IKEv2 with Windows 7 IKEv2 Agile VPN Client and Certificate Authentication on FlexVPN

Document ID: 115907

Contributed by Praveena Shanubhogue and Atri Basu, Cisco TAC Engineers.

May 20, 2013

Contents

Introduction

FlexVPN is the new Internet Key Exchange version 2 (IKEv2)−based VPN infrastructure on Cisco IOS® and is meant to be a unified VPN solution. This document describes how to configure the IKEv2 client that is built into Windows 7 in order to connect a Cisco IOS headend with the utilization of a Certificate Authority (CA).

Note: The Adaptive Security Appliance (ASA) now supports IKEv2 connections with the Windows 7 built−in client as of Release 9.3(2).

Note: SUITE−B protocols do not work because the IOS headend does not support SUITE−B with IKEv1, or the Windows 7 IKEv2 Agile VPN client does not currently support SUITE−B with IKEv2.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Windows 7 built−in VPN client
- Cisco IOS Software Release 15.2(2)T
- Certificate Authority − OpenSSL CA

Components Used

The information in this document is based on these hardware and software versions:

- Windows 7 built−in VPN client
- Cisco IOS Software Release15.2(2)T
- Certificate Authority − 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

Refer to Cisco Technical Tips Conventions for information on document conventions.

Configure

Overview

There are four major steps in configuration of the Windows 7 built−in IKEv2 client in order to connect a Cisco IOS headend with the utilization of a CA:

1. Configure CA

   The CA should allow you to embed the required Extended Key Usage (EKU) in the certificate. For example, on the IKEv2 server, 'Server Auth EKU' is required, while the client certificate needs 'Client Auth EKU.' Local deployments can make use of:

   - ♦ Cisco IOS CA server − Self−signed certificates cannot be used because of bug CSCuc82575.
   - ♦ OpenSSL CA server
   - ♦ Microsoft CA server − In general, this is the preferred option because it can be configured to sign the certificate exactly as desired.
2. Configure Cisco IOS headend
   1. Obtain a certificate
   2. Configure IKEv2
3. Configure Windows 7 built−in client
4. Obtain client certificate

Each of these major steps is explained in detail in the subsequent sections.

Note: Use the Command Lookup Tool (registered customers only) in order to obtain more information on the commands used in this section.

Configure Certificate Authority

This document does not provide detailed steps on how to set up a CA. However, the steps in this section show you how to configure the CA so it can issue certificates for this kind of deployment.

OpenSSL

OpenSSL CA is based on the 'config' file. The 'config' file for the OpenSSL server should have:

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

Cisco IOS CA Server

If you use a Cisco IOS CA server, make sure you use the most recent Cisco IOS Software release, which assigns the 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
```

Configure Cisco IOS Headend

Obtain a Certificate

The certificate must have the EKU fields set to 'Server Authentication' for Cisco IOS and 'Client Authentication' for the client. Typically, the same CA is used to sign both the client and server certificates. In this case, both 'Server Authentication' and 'Client Authentication' are seen on the server certificate and client certificate respectively, which is acceptable.

If the CA issues the certificates in Public−Key Cryptography Standards (PKCS) #12 format on the IKEv2 server to the clients and the server, and if the certificate revocation list (CRL) is not reachable or available, it must be configured:

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

Enter this command in order to import the PKCS#12 certificate:

```
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.
```

If a Cisco IOS CA server auto grants certificates, the IKEv2 server must be configured with the CA server URL in order to receive a certificate as shown in this example:

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

When the trustpoint is configured, you need to:

1. Authenticate the CA with this comand:

   ```
   crypto pki authenticate FlexRootCA
   ```

2. Enroll the IKEv2 server with the CA with this command:

```
crypto pki enroll FlexRootCA
```

In order to see if the certificate contains all the required options, use this ***show*** command:

```
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
```

Configure IKEv2

This is an example of IKEv2 configuration:

```
!! 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
```

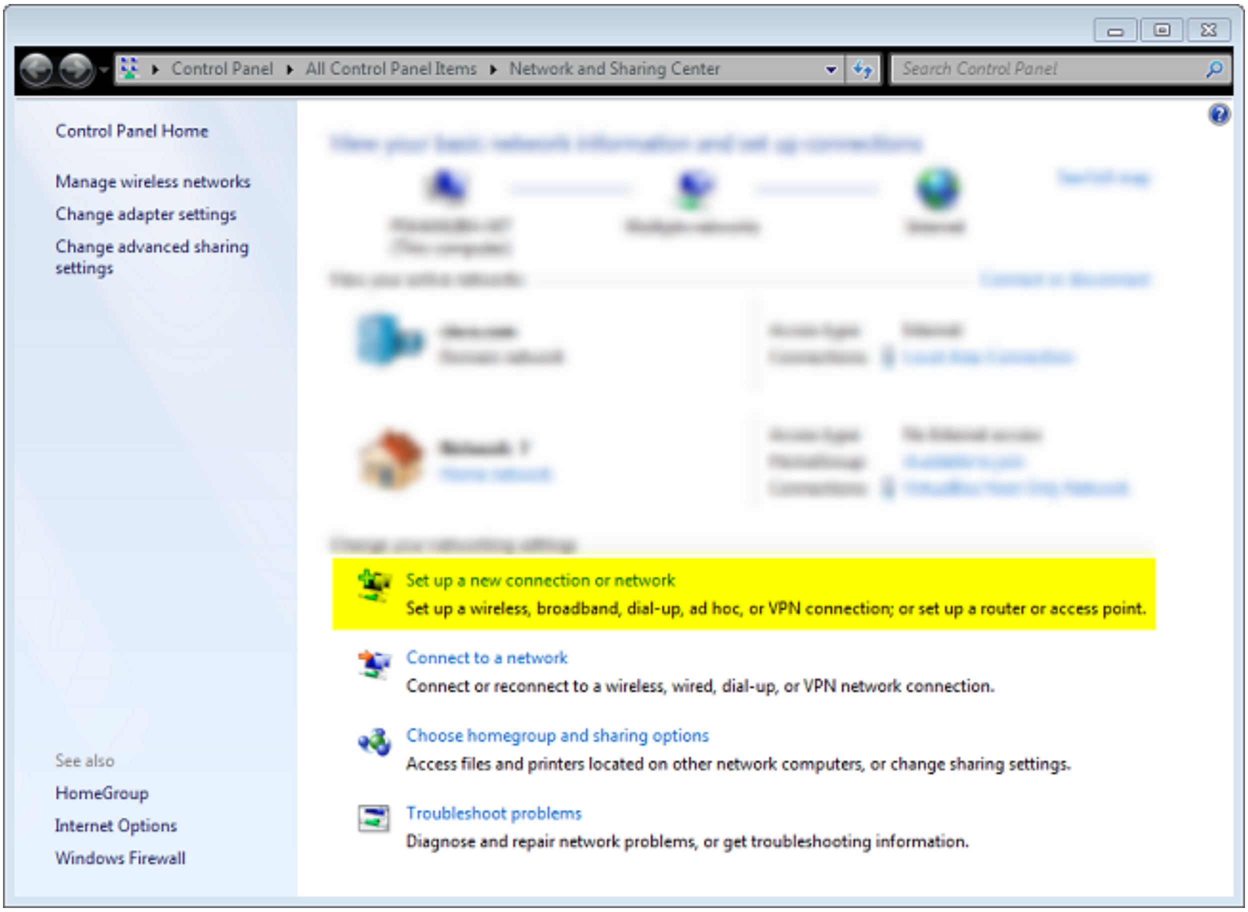
```
crypto ikev2 policy win7
   proposal win7

!! 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
```

The IP unnumbered of the virtual−template should be anything exceptthe local−address used for the IPsec connection. [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.]

Configure Windows 7 Built−In Client

This procedure describes how to configure the Windows 7 built−in client.

1. Navigate to the ***Network and Sharing Center***, and click ***Set up a new connection or network***.



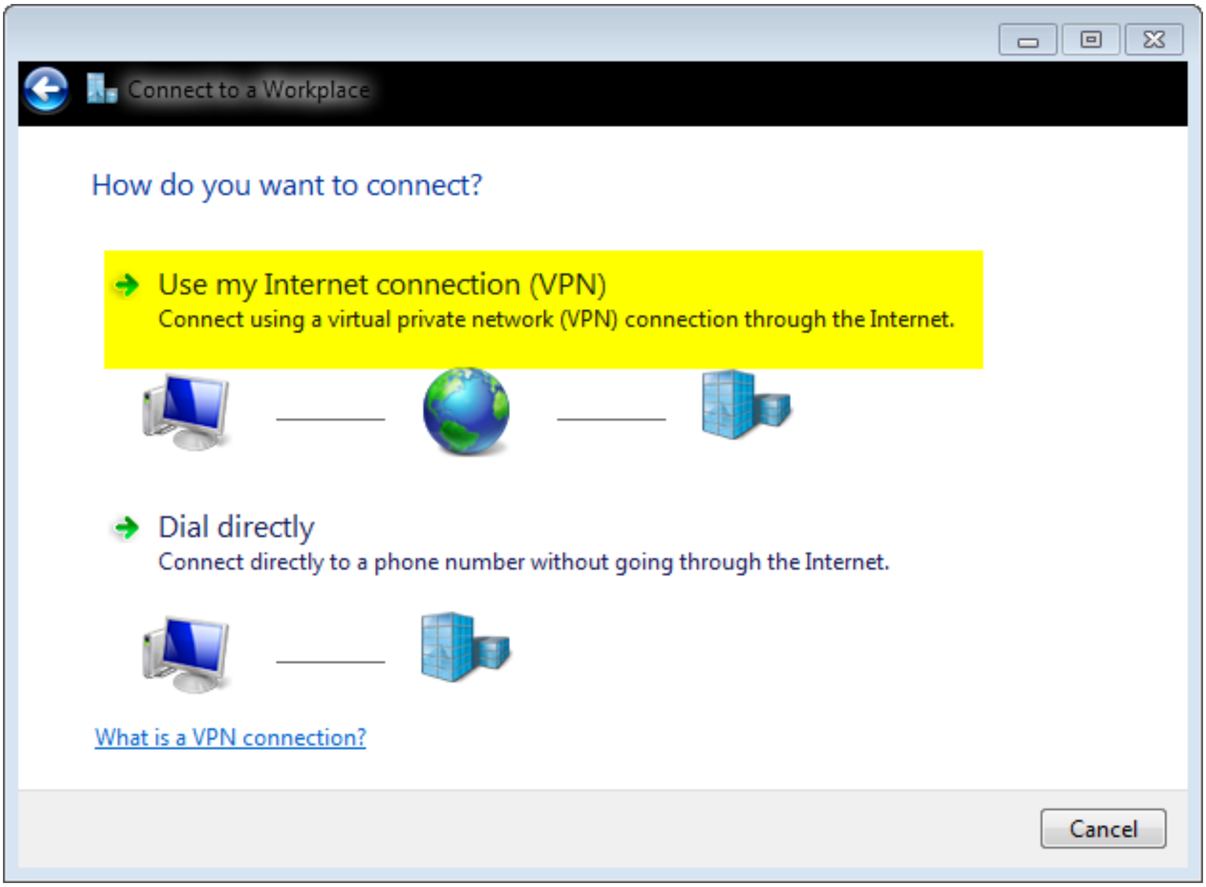
Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

Choose homegroup and sharing options
Access files and printers located on other network computers, or change sharing settings.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

2. Click ***Use my Internet connection (VNP)***. This allows you to setup a VPN connection negotiated over a current Internet connection.



Connect to a Workplace

How do you want to connect?

→ Use my Internet connection (VPN)
Connect using a virtual private network (VPN) connection through the Internet.

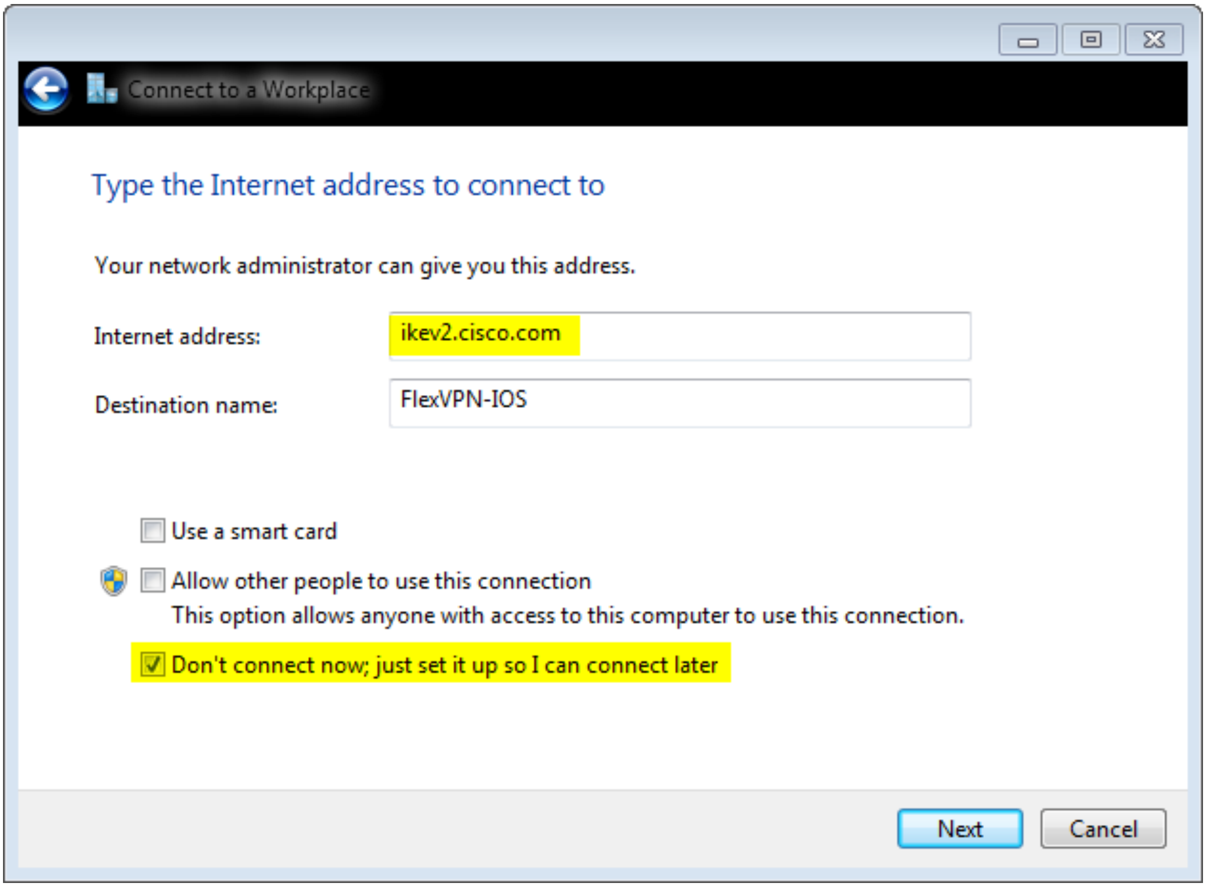
→ Dial directly
Connect directly to a phone number without going through the Internet.

What is a VPN connection?

3. Enter the fully qualified domain name (FQDN) or the IP address of the IKEv2 server, and give it a Destination name to identify it locally.

   Note: The FQDN must match the Common Name (CN) from the router identity certificate. Windows 7 drops the connection with an error 13801 if it detects a mismatch.

   Because additional parameters need to be set, check ***Don't connect now; just set it up so I can connect later***, and click ***Next***:



Type the Internet address to connect to

Your network administrator can give you this address.

Internet address: ikev2.cisco.com

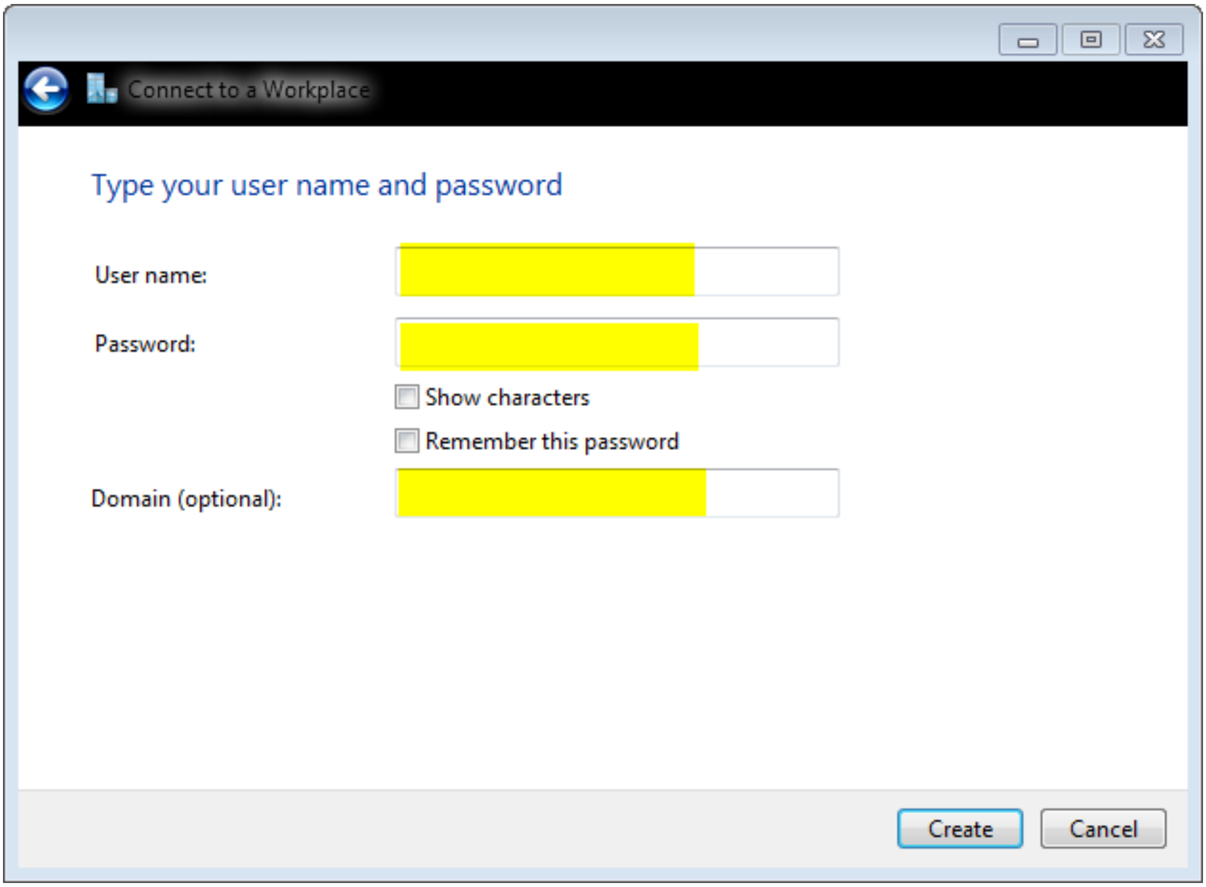
Destination name: FlexVPN-IOS

□ Use a smart card

□ Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.

☑ Don't connect now; just set it up so I can connect later

4. Do not fill in the ***User name***, ***Password*** and ***Domain (optional)*** fields because Certificate Authentication is to be used. Click ***Create***.



Type your user name and password

User name:

Password:

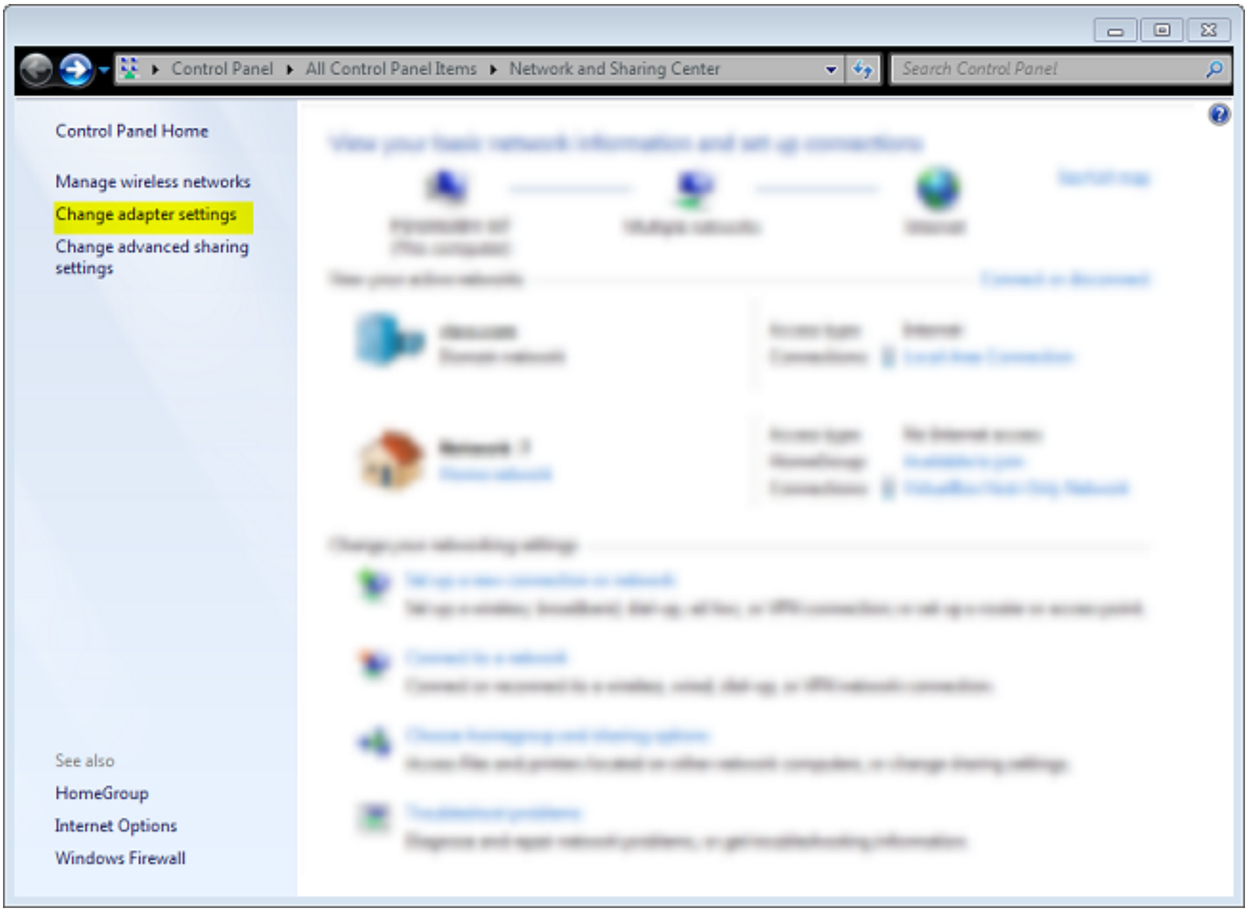
□ Show characters

□ Remember this password

Domain (optional):

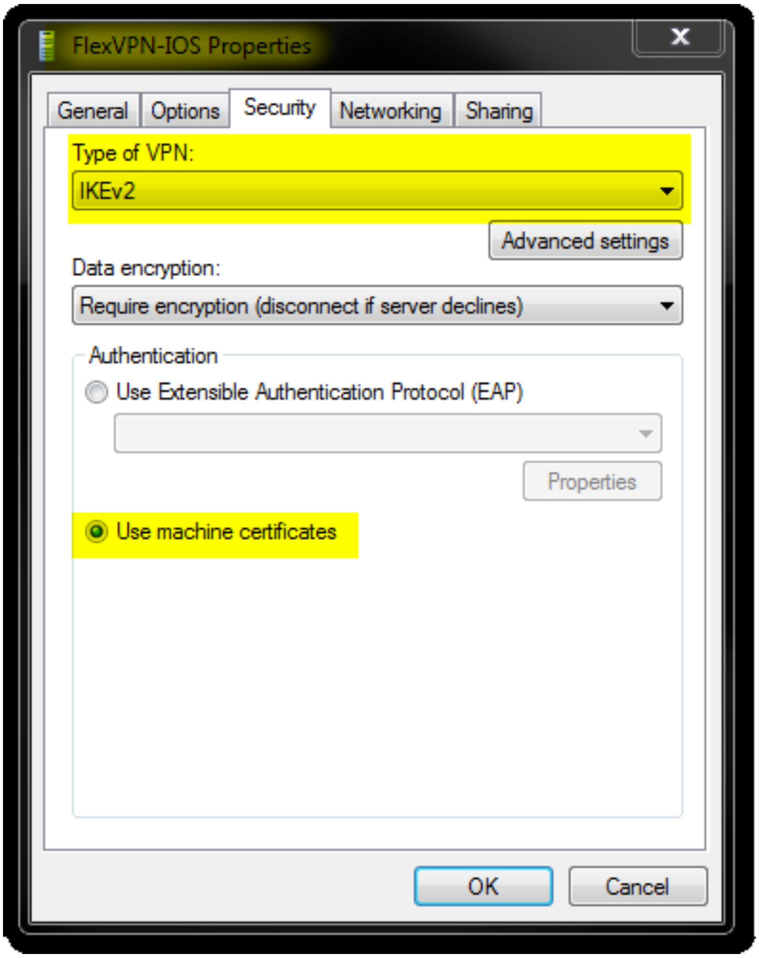
Note: Close the resultant window. ***Do not try to connect.***

5. Navigate back to the ***Network and Sharing Center***, and click ***Change adapter settings***.



6. Choose the Logical Adapter FlexVPN−IOS, which is the result of all the steps taken to this point. Click its properties. These are the properties of the newly created Connection profile called FlexVPN−IOS:

   - On the Security tab, the type of VPN should be IKEv2.
   - In the Authentication section, choose ***Use machine certificates***.



Type of VPN: IKEv2

Data encryption: Require encryption (disconnect if server declines)

Authentication

○ Use Extensible Authentication Protocol (EAP)

● Use machine certificates

The FlexVPN−IOS profile is now ready to be connected after you have imported a certifcate to the machine certificate store.

Obtain Client Certificate

The client certificate requires these factors:

- The client certificate has an EKU of 'Client Authentication'. Also, the CA gives a PKCS#12 certificate:

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

- CA certificate:

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

Important Details

- 'IPSec IKE intermediate' (OID = 1.3.6.1.5.5.8.2.2) should be used as EKU if both of these statements apply:
    - The IKEv2 server is a Windows 2008 server.
    - There are more than one Server Authentication Certificate in use for IKEv2 connections. If this is true, either place both 'Server Authentication' EKU and 'IPSec IKE Intermediate' EKU on one certificate, or distribute these EKUs among the certificates. Make sure at least one certificate contains 'IPSec IKE Intermediate' EKU.

Refer to Troubleshooting IKEv2 VPN Connectionsfor more information.

- In a FlexVPN deployment, do not use 'IPSec IKE Intermediate' in EKU. If you do, the IKEv2 client does not pick up the IKEv2 server certificate. As a result, they are not able to respond to CERTREQ from IOS in the IKE_SA_INIT response message and thus fail to connect with a 13806 Error ID.
- While the Subject Alternative Name (SAN) is not required, it is acceptable if the certificates have one.
- On the Windows 7 Client Certificate Store, make sure that the Machine−Trusted Root Certificate Authorities Store has the least number of certificates possible. If it has more than 50 or so, Cisco IOS might fail to read the entire Cert_Req payload, which contains the Certificate Distinguished Name (DN) of all the known CAs from the Windows 7 box. As a result, the negotiation fails and you see the connection time−out on the client.

Verify

Use this section to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) supports certain ***show*** commands. Use the Output Interpreter Tool in order to view an analysis of ***show*** command output.

```
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

There is currently no specific troubleshooting information available for this configuration.

Related Information

- ***ASA IKEv2 Debugs for Site−to−Site VPN with PSKs TechNote***
- ***ASA IPsec and IKE debugs (IKEv1 Main Mode) Troubleshooting TechNote***
- ***IOS IPSec and IKE debugs − IKEv1 Main Mode Troubleshooting TechNote***
- ***ASA IPSec and IKE debugs − IKEv1 Aggressive Mode TechNote***
- ***Cisco ASA 5500 Series Adaptive Security Appliances***
- ***Cisco ASA 5500 Series Adaptive Security Appliances Software Downloads***
- ***Cisco IOS Firewall***
- ***Cisco IOS Software***
- ***Secure Shell (SSH)***
- ***IPsec Negotiation/IKE Protocols***
- ***Technical Support & Documentation − Cisco Systems***

Updated: May 20, 2013 Document ID: 115907