Técnico e Documentação - Cisco Systems