Настройка VPN Client 3.x для получения цифрового сертификата

Содержание

Введение

Этот документ демонстрирует, как настроить Cisco VPN Client 3.x для получения цифрового сертификата.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения в этом документе основываются на ПК, который выполняет Cisco VPN Client 3. x.

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

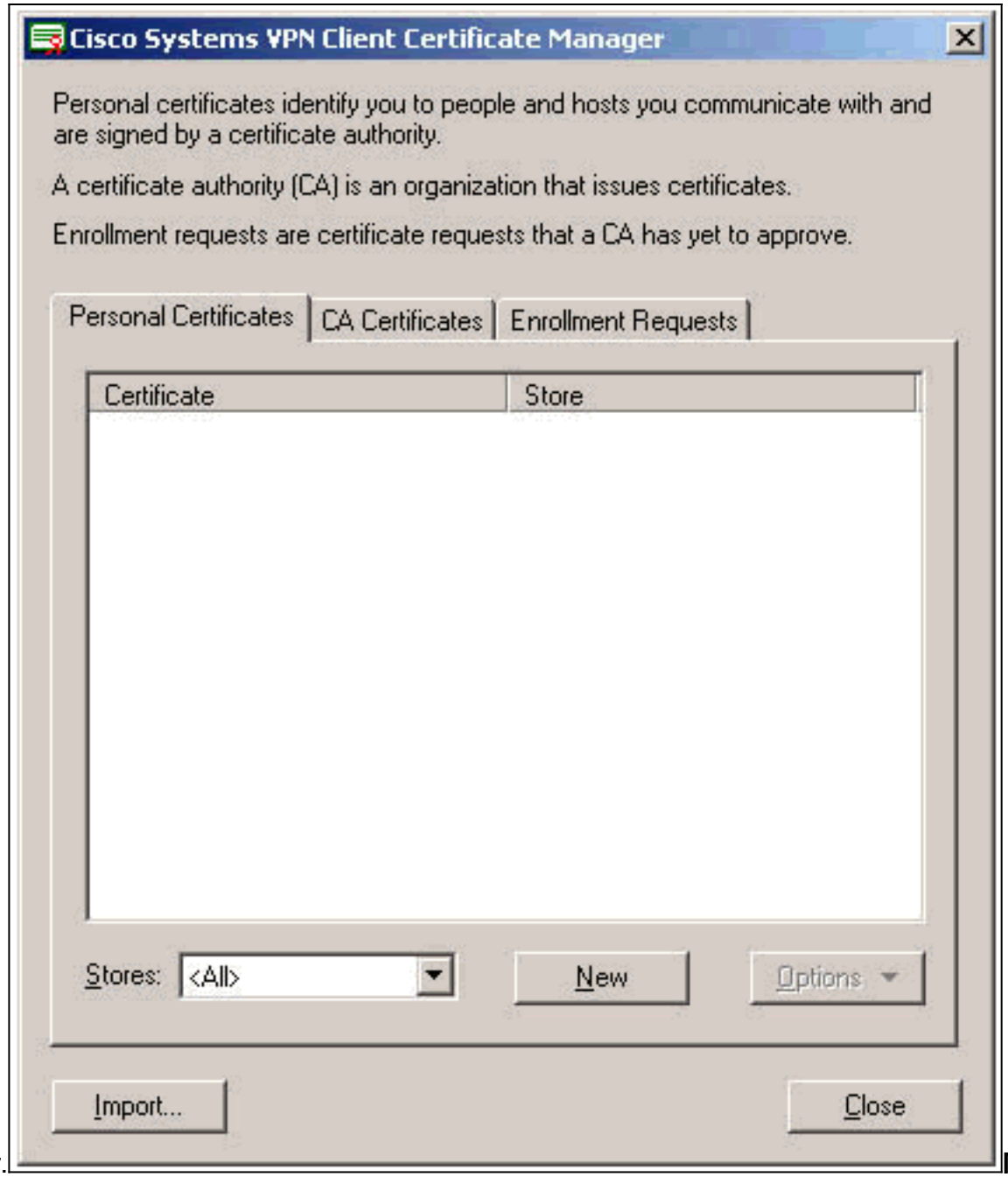
Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Настройка VPN-клиента

Для настройки VPN-клиента выполните следующие шаги.

1. Выберите **Start> Programs> Cisco Systems Inc. VPN client> Certificate Manager** для запуска Менеджера сертификатов Клиента VPN.

2. Выберите вкладку Personal Certificates и нажмите

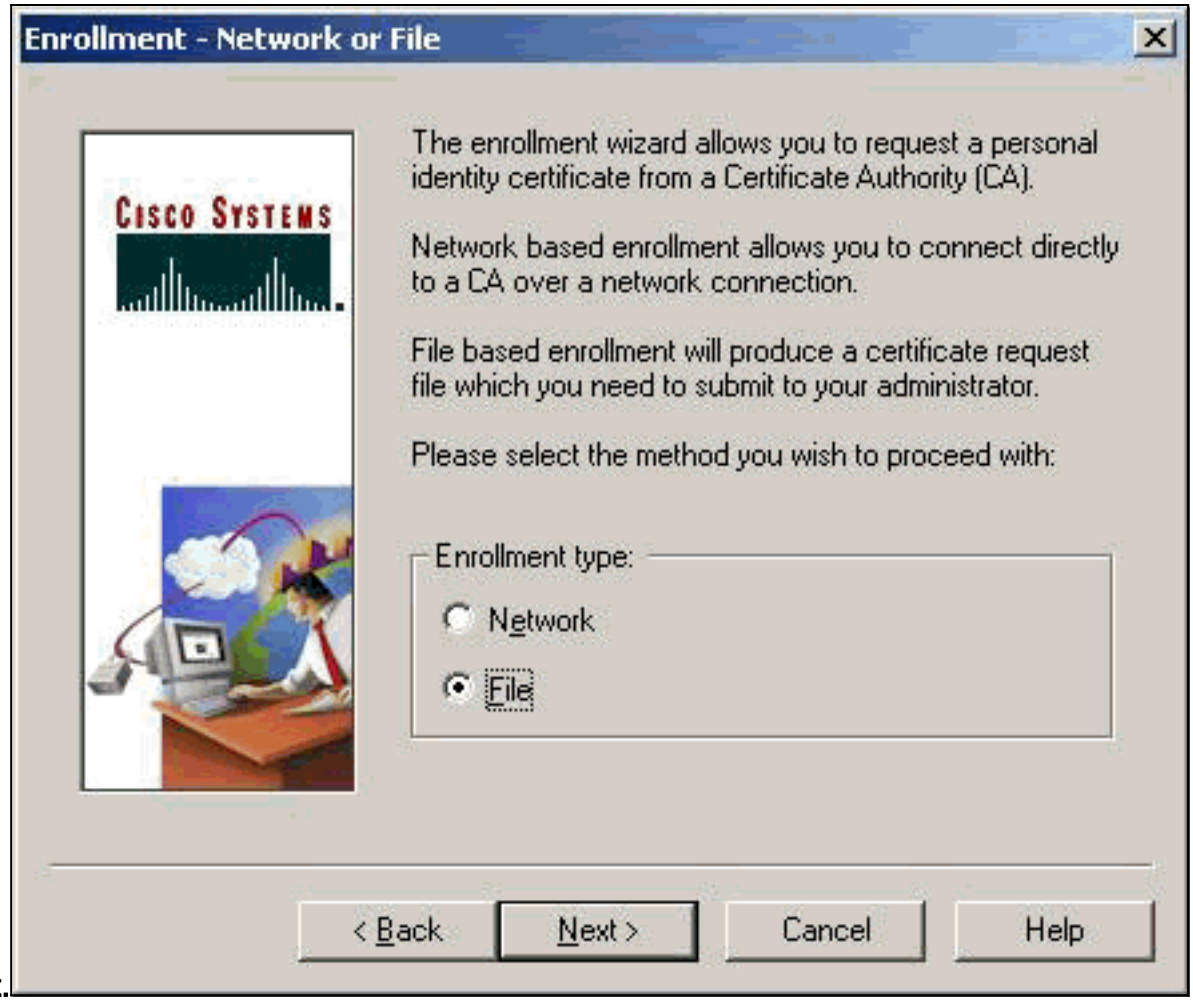


New.**Приме чание:** Сертификаты компьютера для аутентификации пользователей для VPN-подключений не могут быть сделаны с IPsec.

3. Когда Клиент VPN побудит вас для пароля, задайте пароль для защиты сертификата. Любая операция, которая требует доступа к секретному ключу сертификата, требует, чтобы продолжился указанный

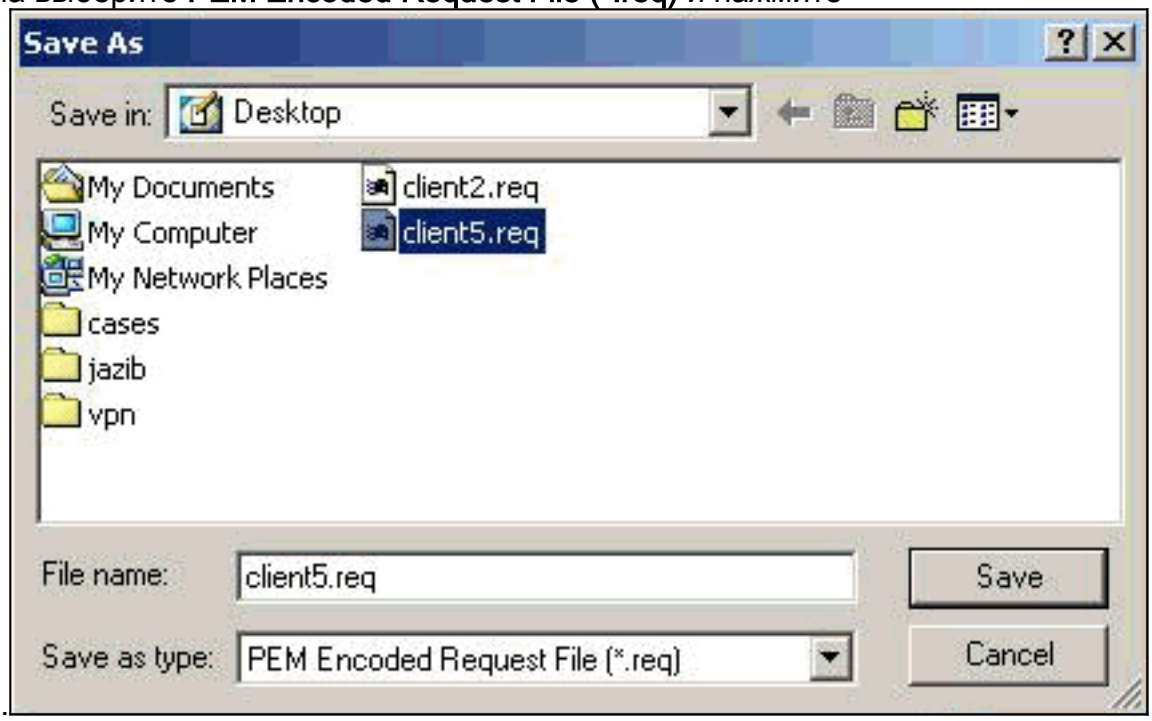
пароль.

4. Выберите **File** для запроса сертификата с помощью PKCS #10 формат на Странице управления сертификатами. **Нажмите кнопку**



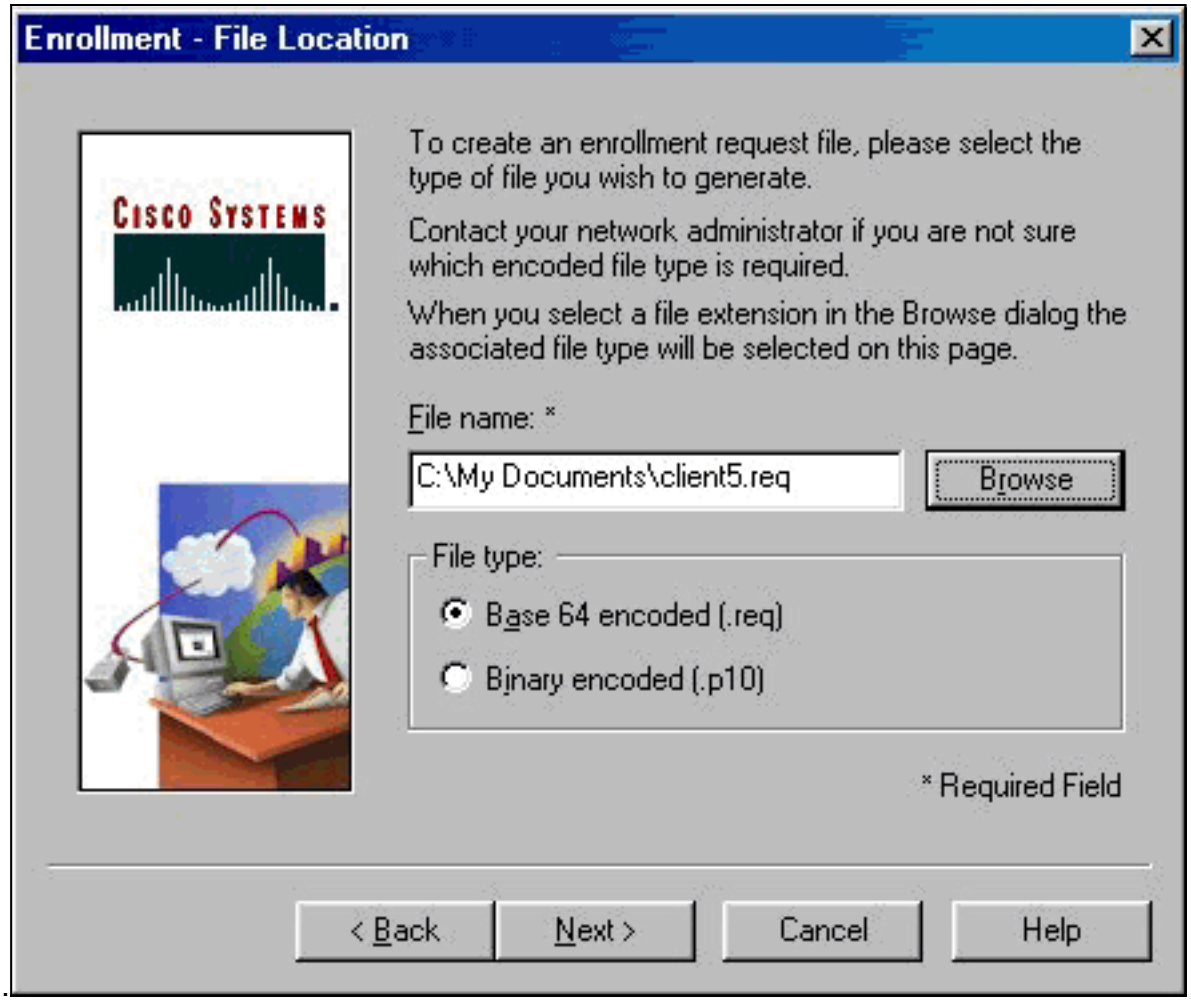
Next.

5. Нажмите **Browse** и задайте имя файла для файла запроса сертификата. Для типа файла выберите **PEM Encoded Request File (*.req)** и нажмите



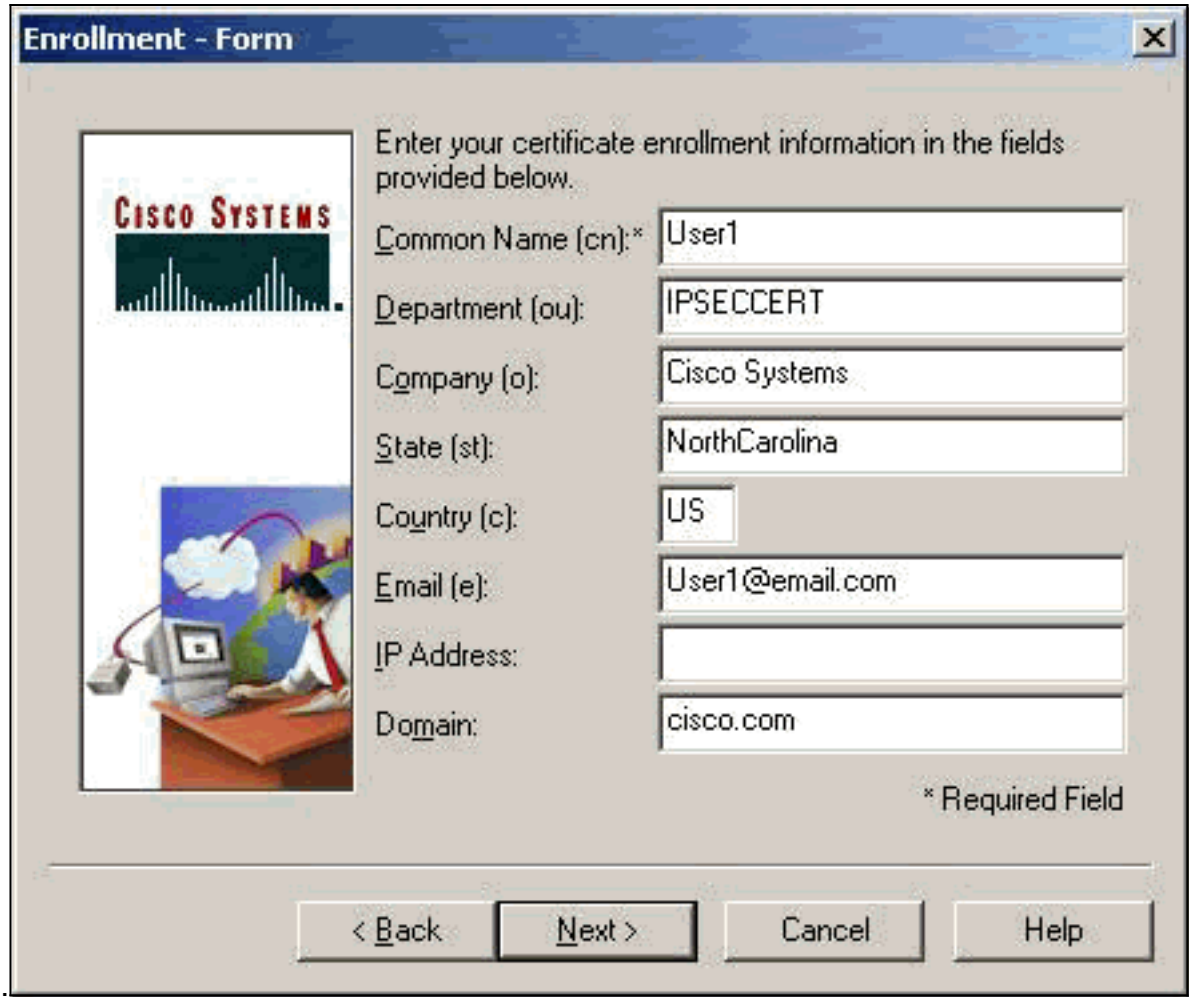
Save.

6. Нажмите **Next** на Странице управления сертификатами Клиента



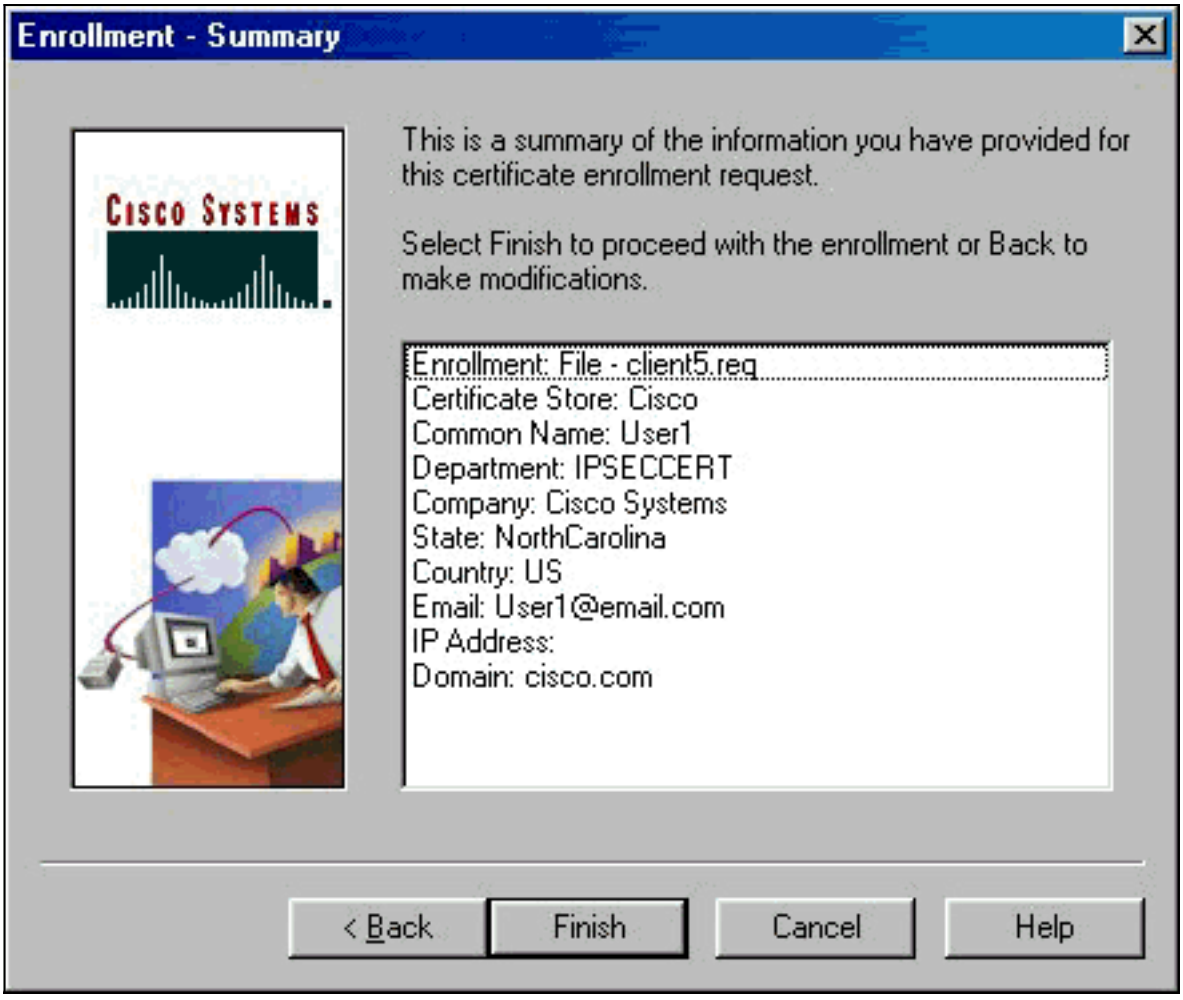
VPN.

7. Заполните поля на Регистрационной форме.Данный пример показывает поля:Общее имя = User1Отдел = IPSECCERT (Это должно совпасть с подразделением (OU) и именем группы на VPN 3000 Concentrator.)Компания = Cisco SystemsСостояние = NorthCarolinaСтрана = USЭлектронная почта = User1@email.comIP-адрес = (дополнительный; используемый для определения IP-адреса на запросе сертификата)Домен = cisco.comНажмите **Next**, когда вы будете

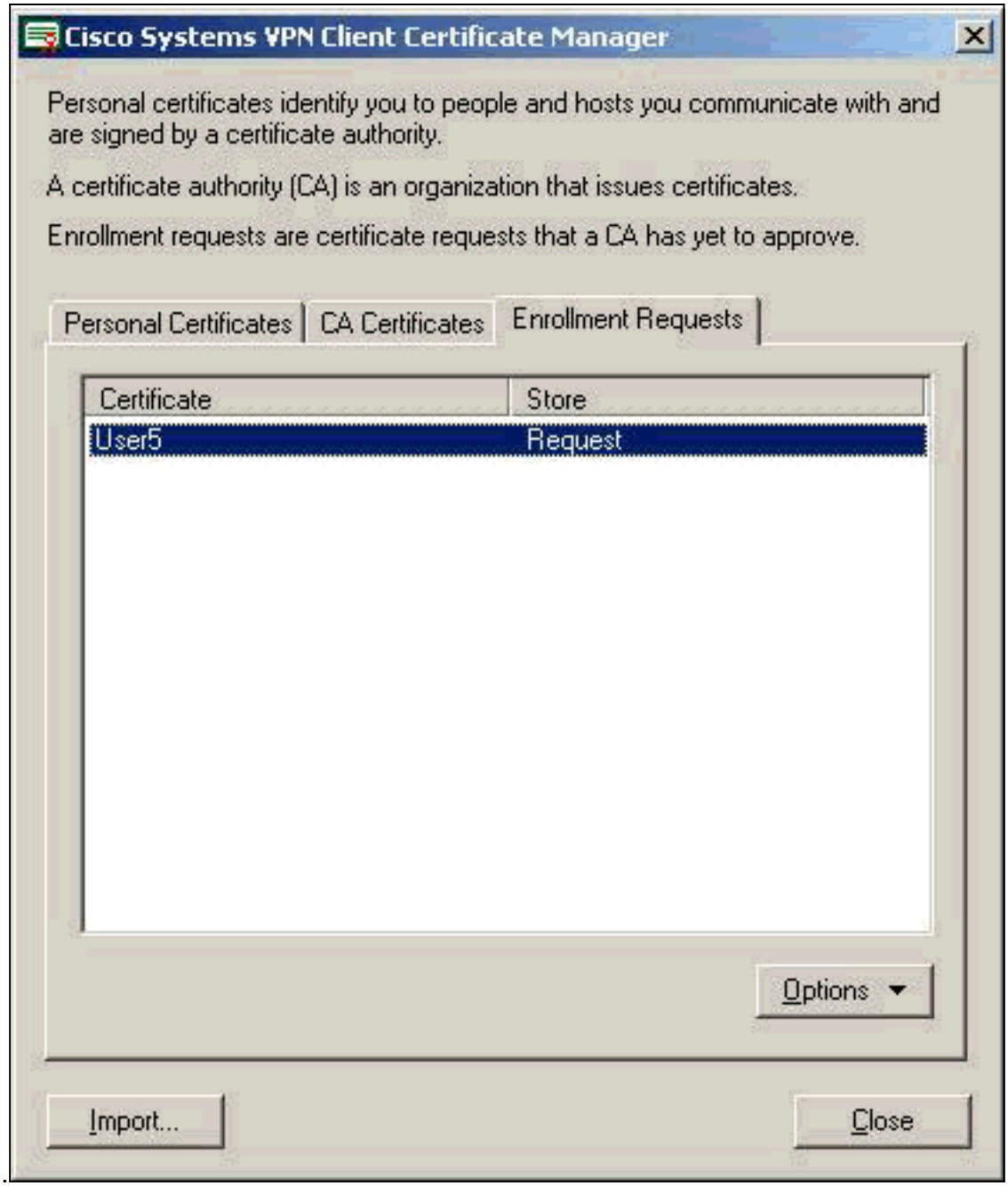


сделаны.

8. Нажмите **Finish** для перехода регистрацию.

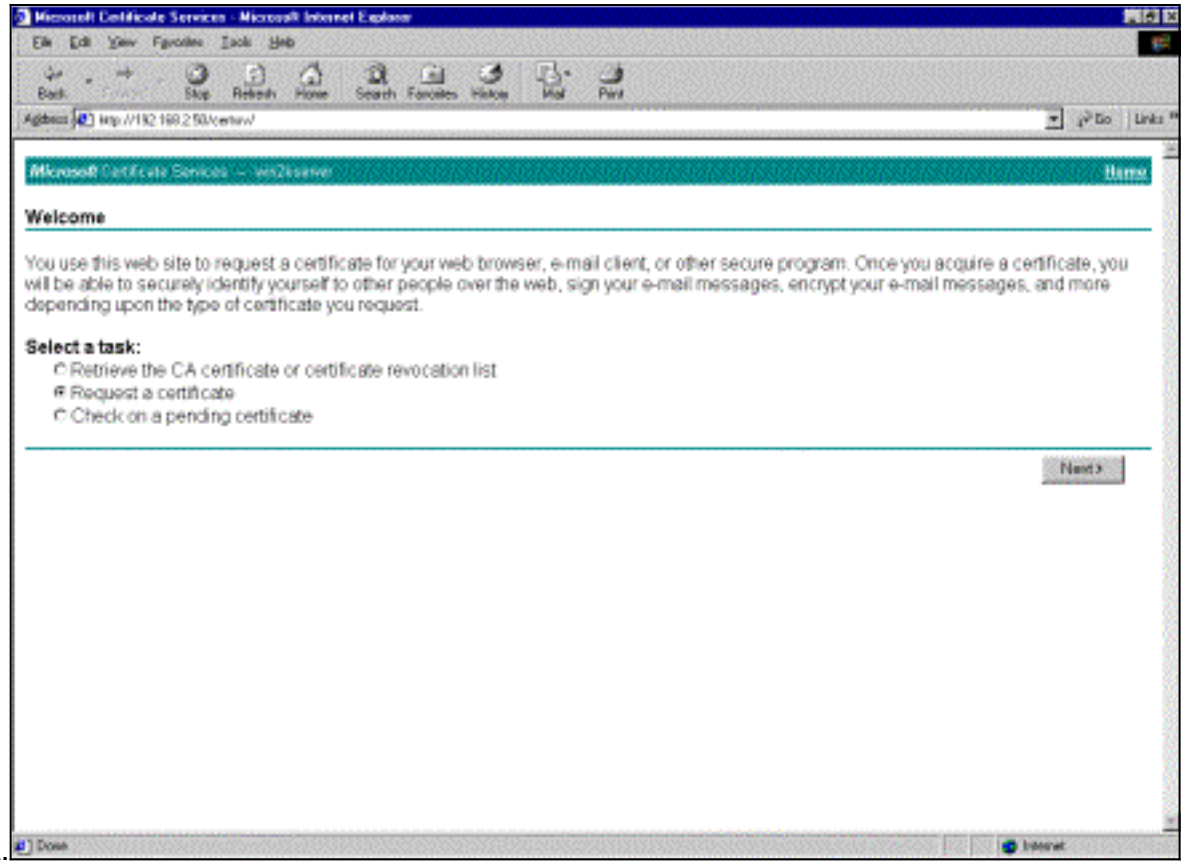


9. Выберите вкладку Enrollment Requests для проверки запроса на Менеджере сертификатов Клиента



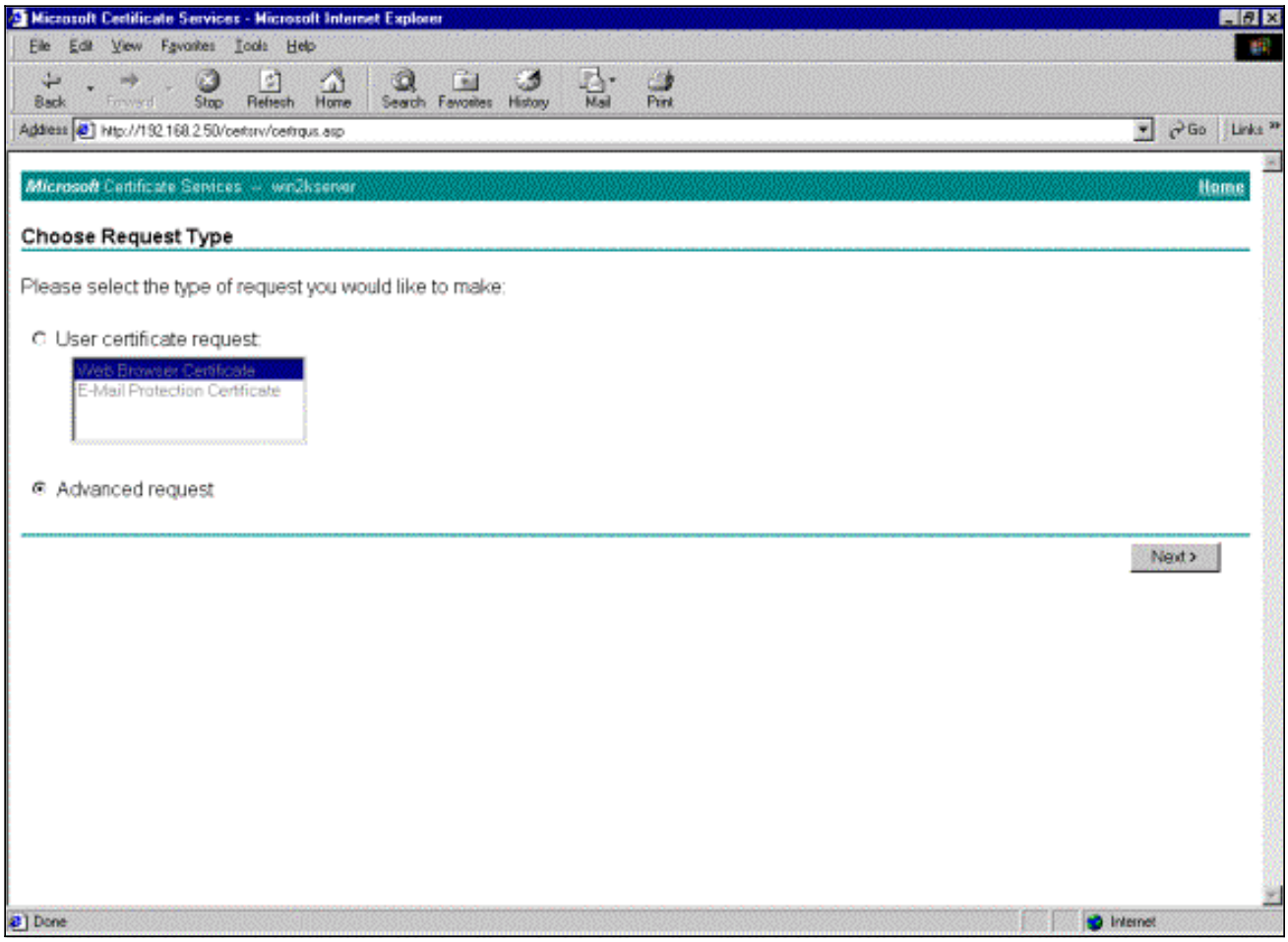
VPN.

10. Переведите в рабочее состояние сервер Центра сертификации (CA) и интерфейсы Клиента VPN одновременно для подачи запроса.
11. Выберите **Request сертификат** и нажмите **Next** на сервере



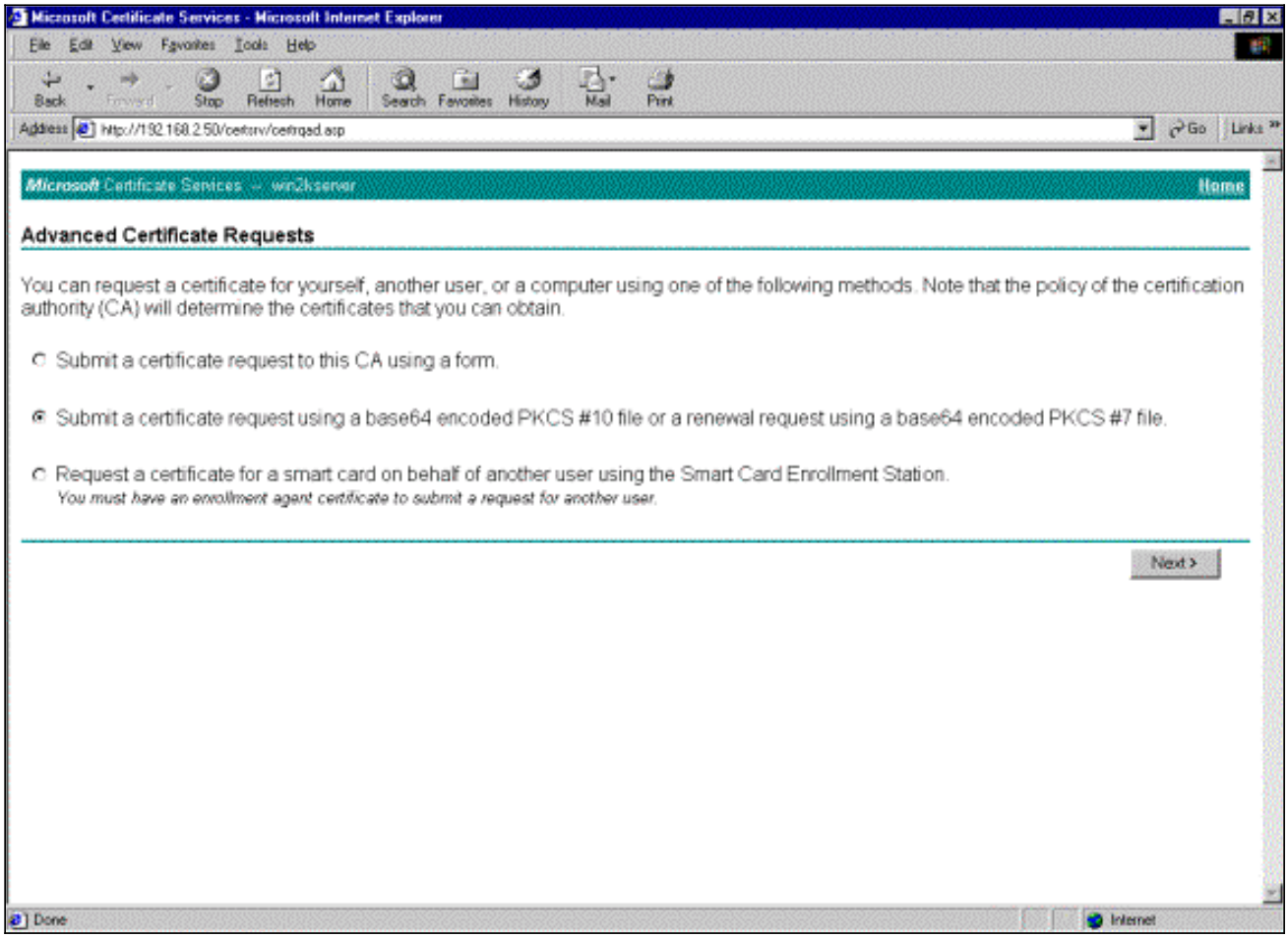
CA.

12. Выберите **Расширенный запрос** для типа запроса и нажмите **Next**.

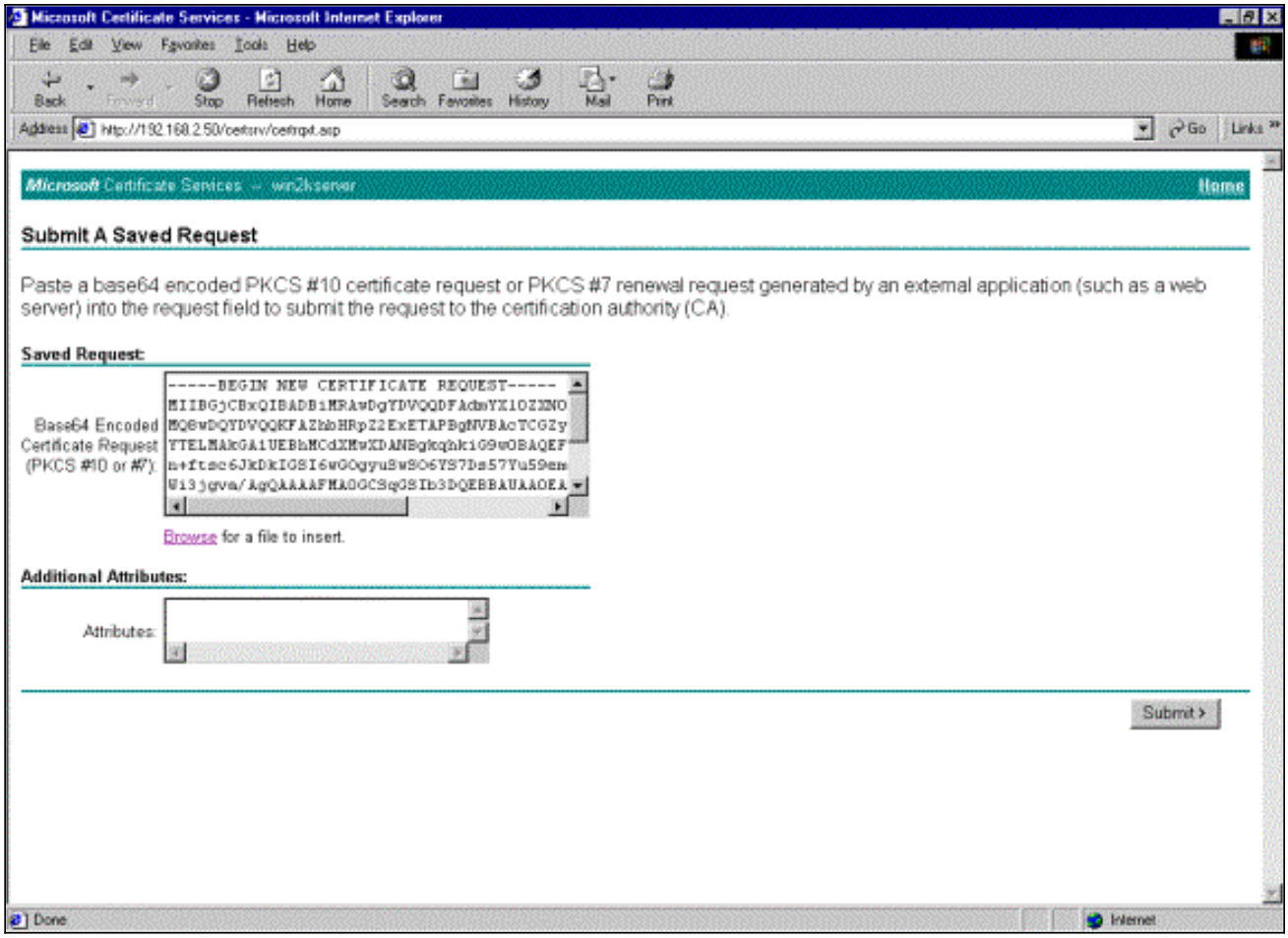


13. Выберите **Submit запрос сертификата с помощью base64 кодированные PKC #10 файл или запрос на обновление с помощью base64 кодированные PKC #7 файл** под Усовершенствованными Запросами сертификата, и затем нажмите

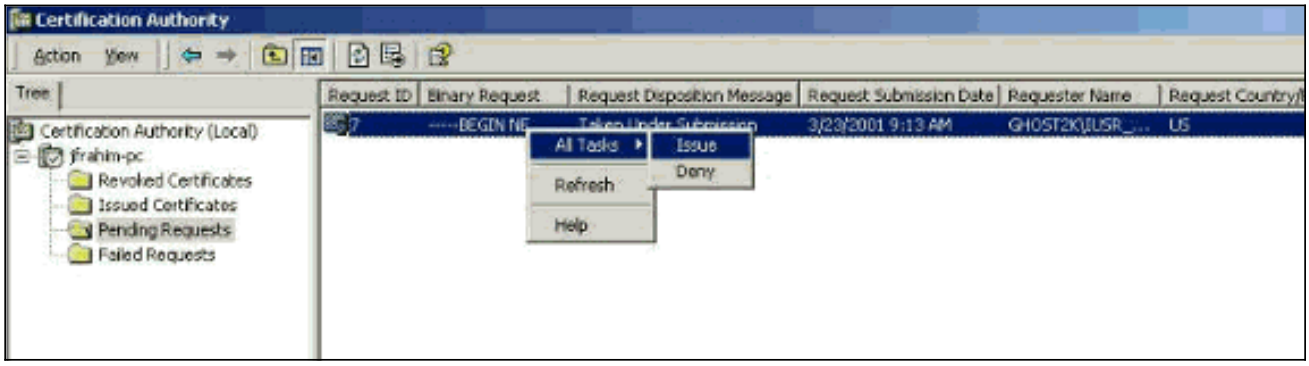
Next.



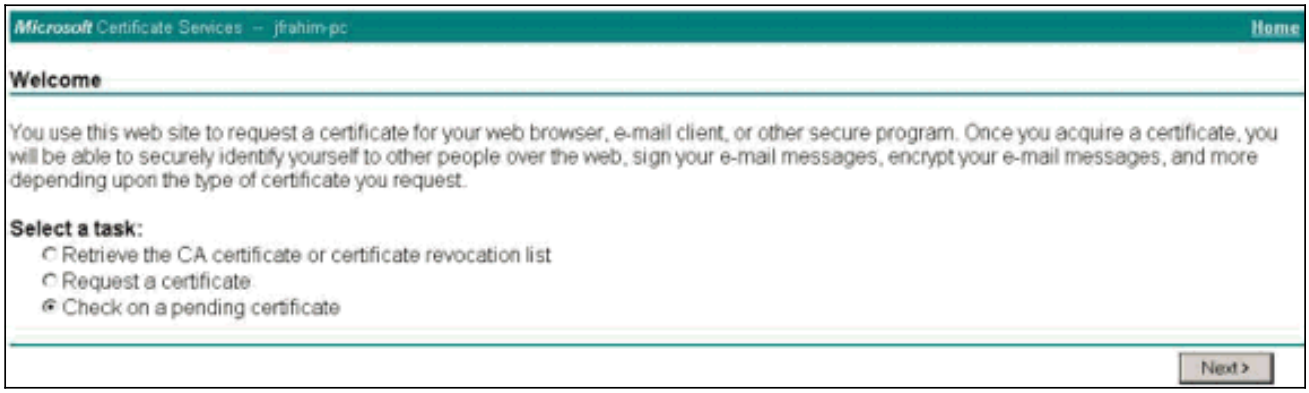
14. Выделите файл запроса Клиента VPN и вставьте его к серверу CA под Сохраненным запросом. **Затем щелкните Submit (Отправить).**



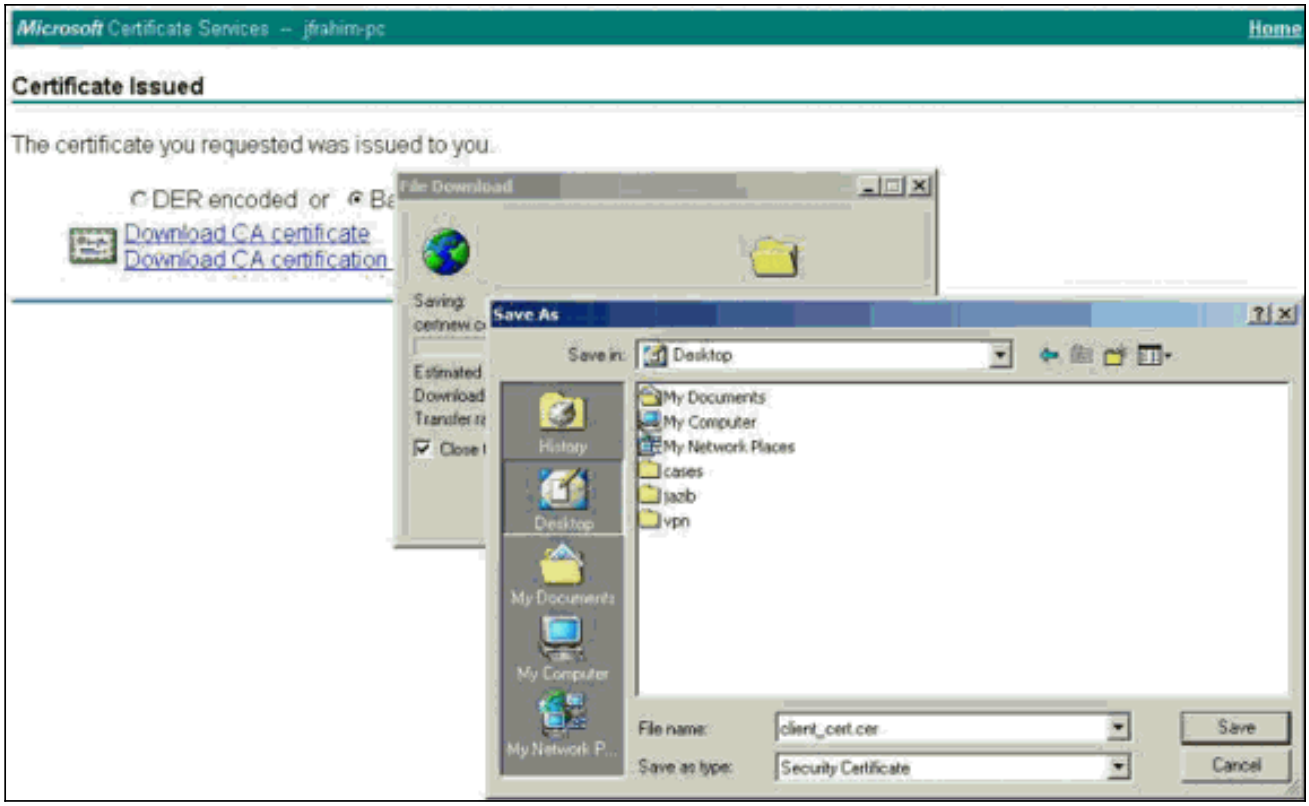
15. На сервере CA выполните сертификат идентификации для запроса Клиента VPN.



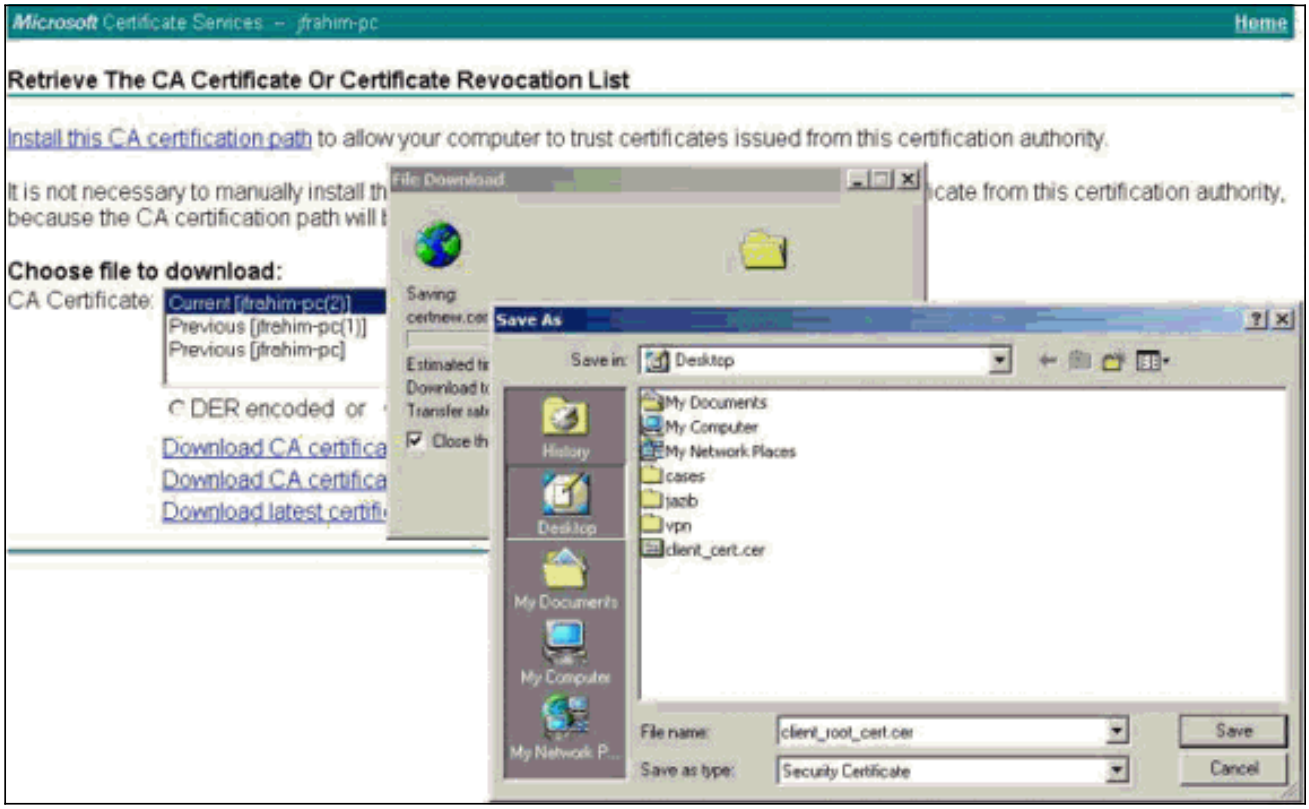
16. Загрузите root и сертификаты идентификации Клиенту VPN. На сервере CA выберите, **проверяют сертификат в состоянии ожидания**, и затем нажимают **Next**.



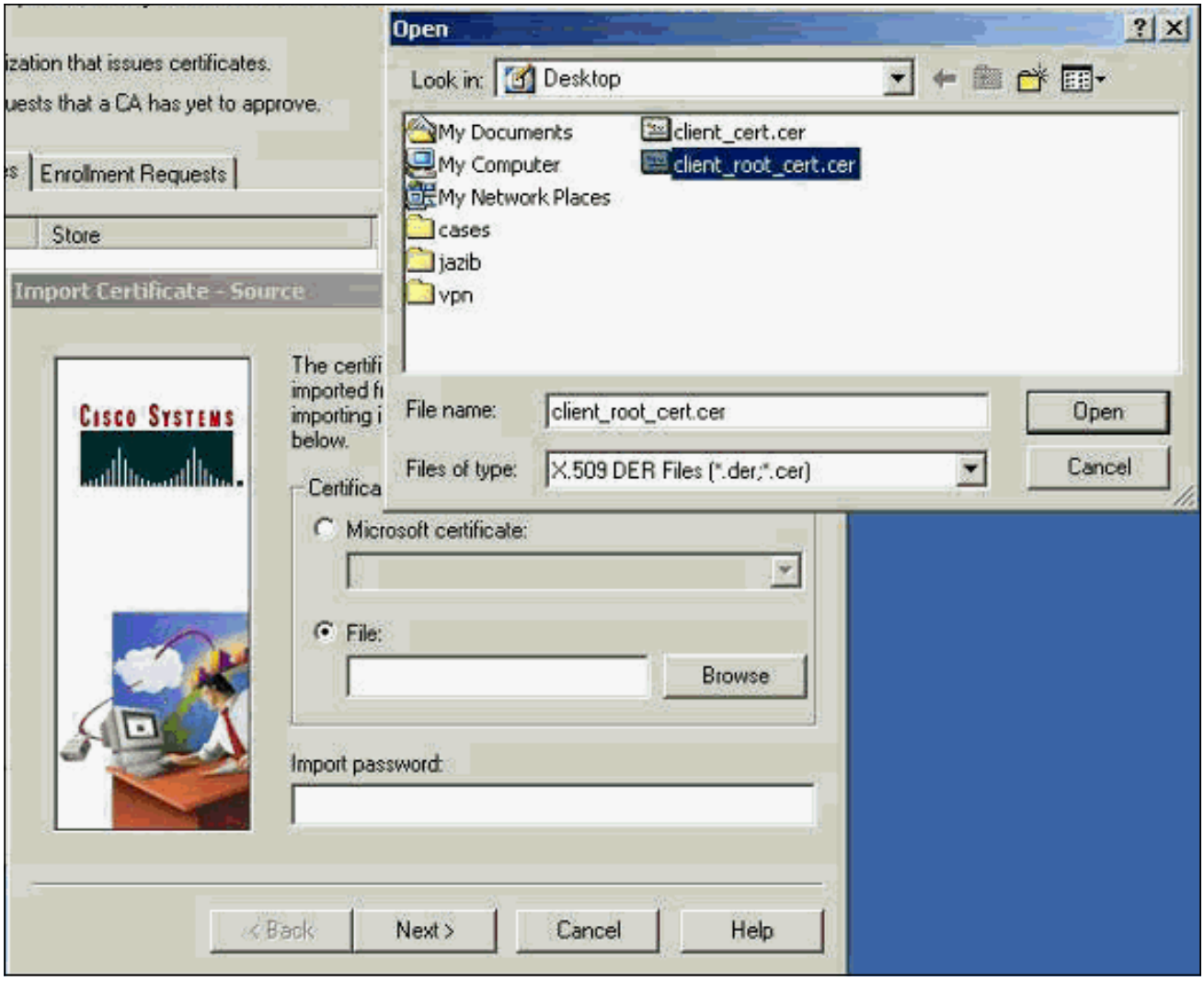
17. Выберите **закодированный Base 64**. Затем нажмите **Download CA certificate** на сервере
CA.



18. Выберите файл для загрузки от страницы Retrieve the CA Certificate или Certificate Revocation List для получения корневого сертификата на сервере CA. **Нажмите кнопку Next.**

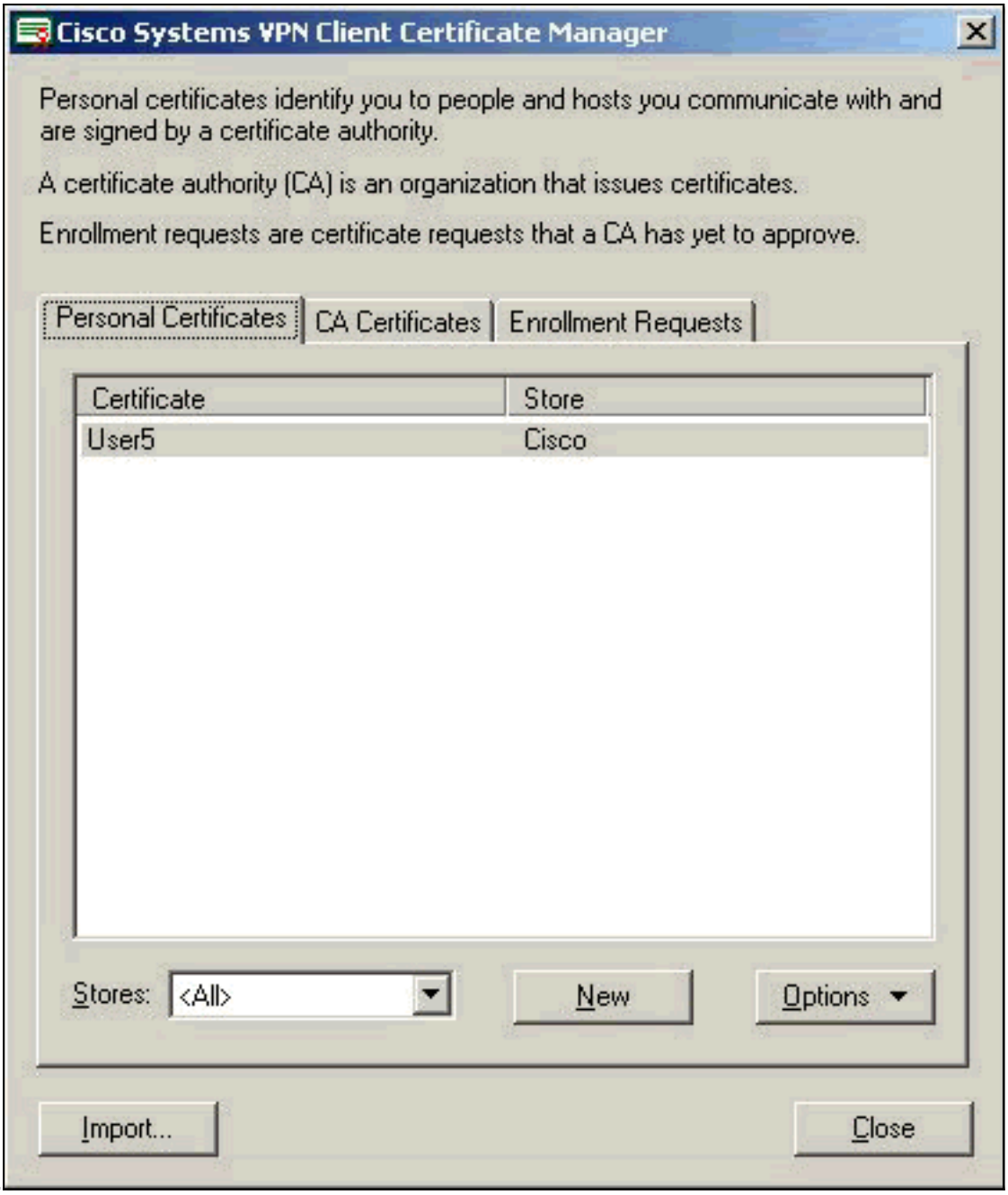


19. Выберите **Certificate Manager> CA Certificate> Import on the VPN Client**, и затем выберите файл узла CA для установки root и сертификатов идентификации.



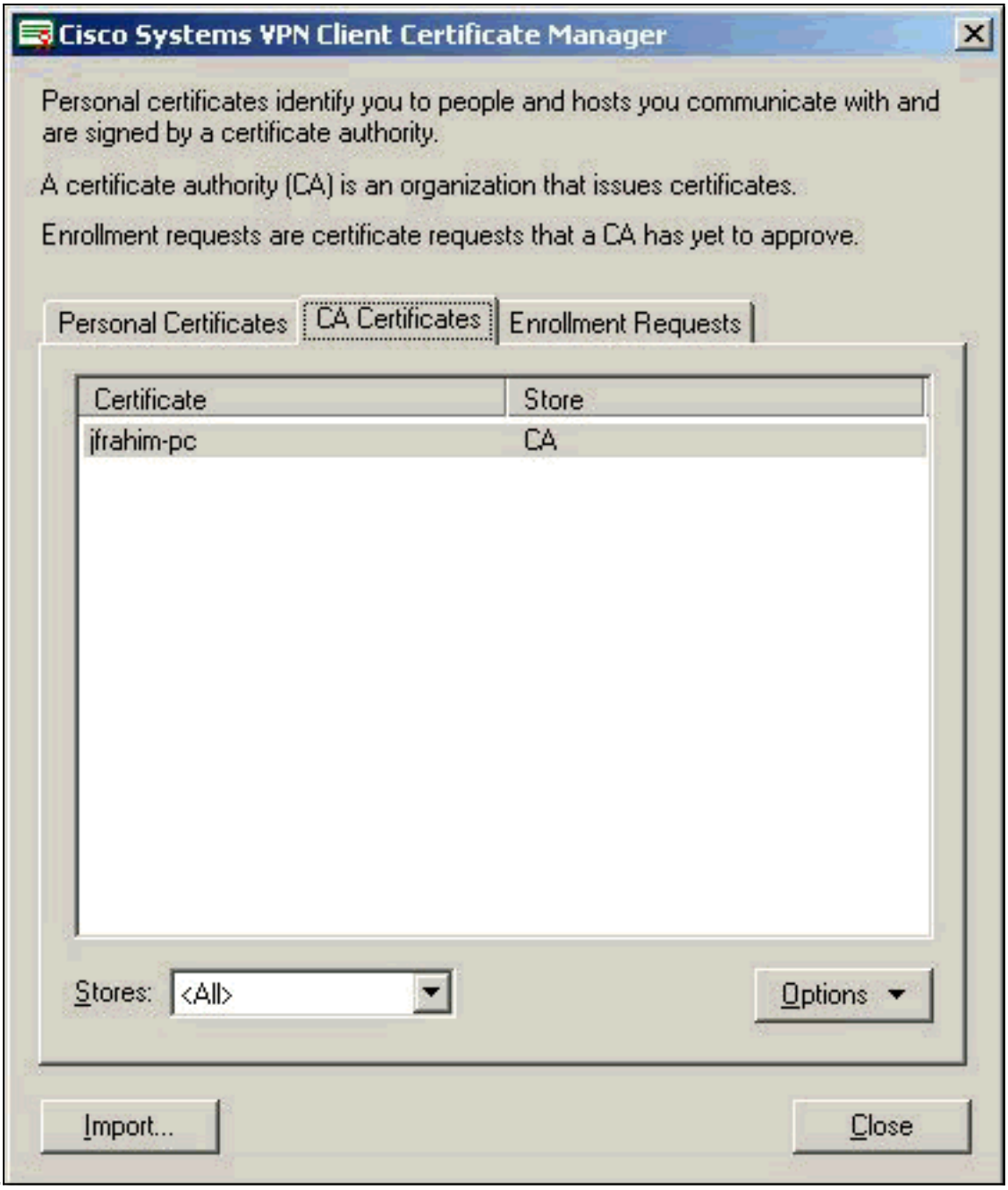
20. Выберите **Certificate Manager> Personal Certificates> Import** и выберите файл сертификата идентификации.

21. Гарантируйте, что сертификат идентификации появляется под вкладкой Personal



Certificates.

22. Гарантируйте, что корневой сертификат появляется под вкладкой CA

Certificates. 

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

Когда вы пытаетесь зарегистрироваться с Microsoft CA server, он может генерировать это сообщение об ошибках.

```
Initiating online request
Generating key pair
Generating self-signed Certificate
Initiating online request
Received a response from the CA
Your certificate request was denied
```

При получении этого сообщения об ошибках обратитесь к журналам Microsoft CA для

подробных данных или обратитесь к этим ресурсам для получения дополнительной информации.

- Windows Can не находят центр сертификации, который обрабатывает запрос
- XCCC: Сообщение об ошибках "your certificate request was denied" Происходит Когда Вы Запрос Сертификат для Безопасных Конференций

Дополнительные сведения

- Согласование IPsec/Протоколы IKE
- Cisco Systems – техническая поддержка и документация