# IKEv2 с Windows 7 IKEv2 Agile VPN Client и проверкой подлинности сертификата на FlexVPN

## Содержание



## Введение

FlexVPN является новой второй версией протокола Internet Key Exchange (IKEv2) - основанная инфраструктура VPN на Cisco IOS® и предназначается, чтобы быть унифицированным решением для VPN. Этот документ описывает, как настроить клиента IKEv2, который встроен в Windows 7 для соединения головной станции Cisco IOS с использованием Центра сертификации (CA).

> **Примечание:** Устройство адаптивной защиты (ASA) теперь поддерживает соединения IKEv2 с Windows 7 встроенный клиент с Выпуска 9.3 (2).

> **Примечание:** Протоколы КОМПЛЕКТА-B не работают, потому что головной узел IOS не поддерживает КОМПЛЕКТ-B с IKEv1, или Windows 7 IKEv2 Agile VPN client в настоящее время не поддерживает КОМПЛЕКТ-B с IKEv2.

## Предварительные условия

### Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Встроенный VPN-клиент Windows 7
- Cisco IOS Software Release 15.2 (2) T
- Центр сертификации - OpenSSL CA

### Используемые компоненты

Сведения в документе приведены на основе данных версий аппаратного и программного обеспечения:

- Встроенный VPN-клиент Windows 7
- Программное обеспечение Cisco IOS Release15.2 (2) T
- Центр сертификации - OpenSSL CA

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

### Условные обозначения

Сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

## Настройка

### Обзор

Существует четыре главных действия в конфигурации Windows 7 встроенный клиент IKEv2 для соединения головной станции Cisco IOS с использованием CA:

1. Настройте CA

   CA должен позволить вам встраивать требуемое расширенное использование ключа (EKU) в сертификат. Например, на сервере IKEv2, 'EKU Аутентификации Сервера' требуется, в то время как сертификату клиента нужен 'Клиентский Подлинный EKU'. Локальные развертывания могут использовать:Cisco IOS CA сервер - Подписанные сертификаты не может использоваться из-за дефекта CSCuc82575.OpenSSL CA серверMicrosoft CA server - В целом, это - предпочтительный вариант, потому что это

может быть настроено для подписания сертификата точно, как желаемый.

2. Настройте головную станцию Cisco IOS

   Получите сертификатНастройте IKEv2

3. Настройте Windows 7 встроенный клиент
4. Получите сертификат клиента

Каждое из этих главных действий объяснено подробно в последующих разделах.

> **Примечание:** Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

## Настройте центр сертификации

Этот документ не предоставляет детализированные действия о том, как установить CA. Однако, шаги в этот раздел показывают вам, как настроить CA, таким образом, это может выполнить сертификаты для этого вида развертываний.

### OpenSSL

OpenSSL CA основывается на файле 'config'. Файл 'config' для сервера OpenSSL должен иметь:

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

### Cisco IOS CA сервер

При использовании Cisco IOS CA сервер удостоверьтесь, что вы используете новый Cisco IOS Software Release, который назначает 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
```

## Настройте головную станцию Cisco IOS

### Получите сертификат

Сертификату нужно было установить поля EKU в 'Проверку подлинности сервера' для Cisco IOS и 'Аутентификацию клиента' для клиента. Как правило, тот же CA используется для подписания обоих сертификаты клиента и сервера. В этом случае и 'Проверка подлинности сервера' и 'Аутентификация клиента'  замечены на серверном сертификате и сертификате клиента соответственно, который приемлем.

Если CA выполняет сертификаты в Стандартах криптографии общего ключа (PKCS) #12

формат на сервере IKEv2 клиентам и сервере, и если список отозванных сертификатов (CRL) не достижим или доступен, это должно быть настроенный:

```
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
```

Введите эту команду для импорта сертификата 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.
```

Если Cisco IOS CA сервер автоматические сертификаты предоставлений, сервер IKEv2 должен быть настроен с URL сервера CA для получения сертификата как показано в данном примере:

```
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.
```

Когда точка доверия настроена, вы должны:

1. Аутентифицируйте CA с этой командой:

   ```
   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. Зарегистрируйте сервер IKEv2 с CA с этой командой:

   ```
   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.
   ```

Чтобы видеть, содержит ли сертификат все обязательные параметры, используйте эту **команду показа**:

```
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
```

### Настройте IKEv2

Это - пример конфигурации IKEv2:

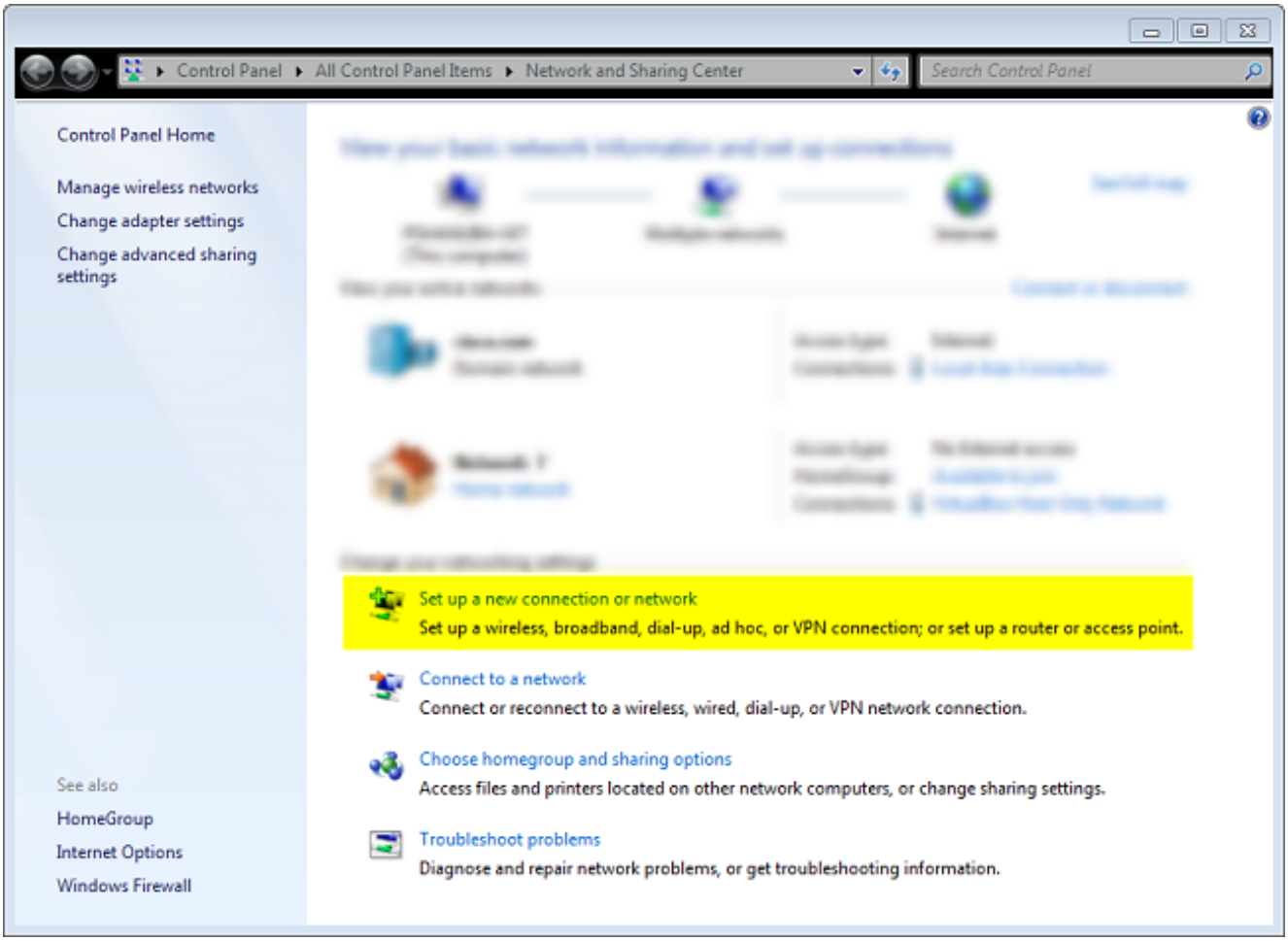
```
ikev2#show crypto pki cert verbose
Certificate
 <snip>
 Issuer:
  <snip>
 Subject:
   Name: ikev2.cisco.com
   ou=TAC
   o=Cisco
   c=BE
  cn=ikev2.cisco.com
<snip>
 Subject Key Info:
   Public Key Algorithm: rsaEncryption
   RSA Public Key: (1024 bit)
 Signature Algorithm: MD5 with RSA Encryption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

IP, ненумерованный из virtual-template, должен быть чем-либо exceptthe local-address, используемый для IP - безопасного соединения. [При использовании аппаратного клиента вы обменивались бы сведениями о маршрутизации через узел конфигурации IKEv2 и создали бы проблему рекурсивной маршрутизации на аппаратном клиенте.]

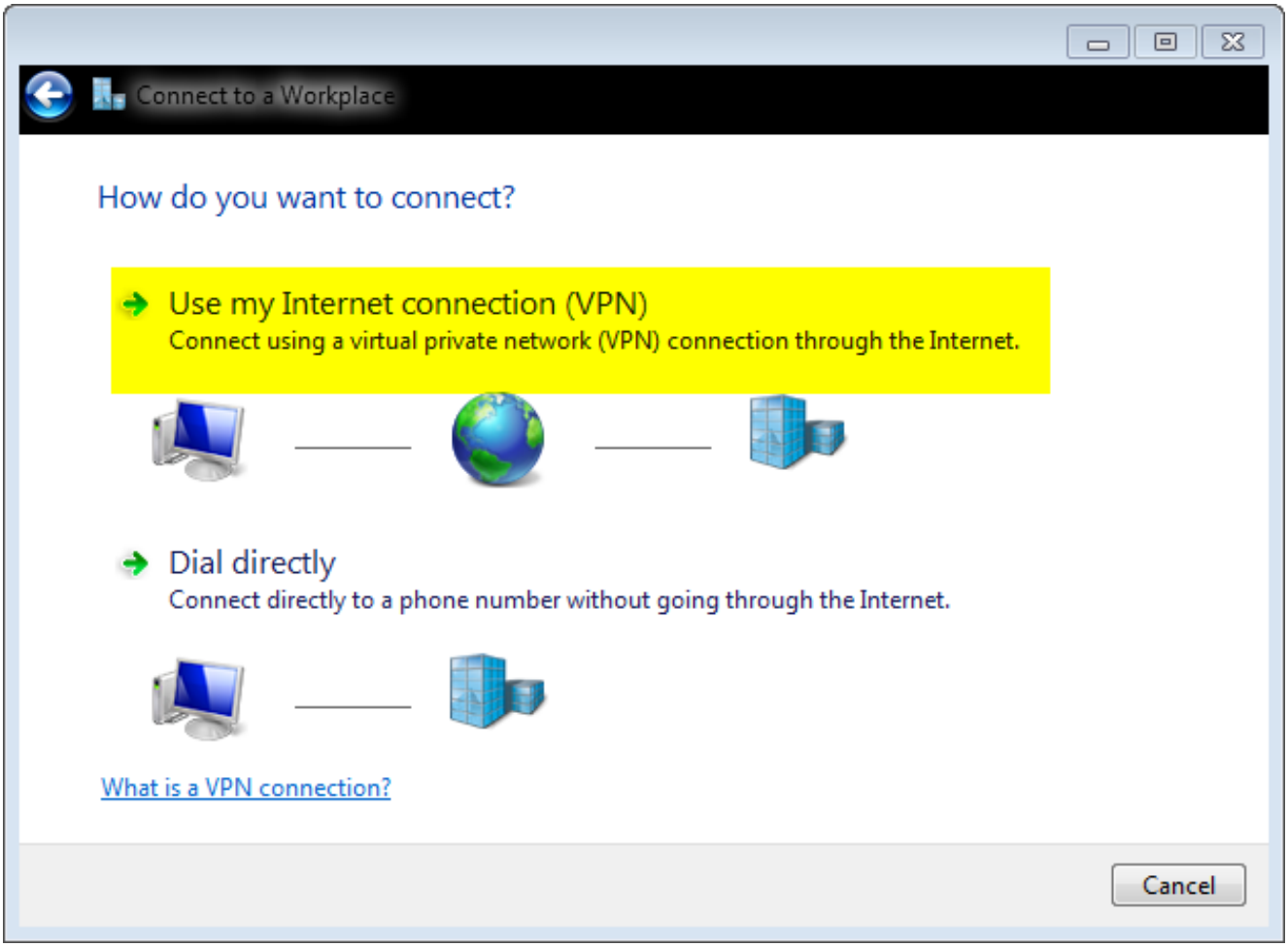
## Настройте Windows 7 Built-In Client

Эта процедура описывает, как настроить Windows 7 встроенный клиент.

1. Перейдите к **Сети и Совместному использованию Центра**, и нажмите **Set up новое соединение или сеть**.

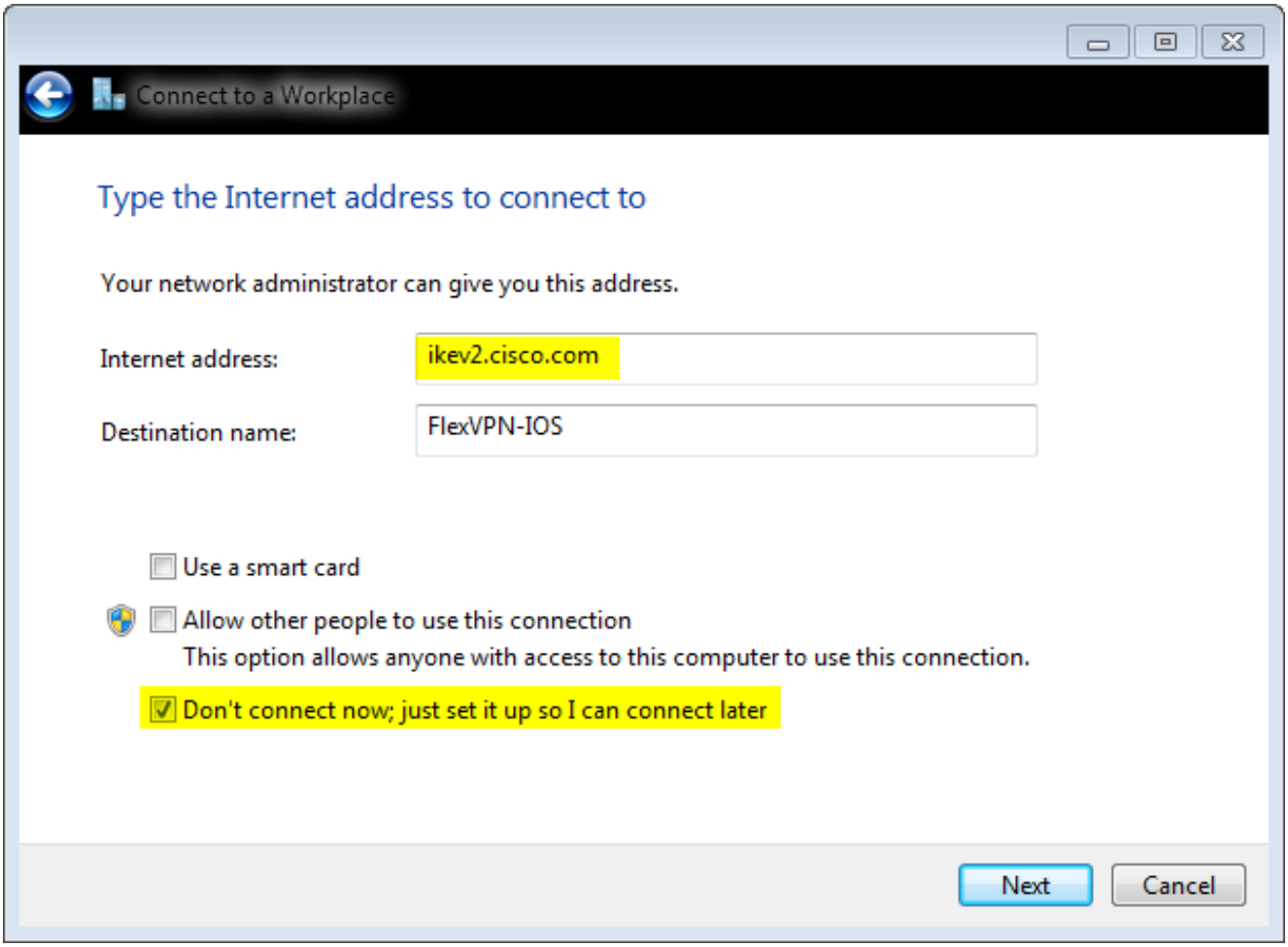



2. Нажмите **Use мое Интернет-соединение (VNP)**. Это позволяет вам устанавливать VPN-подключение, о котором выполняют согласование по текущему Интернет-соединению.

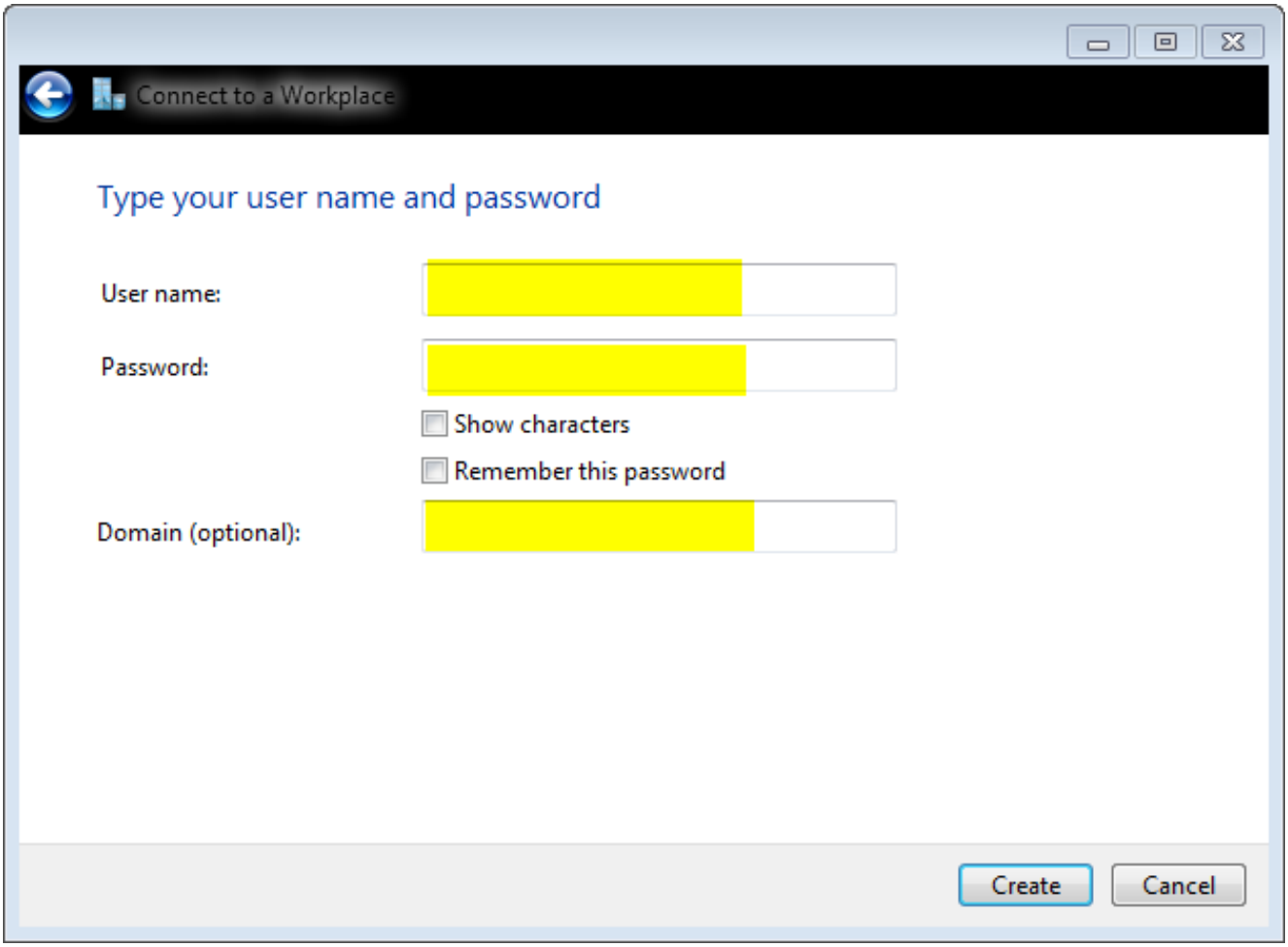



3. Введите полное доменное имя (FQDN) или IP-адрес сервера IKEv2, и дайте ему Целевое название для определения его локально.

   **Примечание:** FQDN должен совпасть с Общим именем (CN) от сертификата идентификации маршрутизатора. Windows 7 отбрасывает соединение с ошибкой 13801, если это обнаруживает несоответствие.
   Поскольку дополнительные параметры должны быть установлены, проверка **не соединяются теперь; просто настройте его так, я могу соединиться позже** и нажать **Next**:

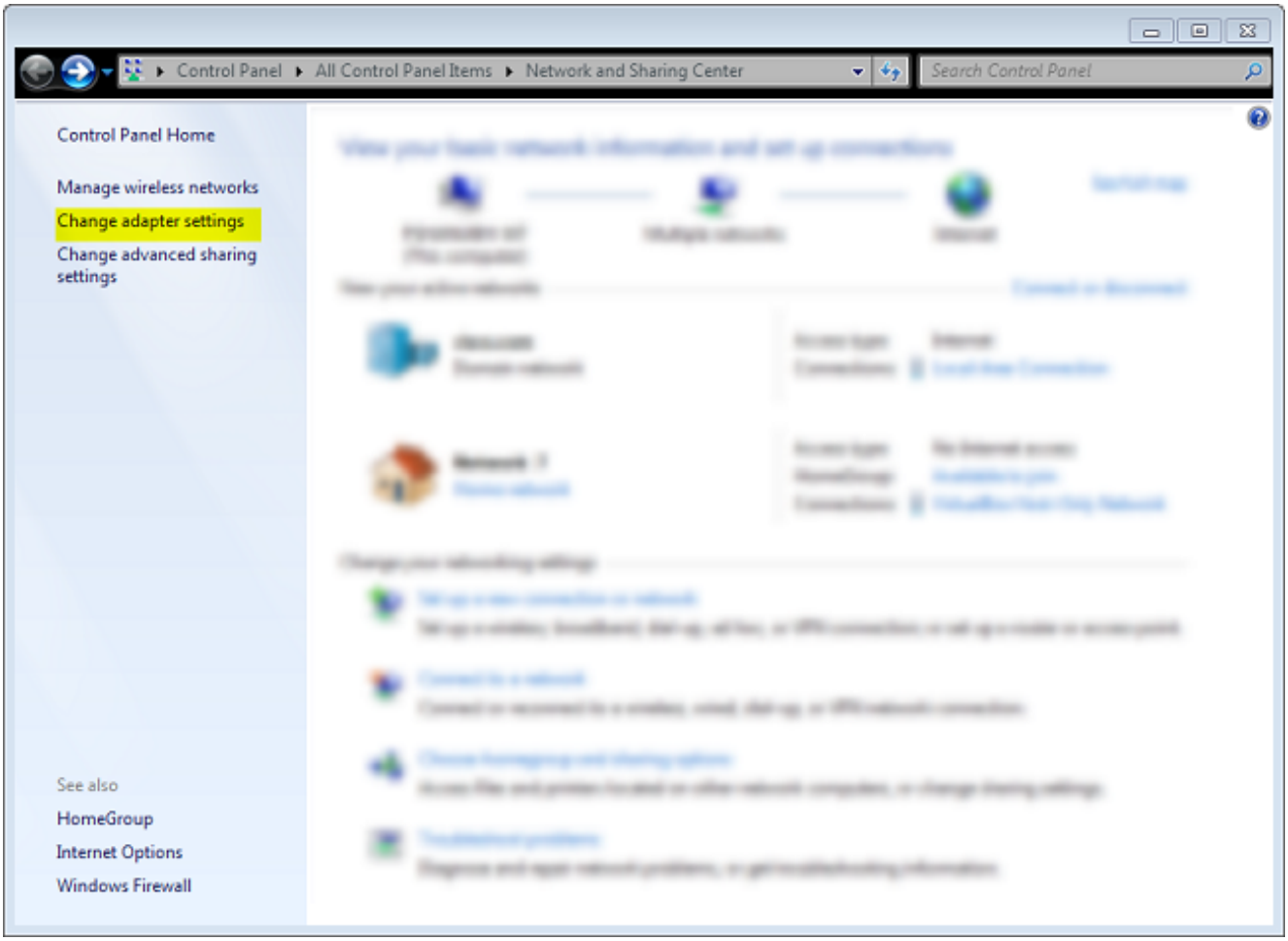



4. Не заполняйте **Имя пользователя**, **Пароль** и **Доменные (дополнительные)** поля, потому что должна использоваться Проверка подлинности сертификата. **Нажмите кнопку Create.**



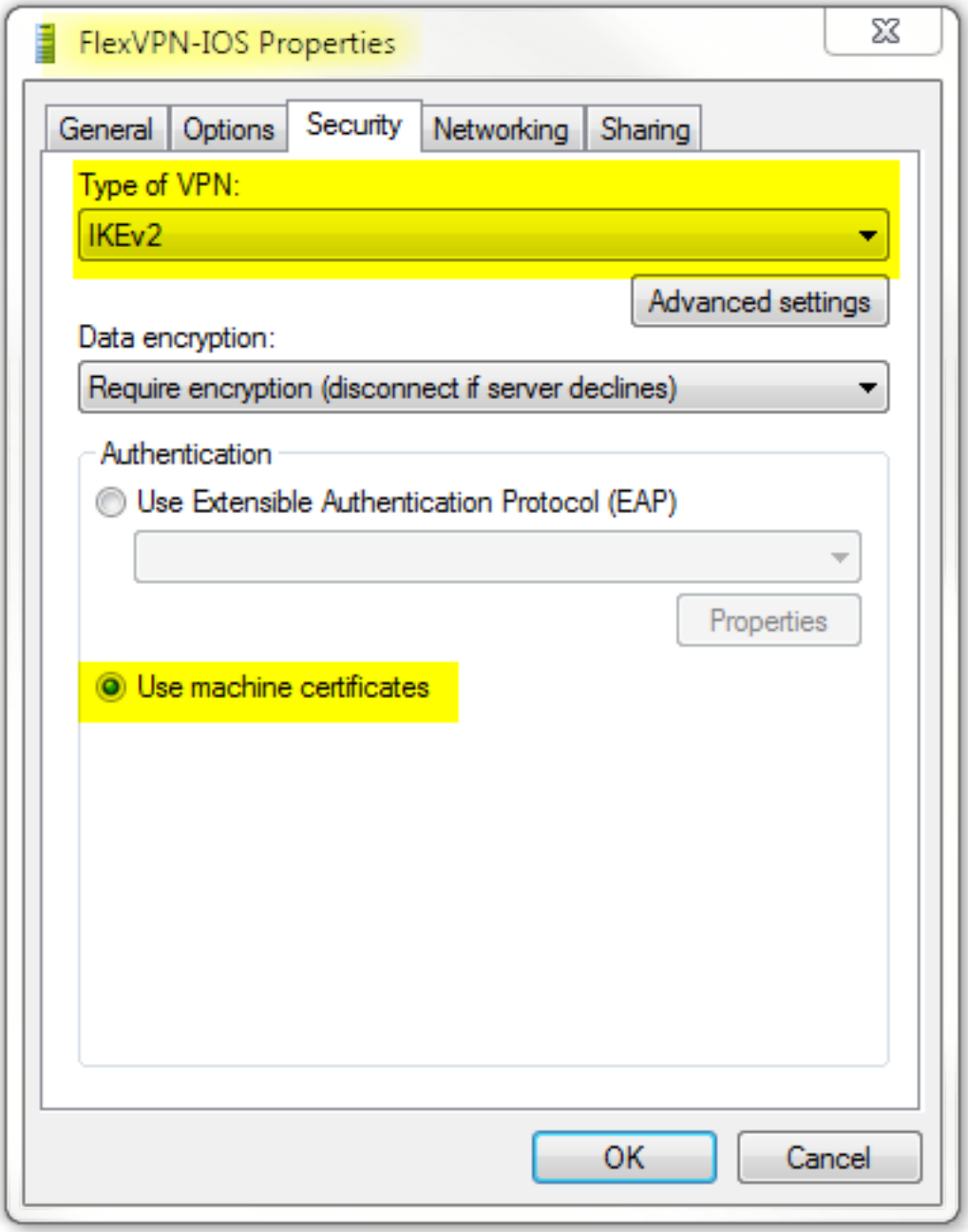

**Примечание:** Закройте результирующее окно. **Не пытайтесь соединиться.**

5. Перейдите назад к **Сети и Совместному использованию Центра**, и нажмите**, изменяют настройки адаптера**.




6. Выберите Logical Adapter FlexVPN-IOS, который является результатом всех шагов, сделанных к этой точке. Нажмите его свойства. Это свойства профиля нового созданного соединения под названием FlexVPN-IOS:

   На Вкладке Безопасность тип VPN должен быть IKEv2.В Опознавательном разделе выберите **сертификаты компьютера Use**.




Профиль FlexVPN-IOS теперь готов быть связанным после импорта certifcate к хранилищу сертификата компьютера.

## Получите сертификат клиента

Сертификат клиента требует этих факторов:

- Сертификат клиента имеет EKU 'Аутентификации клиента'. Кроме того, CA дает сертификат 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
```

- Сертификат 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
```

## Важные подробные данные

- 'Промежуточное звено IKE IPSec' (OID = 1.3.6.1.5.5.8.2.2) должно использоваться в

качестве EKU, если применяются оба из этих операторов:

Сервер IKEv2 является сервером Windows 2008.Существует несколько Сертификатов проверки подлинности сервера в использовании для соединений IKEv2. Если это истинно, или разместите и EKU 'Проверки подлинности сервера' и 'Промежуточный EKU' IKE IPSec на одном сертификате, или распределите эти EKU среди сертификатов. Удостоверьтесь, что по крайней мере один сертификат содержит 'Промежуточный EKU' IKE IPSec.

См. Устранение проблем дополнительных сведений IKEv2 VPN Connectionsfor.

- В развертываниях FlexVPN не используйте 'Промежуточное звено IKE IPSec' в EKU. Если вы делаете, клиент IKEv2 не берет серверный сертификат IKEv2. В результате они не в состоянии ответить на CERTREQ от IOS в ответном сообщении IKE_SA_INIT и таким образом быть не в состоянии соединяться с 13806 Ошибочными ID.

- В то время как альтернативное имя субъекта (SAN) не требуется, приемлемо, если сертификаты имеют тот.

- На Windows 7 Client Certificate Store удостоверьтесь, что Хранилище полномочий Машины сертификата доверенного корня имеет наименьшее количество количества возможных сертификатов. Если это имеет больше чем приблизительно 50, Cisco IOS могла бы быть не в состоянии читать все информационное наполнение Cert_Req, которое содержит Составное имя (DN) Сертификата всего известного CAs от коробки Windows 7. В результате согласование отказывает, и вы видите таймаут соединения на клиенте.

# Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

Средство интерпретации выходных данных (только зарегистрированные клиенты) поддерживает **некоторые команды show. Используйте Средство интерпретации выходных данных, чтобы просмотреть анализ выходных данных команды 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:
```

# Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

# Дополнительные сведения

- Отладки ASA IKEv2 для сквозного VPN-соединение с PSK TechNote
- IPsec ASA и отладки IKE (Основной режим IKEv1) Технические примечания по поиску и устранению проблем
- IPSec IOS и отладки IKE - Технические примечания по поиску и устранению проблем Основного режима IKEv1
- IPSec ASA и отладки IKE - Агрессивный режим IKEv1 TechNote
- CISCO ASA 5500 SERIES ADAPTIVE SECURITY APPLIANCES
- Загрузки программного обеспечения многофункциональных устройств защиты Cisco ASA серии 5500
- (межсетевой экран Cisco IOS)
- ПО Cisco IOS)
- Secure Shell (SSH)
- Согласование IPsec/Протоколы IKE
- Cisco Systems – техническая поддержка и документация