FlexVPN での Windows 7 IKEv2 Agile VPN Client による IKEv2 と証明書認証

目次

概要

FlexVPN は、Cisco IOS® での新しい Internet Key Exchange version 2（IKEv2）ベースの VPN インフラストラクチャであり、統合された VPN ソリューションとなります。 このドキュメントでは、Cisco IOS ヘッドエンドを認証局（CA）の使用率と接続するために Windows 7 に組み込まれている IKEv2 クライアントを設定する方法について説明します。

> **注:** 現在、適応型セキュリティ アプライアンス（ASA）では、リリース 9.3(2) から Windows 7 組み込みクライアントを使用して IKEv2 接続をサポートしています。

> **注:** SUITE-B のプロトコルは、IOS ヘッドエンドが IKEv1 を使用した SUITE-B をサポートしていないため、つまり、現在 Windows 7 IKEv2 の俊敏な VPN クライアントが IKEv2 を使用した SUITE-B をサポートしていないため、機能しません。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Windows 7 組み込み VPN クライアント
- Cisco IOS ソフトウェア リリース 15.2(2)T
- 認証局 - OpenSSL CA

使用するコンポーネント

このドキュメントの情報は、次のハードウェアとソフトウェアのバージョンに基づくものです。

- Windows 7 組み込み VPN クライアント
- Cisco IOS ソフトウェア リリース 15.2(2)T
- 認証局 - OpenSSL CA

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

設定

概要

Cisco IOS ヘッドエンドを CA の使用率と接続するための Windows 7 組み込み IKEv2 クライアントの設定では、主に 4 つの手順があります。

1. CA の設定

   CA を使用すると、必要なキーの拡張用途（EKU）を証明書に埋め込むことができます。 たとえば、IKEv2 サーバで、「サーバ認証 EKU」が必要である一方、クライアント証明書で「クライアント認証 EKU」が必要です。 ローカル展開では、以下を使用できます。Cisco IOS CA サーバ：自己署名証明書は、Bug CSCuc82575 により使用できません。OpenSSL CA サーバMicrosoft CA Server：一般に、必要に応じて証明書を正確に署名するように設定できるため、これが推奨されます。

2. Cisco IOS ヘッドエンドの設定

   証明書の取得IKEv2 の設定

3. Windows 7 組み込みクライアントの設定
4. クライアント証明書の取得

これらの主な手順についてそれぞれ、次のセクションで詳しく説明します。

> **注:** このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

認証局の設定

このドキュメントでは、CA のセットアップ方法の詳細な手順については説明しません。 ただし、このセクションの手順は、CA の設定方法を示すため、このような展開で証明書を発行することができます。

OpenSSL

OpenSSL CA は「config」ファイルに基づいています。 OpenSSL サーバの「config」ファイルの内容は次のようになっています。

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

Cisco IOS CA サーバ

Cisco IOS CA サーバを使用する場合は、EKU を割り当てる最新の Cisco IOS ソフトウェア リリースを使用していることを確認してください。

```
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 ヘッドエンドの設定

証明書の取得

証明書の [EKU] フィールドが、Cisco IOS の場合は「Server Authentication」に、クライアントの場合は「Client Authentication」に設定されている必要があります。 通常、同じ CA を使用して、クライアントとサーバの両方の証明書に署名します。 この場合、「Server Authentication」と「Client Authentication」の両方がそれぞれ、受け入れ可能なサーバ証明書とクライアント証明書に表示されます。

CA が IKEv2 サーバで Public Key Cryptography Standards（PKCS）#12 形式で証明書をクライアントとサーバに発行する場合や、証明書失効リスト（CRL）が到達可能または使用可能でない場合は、証明書を設定する必要があります。

```
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
```

PKCS#12 証明書をインポートするには、次のコマンドを入力します。

```
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.
```

Cisco IOS CA サーバが自動的に証明書を認可する場合、証明書を受信するために、次の例のように IKEv2 サーバを CA サーバ URL で設定する必要があります。

```
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.
```

トラストポイントを設定する際、次の手順を実行する必要があります。

1. 次のコマンドを使用して CA を認証します。

```
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. 次のコマンドを使用して IKEv2 サーバを CA に登録します。

```
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.
```

証明書に必要なすべてのオプションが含まれているかどうかを確認するには、次の **show コマンド**を使用します。

```
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
```

IKEv2 の設定

IKEv2 の設定例を次に示します。

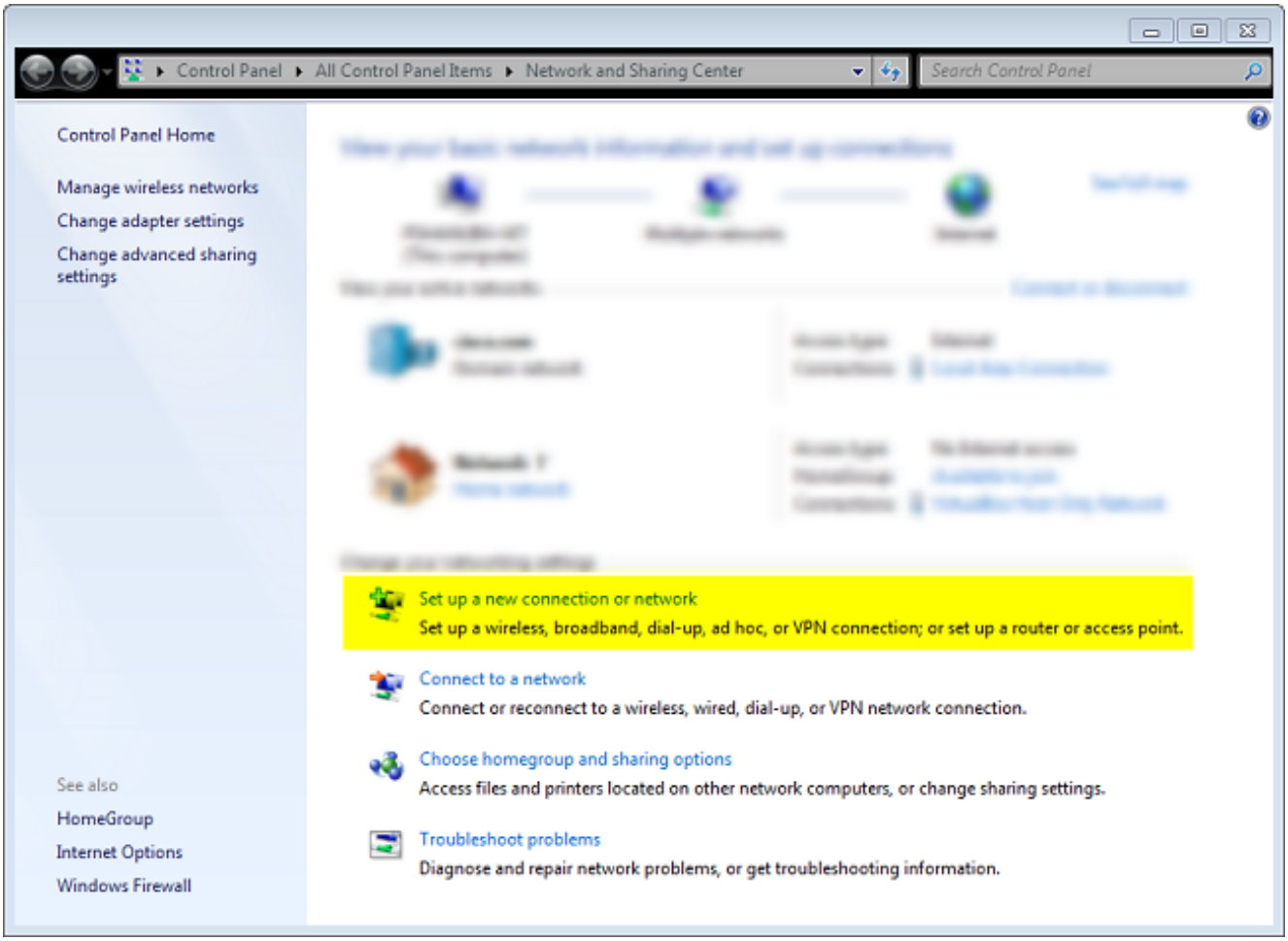
```
ikev2#show crypto pki cert verbose
Certificate
  <snip>
 Issuer:
   <snip>
 Subject:
   Name: ikev2.cisco.com
   ou=TAC
   o=Cisco
   c=BE
   cn=ikev2.cisco.com
<snip>
 Subject Key Info:
   Public Key Algorithm: rsaEncryption
   RSA Public Key: (1024 bit)
 Signature Algorithm: MD5 with RSA Encryption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

virtual-template の IP unnumbered は、IPSec 接続に使用するローカル アドレス以外のアドレスになります。 [ハードウェア クライアントを使用すると、IKEv2 設定ノード経由でルーティング情報を交換するため、ハードウェア クライアントの再帰ルーティングの問題が発生します。]

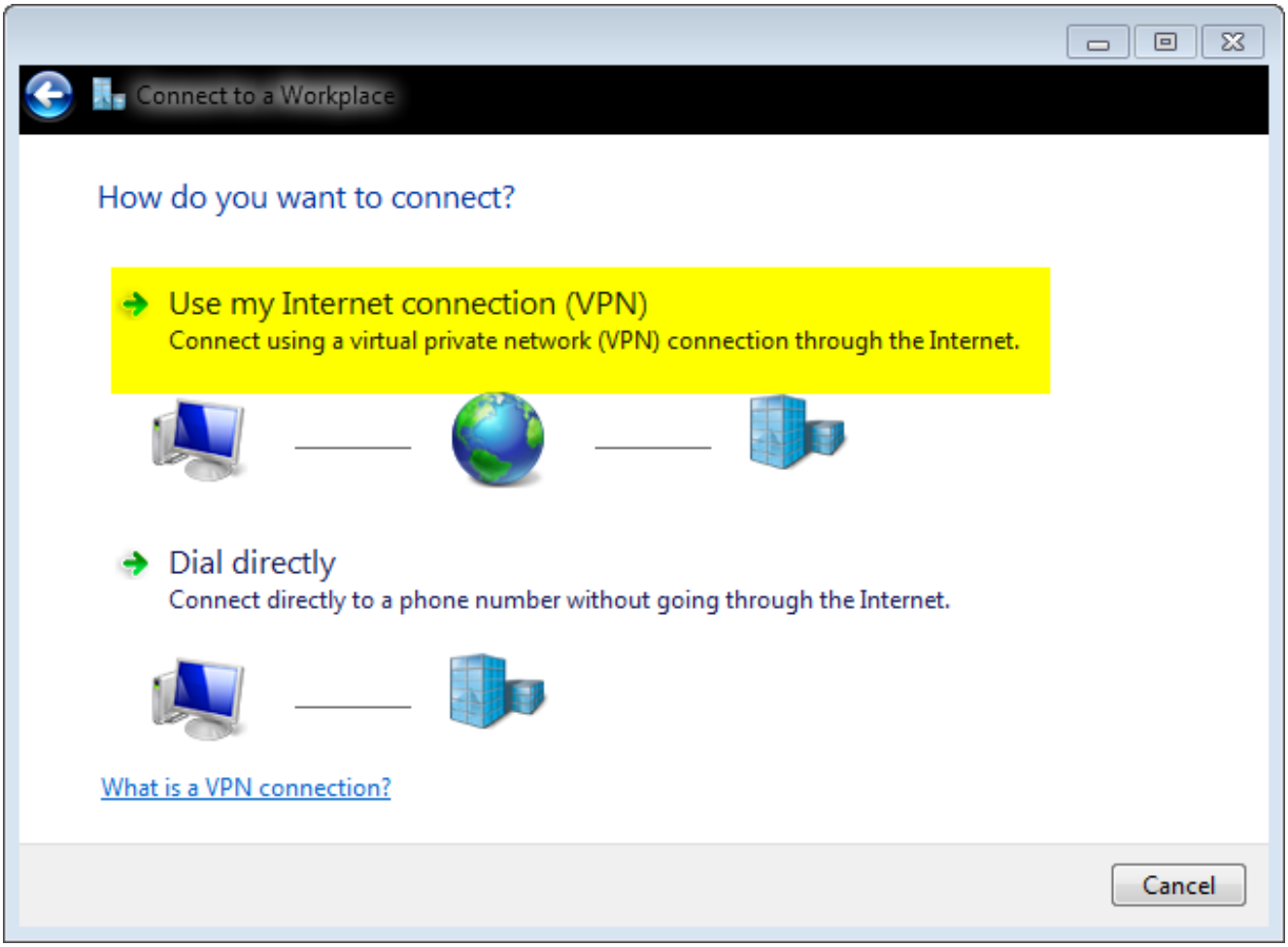
Windows 7 組み込みクライアントの設定

次の手順では、Windows 7 組み込みクライアントを設定する方法について説明します。

1. [Network and Sharing Center] に移動し、[Set up a new connection or network] をクリックします。

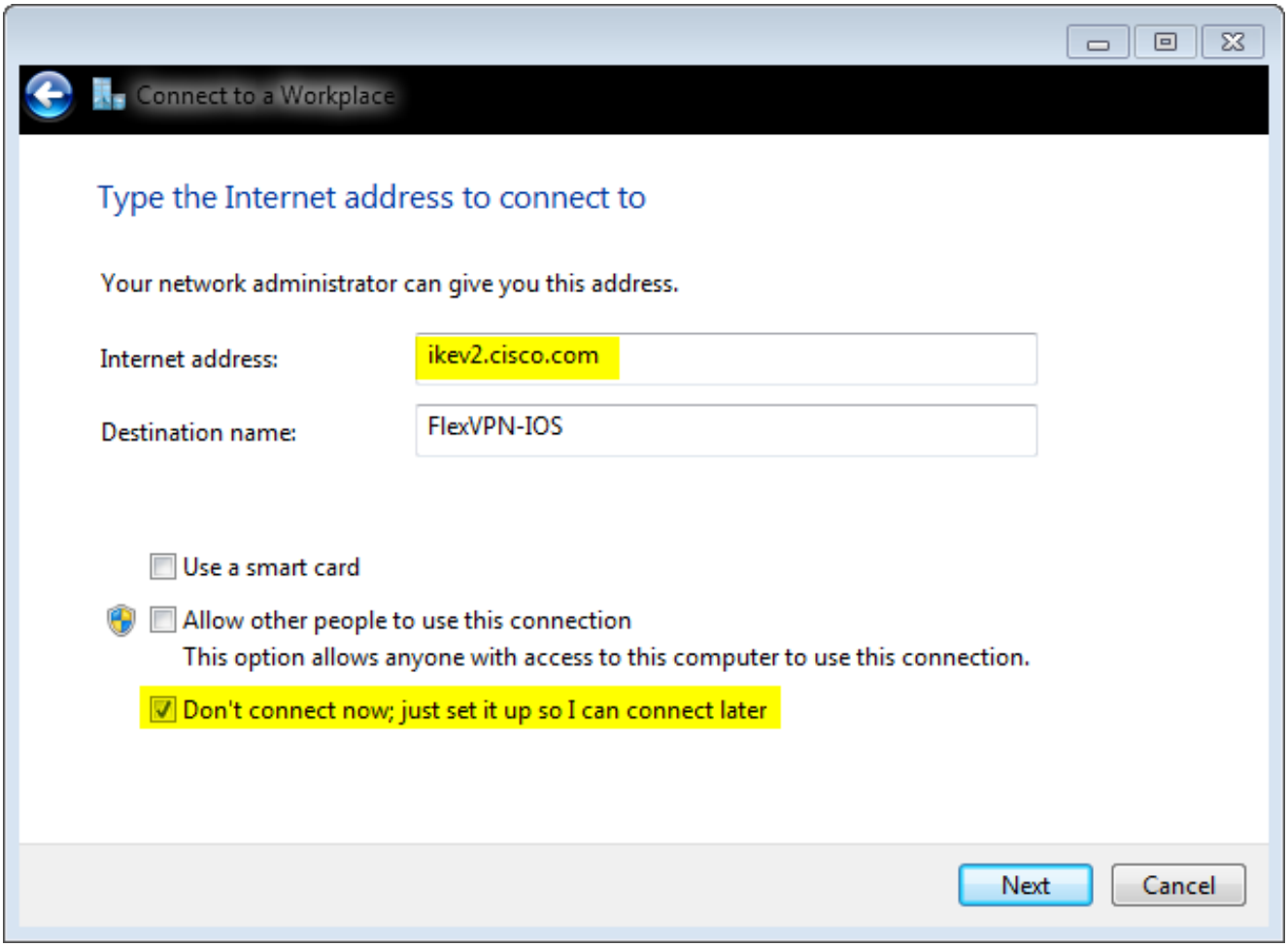


2. [Use my Internet connection (VNP)] をクリックします。 これにより、現在のインターネット接続でネゴシエートされる VPN 接続をセットアップすることができます。

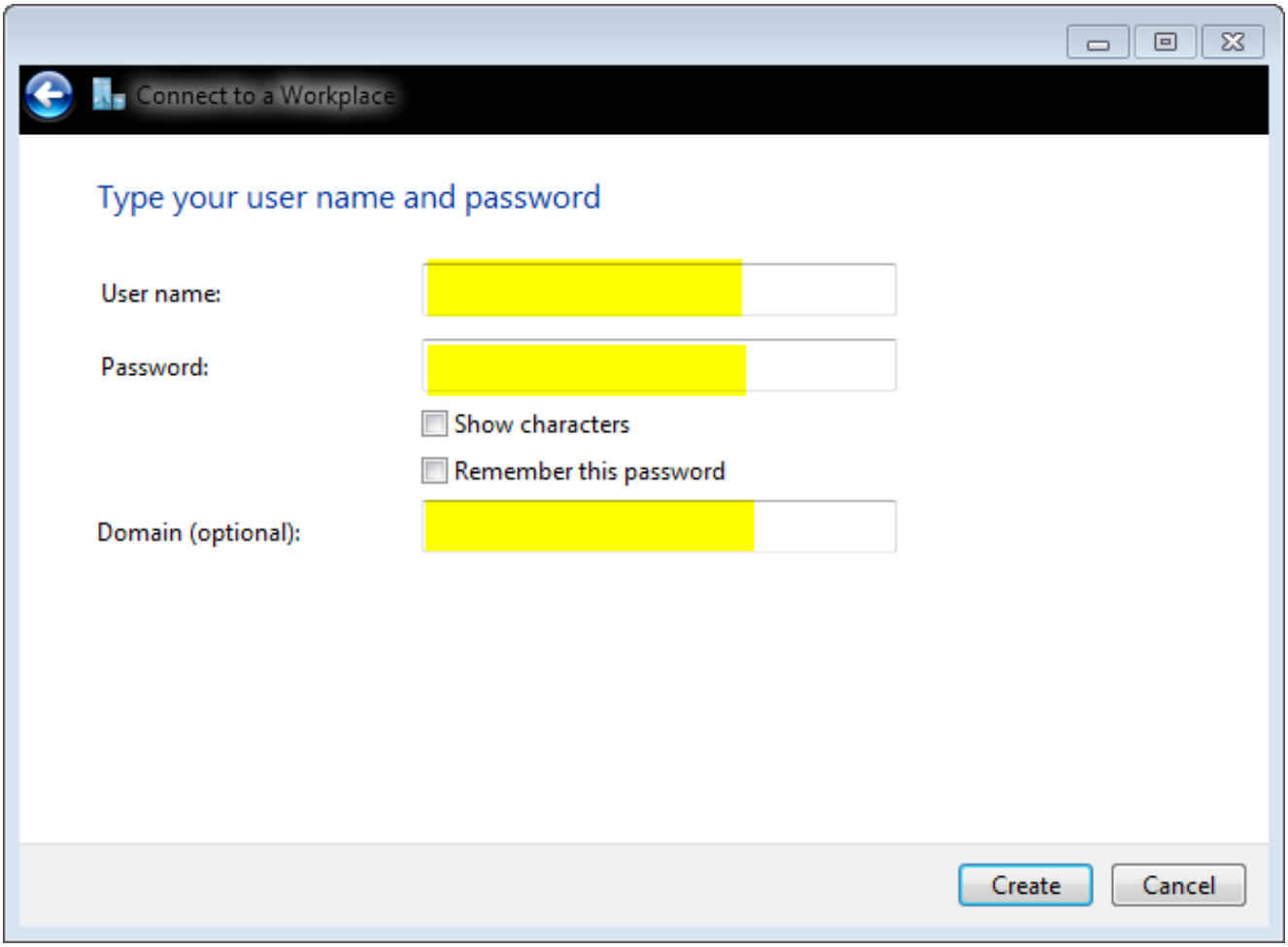


3. IKEv2 サーバの完全修飾ドメイン名（FQDN）または IP アドレスを入力し、それに宛先名を指定してローカルに識別します。

   注: FQDN は、ルータ ID 証明書の Common Name（CN）と一致している必要があります。Windows 7 はミスマッチを検出する場合エラー 13801 の接続を破棄します。
   追加パラメータを設定する必要があるため、[Don't connect now; just set it up so I can connect later] をオンにして [Next] をクリックします。

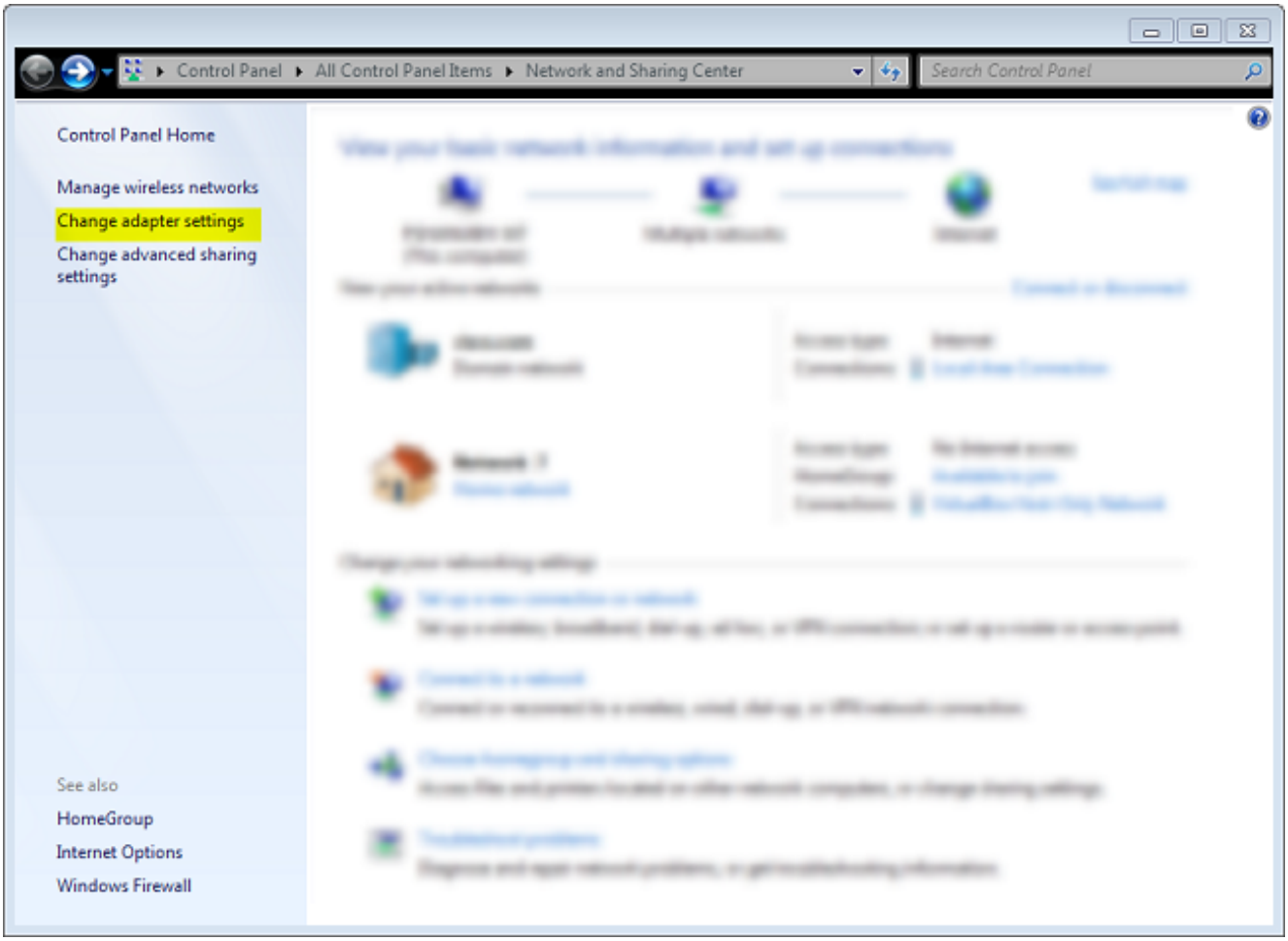


4. 証明書認証を使用するため、[User name]、[Password]、[Domain (optional)] の各フィールドは入力しないでください。 [Create] をクリックします。



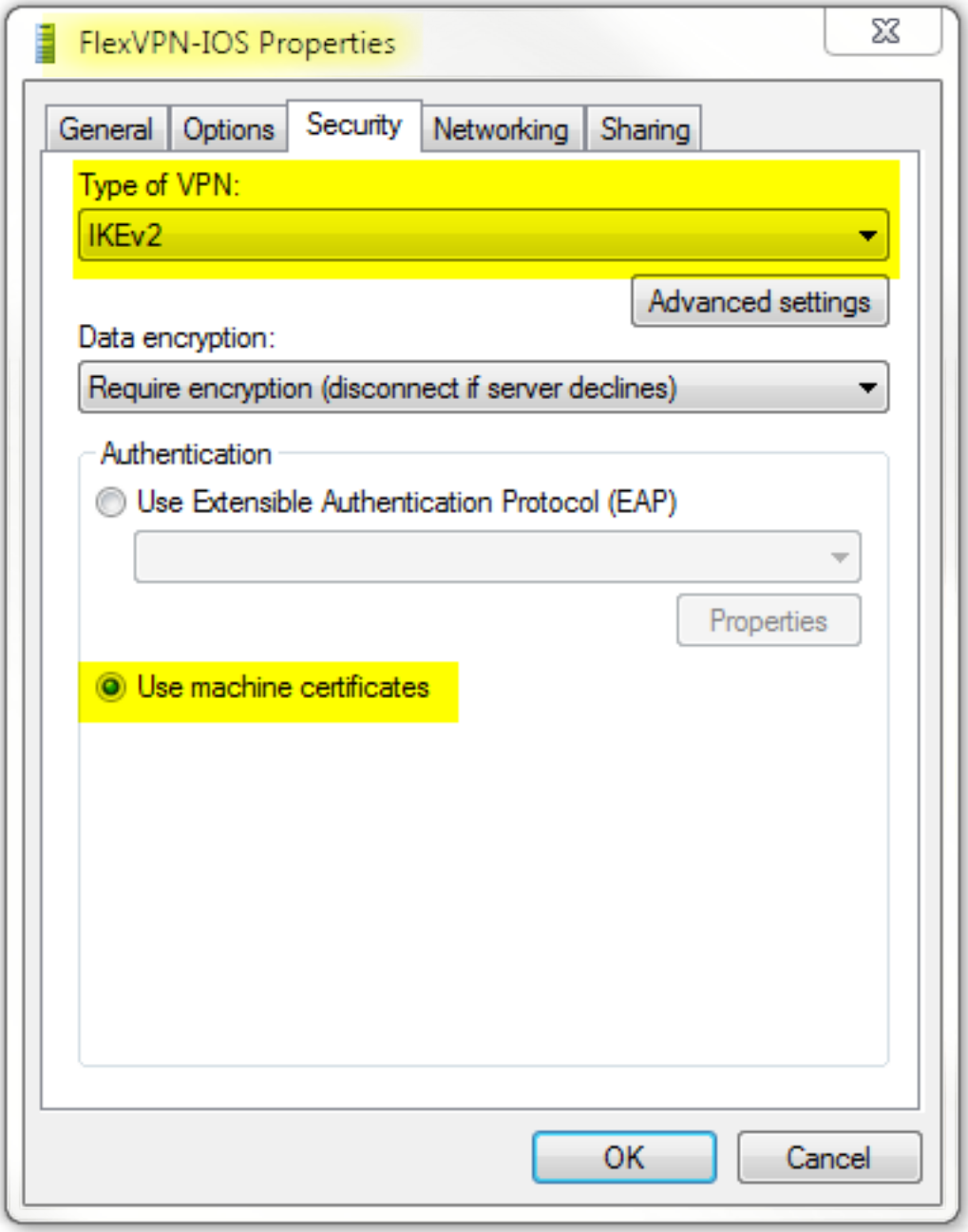
注: 表示されるウィンドウを閉じます。 **接続しないでください。**

5. [Network and Sharing Center] に戻り、[Change adapter settings] をクリックします。



6. [Logical Adapter FlexVPN-IOS] を選択します。これが、このポイントに移動するすべての手順の結果です。 そのプロパティをクリックします。 これらは、FlexVPN IOS と呼ばれる、新たに作成した接続プロファイルのプロパティです。

   [Security] タブで、[Type of VPN] が [IKEv2] になっている必要があります。[Authentication] セクションで、[Use machine certificates] を選択します。



証明書をマシン証明書ストアにインポートした後、FlexVPN IOS プロファイルにできるようになります。

クライアント証明書の取得

クライアント証明書には、次の要素が必要です。

- クライアント証明書に「Client Authentication」の EKU があります。 また、CA は PKCS#12 証明書を提供します。

```
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
```

- CA 証明書：

```
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
```

重要事項

- 次のどちらの内容も当てはまる場合は、「IPSec IKE intermediate」（OID =

1.3.6.1.5.5.8.2.2 ）を EKU として使用する必要があります。

IKEv2 サーバが Windows 2008 Server である。IKEv2 接続で使用中の Server Authentication Certificate が複数ある。 これが当てはまる場合、1 つの証明書に「Server Authentication」の EKU と「IPSec IKE Intermediate」の EKU の両方を配置するか、これらの EKU を証明書間で配布します。 少なくとも 1 つの証明書に「IPSec IKE Intermediate」の EKU が含まれていることを確認します。

詳細については、『IKEv2 VPN 接続のトラブルシューティング』を参照してください。

- FlexVPN の展開では、EKU で「IPSec IKE Intermediate」を使用しないでください。 使用した場合、IKEv2 クライアントで IKEv2 サーバ証明書が取得されません。 その結果、IKE_SA_INIT 応答メッセージで IOS からの CERTREQ に応答できないため、13806 エラー ID で接続が失敗します。

- Subject Alternative Name （ SAN ）は不要ですが、証明書に含まれている場合には受け入れ可能です。

- Windows 7 のクライアント証明書ストアで、[Machine-Trusted Root Certificate Authorities] ストアに可能な証明書の最小数が設定されていることを確認します。 これが 50 程度を超える場合、Cisco IOS で Windows 7 ボックスからの既知のすべての CA の証明書の識別名（ DN ）を含む Cert_Req ペイロード全体の読み取りに失敗する場合があります。 その結果、ネゴシエーションが失敗し、クライアントで接続タイムアウトが表示されます。

確認

ここでは、設定が正常に動作していることを確認します。

特定の show コマンドがアウトプット インタープリタ ツール（登録ユーザ専用）でサポートされています。 show コマンド出力の分析を表示するには、アウトプット インタープリタ ツールを使用します。

```
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:
```

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- PSK によるサイト間 VPN の ASA IKEv2 デバッグ テクニカルノート
- ASA IPsec および IKE のデバッグ（IKEv1 メイン モード）のトラブルシューティング テクニカルノート
- IOS IPSec および IKE のデバッグ（IKEv1 メイン モード）のトラブルシューティング テクニカルノート
- ASA IPSec および IKE デバッグ：IKEv1 アグレッシブ モード テクニカルノート
- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス
- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスのソフトウェア ダウンロード
- Cisco IOS ファイアウォール
- Cisco IOS ソフトウェア
- セキュア シェル（SSH）
- IPSec ネゴシエーション/IKE プロトコル
- テクニカルサポートとドキュメント - Cisco Systems