Windows 7 IKEv2 Agile VPN Client 및 FlexVPN에서 인증서 인증을 사용하는 IKEv2

목차

소개

FlexVPN은 Cisco IOS®의 새로운 IKEv2(Internet Key Exchange version 2) 기반 VPN 인프라로, 통합 VPN 솔루션이어야 합니다.이 문서에서는 Windows 7에 내장된 IKEv2 클라이언트를 구성하여 Cisco IOS 헤드엔드를 CA(Certificate Authority)의 활용도와 연결하는 방법에 대해 설명합니다.

> **참고:**이제 ASA(Adaptive Security Appliance)는 릴리스 9.3(2)부터 Windows 7 내장 클라이언트와의 IKEv2 연결을 지원합니다.

> **참고:**IOS 헤드엔드가 IKEv1의 SUITE-B를 지원하지 않거나 Windows 7 IKEv2 Agile VPN 클라이언트가 현재 IKEv2의 SUITE-B를 지원하지 않으므로 SUITE-B 프로토콜이 작동하지 않습니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Windows 7 내장 VPN 클라이언트
- Cisco IOS Software 릴리스 15.2(2)T
- 인증 기관 - OpenSSL CA

사용되는 구성 요소

이 문서의 정보는 다음 하드웨어 및 소프트웨어 버전을 기반으로 합니다.

- Windows 7 내장 VPN 클라이언트
- Cisco IOS Software 릴리스 15.2(2)T
- 인증 기관 - OpenSSL CA

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

구성

개요

Cisco IOS 헤드엔드를 CA 활용도와 연결하기 위한 Windows 7 내장 IKEv2 클라이언트 컨피그레이션의 4가지 주요 단계가 있습니다.

1. CA 구성

   CA에서 필요한 EKU(Extended Key Usage)를 인증서에 포함할 수 있어야 합니다.예를 들어 IKEv2 서버에서 'Server Auth EKU'가 필요하지만 클라이언트 인증서에는 'Client Auth EKU'가 필요합니다. 로컬 구축에서는 다음을 사용할 수 있습니다.Cisco IOS CA 서버 - 버그 CSCuc82575 때문에 자체 서명 인증서를 사용할 수 없습니다.OpenSSL CA 서버Microsoft CA 서버 - 일반적으로 인증서를 원하는 대로 서명하도록 구성할 수 있으므로 이 옵션이 기본 옵션입니다.

2. Cisco IOS 헤드엔드 구성

   인증서 가져오기IKEv2 구성

3. Windows 7 기본 제공 클라이언트 구성

4. 클라이언트 인증서 가져오기

이러한 각 주요 단계는 다음 섹션에서 자세히 설명합니다.

> **참고:**이 섹션에 사용된 명령에 대한 자세한 내용을 보려면 Command Lookup Tool(등록된 고객만 해당)을 사용합니다.

인증 기관 구성

이 문서에서는 CA 설정 방법에 대한 자세한 단계를 제공하지 않습니다.그러나 이 섹션의 단계는 CA가 이러한 유형의 구축에 대한 인증서를 발급할 수 있도록 CA를 구성하는 방법을 보여줍니다.

OpenSSL

OpenSSL CA는 'config' 파일을 기반으로 합니다.OpenSSL 서버의 'config' 파일에는 다음이 있어야 합니다.

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

Cisco IOS CA 서버

Cisco IOS CA 서버를 사용하는 경우 EKU를 할당하는 최신 Cisco IOS Software 릴리스를 사용해야 합니다.

```
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 Headend 구성

인증서 가져오기

인증서에는 Cisco IOS의 경우 EKU 필드가 '서버 인증'으로 설정되고 클라이언트의 경우 '클라이언트 인증'이 설정되어야 합니다.일반적으로 동일한 CA를 사용하여 클라이언트와 서버 인증서를 모두 서명합니다.이 경우 서버 인증서와 클라이언트 인증서에서 각각 '서버 인증'과 '클라이언트 인증'이 모두 표시되는데, 이는 허용됩니다.

CA가 IKEv2 서버의 PKCS(Public-Key Cryptography Standards) #12 형식으로 인증서를 클라이언트와 서버에 발급하고, CRL(Certificate Revocation List)에 연결할 수 없거나 사용할 수 없는 경우 다음을 구성해야 합니다.

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

PKCS#12 인증서를 가져오려면 다음 명령을 입력합니다.

```
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 서버가 인증서를 자동 부여하는 경우 다음 예와 같이 인증서를 받으려면 CA 서버 URL을 사용하여 IKEv2 서버를 구성해야 합니다.

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

신뢰 지점이 구성된 경우 다음을 수행해야 합니다.

1. 다음 명령을 사용하여 CA를 인증합니다.

```
crypto pki authenticate FlexRootCA
```

2. 다음 명령을 사용하여 CA에 IKEv2 서버를 등록합니다.

```
crypto pki enroll FlexRootCA
```

인증서에 필요한 옵션이 모두 포함되어 있는지 확인하려면 다음 **show** 명령을 사용합니다.

```
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
```

IKEv2 구성

다음은 IKEv2 컨피그레이션의 예입니다.

```
!! 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
```

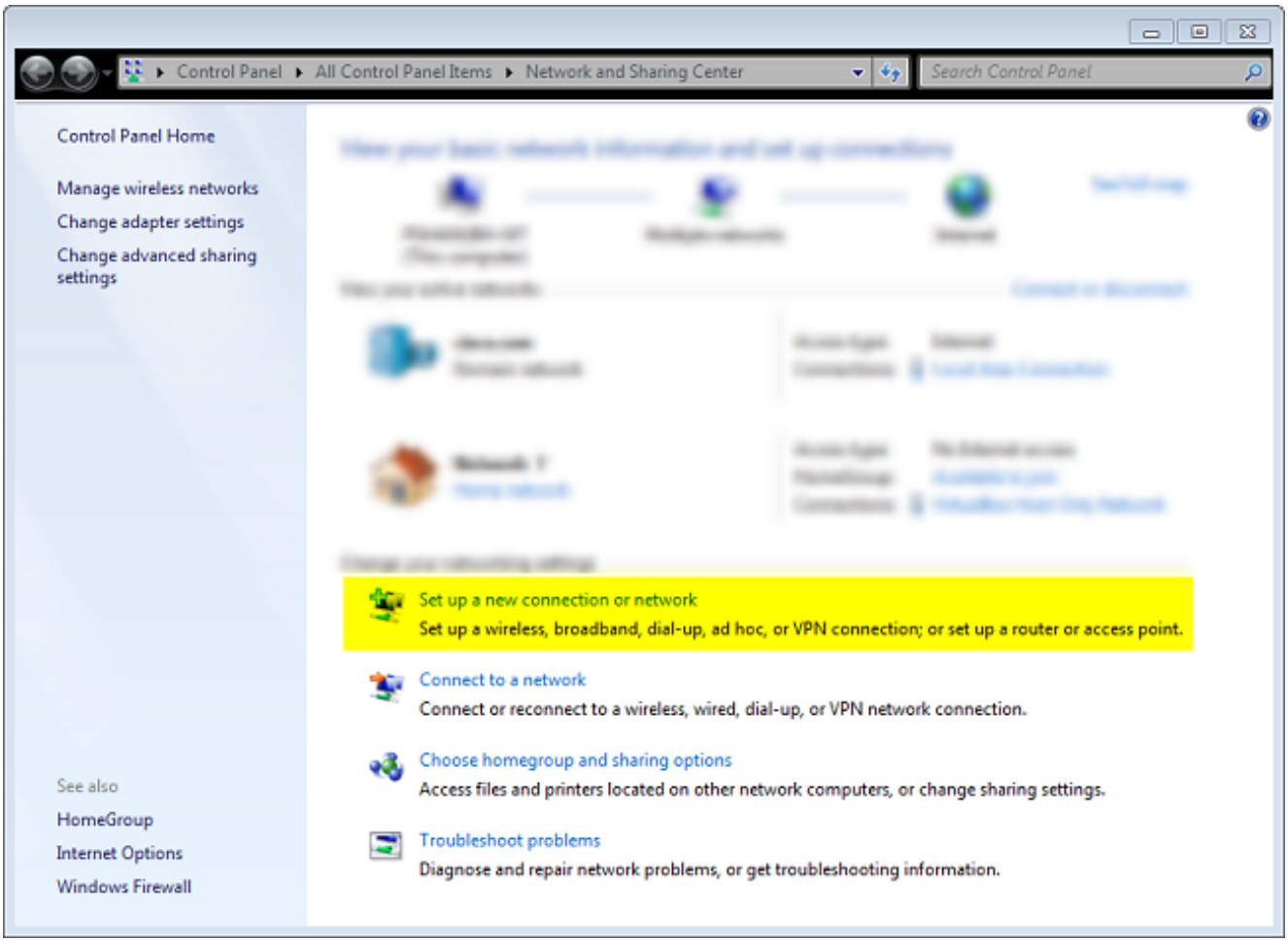
가상 템플릿의 IP 번호가 지정되지 않은 IP는 IPsec 연결에 사용되는 로컬 주소를 제외한 모든 것이어야 합니다. [하드웨어 클라이언트를 사용하는 경우 IKEv2 컨피그레이션 노드를 통해 라우팅 정보

를 교환하고 하드웨어 클라이언트에 재귀 라우팅 문제를 생성합니다.]

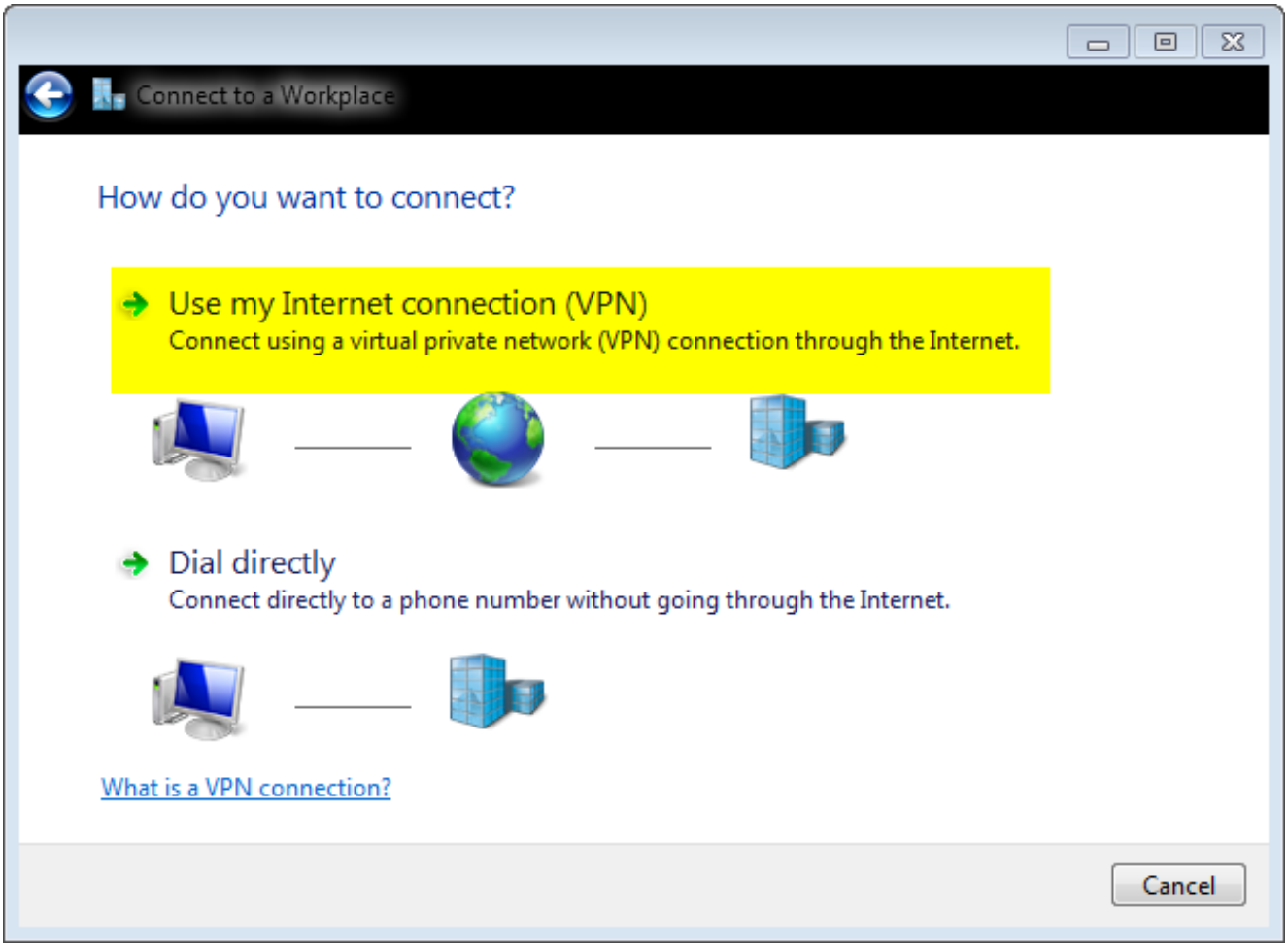
Windows 7 기본 제공 클라이언트 구성

이 절차에서는 Windows 7 기본 제공 클라이언트를 구성하는 방법에 대해 설명합니다.

1. **Network and Sharing Center(네트워크 및 공유 센터)**로 이동하고 **Set up a new connection or network(새 연결 또는 네트워크 설정)를** 클릭합니다.

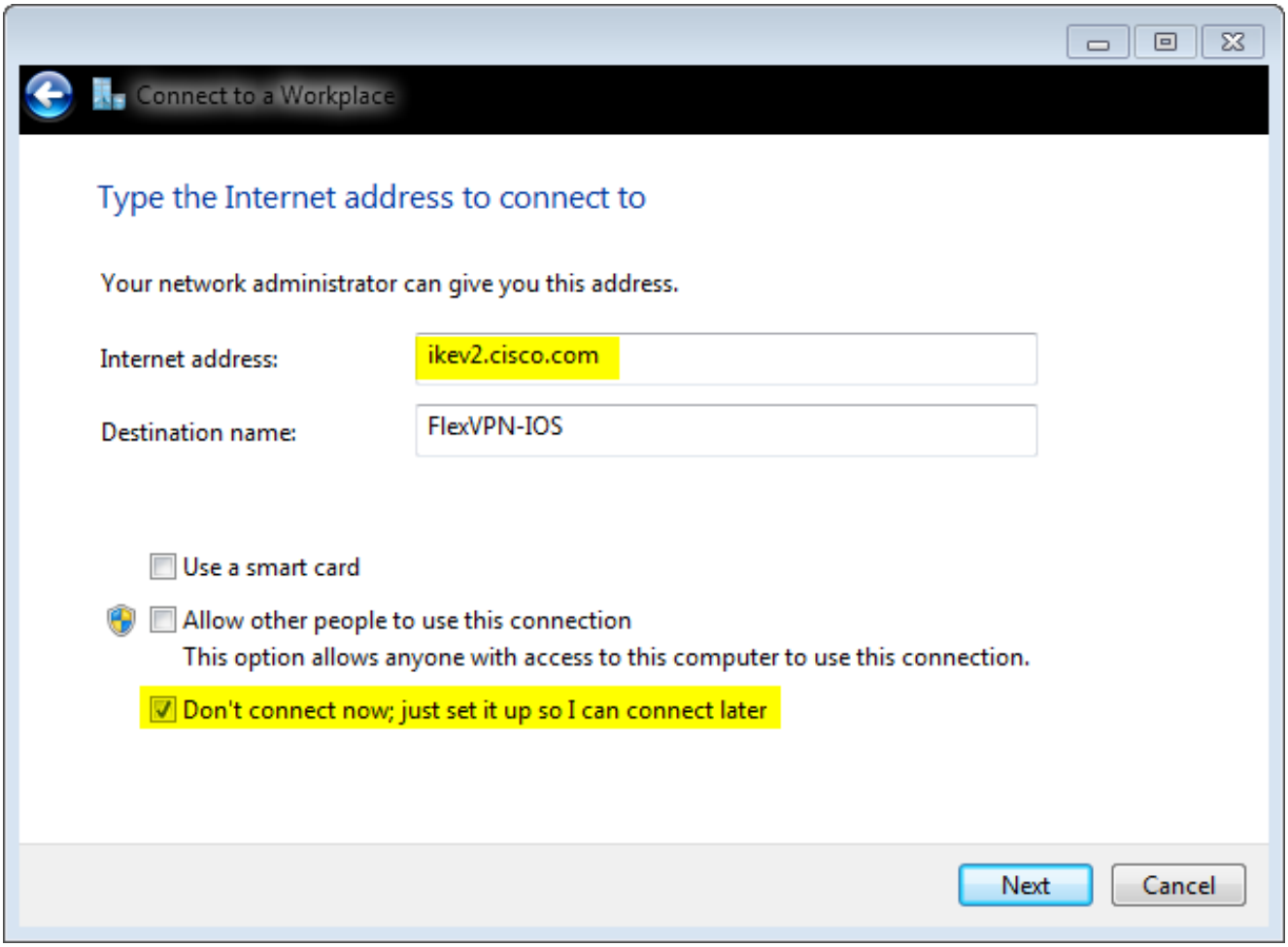


2. **내 인터넷 연결 사용(VNP)을** 클릭합니다. 이를 통해 현재 인터넷 연결을 통해 협상된 VPN 연결을 설정할 수 있습니다.

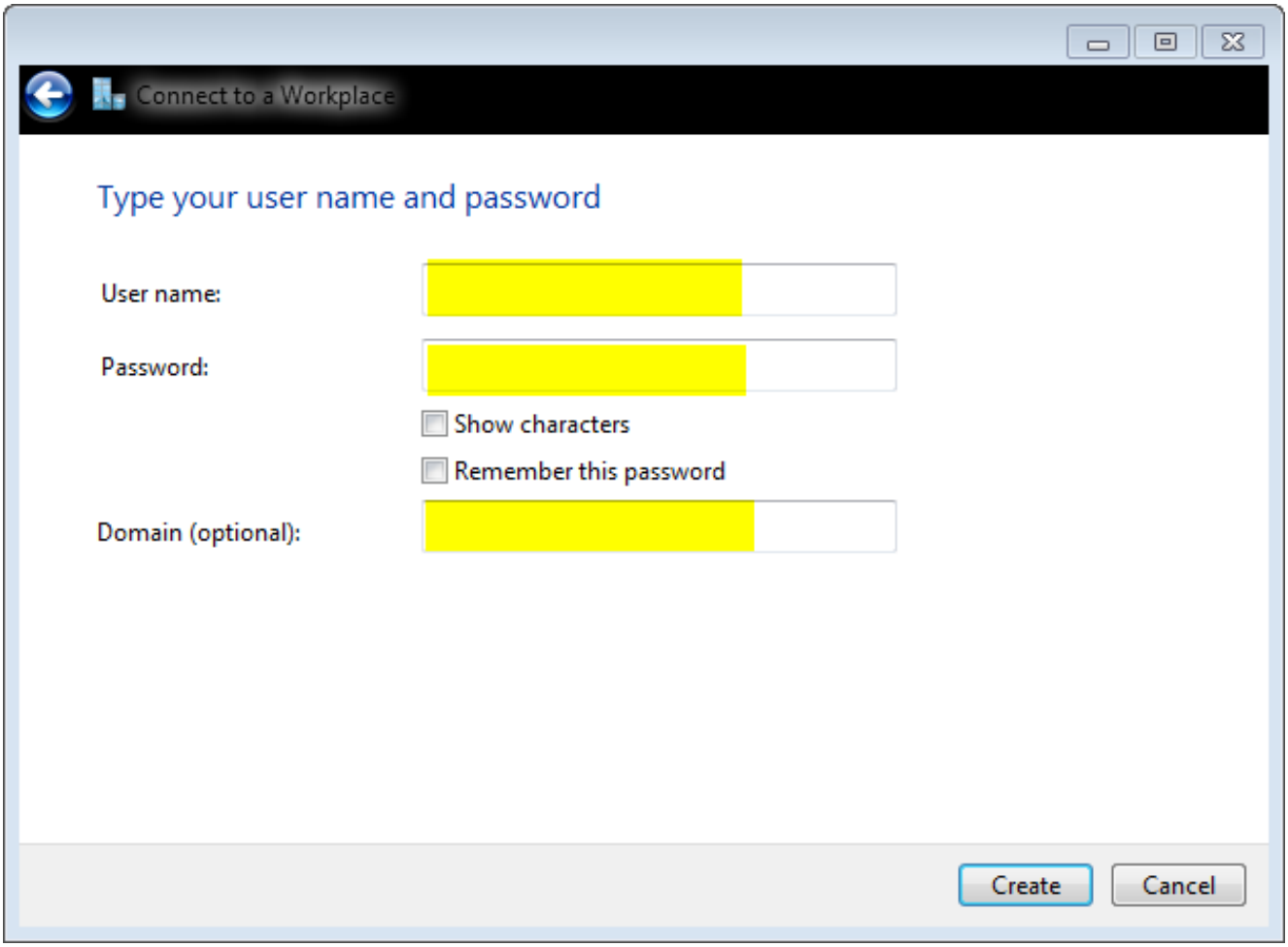


3. IKEv2 서버의 FQDN(Fully Qualified Domain Name) 또는 IP 주소를 입력하고 이를 로컬로 식별하려면 Destination 이름을 지정합니다.

   참고:FQDN은 라우터 ID 인증서의 CN(Common Name)과 일치해야 합니다.Windows 7이 불일치를 탐지하면 13801 오류와 함께 연결을 삭제합니다.
   추가 매개 변수를 설정해야 하므로 **지금 연결 안 함을** 선택합니다.**나중에 연결할 수 있도록 설정하고 다음**을 클릭합니다.

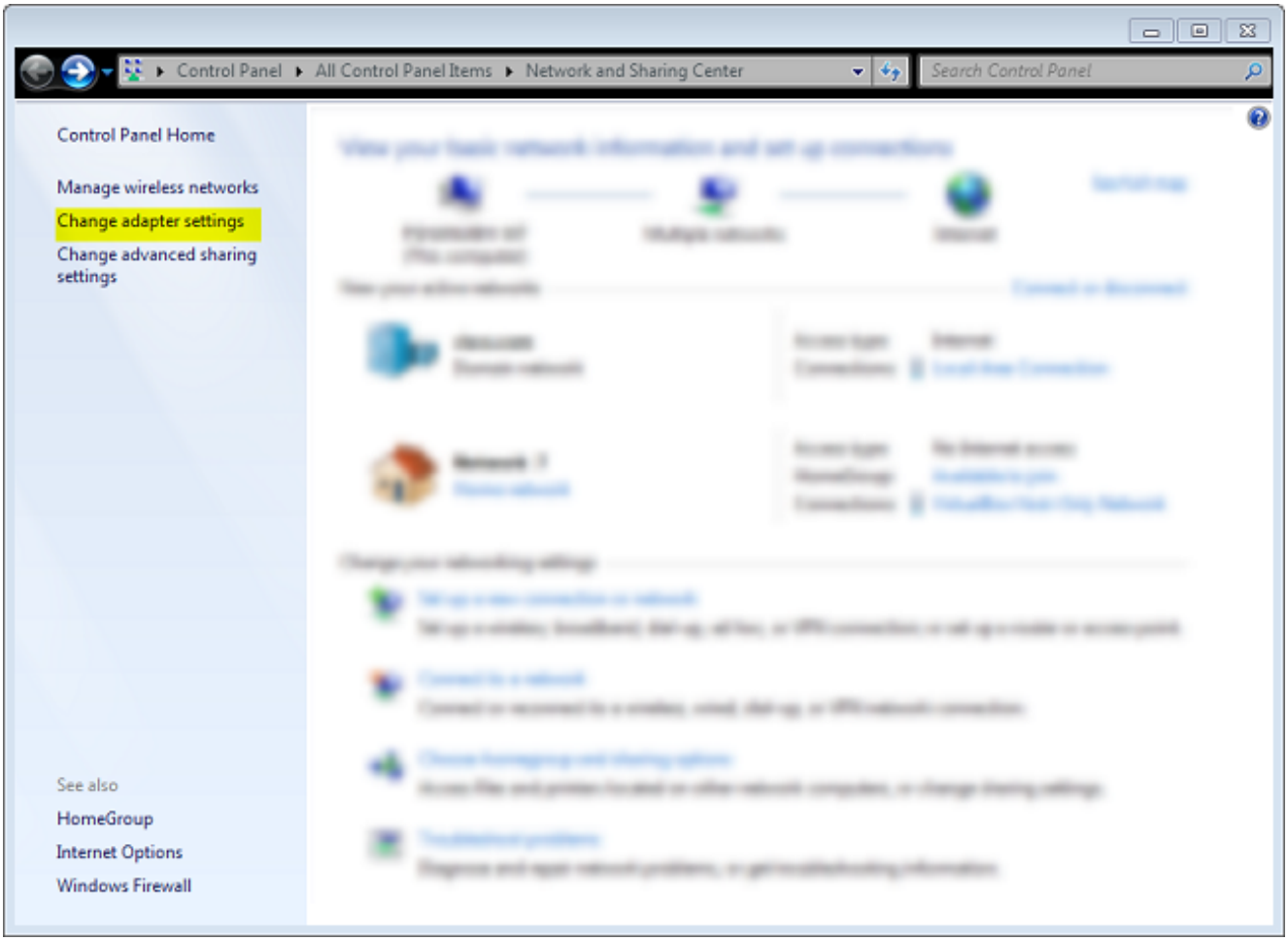


4. Certificate Authentication(인증서 인증)을 사용하기 때문에 **User name**, **Password** and **Domain(선택 사항) 필드**를 입력하지 마십시오.Create를 **클릭합니다**.



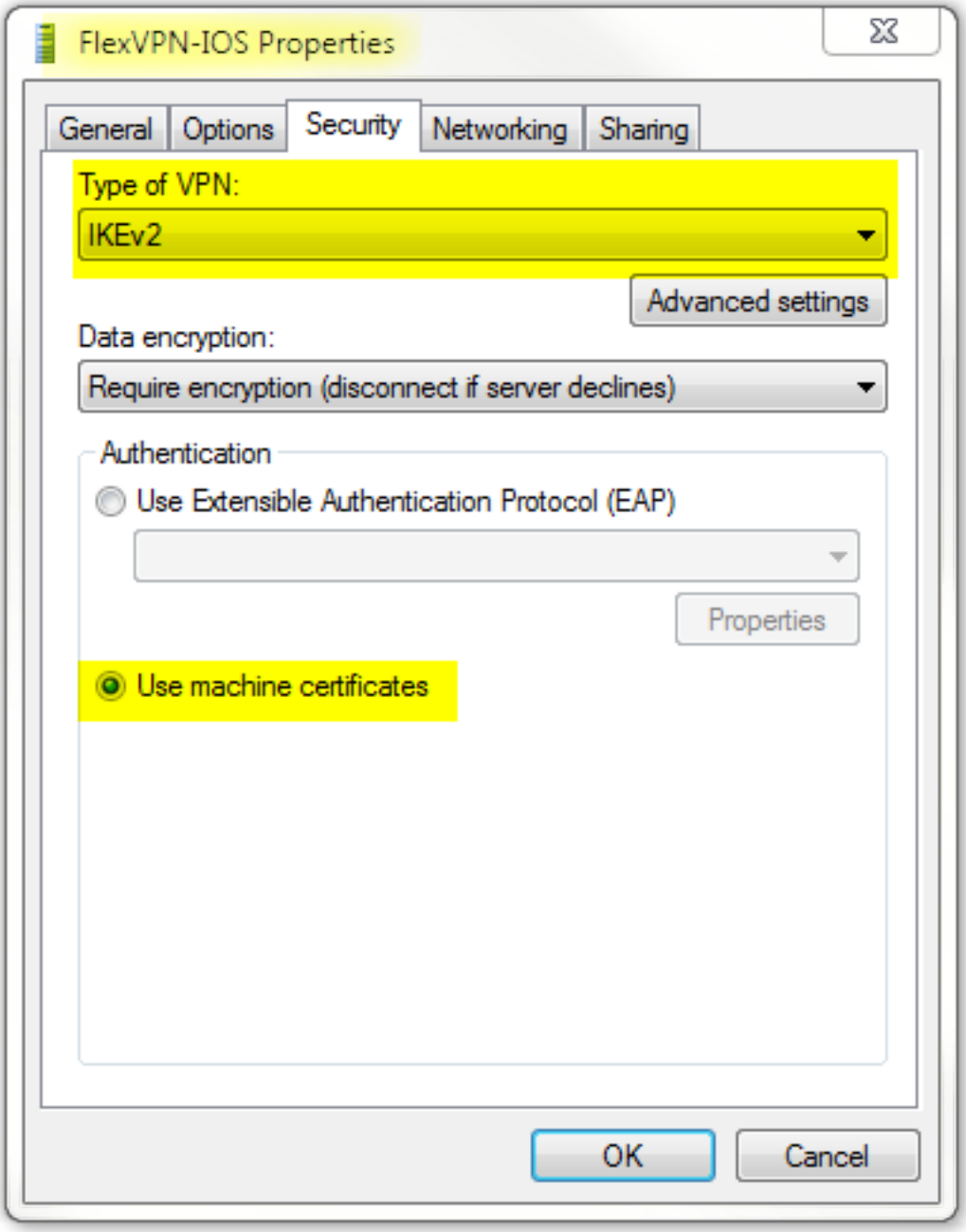
참고:결과 창을 닫습니다.**연결을 시도하지 마십시오.**

5. **Network and Sharing Center(네트워크 및 공유 센터)**로 다시 이동하고 **어댑터 설정 변경**을 클릭합니다.



6. Logical Adapter FlexVPN-IOS를 선택합니다. 이는 이 시점까지 모든 단계를 수행한 결과입니다.해당 속성을 클릭합니다.다음은 FlexVPN-IOS라는 새로 생성된 연결 프로파일의 속성입니다.

   Security(보안) 탭에서 VPN 유형은 IKEv2여야 합니다.Authentication(인증) 섹션에서 Use machine **certificates(머신 인증서 사용)를** 선택합니다.



머신 인증서 저장소로 인증서를 가져온 후 FlexVPN-IOS 프로파일을 연결할 준비가 되었습니다.

클라이언트 인증서 가져오기

클라이언트 인증서에 다음 요소가 필요합니다.

- 클라이언트 인증서에 '클라이언트 인증'의 EKU가 있습니다. 또한 CA는 PKCS#12 인증서를 제공합니다.

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

- CA 인증서:

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

중요 세부 정보

- 다음 두 명령문이 모두 적용되는 경우 'IPSec IKE intermediate'(OID = 1.3.6.1.5.5.8.2.2)을 EKU로 사용해야 합니다.

  IKEv2 서버는 Windows 2008 서버입니다.IKEv2 연결에 둘 이상의 서버 인증 인증서가 사용 중입니다.true이면 'Server Authentication' EKU와 'IPSec IKE Intermediate' EKU를 모두 하나의 인증서에 배치하거나 이러한 EKU를 인증서 간에 배포합니다.하나 이상의 인증서에 'IPSec IKE Intermediate' EKU가 포함되어 있는지 확인하십시오.

  자세한 내용은 IKEv2 VPN 연결 문제 해결을 참조하십시오.

- FlexVPN 구축에서는 EKU에서 'IPSec IKE Intermediate'를 사용하지 마십시오.이 경우 IKEv2 클라이언트는 IKEv2 서버 인증서를 선택하지 않습니다.따라서 IKE_SA_INIT 응답 메시지의 IOS에서 CERTREQ에 응답할 수 없으므로 13806 오류 ID로 연결하지 못했습니다.

- SAN(Subject Alternative Name)은 필요하지 않지만 인증서에 있는 경우 허용됩니다.

- Windows 7 클라이언트 인증서 저장소에서 시스템 신뢰 루트 인증 기관 저장소에 가능한 인증서 수가 가장 적은지 확인합니다.50개가 넘는 경우 Cisco IOS가 Windows 7 상자에서 알려진 모든 CA의 DN(Certificate Distinguished Name)을 포함하는 전체 Cert_Req 페이로드를 읽지 못할 수 있습니다.따라서 협상이 실패하고 클라이언트에서 연결 시간 초과가 표시됩니다.

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

Output Interpreter 도구(등록된 고객만 해당)는 특정 **show** 명령을 지원합니다.**show** 명령 출력의 분석을 보려면 [출력 인터프리터 도구]를 사용합니다.

```
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:
```

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- PSK가 포함된 Site-to-Site VPN용 ASA IKEv2 디버그 TechNote
- ASA IPsec 및 IKE 디버깅(IKEv1 기본 모드) 문제 해결 TechNote
- IOS IPSec 및 IKE 디버깅 - IKEv1 기본 모드 문제 해결 TechNote

- ASA IPSec 및 IKE 디버깅 - IKEv1 Aggressive Mode TechNote
- Cisco ASA 5500 Series Adaptive Security Appliance
- Cisco ASA 5500 Series Adaptive Security Appliances 소프트웨어 다운로드
- Cisco IOS Firewall
- Cisco IOS 소프트웨어
- SSH(Secure Shell)
- IPsec 협상/IKE 프로토콜
- 기술 지원 및 문서 – Cisco Systems