# Пример конфигурации L2TP по IPsec между Windows 2000 и концентратором VPN 3000 с использованием цифровых сертификатов

## Содержание



## Введение

Этот документ показывает, что пошаговая процедура использовала подключать с VPN 3000 Concentrator от клиента Windows 2000 использование L2TP/IPSec встроенный клиент. Предполагается, что вы используете цифровые сертификаты (автономный корневой центр сертификации (CA) без Протокола регистрации сертификата (CEP)) для аутентификации соединения с Концентратором VPN. Этот документ использует Microsoft Certificate Service для рисунка. См. Веб-узел Microsoft для документации относительно того, как настроить его.

**Примечание:** Это - пример только потому, что может измениться появление экранов Windows 2000.

## Предварительные условия

### Требования

Для этого документа отсутствуют особые требования.

## Используемые компоненты

Сведения в этом документе для Концентратора серии Cisco VPN 3000.

## Цели

В этой процедуре, вы выполняете следующие шаги:

1. Получите корневой сертификат.
2. Получите сертификат идентификации для клиента.
3. Создайте соединение с VPN 3000 с помощью Мастера сетевых подключений.
4. Настройка концентратора VPN 3000.

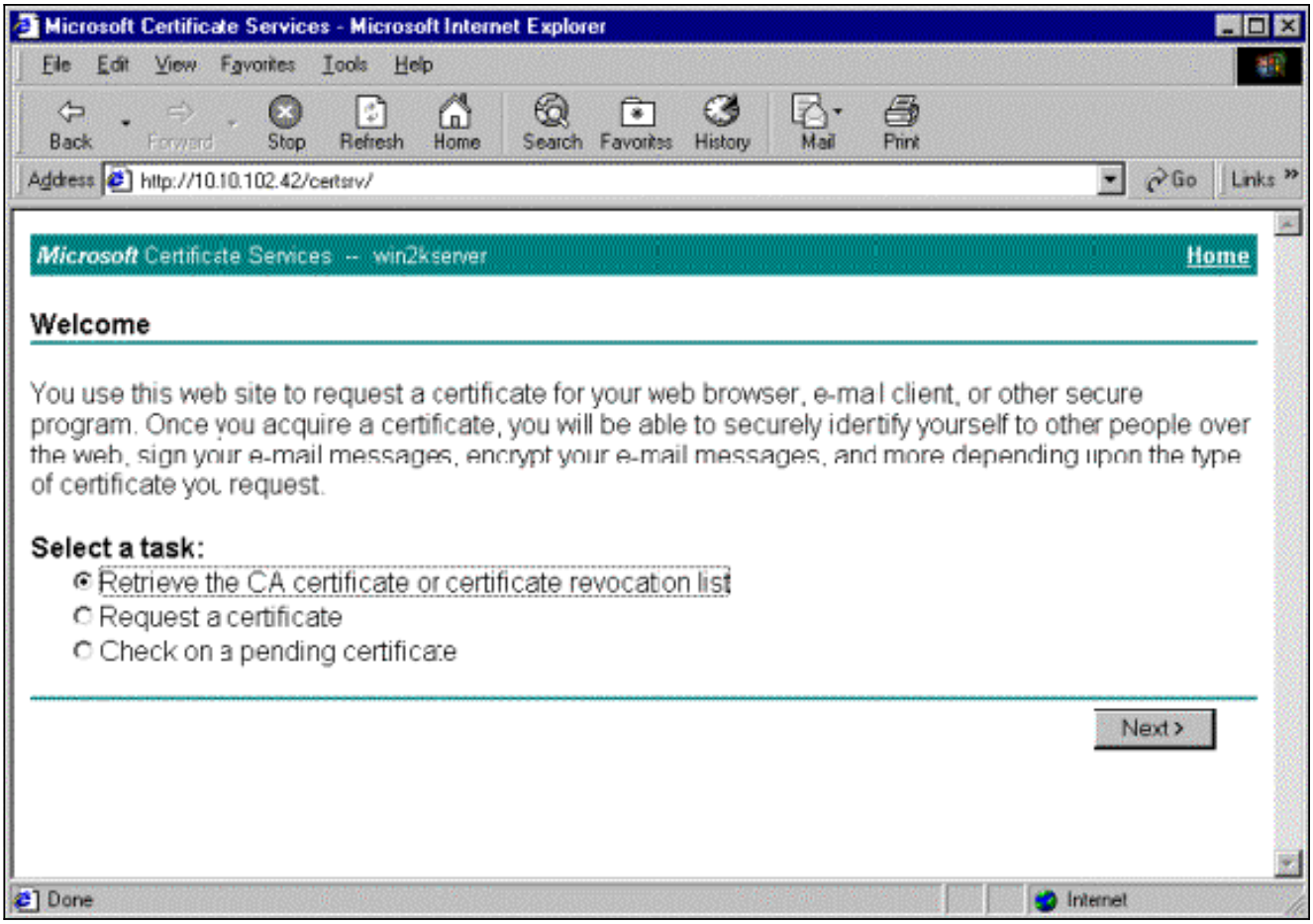
## Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.

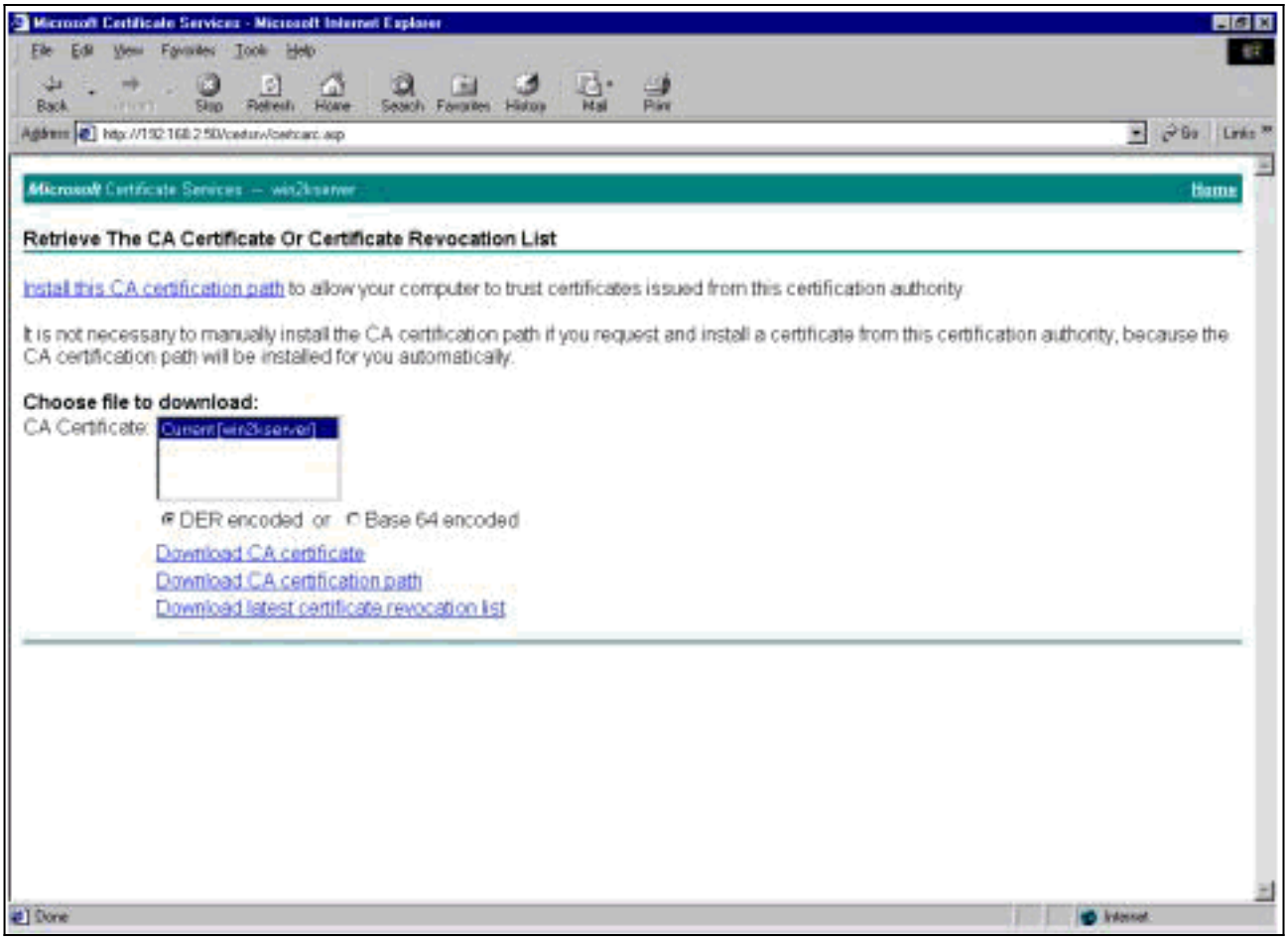
# Получите корневой сертификат

Завершите эти инструкции для получения корневого сертификата:

1. Откройте окно браузера и введите URL для Microsoft Certificate Authority (обычно http://servername или IP-адрес CA/certsrv).Окно приветствия для извлечений сертификата и показов запросов.
2. На Окне приветствия под Выбором задача выберите **Retrieve the CA certificate или список отозванных сертификатов** и нажмите **Next**.



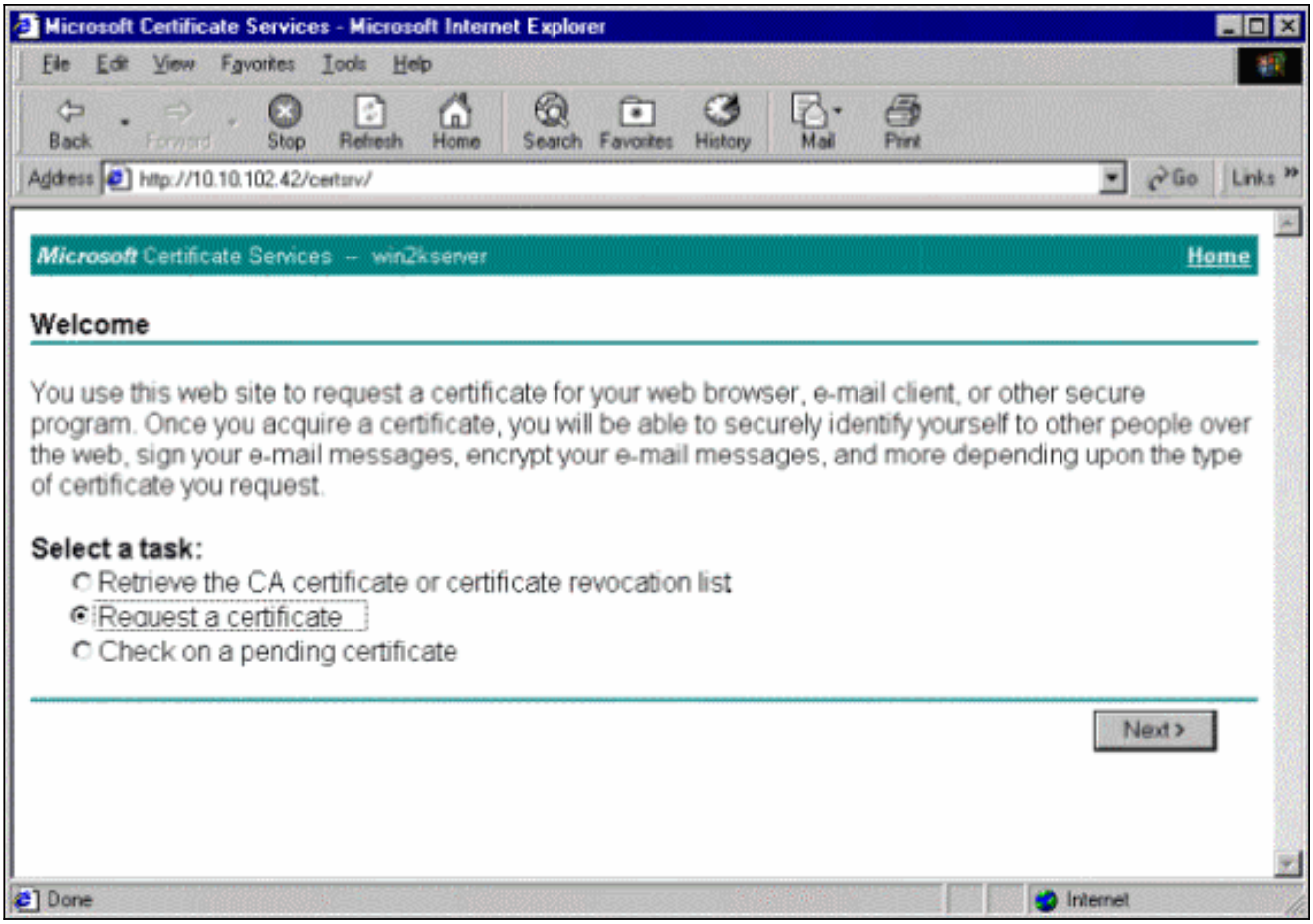

3. От Получения сертификата CA или окна списка отозванных сертификатов, нажмите **Install этот путь сертификации CA** в левом угле.Это добавляет сертификат CA к хранилищу полномочий Сертификата доверенного корня. Это означает, что доверяют любым сертификатам этот CA проблемы этому клиенту.



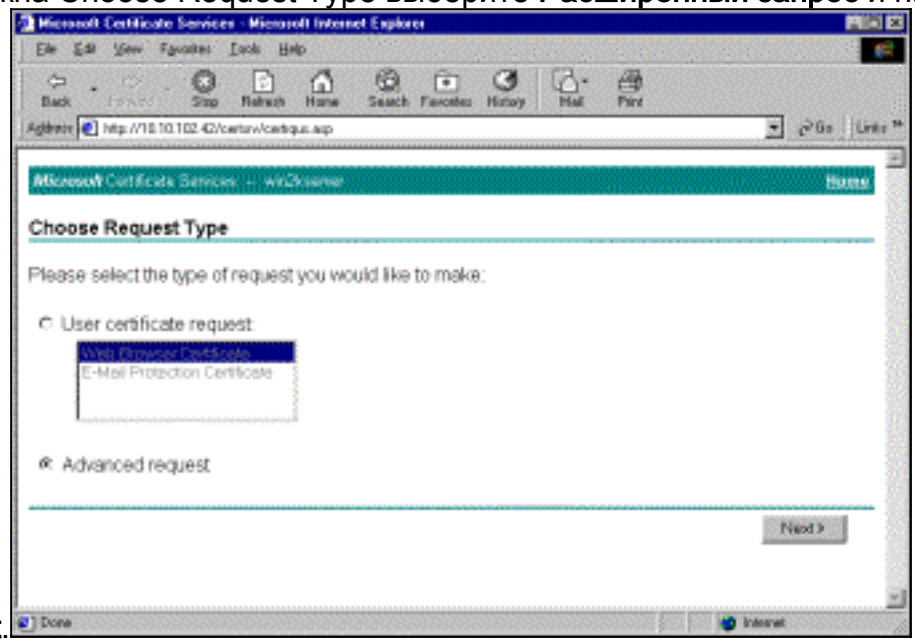

## Получите сертификат идентификации для клиента

Выполните эти шаги для получения сертификата идентификации для клиента:

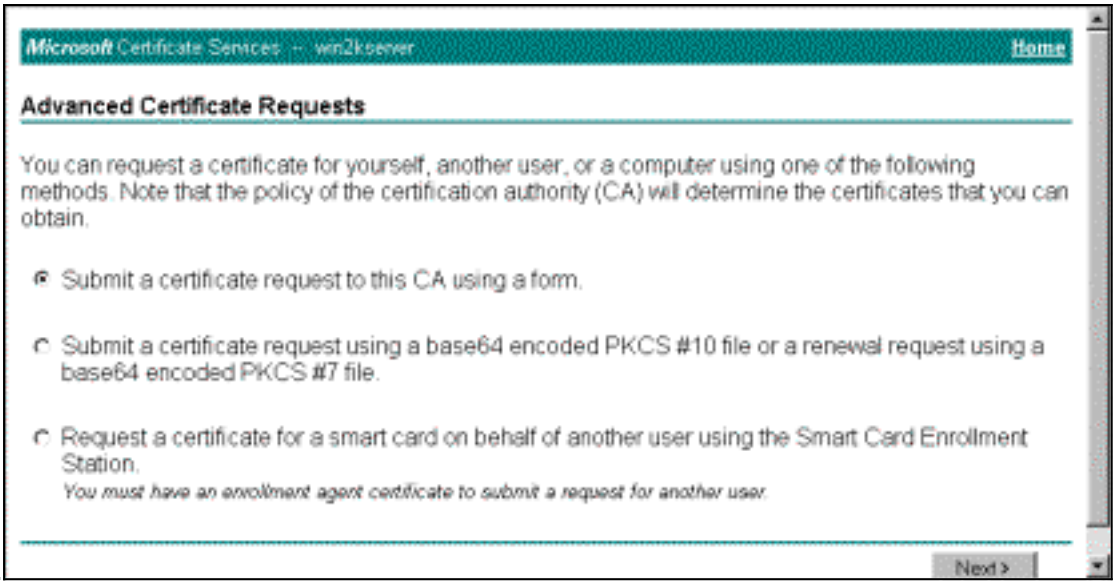
1. Откройте окно браузера и введите URL для Microsoft Certificate Authority (обычно http://servername или IP-адрес CA/certsrv).Окно приветствия для извлечений сертификата и показов запросов.
2. От Окна приветствия, под Выбором задача, выбирают **Request сертификат** и нажимают **Next**.



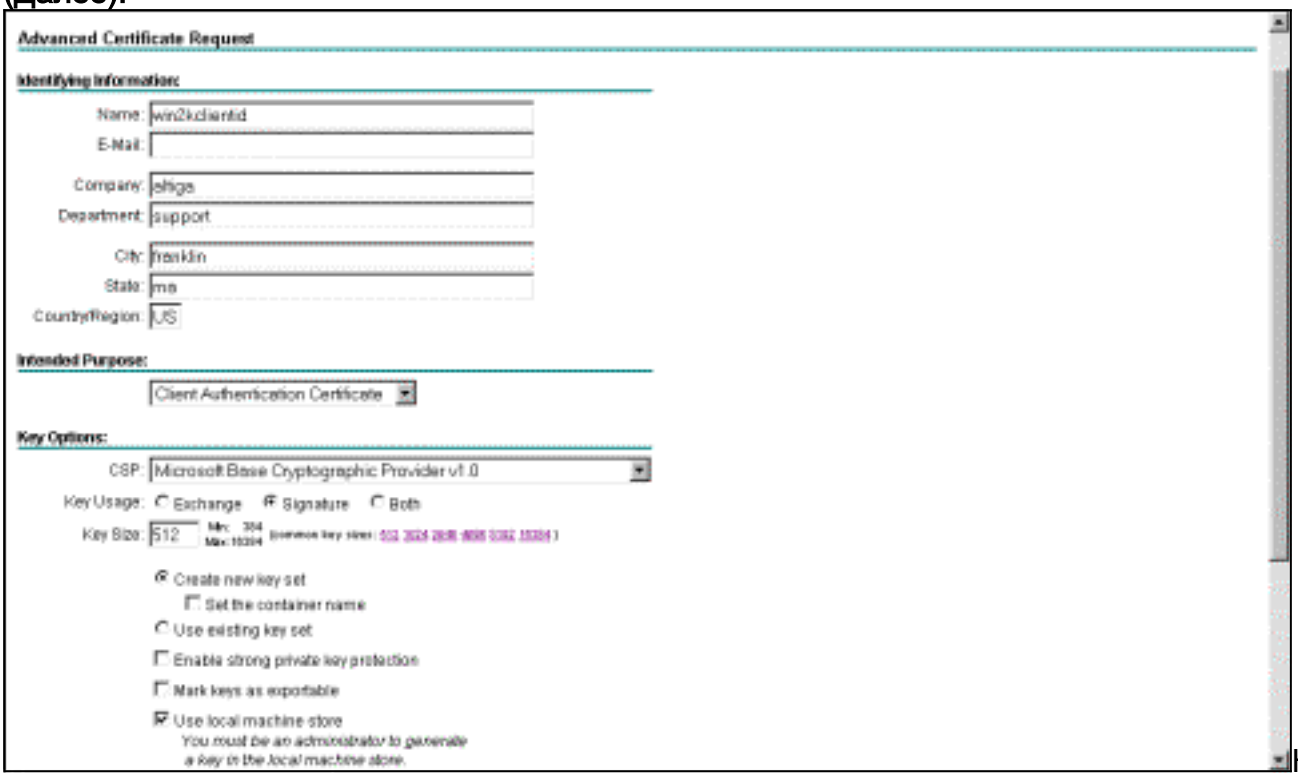

3. Из окна Choose Request Type выберите **Расширенный запрос** и нажмите **Next**.



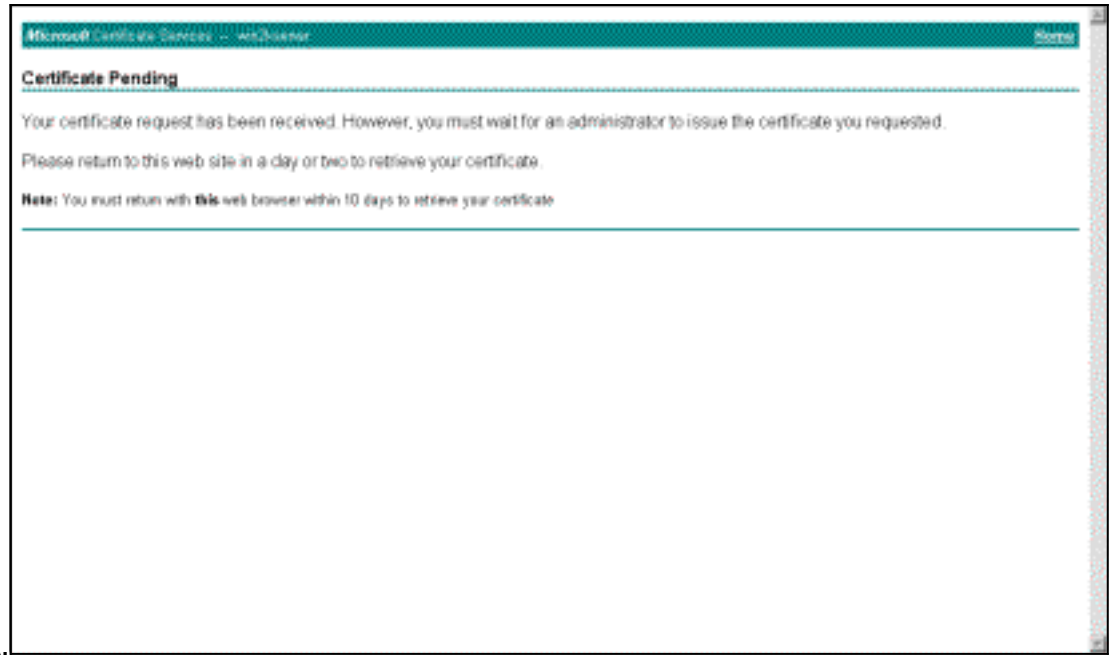

4. Из окна Advanced Certificate Requests выберите **Подтверждение запроса о сертификате в данный центр сертификации с использованием**

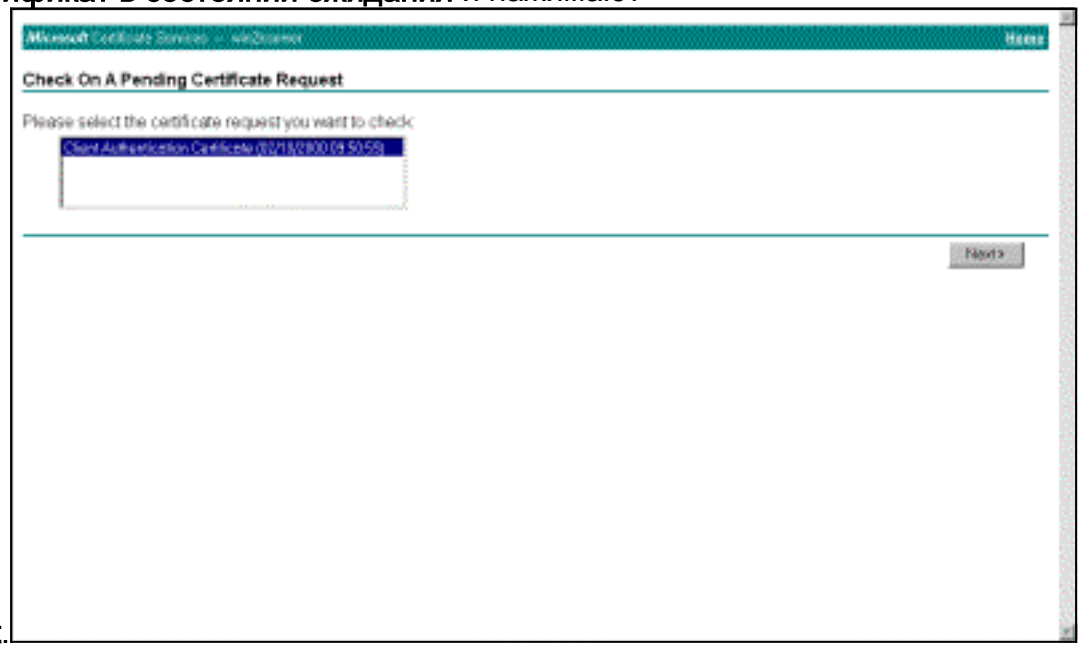
формы. 

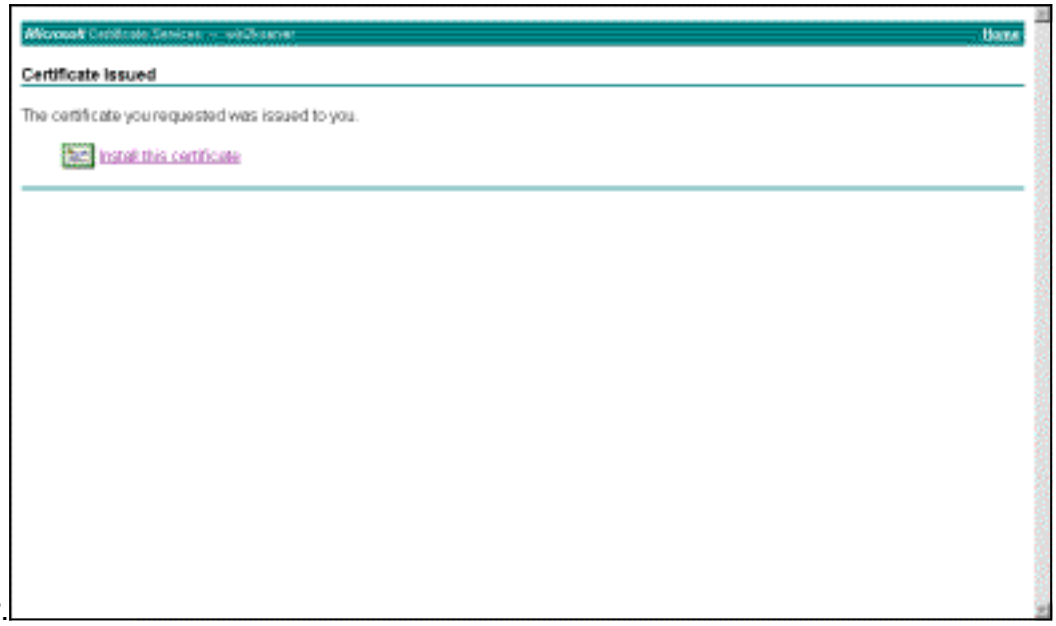

5. Заполните поля как в данном примере.Значение для Отдела (подразделение) должно совпасть с группой, настроенной на Концентраторе VPN. Не задавайте размер ключа, больше, чем 1024. Обязательно установите флажок для **памяти локального компьютера Использования. Закончив, нажмите кнопку Next (Далее).**



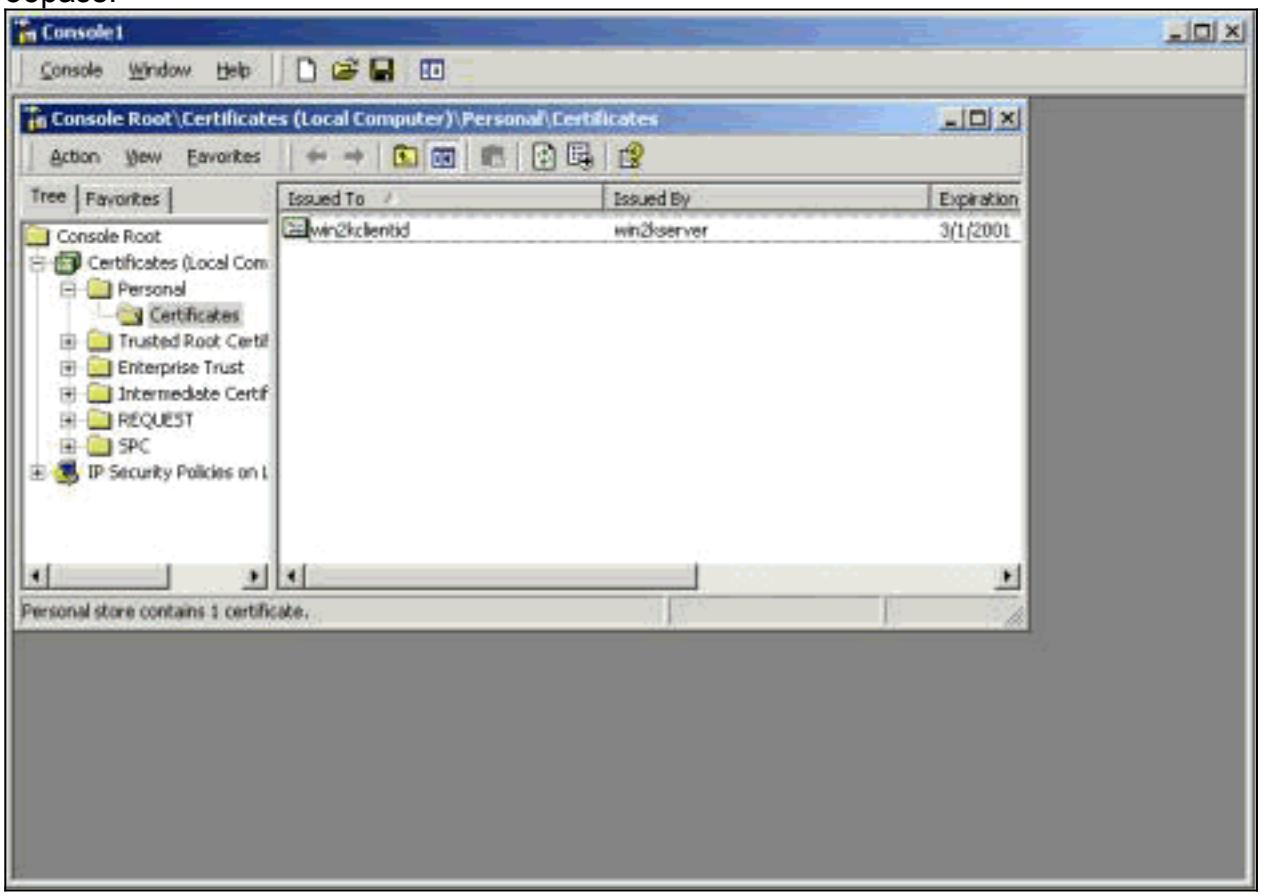

На основе того, как настроен сервер CA, это окно иногда появляется. Если это делает, свяжитесь с администратором

CA. 


6. Нажмите **Home**, чтобы возвратиться к основному экрану, выбрать**, проверяют сертификат в состоянии ожидания** и нажимают **Next**. 


7. На окне Certificate Issued нажмите **Install этот сертификат**. 

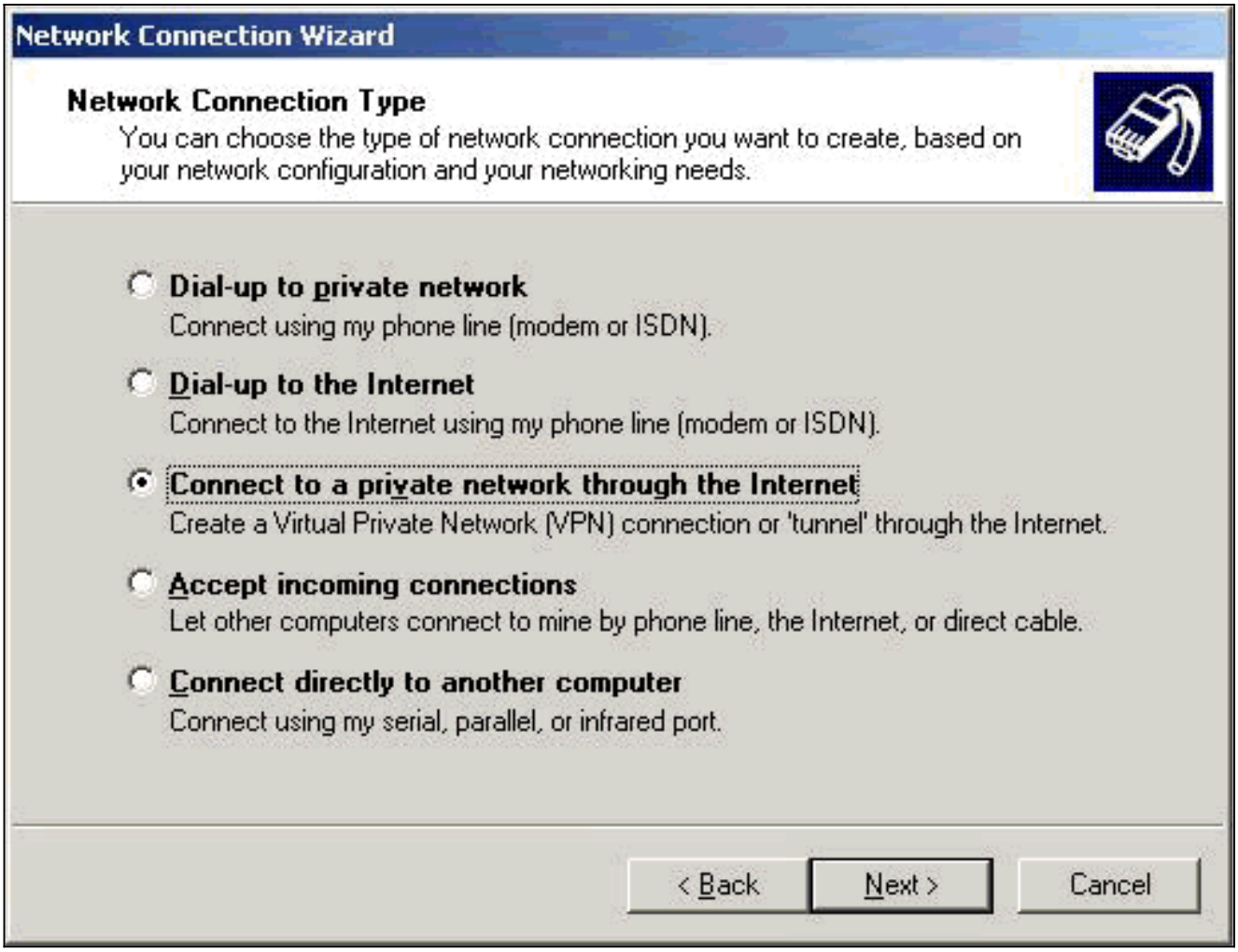
8. Для просмотра сертификата клиента выберите **Start> Run** и выполните Консоль управления Microsoft (MMC).
9. **Кликните Console и выберите Add/Remove Snap-in.**
10. **Нажмите Add** и выберите **Certificate** из списка.
11. Когда окно появляется, который спрашивает вас область сертификата, выберите **Computer Account**.
12. Проверьте, что сертификат сервера CA расположен под Доверенными корневыми центрами сертификации. Также проверьте, что у вас есть сертификат путем выбора **Console Root> Certificate (Local Computer)> Personal> Certificates**, как показано в этом образе.



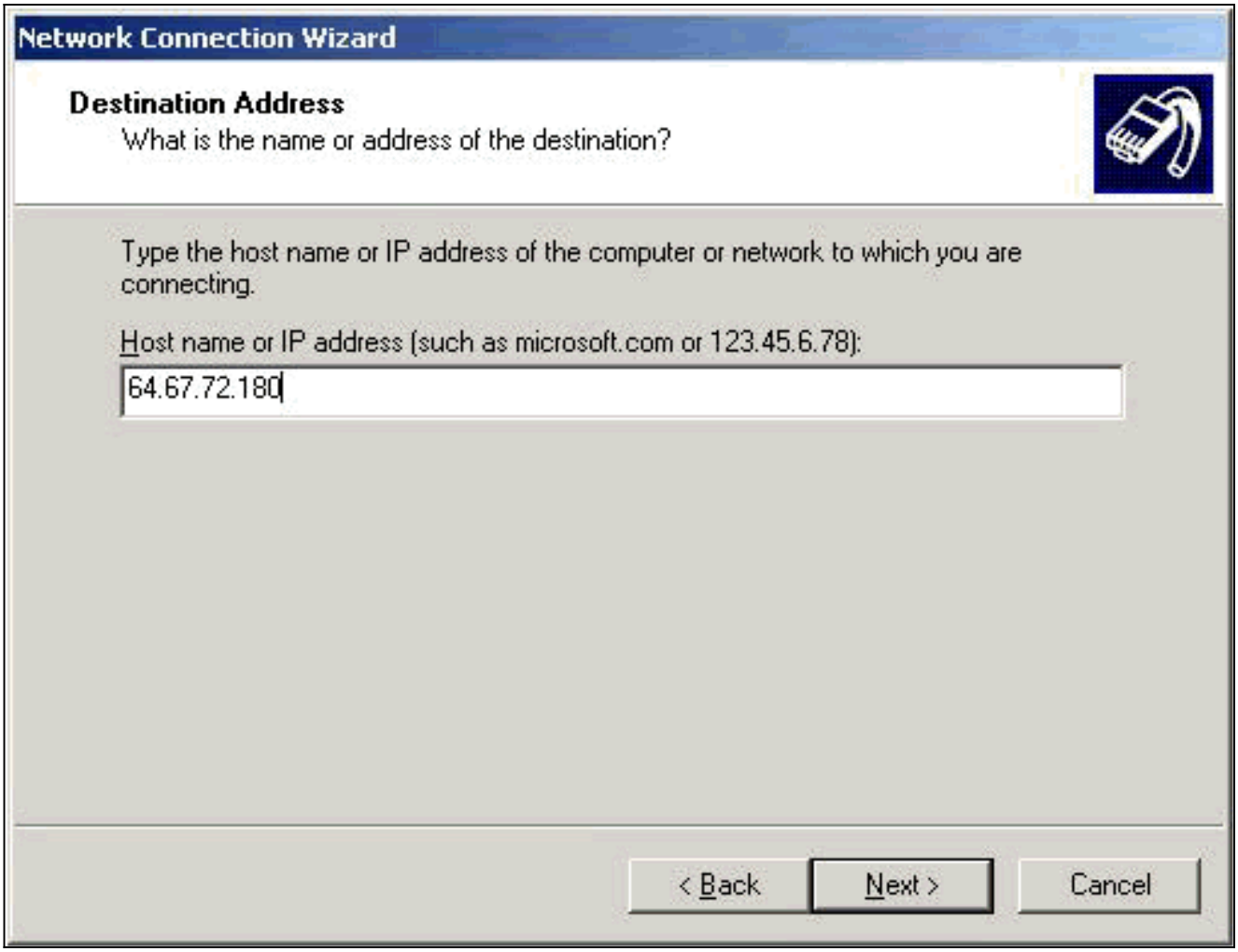

## Создайте соединение с VPN 3000 Использование мастера сетевых подключений

Завершите эту процедуру для создания соединения с VPN 3000 с помощью мастера сетевых подключений:

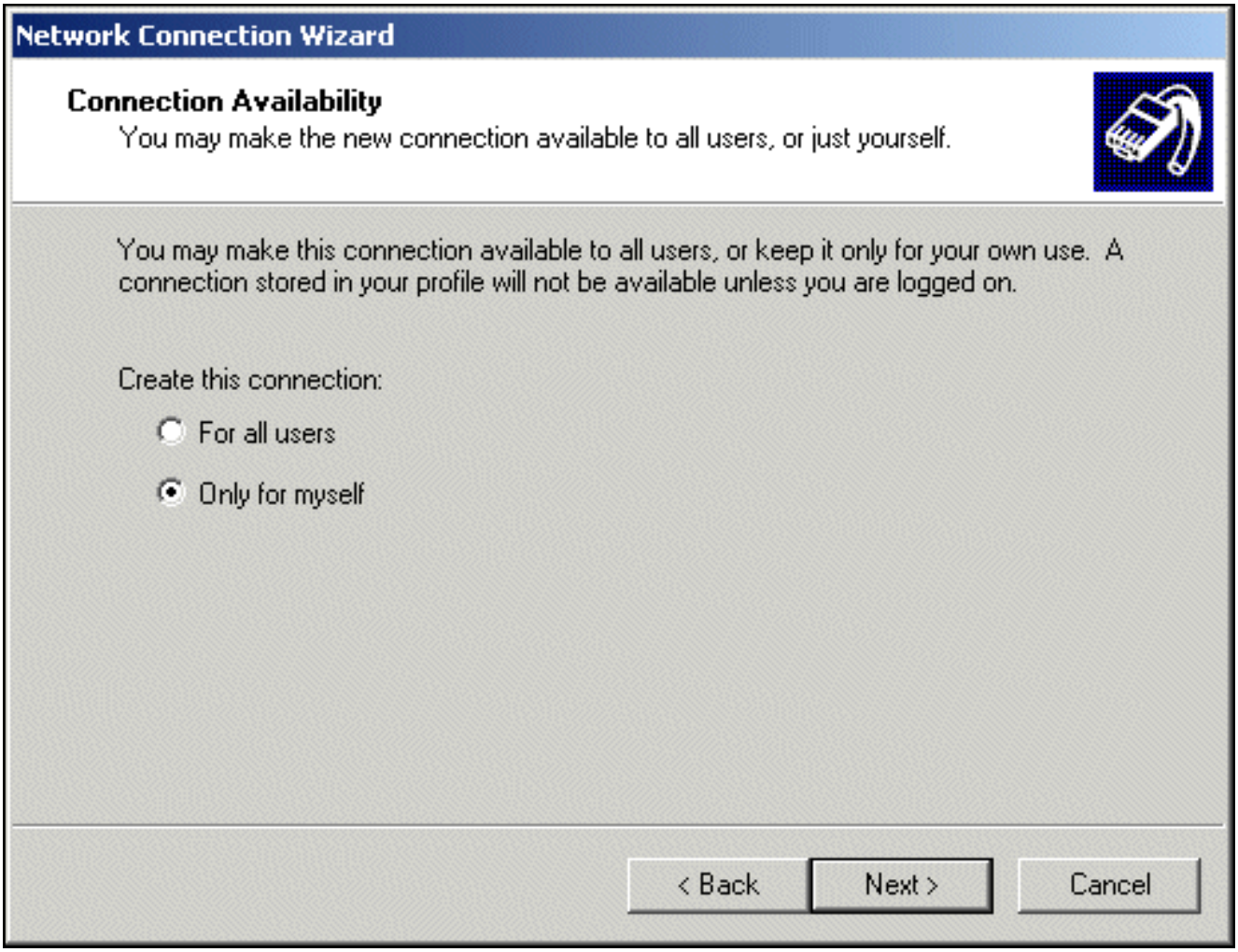
1. Щелкните правой кнопкой мыши **My Network Places**, выберите **Properties** и нажмите **Make New Connection**.
2. Из окна Network Connection Type выберите **Connect к частной сети через Интернет** и затем нажмите
   **Next**.



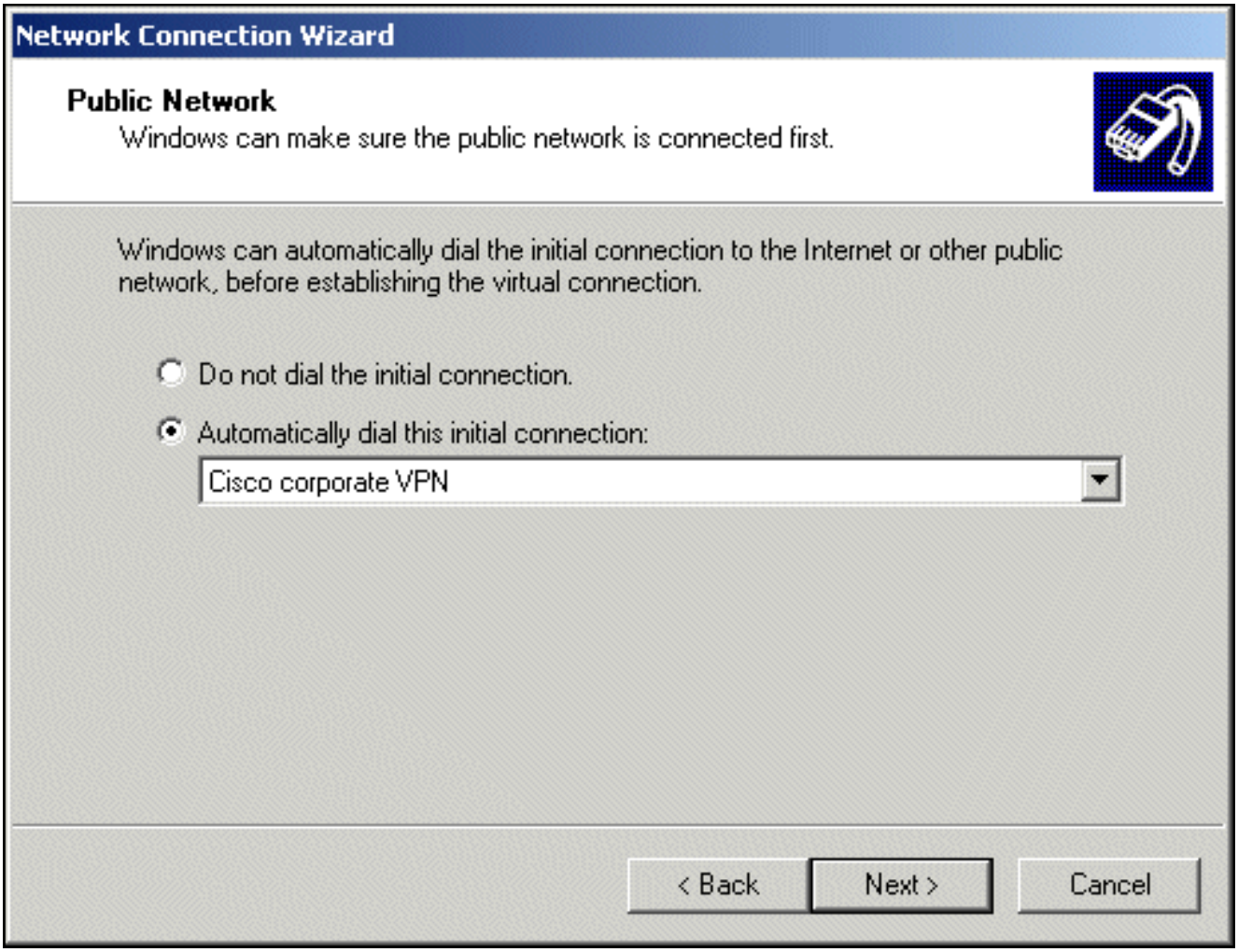

3. Введите имя хоста или IP-адрес открытого интерфейса Концентратора VPN, и нажмите **Next**.



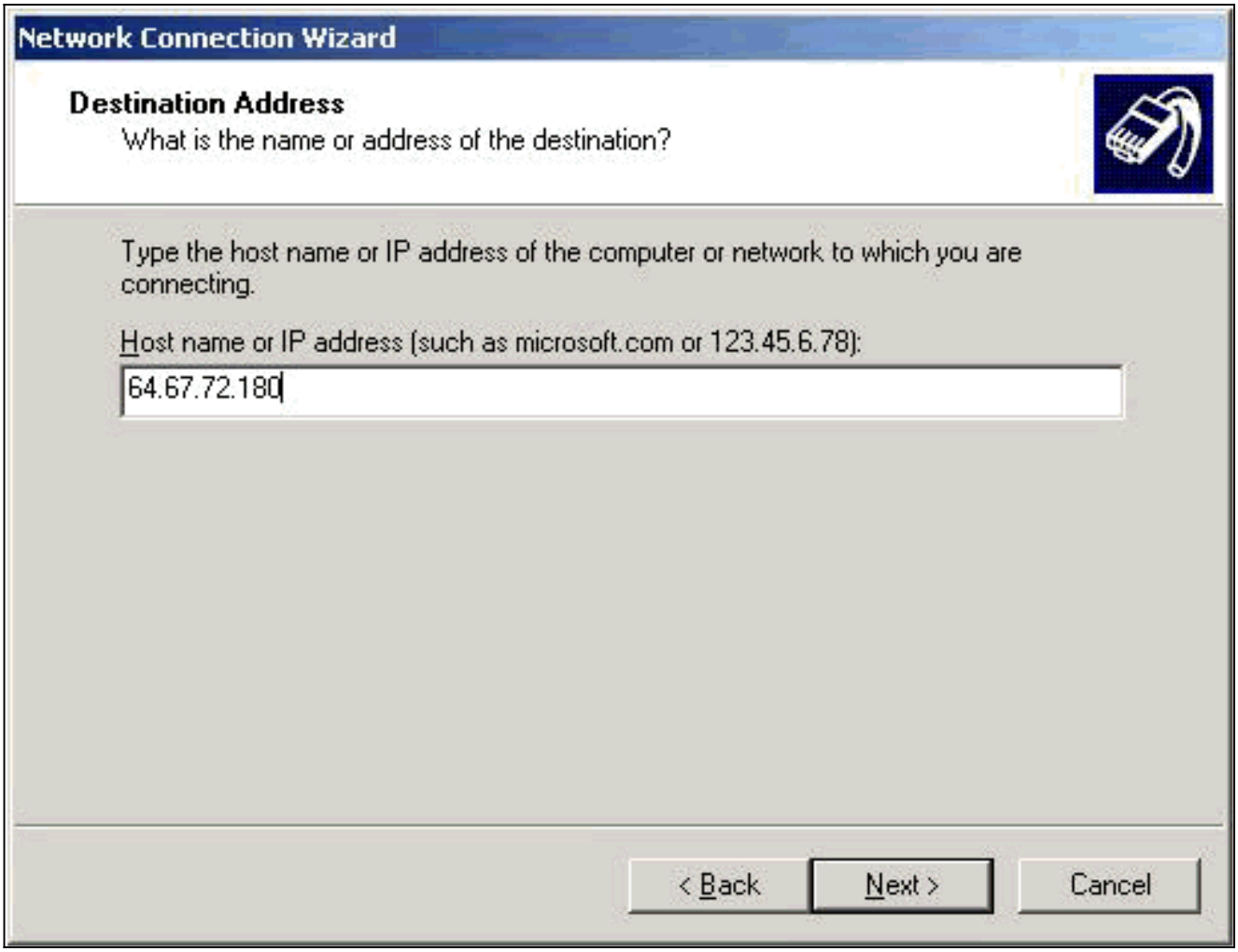

4. На окне Connection Availability выберите **Only для меня** и нажмите **Next**.




5. На окне Public Network выберите, набрать ли номер первоначальное подключение (учетная запись интернет-провайдера)
автоматически.

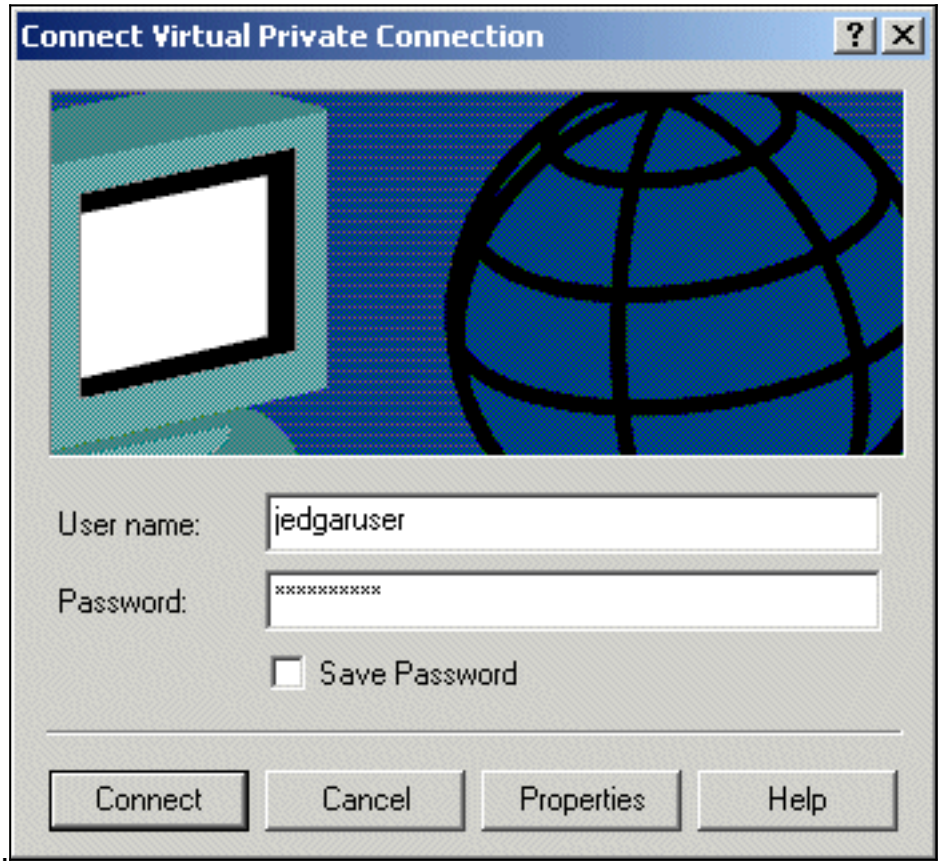



6. На экране Destination Address введите имя хоста или IP-адрес VPN 3000 Concentrator, и нажмите
**Next**.

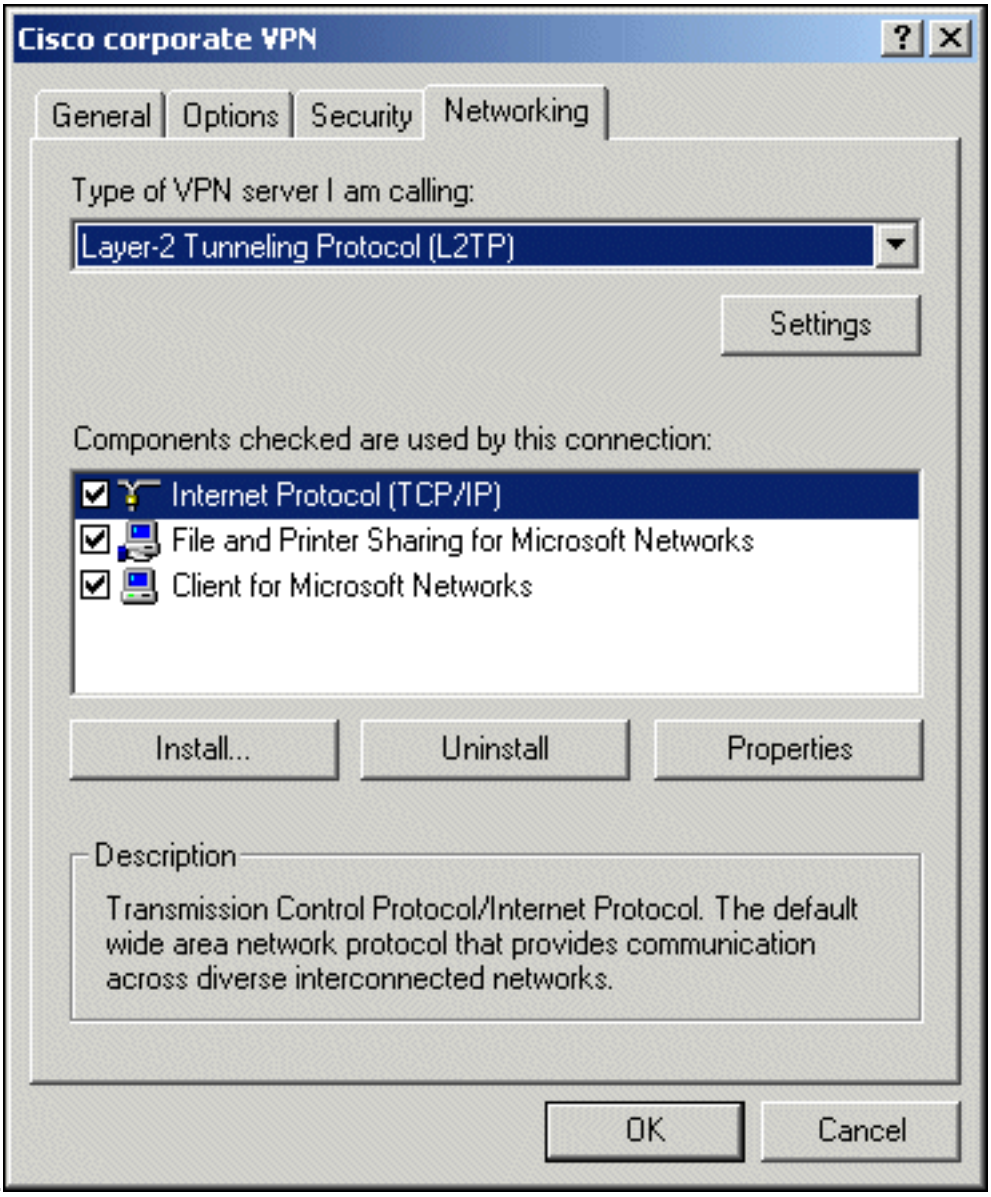



7. На окне Network Connection Wizard введите имя для соединения и нажмите **Finish**.В данном примере соединение называют "Cisco корпоративной VPN".


8. На окне Virtual Private Connection нажмите **Properties**.

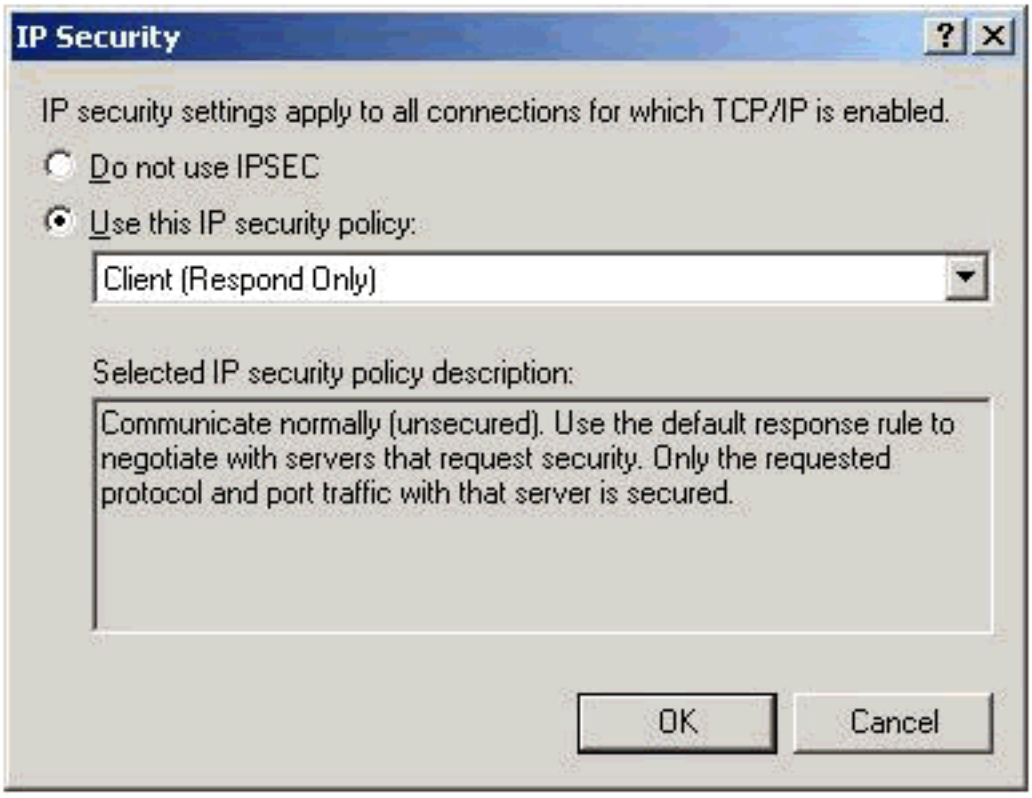



9. На Окне свойств выберите Вкладку Сеть.
10. Под Типом сервера VPN я звоню, выберите **L2TP** из ниспадающего меню, выделите **TCP/IP Протокола Интернета** и нажмите




**Properties.**

11. Выберите **Advanced> Options> Properties.**
12. На окне IP Security выберите **политику безопасности Use this**




**IP**.

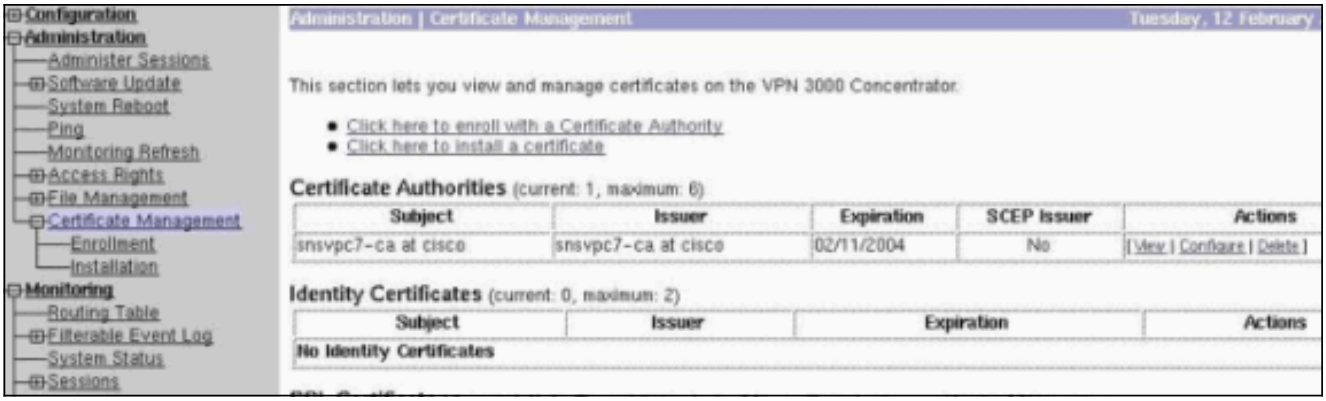
13. Выберите **Client (Respond Only)** политика от ниспадающего меню и нажимайте **OK** несколько раз, пока вы не возвратитесь к экрану Connect.
14. Для инициирования соединения введите имя пользователя и пароль и нажмите **Connect**.

## Настройка концентратора VPN 3000

### Получите корневой сертификат

Выполните эти шаги для получения корневого сертификата для VPN 3000 Concentrator:

1. Укажите свой браузер к вашему CA (обычно что-то, такому как http://ip_add_of_ca/certsrv/), **Получите сертификат CA или список отозванных сертификатов**, и нажмите **Next**.
2. Нажмите **Download CA certificate** и сохраните файл где-нибудь на вашем локальном диске.
3. На VPN 3000 Concentrator выберите **Administration> Certificate Management** и нажмите **Click here для установки Сертификата CA Установки** и **сертификата**.
4. Нажмите **Upload File from Workstation**.
5. Нажмите **Browse** и выберите файл сертификата CA, который вы только что загрузили.
6. Выделите имя файла и нажмите **Install**.




## Получите сертификат идентификации для VPN 3000 Concentrator

Выполните эти шаги для получения сертификата идентификации для VPN 3000 Concentrator:

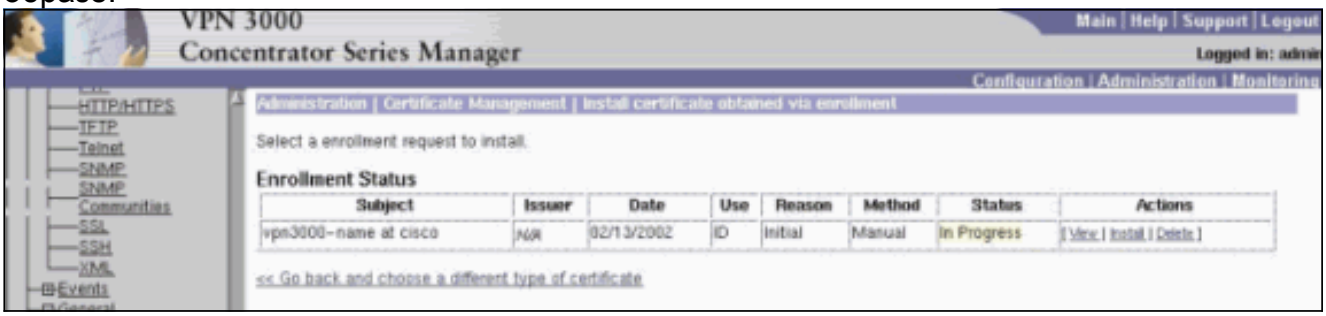
1. Выберите**> Certificate Management ConfAdministration>, Регистрируются> Сертификат идентификации**, затем нажимают **Enroll via PKCS10 Request (Manual)**. Заполните форму как показано здесь и нажмите
**Enroll**.



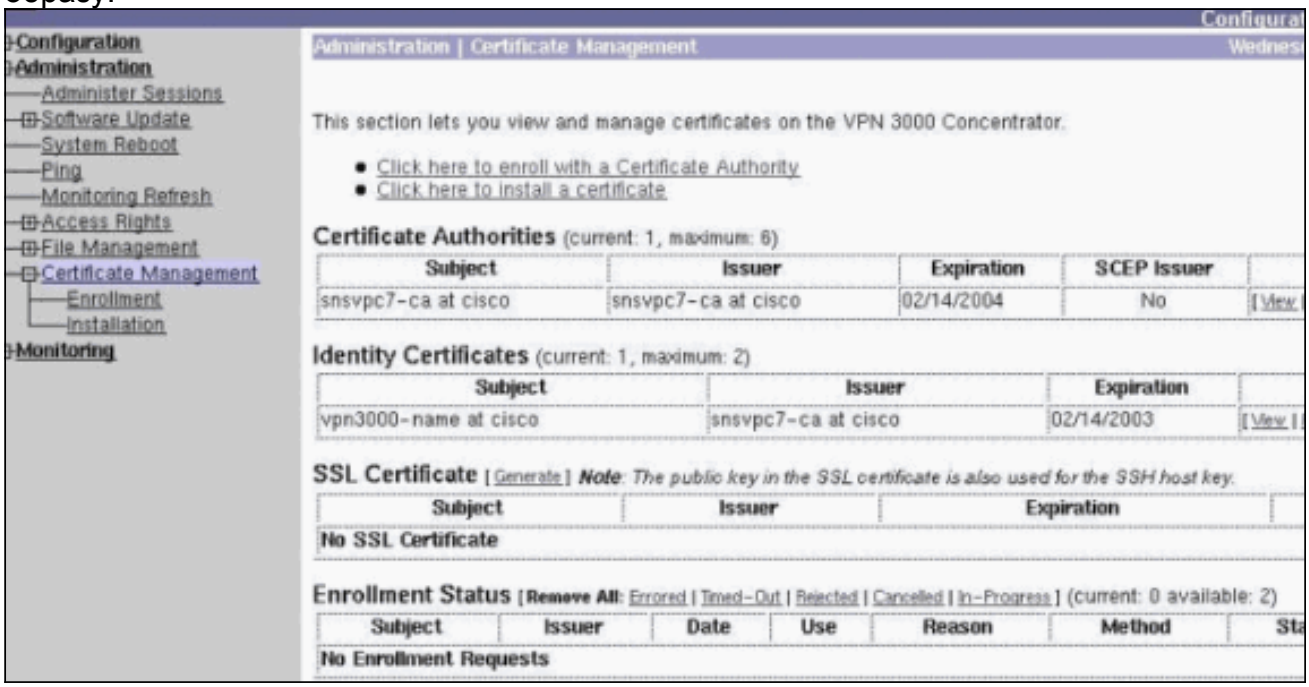
Появится окно браузера с запросом сертификата. Это должно содержать текст, подобный этим выходным данным:
```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBPDCB5wIBADBQMRUwEwYDVQQDEwx2cG4zMDAwLW5hbWUxDDAKBgNVBAsTA3Nu
czEOMAwGA1UEChMFY2lzY28xDDAKBgNVBAcTA2J4bDELMAkGA1UEBhMCYmUwWjAN
BgkqhkiG9w0BAQEFAANJADBGAkEAx7K+pvE004qILNNw3kPVWXrdlqZV4yeOIPdh
C8/V5Yuqq5tMWY3L1W6DC0p256bvGqzd5fhqSkOhBVnNJ1Y/KQIBA6A0MDIGCSqG
SIb3DQEJDjElMCMwIQYDVR0RBBowGIIWdnBuMzAwMC1uYW1lLmNpc2NvLmNvbTAN
BgkqhkiG9w0BAQQFAANBABzcG3IKaWnDLFtrNf1QDi+D7w8dxPu74b/BRHn9fsKI
X6+X0ed0EuEgm1/2nfj8Ux0nV5F/c5wukUfysMmJ/ak=
-----END NEW CERTIFICATE REQUEST-----
```
2. Укажите свой браузер к вашему серверу CA, проверьте **Запрос сертификат** и нажмите **Next**.
3. Проверьте **Расширенный запрос**, **нажмите Next** и выберите **Submit запрос сертификата с помощью base64 кодированные PKC #10 файл или запрос на обновление с помощью**

**base64 кодированные PKC #7 файл**.

4. **Нажмите кнопку Next.** Вырежьте и вставить текст запроса сертификата, показанного ранее в области для текста. **Нажмите кнопку Submit (Отправить).**
5. На основе того, как настроен сервер CA, можно нажать **Download CA certificate**. Или поскольку скоро сертификат был выполнен CA, вернитесь к своему серверу CA, и проверка **Проверяют сертификат в состоянии ожидания**.
6. **Нажмите Next**, выберите свой запрос и нажмите **Next** снова.
7. Нажмите **Download CA certificate** и сохраните файл на локальном диске.
8. На VPN 3000 Concentrator выберите **Administration> Certificate Management> Install** и нажмите **сертификат Install, полученный через регистрацию**.Вы тогда видите свой запрос в состоянии ожидания со статусом "Происходящих", как в этом образе.




9. Нажмите **Install**, придерживавшийся **Файлом Загрузки от Рабочей станции**.
10. Нажмите **Browse** и выберите файл, который содержит ваш сертификат, выполненный CA.
11. Выделите имя файла и нажмите **Install**.
12. **Выберите Administration (Администрирование) > Certificate Management (Управление сертификатами).** Появляется экран, подобный этому образу.



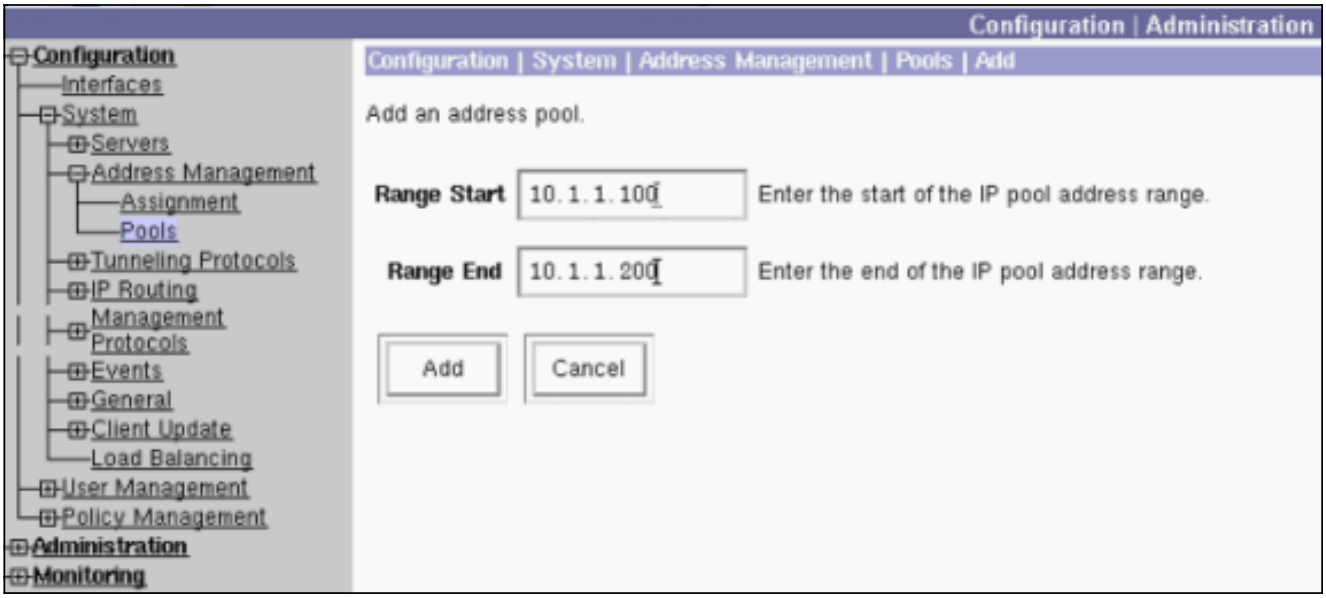

## Настройте пул для клиентов

Завершите эту процедуру для настройки пула для клиентов:

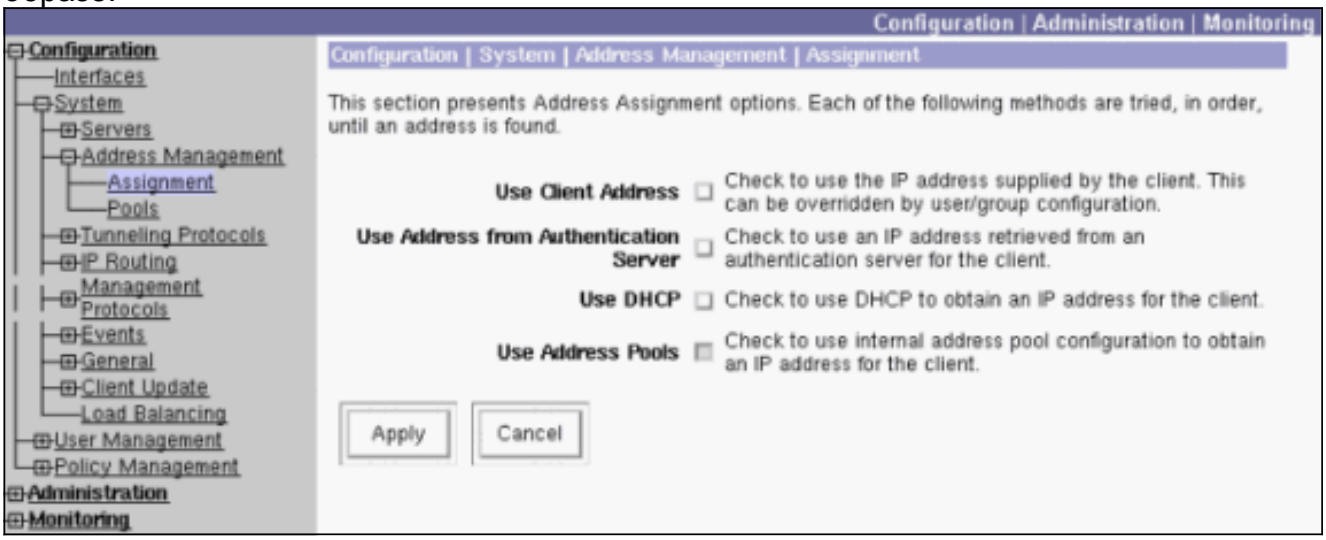
1. Для присвоения доступного диапазона IP-адресов укажите браузер к внутреннему

интерфейсу VPN 3000 Concentrator и выберите **Configuration> System> Address Management> Pools> Add**.

2. Задайте диапазон IP-адресов, которые не конфликтуют ни с какими другими устройствами на внутренней сети и **нажмите Add**.



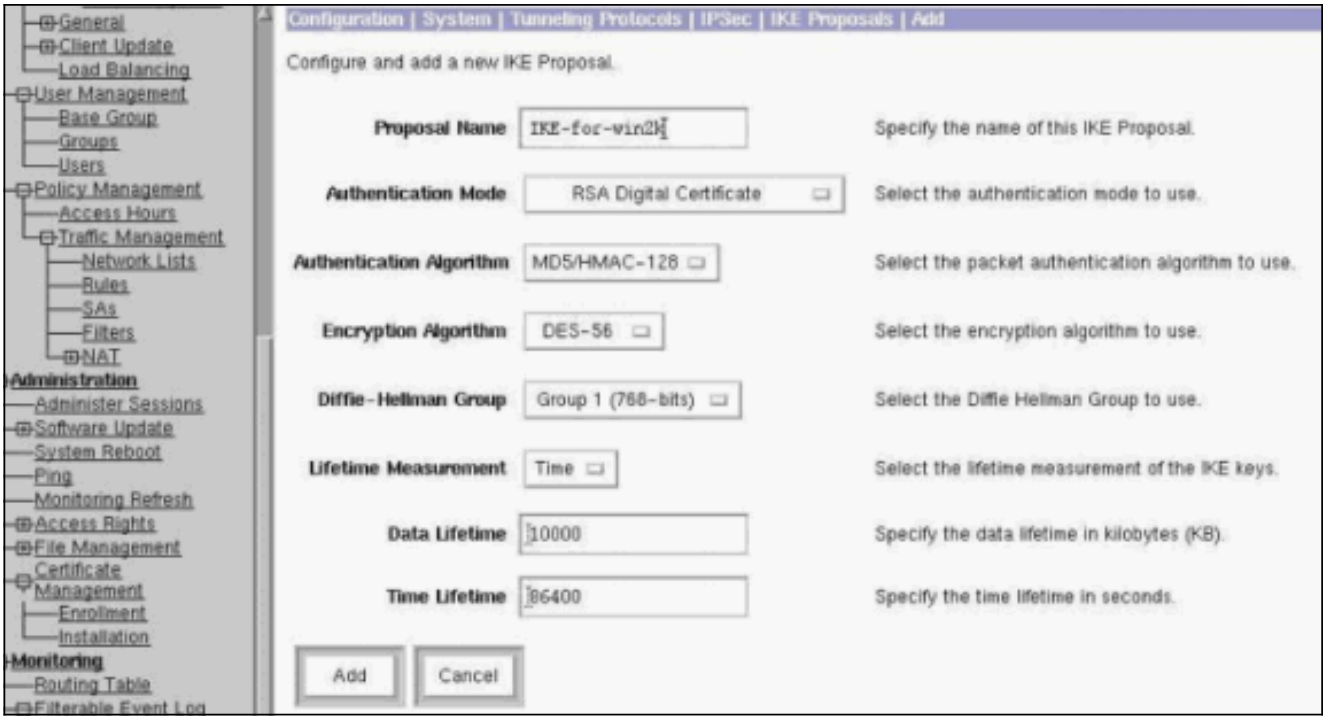

3. Чтобы сказать VPN 3000 Concentrator использовать пул, выберите **Configuration> System> Address Management> Assignment**, установите флажок **Пулов адресов Использования** и нажмите **Apply**, как в этом образе.




## Настройте предложение ike

Выполните эти шаги для настройки Предложения ike:

1. Выберите **Configuration> System> Tunneling Protocols> IPSec> IKE Proposals**, **нажмите Add** и выберите параметры, как показано в этом образе.




2. **Нажмите Add**, выделите новое предложение в правом столбце и нажмите **Activate**.

## Настройте SA

Завершите эту процедуру для настройки Сопоставления безопасности (SA):

1. Выберите **Configuration> Policy Management> Traffic Management> SA** и нажмите **ESP-L2TP-TRANSPORT**.Если этот SA не доступен или если вы используете его для некоторой другой цели, создаете новый SA, подобный этому. Другие параметры настройки для SA приемлемы. Измените этот параметр на основе своей политики безопасности.
2. Выберите цифровой сертификат, который вы настроили ранее под ниспадающим меню **Цифрового сертификата**. Выберите предложение по Протоколу IKE **IKE ДЛЯ WIN2K.Примечание:** Это не является обязательным. Когда подключения клиента L2TP/IPSec к Концентратору VPN, все Предложения ike, настроенные в соответствии с активным столбцом **страницы Configuration> System> Tunneling Protocols> IPSec> IKE Proposals**, пробуют в заказе.Этот образ показывает конфигурацию, необходимую для SA:


## Настройте группу и пользователя

Завершите эту процедуру для настройки Группы и Пользователя:

1. Выберите **Configuration> User Management> Base Group**.
2. Под Вкладкой Общие удостоверьтесь, что проверен **L2TP по IPSec**.
3. Под вкладкой IPSec выберите **ESP-L2TP-TRANSPORT SA**.
4. Под вкладкой PPTP/L2TP снимите флажок со всеми **Параметрами шифрования L2TP**.
5. Выберите**> Users Configuration> User Management** и **нажмите Add**.
6. Введите имя и пароль, которое вы используете для соединения от Клиента Windows 2000. Удостоверьтесь, что вы выбираете **Base Group** под Выбором группы.
7. Под Вкладкой Общие проверьте **L2TP по** протоколу **Туннелирования IPSec**.
8. Под вкладкой IPSec выберите **ESP-L2TP-TRANSPORT SA**.
9. Под вкладкой PPTP/L2TP снимите флажок со всеми **Параметрами шифрования L2TP** и **нажмите Add**.Вы теперь в состоянии подключить с помощью L2TP/IPSec Клиента Windows 2000.**Примечание:** Вы приняли решение настроить базовую группу для принятия удаленного соединения L2TP/IPSec. Также возможно настроить группу, которая совпадает с полем Организационной единицы (OU) SA для принятия входящего соединения. Конфигурация идентична.

# Данные отладки

```
269 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3868 10.48.66.76
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 7

271 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3869 10.48.66.76
```

```
  Phase 1 failure against global IKE proposal # 16:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 1

274 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3870 10.48.66.76
Proposal # 1, Transform # 2, Type ISAKMP, Id IKE
Parsing received transform:
  Phase 1 failure against global IKE proposal # 1:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

279 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3871 10.48.66.76
  Phase 1 failure against global IKE proposal # 2:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

282 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3872 10.48.66.76
  Phase 1 failure against global IKE proposal # 3:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

285 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3873 10.48.66.76
  Phase 1 failure against global IKE proposal # 4:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 1

288 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3874 10.48.66.76
  Phase 1 failure against global IKE proposal # 5:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 1

291 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3875 10.48.66.76
  Phase 1 failure against global IKE proposal # 6:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

294 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3876 10.48.66.76
  Phase 1 failure against global IKE proposal # 7:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

297 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3877 10.48.66.76
  Phase 1 failure against global IKE proposal # 8:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

300 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3878 10.48.66.76
  Phase 1 failure against global IKE proposal # 9:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

303 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3879 10.48.66.76
  Phase 1 failure against global IKE proposal # 10:
  Mismatched attr types for class DH Group:
```

```
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 1

306 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3880 10.48.66.76
  Phase 1 failure against global IKE proposal # 11:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 1

309 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3881 10.48.66.76
  Phase 1 failure against global IKE proposal # 12:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

312 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3882 10.48.66.76
  Phase 1 failure against global IKE proposal # 13:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

315 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3883 10.48.66.76
  Phase 1 failure against global IKE proposal # 14:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 1

318 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3884 10.48.66.76
  Phase 1 failure against global IKE proposal # 15:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 7

321 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3885 10.48.66.76
  Phase 1 failure against global IKE proposal # 16:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 1

324 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3886 10.48.66.76
Proposal # 1, Transform # 3, Type ISAKMP, Id IKE
Parsing received transform:
  Phase 1 failure against global IKE proposal # 1:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

329 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3887 10.48.66.76
  Phase 1 failure against global IKE proposal # 2:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

332 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3888 10.48.66.76
  Phase 1 failure against global IKE proposal # 3:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

335 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3889 10.48.66.76
  Phase 1 failure against global IKE proposal # 4:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES
```

```
338 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3890 10.48.66.76
  Phase 1 failure against global IKE proposal # 5:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

341 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3891 10.48.66.76
  Phase 1 failure against global IKE proposal # 6:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

344 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3892 10.48.66.76
  Phase 1 failure against global IKE proposal # 7:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

347 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3893 10.48.66.76
  Phase 1 failure against global IKE proposal # 8:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

350 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3894 10.48.66.76
  Phase 1 failure against global IKE proposal # 9:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

353 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3895 10.48.66.76
  Phase 1 failure against global IKE proposal # 10:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

356 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3896 10.48.66.76
  Phase 1 failure against global IKE proposal # 11:
  Mismatched attr types for class Hash Alg:
    Rcv'd: SHA
    Cfg'd: MD5

358 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3897 10.48.66.76
  Phase 1 failure against global IKE proposal # 12:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

361 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3898 10.48.66.76
  Phase 1 failure against global IKE proposal # 13:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

364 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3899 10.48.66.76
  Phase 1 failure against global IKE proposal # 14:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

367 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3900 10.48.66.76
  Phase 1 failure against global IKE proposal # 15:
  Mismatched attr types for class DH Group:
```

```
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 7

370 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3901 10.48.66.76
  Phase 1 failure against global IKE proposal # 16:
  Mismatched attr types for class Hash Alg:
    Rcv'd: SHA
    Cfg'd: MD5

372 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3902 10.48.66.76
Proposal # 1, Transform # 4, Type ISAKMP, Id IKE
Parsing received transform:
  Phase 1 failure against global IKE proposal # 1:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

377 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3903 10.48.66.76
  Phase 1 failure against global IKE proposal # 2:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

380 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3904 10.48.66.76
  Phase 1 failure against global IKE proposal # 3:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

383 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3905 10.48.66.76
  Phase 1 failure against global IKE proposal # 4:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

386 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3906 10.48.66.76
  Phase 1 failure against global IKE proposal # 5:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

389 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3907 10.48.66.76
  Phase 1 failure against global IKE proposal # 6:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

392 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3908 10.48.66.76
  Phase 1 failure against global IKE proposal # 7:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

395 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3909 10.48.66.76
  Phase 1 failure against global IKE proposal # 8:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

398 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3910 10.48.66.76
  Phase 1 failure against global IKE proposal # 9:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2
```

```
401 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3911 10.48.66.76
  Phase 1 failure against global IKE proposal # 10:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

404 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3912 10.48.66.76
  Phase 1 failure against global IKE proposal # 11:
  Mismatched attr types for class Auth Method:
    Rcv'd: RSA signature with Certificates
    Cfg'd: Preshared Key

407 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3913 10.48.66.76
  Phase 1 failure against global IKE proposal # 12:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

410 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3914 10.48.66.76
  Phase 1 failure against global IKE proposal # 13:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

413 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3915 10.48.66.76
  Phase 1 failure against global IKE proposal # 14:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

416 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3916 10.48.66.76
  Phase 1 failure against global IKE proposal # 15:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 7

419 02/15/2002 12:47:24.430 SEV=7 IKEDBG/28 RPT=20 10.48.66.76
IKE SA Proposal # 1, Transform # 4 acceptable
Matches global IKE entry # 16

420 02/15/2002 12:47:24.440 SEV=9 IKEDBG/0 RPT=3917 10.48.66.76
constructing ISA_SA for isakmp

421 02/15/2002 12:47:24.490 SEV=8 IKEDBG/0 RPT=3918 10.48.66.76
SENDING Message (msgid=0) with payloads :
HDR + SA (1) + NONE (0) ... total length : 80

423 02/15/2002 12:47:24.540 SEV=8 IKEDBG/0 RPT=3919 10.48.66.76
RECEIVED Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 152

425 02/15/2002 12:47:24.540 SEV=8 IKEDBG/0 RPT=3920 10.48.66.76
RECEIVED Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 152

427 02/15/2002 12:47:24.540 SEV=9 IKEDBG/0 RPT=3921 10.48.66.76
processing ke payload

428 02/15/2002 12:47:24.540 SEV=9 IKEDBG/0 RPT=3922 10.48.66.76
processing ISA_KE

429 02/15/2002 12:47:24.540 SEV=9 IKEDBG/1 RPT=104 10.48.66.76
processing nonce payload
```

```
430 02/15/2002 12:47:24.600 SEV=9 IKEDBG/0 RPT=3923 10.48.66.76
constructing ke payload

431 02/15/2002 12:47:24.600 SEV=9 IKEDBG/1 RPT=105 10.48.66.76
constructing nonce payload

432 02/15/2002 12:47:24.600 SEV=9 IKEDBG/0 RPT=3924 10.48.66.76
constructing certreq payload

433 02/15/2002 12:47:24.600 SEV=9 IKEDBG/0 RPT=3925 10.48.66.76
Using initiator's certreq payload data

434 02/15/2002 12:47:24.600 SEV=9 IKEDBG/46 RPT=61 10.48.66.76
constructing Cisco Unity VID payload

435 02/15/2002 12:47:24.600 SEV=9 IKEDBG/46 RPT=62 10.48.66.76
constructing xauth V6 VID payload

436 02/15/2002 12:47:24.600 SEV=9 IKEDBG/48 RPT=39 10.48.66.76
Send IOS VID

437 02/15/2002 12:47:24.600 SEV=9 IKEDBG/38 RPT=20 10.48.66.76
Constructing VPN 3000 spoofing IOS Vendor ID payload
(version: 1.0.0, capabilities: 20000001)

439 02/15/2002 12:47:24.600 SEV=9 IKEDBG/46 RPT=63 10.48.66.76
constructing VID payload

440 02/15/2002 12:47:24.600 SEV=9 IKEDBG/48 RPT=40 10.48.66.76
Send Altiga GW VID

441 02/15/2002 12:47:24.600 SEV=9 IKEDBG/0 RPT=3926 10.48.66.76
Generating keys for Responder...

442 02/15/2002 12:47:24.610 SEV=8 IKEDBG/0 RPT=3927 10.48.66.76
SENDING Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + CERT_REQ (7) + VENDOR (13) + VENDOR (13)
+ VENDOR (13) + VENDOR (13) + NONE (0) ... total length : 229

445 02/15/2002 12:47:24.640 SEV=8 IKEDBG/0 RPT=3928 10.48.66.76
RECEIVED Message (msgid=0) with payloads :
HDR + ID (5) + CERT (6) + SIG (9) + CERT_REQ (7) + NONE (0)
... total length : 1186

448 02/15/2002 12:47:24.640 SEV=9 IKEDBG/1 RPT=106 10.48.66.76
Processing ID

449 02/15/2002 12:47:24.640 SEV=9 IKEDBG/0 RPT=3929 10.48.66.76
processing cert payload

450 02/15/2002 12:47:24.640 SEV=9 IKEDBG/1 RPT=107 10.48.66.76
processing RSA signature

451 02/15/2002 12:47:24.640 SEV=9 IKEDBG/0 RPT=3930 10.48.66.76
computing hash

452 02/15/2002 12:47:24.650 SEV=9 IKEDBG/0 RPT=3931 10.48.66.76
processing cert request payload

453 02/15/2002 12:47:24.650 SEV=9 IKEDBG/0 RPT=3932 10.48.66.76
Storing cert request payload for use in MM msg 4

454 02/15/2002 12:47:24.650 SEV=9 IKEDBG/23 RPT=20 10.48.66.76
```

```
Starting group lookup for peer 10.48.66.76

455 02/15/2002 12:47:24.650 SEV=9 IKE/21 RPT=12 10.48.66.76
No Group found by matching IP Address of Cert peer 10.48.66.76

456 02/15/2002 12:47:24.650 SEV=9 IKE/20 RPT=12 10.48.66.76
No Group found by matching OU(s) from ID payload:
 ou=sns,

457 02/15/2002 12:47:24.650 SEV=9 IKE/0 RPT=12 10.48.66.76
Group [VPNC_Base_Group]
No Group name for IKE Cert session, defaulting to BASE GROUP

459 02/15/2002 12:47:24.750 SEV=7 IKEDBG/0 RPT=3933 10.48.66.76
Group [VPNC_Base_Group]
Found Phase 1 Group (VPNC_Base_Group)

460 02/15/2002 12:47:24.750 SEV=7 IKEDBG/14 RPT=20 10.48.66.76
Group [VPNC_Base_Group]
Authentication configured for Internal

461 02/15/2002 12:47:24.750 SEV=9 IKEDBG/19 RPT=20 10.48.66.76
Group [VPNC_Base_Group]
IKEGetUserAttributes: default domain = fenetwork.com

462 02/15/2002 12:47:24.770 SEV=5 IKE/79 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
Validation of certificate successful
(CN=my_name, SN=6102861F000000000005)

464 02/15/2002 12:47:24.770 SEV=7 IKEDBG/0 RPT=3934 10.48.66.76
Group [VPNC_Base_Group]
peer ID type 9 received (DER_ASN1_DN)

465 02/15/2002 12:47:24.770 SEV=9 IKEDBG/1 RPT=108 10.48.66.76
Group [VPNC_Base_Group]
constructing ID

466 02/15/2002 12:47:24.770 SEV=9 IKEDBG/0 RPT=3935 10.48.66.76
Group [VPNC_Base_Group]
constructing cert payload

467 02/15/2002 12:47:24.770 SEV=9 IKEDBG/1 RPT=109 10.48.66.76
Group [VPNC_Base_Group]
constructing RSA signature

468 02/15/2002 12:47:24.770 SEV=9 IKEDBG/0 RPT=3936 10.48.66.76
Group [VPNC_Base_Group]
computing hash

469 02/15/2002 12:47:24.800 SEV=9 IKEDBG/46 RPT=64 10.48.66.76
Group [VPNC_Base_Group]
constructing dpd vid payload

470 02/15/2002 12:47:24.800 SEV=8 IKEDBG/0 RPT=3937 10.48.66.76
SENDING Message (msgid=0) with payloads :
HDR + ID (5) + CERT (6) + SIG (9) + VENDOR (13) + NONE (0)
... total length : 1112

473 02/15/2002 12:47:24.800 SEV=4 IKE/119 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
PHASE 1 COMPLETED

474 02/15/2002 12:47:24.800 SEV=6 IKE/121 RPT=4 10.48.66.76
```

```
Keep-alive type for this connection: None

475 02/15/2002 12:47:24.800 SEV=6 IKE/122 RPT=4 10.48.66.76
Keep-alives configured on but peer does not support keep-alives (type = None)

476 02/15/2002 12:47:24.800 SEV=7 IKEDBG/0 RPT=3938 10.48.66.76
Group [VPNC_Base_Group]
Starting phase 1 rekey timer: 21600000 (ms)

477 02/15/2002 12:47:24.810 SEV=8 IKEDBG/0 RPT=3939 10.48.66.76
RECEIVED Message (msgid=781ceadc) with payloads :
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0)
... total length : 1108

480 02/15/2002 12:47:24.810 SEV=9 IKEDBG/0 RPT=3940 10.48.66.76
Group [VPNC_Base_Group]
processing hash

481 02/15/2002 12:47:24.810 SEV=9 IKEDBG/0 RPT=3941 10.48.66.76
Group [VPNC_Base_Group]
processing SA payload

482 02/15/2002 12:47:24.810 SEV=9 IKEDBG/1 RPT=110 10.48.66.76
Group [VPNC_Base_Group]
processing nonce payload

483 02/15/2002 12:47:24.810 SEV=9 IKEDBG/1 RPT=111 10.48.66.76
Group [VPNC_Base_Group]
Processing ID

484 02/15/2002 12:47:24.810 SEV=5 IKE/25 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
Received remote Proxy Host data in ID Payload:
Address 10.48.66.76, Protocol 17, Port 1701

487 02/15/2002 12:47:24.810 SEV=9 IKEDBG/1 RPT=112 10.48.66.76
Group [VPNC_Base_Group]
Processing ID

488 02/15/2002 12:47:24.810 SEV=5 IKE/24 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
Received local Proxy Host data in ID Payload:
Address 10.48.66.109, Protocol 17, Port 0

491 02/15/2002 12:47:24.810 SEV=8 IKEDBG/0 RPT=3942
QM IsRekeyed old sa not found by addr

492 02/15/2002 12:47:24.810 SEV=5 IKE/66 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
IKE Remote Peer configured for SA: ESP-L2TP-TRANSPORT

493 02/15/2002 12:47:24.810 SEV=9 IKEDBG/0 RPT=3943 10.48.66.76
Group [VPNC_Base_Group]
processing IPSEC SA

494 02/15/2002 12:47:24.810 SEV=7 IKEDBG/27 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
IPSec SA Proposal # 1, Transform # 1 acceptable

495 02/15/2002 12:47:24.810 SEV=7 IKEDBG/0 RPT=3944 10.48.66.76
Group [VPNC_Base_Group]
IKE: requesting SPI!

496 02/15/2002 12:47:24.810 SEV=8 IKEDBG/6 RPT=4
```

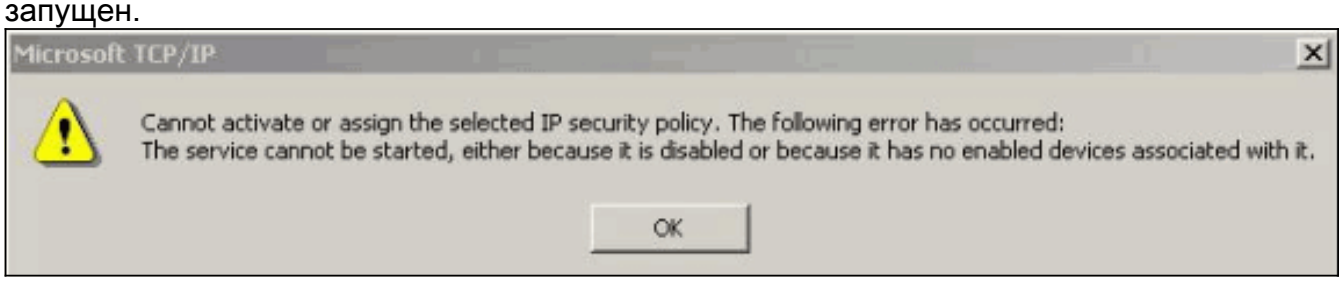
```
IKE got SPI from key engine: SPI = 0x10d19e33

497 02/15/2002 12:47:24.810 SEV=9 IKEDBG/0 RPT=3945 10.48.66.76
Group [VPNC_Base_Group]
oakley constucting quick mode

498 02/15/2002 12:47:24.810 SEV=9 IKEDBG/0 RPT=3946 10.48.66.76
Group [VPNC_Base_Group]
constructing blank hash

499 02/15/2002 12:47:24.820 SEV=9 IKEDBG/0 RPT=3947 10.48.66.76
Group [VPNC_Base_Group]
constructing ISA_SA for ipsec

500 02/15/2002 12:47:24.820 SEV=9 IKEDBG/1 RPT=113 10.48.66.76
Group [VPNC_Base_Group]
constructing ipsec nonce payload

501 02/15/2002 12:47:24.820 SEV=9 IKEDBG/1 RPT=114 10.48.66.76
Group [VPNC_Base_Group]
constructing proxy ID

502 02/15/2002 12:47:24.820 SEV=7 IKEDBG/0 RPT=3948 10.48.66.76
Group [VPNC_Base_Group]
Transmitting Proxy Id:
  Remote host: 10.48.66.76  Protocol 17  Port 1701
  Local host:  10.48.66.109  Protocol 17  Port 0

506 02/15/2002 12:47:24.820 SEV=9 IKEDBG/0 RPT=3949 10.48.66.76
Group [VPNC_Base_Group]
constructing qm hash

507 02/15/2002 12:47:24.820 SEV=8 IKEDBG/0 RPT=3950 10.48.66.76
SENDING Message (msgid=781ceadc) with payloads :
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0)
... total length : 156

510 02/15/2002 12:47:24.820 SEV=8 IKEDBG/0 RPT=3951 10.48.66.76
RECEIVED Message (msgid=781ceadc) with payloads :
HDR + HASH (8) + NONE (0) ... total length : 48

512 02/15/2002 12:47:24.830 SEV=9 IKEDBG/0 RPT=3952 10.48.66.76
Group [VPNC_Base_Group]
processing hash

513 02/15/2002 12:47:24.830 SEV=9 IKEDBG/0 RPT=3953 10.48.66.76
Group [VPNC_Base_Group]
loading all IPSEC SAs

514 02/15/2002 12:47:24.830 SEV=9 IKEDBG/1 RPT=115 10.48.66.76
Group [VPNC_Base_Group]
Generating Quick Mode Key!

515 02/15/2002 12:47:24.830 SEV=9 IKEDBG/1 RPT=116 10.48.66.76
Group [VPNC_Base_Group]
Generating Quick Mode Key!

516 02/15/2002 12:47:24.830 SEV=7 IKEDBG/0 RPT=3954 10.48.66.76
Group [VPNC_Base_Group]
Loading host:
  Dst: 10.48.66.109
  Src: 10.48.66.76

517 02/15/2002 12:47:24.830 SEV=4 IKE/49 RPT=4 10.48.66.76
```

```
Group [VPNC_Base_Group]
Security negotiation complete for User ()
Responder, Inbound SPI = 0x10d19e33, Outbound SPI = 0x15895ab9

520 02/15/2002 12:47:24.830 SEV=8 IKEDBG/7 RPT=4
IKE got a KEY_ADD msg for SA: SPI = 0x15895ab9

521 02/15/2002 12:47:24.830 SEV=8 IKEDBG/0 RPT=3955
pitcher: rcv KEY_UPDATE, spi 0x10d19e33

522 02/15/2002 12:47:24.830 SEV=4 IKE/120 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
PHASE 2 COMPLETED (msgid=781ceadc)

523 02/15/2002 12:47:24.840 SEV=8 IKEDBG/0 RPT=3956
pitcher: recv KEY_SA_ACTIVE spi 0x10d19e33

524 02/15/2002 12:47:24.840 SEV=8 IKEDBG/0 RPT=3957
KEY_SA_ACTIVE no old rekey centry found with new spi 0x10d19e33, mess_id 0x0
```

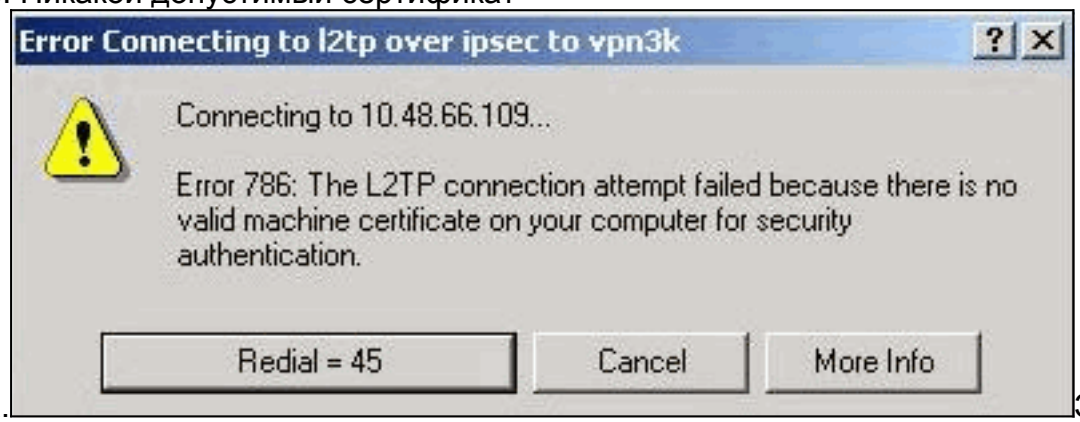
## Информация об устранении неполадок

Этот раздел иллюстрирует некоторые типичные проблемы и методы устранения неполадок для каждой из них.

- Сервер не может быть запущен.

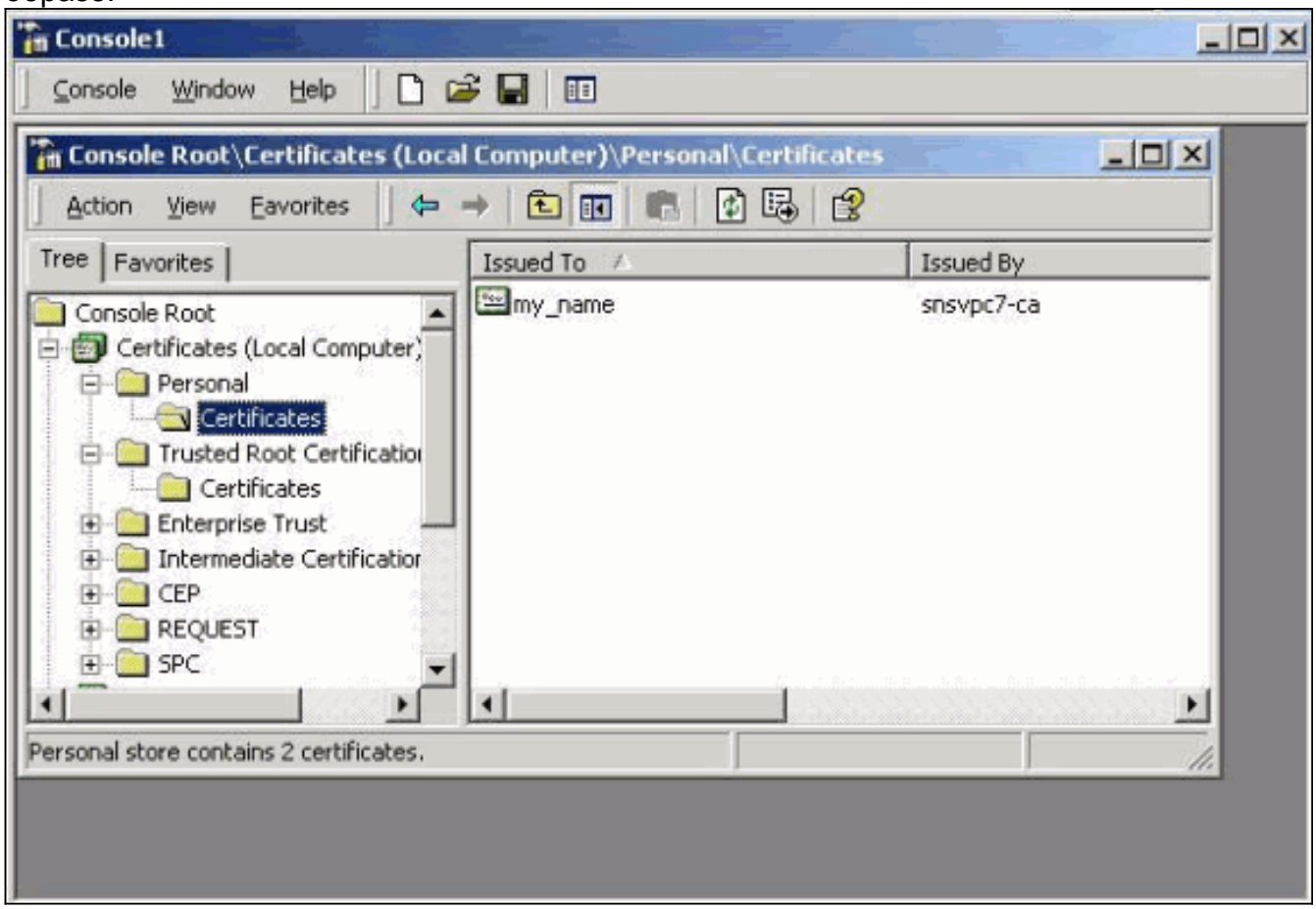



  Скорее всего, Сервис IPSec не запущен. Выберите **Пуск> Программы> Средства администрирования> Сервис** и удостоверьтесь, что включен **Сервис IPSec**.
- Ошибка 786: Никакой допустимый сертификат




  компьютера. Эта ошибка указывает на проблему с сертификатом на локальном компьютере. Для легкого рассмотрения сертификата выберите **Start> Run** и выполните MMC. **Кликните Console и выберите Add/Remove Snap-in**. **Нажмите Add** и выберите **Certificate** из списка. Когда окно появляется, который спрашивает вас область сертификата, выберите **Computer Account**.Теперь можно проверить, что сертификат сервера CA расположен под **Доверенными корневыми центрами сертификации**. Можно также проверить, что у вас есть сертификат путем выбора **Console Root> Certificate (Local Computer)> Personal>**

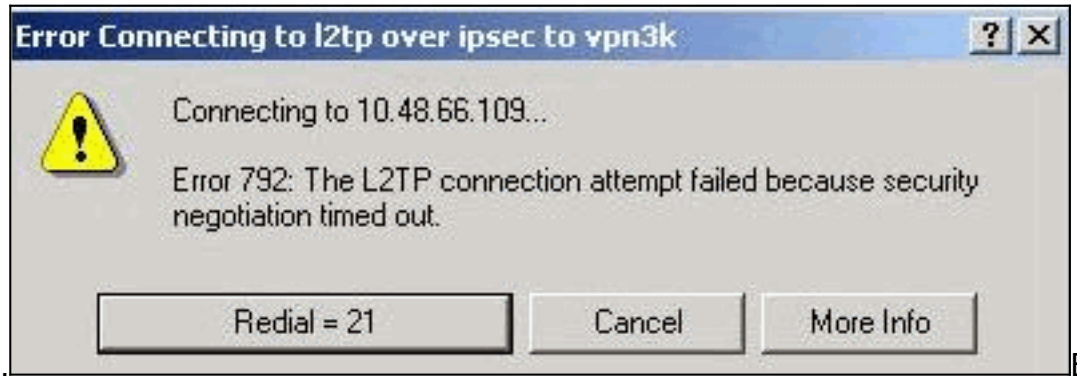
**Certificates**, как показано в этом образе.




Нажмите **сертификат**. Проверьте, что все корректно. В данном примере существует секретный ключ, привязанный к сертификату. Однако этот сертификат истек. Это - причина


проблемы.

- Ошибка 792: таймаут Согласования безопасности.Это сообщение появляется после длительного



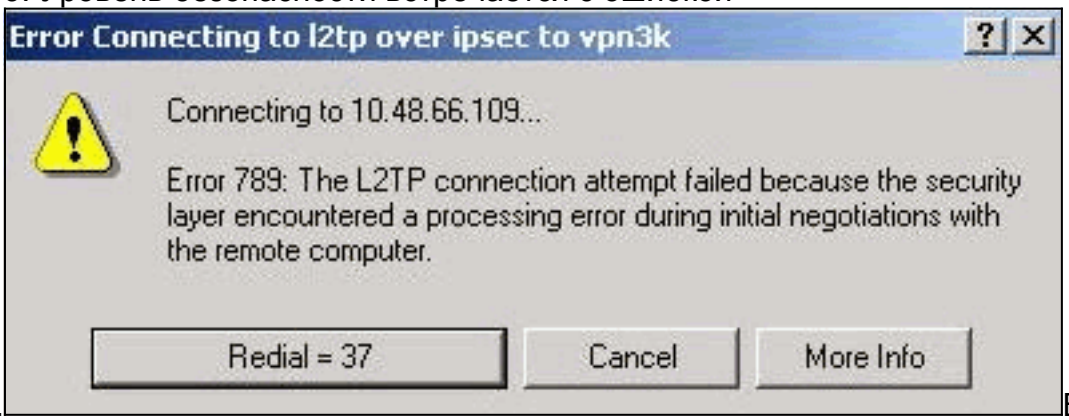

времени.Включите соответствующие отладки, как объяснено в часто задаваемых вопросах Cisco VPN 3000 Concentrator. Прочитайте их. Необходимо видеть что-то подобное этим выходным данным:

```
9337 02/15/2002 15:06:13.500 SEV=8 IKEDBG/0 RPT=7002 10.48.66.76
  Phase 1 failure against global IKE proposal # 6:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

9340 02/15/2002 15:06:13.510 SEV=8 IKEDBG/0 RPT=7003 10.48.66.76
```

```
  Phase 1 failure against global IKE proposal # 7:
  Mismatched attr types for class Auth Method:
    Rcv'd: RSA signature with Certificates
    Cfg'd: Preshared Key

9343 02/15/2002 15:06:13.510 SEV=8 IKEDBG/0 RPT=7004 10.48.66.76
  Phase 1 failure against global IKE proposal # 8:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 7

9346 02/15/2002 15:06:13.510 SEV=7 IKEDBG/0 RPT=7005 10.48.66.76
All SA proposals found unacceptable

9347 02/15/2002 15:06:13.510 SEV=4 IKE/48 RPT=37 10.48.66.76
Error processing payload: Payload ID: 1

9348 02/15/2002 15:06:13.510 SEV=9 IKEDBG/0 RPT=7006 10.48.66.76
IKE SA MM:261e40dd terminating:
flags 0x01000002, refcnt 0, tuncnt 0

9349 02/15/2002 15:06:13.510 SEV=9 IKEDBG/0 RPT=7007
sending delete message
```

Это указывает, что Предложение ike не было настроено должным образом. Проверьте информацию от Настройки раздел Предложения ike этого документа.

- Ошибка 789: Уровень безопасности встречается с ошибкой




обработки. Включ ите соответствующие отладки, как объяснено в часто задаваемых вопросах Cisco VPN 3000 Concentrator. Прочитайте их. Необходимо видеть что-то подобное этим выходным данным:

```
11315 02/15/2002 15:36:32.030 SEV=8 IKEDBG/0 RPT=7686
Proposal # 1, Transform # 2, Type ESP, Id DES-CBC
Parsing received transform:
  Phase 2 failure:
  Mismatched attr types for class Encapsulation:
    Rcv'd: Transport
    Cfg'd: Tunnel

11320 02/15/2002 15:36:32.030 SEV=5 IKEDBG/0 RPT=7687
AH proposal not supported

11321 02/15/2002 15:36:32.030 SEV=4 IKE/0 RPT=27 10.48.66.76
Group [VPNC_Base_Group]
All IPSec SA proposals found unacceptable!
```

- Используемая версияВыберите **Monitoring> System Status** для просмотра этих выходных данных:

```
VPN Concentrator Type: 3005
Bootcode Rev: Altiga Networks/VPN Concentrator Version 2.2.int_9 Jan 19 2000 05:36:41
Software Rev: Cisco Systems, Inc./VPN 3000 Concentrator Version 3.5.Rel Nov 27 2001 13:35:16
Up For: 44:39:48
Up Since: 02/13/2002 15:49:59
```

```
RAM Size: 32 MB
```

## Дополнительные сведения

- Поддержка продуктов Протоколов IPSec Negotiation/IKE
- Техническая поддержка - Cisco Systems