SBSI Step-By-Step Instructions пошаговые инструкции SBSI

Главное меню
Главная
О проекте
Для разработчиков
ПО и оборудования
Прислать пошаговую инструкцию
Ссылки
Контакты

Поиск...
Поиск

Организация удаленного доступа по протоколу SSTP

## Содержание



## 1. Пошаговое руководство по организации удаленного доступа по протоколу SSTP

В настоящем руководстве предлагаются подробные инструкции по созданию лаборатории тестирования на основе трех компьютеров, а также по настройке и тестированию удаленного доступа через виртуальную частную сеть (VPN) под управлением ОС Windows Server® 2008 и Windows Vista® с пакетом обновления 1 (SP1). Эти инструкции описывают поэтапный процесс настройки SSTP-соединения.

> **Примечание**
> Нижеследующие инструкции позволяют сформировать лабораторию тестирования с ограниченным числом компьютеров минимальными усилиями. Чтобы сократить время настройки и упростить этот процесс, службы не распределяются по отдельным компьютерам, что позволило бы повысить степень защиты, а совмещаются на сетевых серверах. Такая конфигурация не является рекомендуемой для внедрения в действующей сети. Эта конфигурация, не исключая IP-адреса и все прочие параметры, предназначена исключительно для работы в изолированной сети лаборатории тестирования.

### ПО Virtual PC или виртуальный сервер

ПО Microsoft Virtual PC и виртуальные серверы помогают сформировать лабораторию

тестирования, которая описывается в настоящем документе, ограничив количество участвующих компьютеров двумя или даже одним. Настроив виртуальную лабораторию, вы сможете перемещаться между тремя виртуальными компьютерами одним щелчком мыши.

## 2. Протокол SSTP

Протокол SSTP (Secure Socket Tunneling Protocol) – это новая разновидность VPN-туннеля, позволяющая передавать данные через брандмауэры, которые блокируют трафик протоколов PPTP и L2TP/IPsec. В протоколе SSTP предусмотрен механизм инкапсуляции трафика PPP через канал SSL протокола HTTPS. Применение протокола PPP, в свою очередь, делает возможной поддержку методов строгой проверки подлинности – в частности, EAP-TLS. Протокол HTTPS пропускает данные через порт TCP 443 – стандартный порт веб-доступа. Наконец, протокол SSL (Secure Sockets Layer) обеспечивает защиту на транспортном уровне, а также широкие возможности согласования ключей, шифрования и проверки целостности.

### Процесс VPN-подключения по протоколу SSTP

Ниже описывается поток данных VPN-подключения по протоколу SSTP.
Когда пользователь компьютера, работающего под управлением ОС Windows Server 2008 или Windows Vista с пакетом обновления 1 (SP1), инициирует VPN-подключение по протоколу SSTP, выполняется следующая последовательность операций.

1. SSTP-клиент устанавливает TCP-соединение с SSTP-сервером между TCP-портом SSTP-клиента, назначенным динамически, и TCP-портом 443 SSTP-сервера.

2. SSTP-клиент отправляет приветствие (SSL Client-Hello), обозначая свое намерение установить сеанс SSL с SSTP-сервером.

3. SSTP-сервер отправляет SSTP-клиенту свой сертификат компьютера.

4. SSTP-клиент проводит проверку сертификата компьютера, определяет метод шифрования для предстоящего сеанса SSL, генерирует ключ сеанса SSL и

зашифровывает его с помощью открытого ключа сертификата SSTP-сервера. После этого зашифрованный ключ сеанса SSL отправляется SSTP-серверу.

5. SSTP-сервер расшифровывает ключ сеанса SSL при помощи закрытого ключа своего сертификата компьютера. Все последующие данные, которыми SSTP-клиент будет обмениваться с SSTP-сервером, подлежат шифрованию согласованным методом и с применением ключа сеанса SSL.

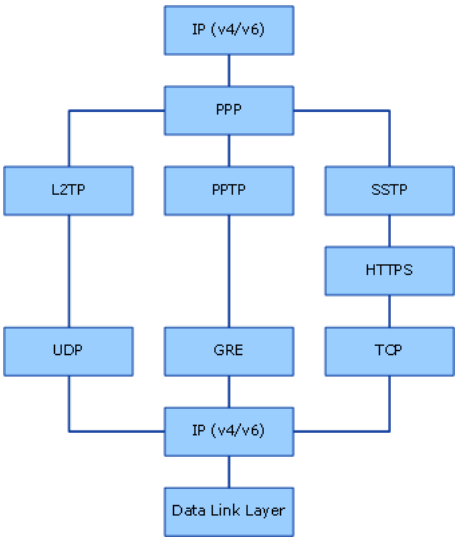
6. SSTP-клиент отправляет SSTP-серверу запрос по протоколу HTTP через SSL.

7. SSTP-клиент согласовывает с SSTP-сервером SSTP-туннель.

8. SSTP-клиент согласовывает с SSTP-сервером PPP-соединение. В рамках согласования производится проверка подлинности учетных данных пользователей методом PPP, а также настраиваются параметры трафика по протоколу IP версии 4 (IPv4) или 6 (IPv6).

9. SSTP-клиент приступает к передаче трафика IPv4 или IPv6 по каналу PPP.

**Рисунок 1. Архитектура SSTP на уровне протоколов.**




### 3. Создание лаборатории тестирования VPN-подключений по протоколу SSTP

В рамках лаборатории тестирования VPN-подключений сеть состоит из трех компьютеров, которые выполняют нижеперечисленные роли.

· Сервер DC1, работающий под управлением ОС Windows Server 2008, исполняет роли контроллера домена, DNS-сервера и файлового сервера в частной сети (интрасети).

· Сервер маршрутизации и удаленного доступа под именем VPN1, работающий под управлением ОС Windows Server 2008, действует в качестве VPN-сервера. Кроме того, на сервере VPN1 установлены службы сертификации Active Directory и службы IIS. Они обеспечивают возможность подачи заявок на сертификат компьютера через Интернет, что необходимо для организации VPN-подключений по протоколу SSTP. Наконец, на сервере VPN1 установлено два сетевых адаптера.

· Клиентский компьютер CLIENT1, работающий под управлением ОС Windows Vista с пакетом обновления 1 (SP1) и исполняющий роль VPN-клиента в общедоступной сети (Интернете).

Конфигурация лаборатории тестирования VPN-подключений изображена на следующей схеме.

**Рисунок 2. Конфигурация лаборатории тестирования подключений по протоколу SSTP.**


### 4. Настройка компьютера DC1

Компьютер DC1, работающий под управлением ОС Windows Server 2008, исполняет следующие роли:

- контроллер домена Contoso.com службы каталогов Active Directory®;
- DNS-сервер домена Contoso.com;
- файловый сервер.

Процесс настройки компьютера DC1 состоит из нескольких этапов:

- установка операционной системы;
- настройка протокола TCP/IP;
- установка служб Active Directory и DNS;
- создание учетной записи пользователя и присвоение ей прав удаленного доступа;
- создание общей папки и файла.

В нижеследующих подразделах эти операции описаны подробнее.

### Установка операционной системы

### Установка ОС Windows Server 2008

1. Запустите компьютер DC1 с установочного диска ОС Windows Server 2008.
2. Следуйте инструкциям на экране. При появлении запроса на ввод пароля введите P@ssword.

### Настройка протокола TCP/IP

Необходимо настроить следующие свойства протокола TCP/IP на компьютере DC1: IP-адрес 192.168.0.1, маску подсети 255.255.255.0 и основной шлюз 192.168.0.2.

### Настройка свойств протокола TCP/IP

1. В секции Provide Computer Information (предоставить сведения о компьютере) окна Initial Configuration Tasks (задачи начальной настройки) на компьютере DC1 щелкните ссылку Configure networking (настроить сеть).

**Примечание**
Если окно Initial Configuration Tasks не было открыто ранее, откройте его. Для этого выберите Start (пуск), Run (выполнить), введите в текстовом поле oobe и нажмите кнопку OK.

**Рисунок 3. Окно Initial Configuration Tasks.**


2. В окне Network Connections (сетевые подключения) щелкните правой кнопкой мыши запись Local Area Connection (подключение по локальной сети) и выберите пункт Properties (свойства).

3. Во вкладке Networking (сеть) выберите запись Internet Protocol Version 4 (TCP/IPv4) (протокол Интернета версии 4 (TCP/IPv4)) и нажмите кнопку Properties.

4. Установите переключатель в положение Use the following IP address (использовать следующий IP-адрес). Укажите IP-адрес 192.168.0.1, маску подсети 255.255.255.0, основной шлюз 192.168.0.2 и предпочитаемый DNS-сервер 192.168.0.1.

5. Последовательно нажмите кнопки **OK** и **Close** (закрыть).

**Установка служб Active Directory и DNS**

Компьютер следует назначить контроллером домена Contoso.com. Он будет первым и единственным контроллером домена в сети.

**Настройка компьютера DC1 в роли контроллера домена**

1. В секции Provide Computer Information окна Initial Configuration Tasks на компьютере DC1 щелкните ссылку Provide computer name and domain (указать имя компьютера и домен).

   Примечание
   Если окно Initial Configuration Tasks не было открыто ранее, откройте его. Для этого выберите Start, Run, введите в текстовом поле oobe и нажмите кнопку OK.

2. Во вкладке Computer Name (имя компьютера) диалогового окна System Properties (свойства системы) нажмите кнопку Change (изменить).

3. Присвоив компьютеру имя DC1, нажмите кнопку OK.

4. Нажмите кнопку **OK** в диалоговом окне Computer Name/Domain Changes (изменение имени компьютера или домена).

5. Последовательно нажмите кнопки Close и Restart Now (перезагрузить сейчас).

6. После перезапуска сервера щелкните ссылку Add roles (добавить роли) в секции Customize This Server (настроить этот сервер) окна Initial Configuration Tasks.

7. На странице Before You Begin (перед началом работы) диалогового окна Add Roles Wizard (мастер добавления ролей) нажмите кнопку Next (далее).

8. Установите флажок Active Directory Domain Services (доменные службы Active Directory) и нажмите кнопку Next.

9. При появлении диалогового окна Active Directory Domain Services нажмите кнопку Next.

10. В диалоговом окне Confirm Installation Selections (подтвердите выбранные элементы) нажмите кнопку Install (установить).

11. В диалоговом окне Installation Results (результаты установки) нажмите кнопку Close.

12. Нажмите кнопку Start и выберите Run. Введите команду dcpromo в поле Open (открыть) и нажмите кнопку OK.

13. На странице Welcome to the Active Directory Domain Services Installation Wizard (мастер установки Active Directory) нажмите кнопку Next.

14. Установив параметр **Create a new** domain in a new forest (создать новый домен в новом лесу), нажмите кнопку Next.

15. Введите имя contoso.com в поле FQDN of the forest root domain (полное доменное имя корневого домена леса) и нажмите кнопку Next.

16. Выбрав в списке Forest functional level (режим работы леса) пункт Windows Server 2003, нажмите кнопку Next.

17. Чтобы подтвердить режим работы леса Windows Server 2003, нажмите кнопку Next.

18. Чтобы установить DNS server (DNS-сервер) в качестве дополнительного свойства контроллера домена, нажмите кнопку Next.

19. Установите параметр Yes, the computer will use a dynamically assigned IP address (not recommended) (да, компьютер будет использовать динамически назначаемый IP-адрес (не рекомендуется)).

20. Нажмите кнопку Yes (да) в диалоговом окне подтверждения.

21. Чтобы согласиться с предложенным по умолчанию размещением папок, нажмите кнопку Next.

22. Введите пароль в поле Directory Services Restore Mode Administrator Password (пароль администратора для режима восстановления служб каталогов) и нажмите кнопку Next.

23. Нажмите кнопку **Next**.

24. Мастер Active Directory Domain Services Installation Wizard приступит к настройке службы Active Directory. По завершении настройки последовательно нажмите кнопки Finish (готово) и Restart Now.

## Создание учетной записи пользователя и присвоение ей прав удаленного доступа

Теперь необходимо создать учетную запись пользователя и присвоить ей права удаленного доступа.

**Создание учетной записи пользователя в службе Active Directory и присвоение ей прав**

1. На компьютере DC1 нажмите кнопку Start, а затем выберите Administrative Tools (администрирование) и Active Directory Users and Computers (Active Directory – пользователи и компьютеры).

2. Раскройте узел contoso.com в дереве консоли, находящемся в левой части окна, щелкните правой кнопкой мыши запись Users (пользователи), затем выберите New (создать) и User (пользователь).

3. Введите user1 в полях Full name (полное имя) и User logon name (имя входа пользователя).

4. Нажмите кнопку **Next**.

5. Введите P@ssword в полях Password (пароль) и Confirm password (подтверждение).

6. Снимите флажок User must change password at next logon (требовать смену пароля при следующем входе в систему), а затем установите флажки User cannot change password (запретить смену пароля пользователями) и Password never expires (срок действия пароля не ограничен).

7. Последовательно нажмите кнопки Next и Finish.

Чтобы предоставить права удаленного доступа пользователю user1, выполните следующие действия:

1. Щелкните узел Users в дереве консоли в левой части окна. В области сведений щелкните правой кнопкой мыши запись user1 и выберите пункт Properties.

2. В секции Network Access Permission (права доступа к сети) вкладки Dial-in (удаленный доступ) установите параметр Allow access (разрешить доступ) и нажмите кнопку OK.

Примечание
В рабочей среде политики удаленного доступа настраиваются и вводятся в действие посредством сервера сетевых политик (NPS).

3. Закройте консоль оснастки Active Directory Users and Computers.

### 5. Настройка компьютера VPN1

Компьютер VPN1, работающий под управлением ОС Windows Server 2008, исполняет следующие роли:

· службы сертификации Active Directory – центр сертификации (CA), который выдает сертификат компьютера, необходимый для VPN-подключения по протоколу SSTP;

· служба подачи заявок в центр сертификации через Интернет, которая обеспечивает возможность предоставления сертификатов через веб-обозреватель;

· веб-сервер (IIS), установленный в качестве обязательной службы роли для службы подачи заявок в центр сертификации через Интернет;

**Примечание**
Службе маршрутизации и удаленного доступа не нужен сервер IIS, поскольку она прослушивает HTTPS-соединения непосредственно при помощи драйвера HTTP.SYS. Сервер IIS в данном сценарии требуется для того, чтобы компьютер CLIENT1 смог получить от компьютера VPN1 сертификат через Интернет.

· службы политики сети и доступа, обеспечивающие поддержку VPN-подключений через службу удаленного доступа.

Процесс настройки компьютера VPN1 состоит из нескольких этапов:

· установка операционной системы;

· настройка протокола TCP/IP для работы в Интернете и интрасетях;

· присоединение к домену Contoso.com;

· установка двух ролей сервера: служб сертификации Active Directory и веб-сервера (IIS);

· создание и установка сертификата проверки подлинности сервера;

· установка роли служб политики сети и доступа (службы маршрутизации и удаленного доступа);

· настройка компьютера VPN1 в качестве VPN-сервера.

В нижеследующих подразделах эти операции описаны подробнее.

#### Установка операционной системы

Для установки ОС Windows Server 2008 на компьютере VPN1 выполните следующие действия:

**Установка ОС Windows Server 2008**

1. В секции Provide Computer Information окна Initial Configuration Tasks на компьютере VP1 щелкните ссылку Configure networking.

**Примечание**
Если окно Initial Configuration Tasks не было открыто ранее, откройте его. Для этого выберите Start, Run, введите в текстовом поле oobe и нажмите кнопку OK.

2. В окне Network Connections щелкните правой кнопкой мыши запись сетевого подключения и выберите пункт Properties.

3. Во вкладке Networking выберите запись Internet Protocol Version 4 (TCP/IPv4) и нажмите кнопку Properties.

4. Установите переключатель в положение Use the following IP address.

5. Установите следующие значения IP-адреса и маски подсети:

а) для сетевой карты, подключенной к общедоступной сети (Интернету) – IP-адрес 131.107.0.2 и маска подсети 255.255.0.0;

б) для сетевой карты, подключенной к частной сети (интрасети) – IP-адрес 192.168.0.2, маска подсети 255.255.255.0, предпочитаемый DNS-сервер 192.168.0.1.

6. Последовательно нажмите кнопки **OK** и **Clo**se.

7. Чтобы переименовать сетевое подключение, щелкните его запись правой кнопкой мыши и выберите команду Rename (переименовать).

8. Присвойте сетевым подключениям следующие имена:

а) подключению к общедоступной сети (Интернету) – Public;

б) подключению к частной сети (интрасети) – Private.

9. Закройте окно Network Connections.

Чтобы удостовериться в наличии связи между компьютерами VPN1 и DC1, выполните команду ping на компьютере VPN1.

**Проверка сетевого подключения при помощи команды ping**

1. На компьютере VPN1 нажмите кнопку Start, выберите Run, а затем введите cmd в поле **Open**. Нажмите кнопку OK. Введите ping192.168.0.1 в окне команд.

2. Убедитесь в том, что проверка связи с компьютером DC1 прошла успешно.

3. Закройте окно команд.

Присоединение к домену Contoso

Компьютер VPN1 следует настроить в качестве рядового сервера в домене Contoso.com.

**Присоединение компьютера VPN1 к домену Contoso.com**

1. В секции Provide Computer Information окна Initial Configuration Tasks на компьютере VPN1 щелкните ссылку Provide computer name and domain.

**Примечание**
Если окно Initial Configuration Tasks не было открыто ранее, откройте его. Для этого выберите Start, Run, введите в текстовом поле oobe и нажмите кнопку OK.

2. Во вкладке Computer Name диалогового окна System Properties нажмите кнопку Change.

3. Вместо имеющейся строки в поле Computer name введите VPN1.

4. Выберите значение **Domain** (домен) параметра Member of (входит в состав), введите contoso и нажмите кнопку OK.

5. Укажите имя пользователя administrator и пароль P@ssword.

6. При появлении диалогового окна, оповещающего о вхождении компьютера в состав домена contoso.com, нажмите кнопку OK.

7. При появлении диалогового окна с предложением перезагрузить компьютер нажмите кнопку OK. Последовательно нажмите кнопки Close и Restart Now.

## Установка служб сертификации Active Directory и веб-сервера

Для поддержки VPN-подключений по протоколу SSTP необходимо в первую очередь установить службы сертификации Active Directory и веб-сервер (IIS), которые делают возможным подачу заявок на сертификат компьютера через Интернет.

**Установка ролей VPN-сервера и служб сертификации**

1. Войдите в систему VPN1, указав имя пользователя administrator@contoso.com и пароль P@ssword.

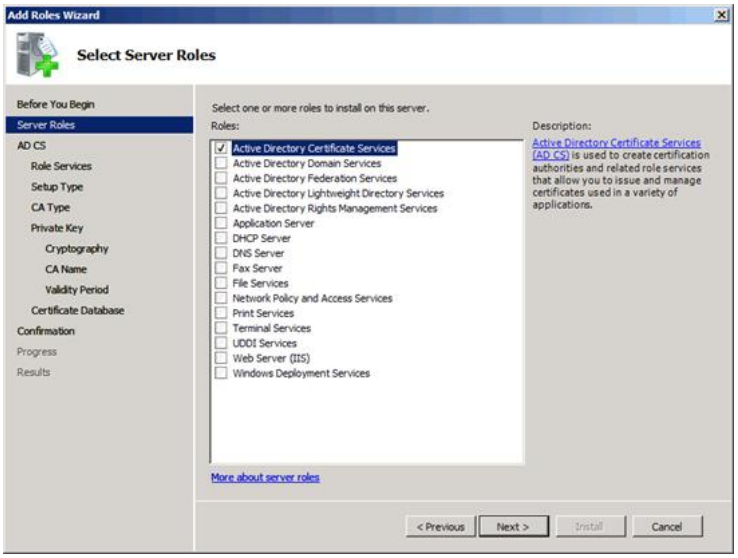
2. Щелкните ссылку Add roles в секции Customize This Server окна Initial Configuration Tasks.

**Примечание**
Если окно Initial Configuration Tasks не было открыто ранее, откройте его. Для этого выберите Start, Run, введите в текстовом поле oobe и нажмите кнопку OK.

3. На странице Before You Begin диалогового окна Add Roles Wizard нажмите кнопку Next.

4. Установите флажок Active Directory Certificate Services (службы сертификации Active Directory).

**Рисунок 4. Окно Select Server Roles.**

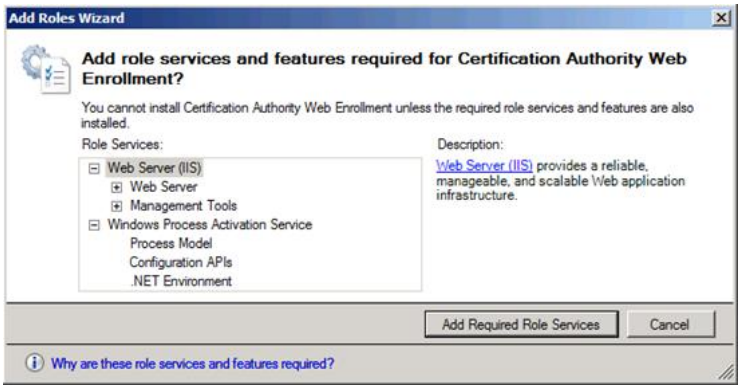



5. Дважды нажмите кнопку Next.

6. В секции **Role Services** (службы роли) диалогового окна Select Role Services (выбор служб ролей) установите флажок Certification Authority Web Enrollment (служба подачи заявок в центр сертификации через Интернет).

7. Нажмите кнопку Add Required Role Services (добавить требуемые службы роли) в диалоговом окне Add Roles Wizard.

**Рисунок 5. Диалоговое окно Add Roles Wizard.**




8. Нажмите кнопку **Next**.

9. Выберите пункт Standalone (изолированный) и нажмите кнопку Next.

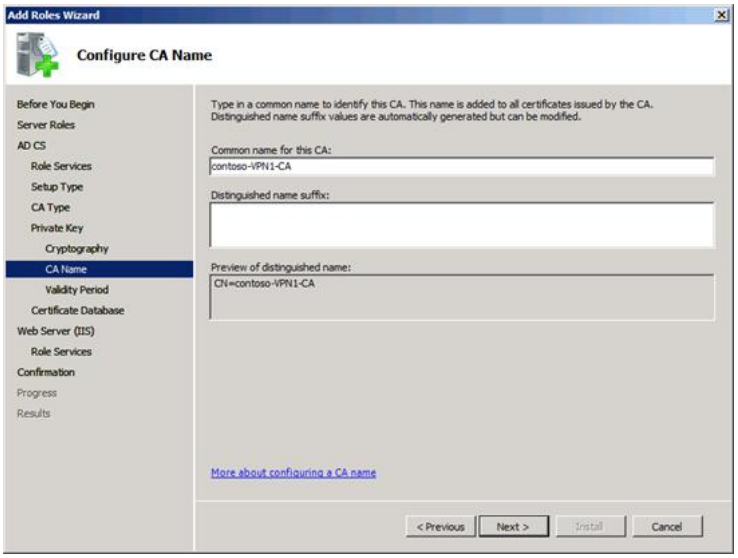
10. Выберите пункт Root CA (recommended) (корневой ЦС (рекомендуется)) и нажмите кнопку Next.

11. Выберите пункт Create a new private key (создать новый закрытый ключ) и нажмите кнопку Next.

12. Чтобы согласиться с предложенными по умолчанию параметрами криптографии, нажмите кнопку Next.

13. Чтобы согласиться с предложенным по умолчанию именем ЦС, нажмите кнопку **Next** в диалоговом окне Configure CA Name (задание имени ЦС).

**Рисунок 6. Диалоговое окно Configure CA Name.**




14. Нажмите кнопку Next столько раз, сколько потребуется для того, чтобы согласиться со всеми предлагаемыми по умолчанию параметрами.

15. В диалоговом окне Confirm Installation Selections нажмите кнопку Install. Установка может занять несколько минут.

16. В диалоговом окне Installation Results нажмите кнопку Close.

### Создание и установка сертификата проверки подлинности сервера

Сертификат проверки подлинности сервера нужен для того, чтобы компьютер CLIENT1 смог проверить подлинность компьютера VPN1. Перед установкой этого сертификата следует разрешить публикацию сертификатов в настройках обозревателя Internet Explorer.

**Настройка обозревателя Internet Explorer**

1. На компьютере VPN1 нажмите кнопку Start, щелкните правой кнопкой мыши запись Internet Explorer и выберите пункт Run as administrator (запуск от имени администратора).

2. В случае вывода оповещения фильтра фишинга выберите пункт Turn off automatic Phishing Filter (отключить автоматический фильтр фишинга) и нажмите кнопку OK.

3. Откройте меню Tools (сервис) и выберите команду Internet Options (свойства обозревателя).

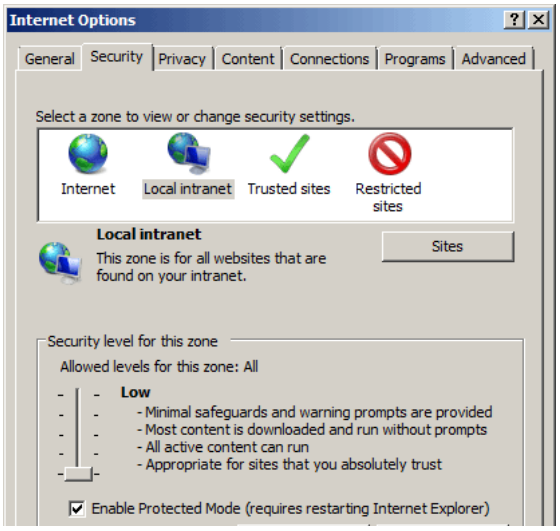
4. Откройте вкладку **Security** (безопасность) диалогового окна Internet Options.

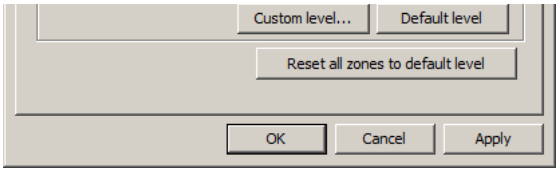
5. В области Select a zone to view or change security settings (выберите зону для настройки ее параметров безопасности) выберите пункт Local intranet (местная интрасеть).

6. Снизьте уровень безопасности в местной интрасети с Medium-low (ниже среднего) до Low (низкий) и нажмите кнопку OK.

> **Примечание**
> В рабочей среде вместо снижения уровня безопасности следует настроить отдельные параметры элементов управления ActiveX®, нажав кнопку Custom level (другой).

**Рисунок 7. Диалоговое окно Internet Options.**






Теперь следует отправить запрос на получение сертификата проверки подлинности сервера средствами обозревателя Internet Explorer.

**Отправка запроса на получение сертификата проверки подлинности сервера**

1. В адресной строке обозревателя Internet Explorer на компьютере VPN1 введите адрес http://localhost/certsrv и нажмите клавишу ВВОД.

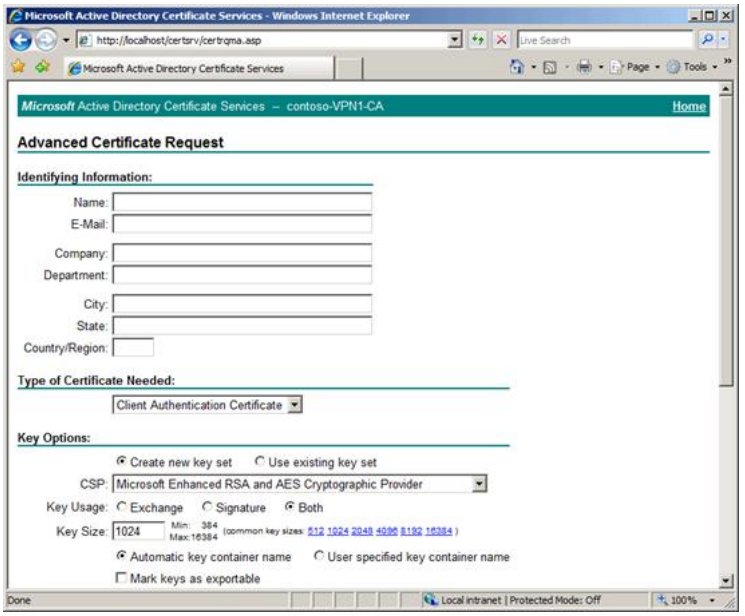
2. В области Select a task (выберите действие) выберите пункт Request a certificate (запросить сертификат).

3. В области Request a Certificate выберите пункт advanced certificate request (расширенный запрос сертификата).

4. В области Advanced Certificate Request выберите пункт Create and submit a request to this CA (создать и выдать запрос этому ЦС).

5. Чтобы разрешить элемент управления ActiveX, нажмите кнопку Yes.

Рисунок 8. Страница Advanced Certificate Request.




6. В поле **Name** (имя) в области Identifying Information (идентифицирующие сведения) введите vpn1.contoso.com, а в поле Country/Region (страна или регион) – введите US.

> **Примечание**
> Под именем подразумевается имя субъекта сертификата. Оно должно совпадать с Интернет-адресом в параметрах подключения по протоколу SSTP, которые вам предстоит настроить позже.

7. В области Type of Certificate Needed (тип требуемого сертификата) выберите пункт Server Authentication Certificate (сертификат проверки подлинности сервера).

8. Установите флажок Mark keys as exportable (пометить ключ как экспортируемый) в области Key Options (параметры ключа) и нажмите кнопку Submit (отправить).

9. Нажмите кнопку Yes в диалоговом окне подтверждения.

Теперь сертификат проверки подлинности сервера находится в состоянии ожидания. Для того, чтобы сертификат можно было установить, он должен быть выдан.

**Выдача и установка сертификата проверки подлинности сервера**

1. На компьютере VPN1 нажмите кнопку Start и выберите пункт Run.

2. Введите команду mmc в поле Open и нажмите кнопку OK.

3. При появлении оснастки Console1 откройте меню File (файл) и выберите команду Add/Remove Snap-in (добавить или удалить оснастку).

4. В списке Available snap-ins (доступные оснастки) выберите пункт Certification Authority (центр сертификации) и нажмите кнопку Add.

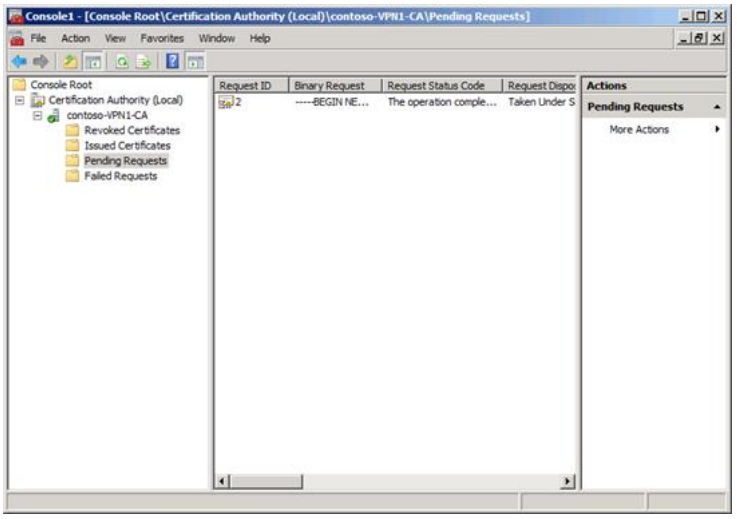
5. Чтобы согласиться с предложенным по умолчанию параметром Local computer (локальный компьютер), нажмите кнопку Finish.

6. Чтобы закрыть диалоговое окно Add or Remove Snap-ins (добавление и удаление оснастки), нажмите кнопку OK.

7. В левой области свежесозданной консоли MMC дважды щелкните пункт Certification Authority (Local) (центр сертификации (локальный)).

8. Дважды щелкните запись contoso-VPN1-CA, а затем выберите пункт Pending Requests (запросы в ожидании).

**Рисунок 9. Консоль Certification Authority.**




9. Щелкните правой кнопкой мыши ожидающий запрос, указанный в средней области консоли, а затем последовательно выберите команды All Tasks (все задачи) и Issue (выдать).

10. На странице Certificate Pending (ожидаемый сертификат) в обозревателе выберите пункт Home (главная). Если эта страница не отображается, введите в адресной строке адрес http://localhost/certsrv.

11. В области Select a task выберите пункт View the status of a pending certificate request (просмотр состояния ожидаемого запроса сертификата).

12. В области View the Status of a Pending Certificate Request выберите сертификат, который был только что выдан.

13. Чтобы разрешить элемент управления ActiveX, нажмите кнопку Yes.

14. В области Certificate Issued (сертификат выдан) нажмите кнопку Install this certificate (установить сертификат).

15. Нажмите кнопку Yes в диалоговом окне подтверждения.

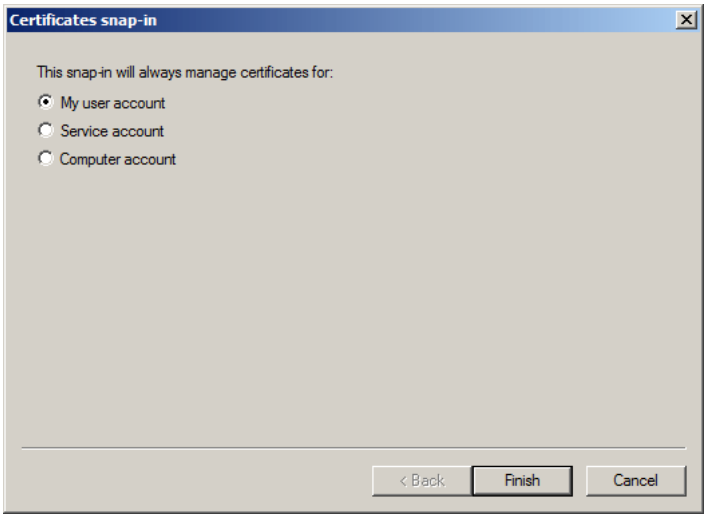
Следующая задача заключается в том, чтобы переместить установленный сертификат из хранилища, в которое он был помещен по умолчанию.

**Перемещение сертификата**

1. В ранее созданной консоли MMC на компьютере VPN1 откройте меню File и выберите пункт Add/Remove Snap-in.

2. В списке Available snap-ins выберите пункт Certificates (сертификаты) и нажмите кнопку Add.

**Рисунок 10. Диалоговое окно Certificates snap-in.**




3. Чтобы согласиться с предложенным по умолчанию параметром My user

account (моей учетной записи пользователя), нажмите кнопку Finish.

4. Нажмите кнопку Add, выберите пункт Computer account (учетной записи компьютера), а затем нажмите кнопку Next.

5. Чтобы согласиться с предложенным по умолчанию параметром Local computer, нажмите кнопку Finish в диалоговом окне Select Computer (выбор компьютера).

6. Чтобы закрыть диалоговое окно Add or Remove Snap-ins, нажмите кнопку OK.

7. Дважды щелкните запись Certificates - Current User (сертификаты – текущий пользователь) в области дерева консоли, дважды щелкните запись Personal (личные), а затем выберите пункт Certificates.

8. В средней области просмотра щелкните правой кнопкой мыши запись сертификата vpn1.contoso.com, после чего последовательно выберите команды All Tasks и Export (экспорт).

9. На странице Welcome (приветствие) нажмите кнопку Next.

10. Выберите пункт Yes, export the private key (да, экспортировать закрытый ключ) и нажмите кнопку Next.

11. Чтобы согласиться с предложенным по умолчанию форматом файла, нажмите кнопку Next.

12. Введите P@ssword в обоих текстовых полях и нажмите кнопку Next.

13. На странице **File to Export** (имя файла экспорта) нажмите кнопку **Browse** (обзор).

14. Введите строку vpn1cert в текстовом поле File name (имя файла), а затем нажмите кнопку Browse Folders (обзор папок).

15. Чтобы сохранить сертификат на рабочем столе, выберите пункт **Desktop** (рабочий стол) в области Favorite Links (избранные ссылки), а затем нажмите кнопку Save (сохранить).

16. На странице **File to Export** нажмите кнопку **Next**.

17. Чтобы закрыть мастер Certificate Export Wizard (мастер экспорта сертификатов), нажмите кнопку Finish. Затем нажмите кнопку OK в диалоговом окне подтверждения.

18. Последовательно дважды щелкните записи Certificates (Local Computer) (сертификаты (локальный компьютер)) и Personal.

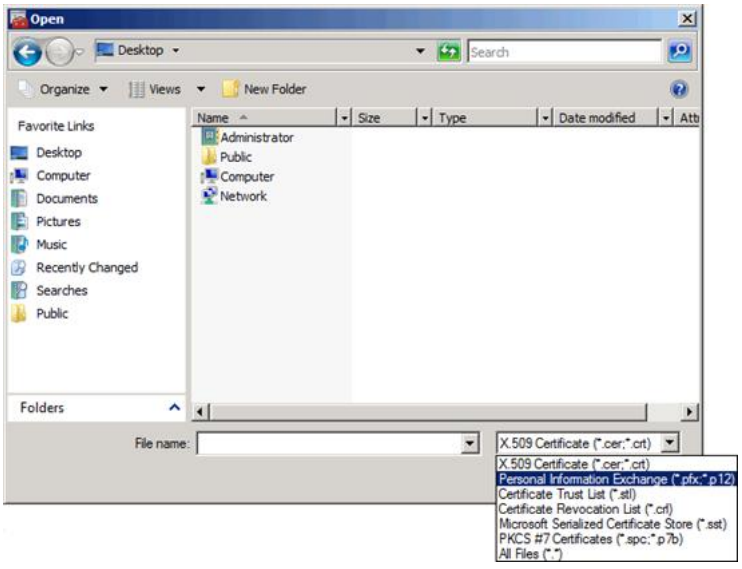
19. Выберите и щелкните правой кнопкой мыши пункт Certificates, после чего последовательно выберите команды All Tasks и Import (импорт).

20. На странице Welcome нажмите кнопку Next.

21. На странице **File to Import** (импортируемый файл) нажмите кнопку **Browse**.

22. В области Favorite Links выберите пункт Desktop, а затем укажите тип файла Personal Information Exchange (файл обмена личной информацией) в раскрывающемся списке.

**Рисунок 11. Мастер Certificate Import Wizard.**




23. Дважды щелкните сертификат vpn1cert в средней области просмотра.

24. На странице **File to Import** нажмите кнопку **Next**.

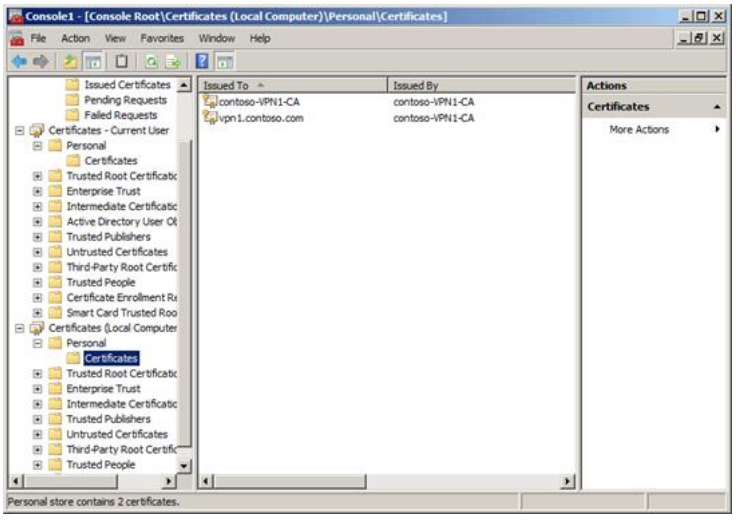
25. Введите P@ssword в текстовом поле Password и нажмите кнопку Next.

26. Чтобы согласиться с предложенным хранилищем личной информации,

нажмите кнопку **Next** на странице Certificate Store (хранилище сертификатов).

27. Чтобы закрыть мастер Import Export Wizard (мастер импорта-экспорта), нажмите кнопку Finish. Затем нажмите кнопку OK в диалоговом окне подтверждения.

**Рисунок 12. Расположение сертификата проверки подлинности сервера.**




**Внимание!**
В случае несоблюдения последовательности процедур, изложенных в настоящем документе, не исключено возникновение проблем, связанных с наличием универсального сертификата (contoso-VPN1-CA). Чтобы обеспечить привязку SSTP-прослушивателя к сертификату проверки подлинности сервера (vpn1.contoso.com), удалите сертификат contoso-VPN1-CA из локального хранилища.

**Удаление универсального сертификата**

1. Дважды щелкните запись Certificates в средней области просмотра, щелкните правой кнопкой мыши запись contoso-VPN1-CA и выберите пункт Delete (удалить).

2. Нажмите кнопку Yes в диалоговом окне подтверждения.

## Установка службы маршрутизации и удаленного доступа

Далее нам следует настроить компьютер VPN1, оснащенный службой маршрутизации и удаленного доступа, в качестве VPN-сервера.

**Установка ролей VPN-сервера и служб сертификации**

1. На компьютере VPN1 щелкните ссылку Add roles в секции Customize This Server окна Initial Configuration Tasks.

**Примечание** Если окно Initial Configuration Tasks не было открыто ранее, откройте его. Для этого выберите Start, Run, введите в текстовом поле oobe и нажмите кнопку OK.

2. На странице Before You Begin диалогового окна Add Roles Wizard нажмите кнопку Next.

3. Установите флажок Network Policy and Access Services (службы политики сети и доступа), а затем дважды нажмите кнопку Next.

4. В секции **Role Services** диалогового окна Select Role Services установите флажок Routing and Remote Access Services (службы маршрутизации и удаленного доступа).

5. Нажмите кнопку Next, а затем – кнопку Install.

6. В диалоговом окне Installation Results нажмите кнопку Close.

## Настройка службы маршрутизации и удаленного доступа

Теперь следует настроить компьютер VPN1 в качестве VPN-сервера, предоставляющего удаленный доступ VPN-клиентам в Интернете.

**Настройка компьютера VPN1 в качестве VPN-сервера**

1. На компьютере VPN1 нажмите кнопку Start, выберите сначала Administrative Tools, а затем – Routing and Remote Access (маршрутизация и удаленный доступ).

2. В дереве консоли Routing and Remote Access щелкните правой кнопкой мыши запись VPN1 и выберите пункт Configure and Enable Routing and Remote Access (настроить и включить маршрутизацию и удаленный доступ).

3. При появлении страницы Welcome to the Routing and Remote Access Server Setup Wizard (мастер установки сервера маршрутизации и удаленного доступа) нажмите кнопку Next.

4. Чтобы согласиться с предложенным по умолчанию параметром Remote access (dial-up or VPN) (удаленный доступ (VPN или модем)) на странице Configuration (настройка), нажмите кнопку Next.

5. На странице Remote Access (удаленный доступ) выберите пункт VPN, а затем нажмите кнопку Next.

6. В области Network interfaces (интерфейсы сети) на странице VPN Connection (VPN-подключение) выберите пункт Public. Именно через этот интерфейс компьютер VPN1 будет подключаться к Интернету.

7. Снимите флажок Enable security on the selected interface by setting up static packet filters (безопасность с использованием фильтров статических пакетов) и нажмите кнопку Next.

> **Примечание**
> В общем случае защиту общедоступного интерфейса следует включать. Этот параметр отключается исключительно для обеспечения связи в рассматриваемой тестовой среде.

8. Выберите пункт From a specified range of addresses (из заданного диапазона адресов) и нажмите кнопку Next.

9. Выбрав пункт New, введите 192.168.0.200 в поле Start IP address (начальный IP-адрес) и 192.168.0.210 в поле End IP address (конечный IP-адрес), а затем последовательно нажмите кнопки OK и Next.

10. Нажмите кнопку Next, чтобы согласиться с предложенным по умолчанию параметром, который подразумевает, что компьютер VPN1 не будет взаимодействовать с RADIUS-сервером. В рамках такого сценария сервер маршрутизации и удаленного доступа будет применять проверку подлинности Windows.

11. При появлении страницы Completing the Routing and Remote Access Server Setup Wizard (завершение мастера сервера маршрутизации и удаленного доступа) нажмите кнопку Finish.

12. В случае открытия диалогового окна, в котором сообщается о необходимости внести данный компьютер в список серверов удаленного доступа, нажмите кнопку OK.

13. В случае открытия диалогового окна, сообщающего о необходимости настройки агента DHCP-ретрансляции, нажмите кнопку OK.

14. Закройте оснастку Routing and Remote Access.

## 6. Настройка компьютера CLIENT1

Компьютер CLIENT1, работающий под управлением ОС Windows Vista с пакетом обновления 1 (SP1), будет исполнять роль VPN-клиента удаленного доступа в домене Contoso.com.
Процесс настройки компьютера CLIENT1 состоит из следующих этапов:

- установка операционной системы;
- настройка протокола TCP/IP.

В нижеследующих подразделах эти операции описаны подробнее.

### Установка операционной системы

Чтобы установить ОС Windows Vista с пакетом обновления 1 (SP1) на компьютере CLIENT1, выполните следующие действия:

**Установка ОС Windows Vista с пакетом обновления 1 (SP1)**

1. Запустите компьютер CLIENT1 с установочного компакт-диска ОС Windows Vista с пакетом обновления 1 (SP1). Следуйте инструкциям на экране.

2. Когда на экране появится запрос на указание типа установки, выберите пункт Custom (выборочная).

3. При появлении запроса на указание имени пользователя введите user1.

4. При появлении запроса на указание имени компьютера введите CLIENT1.

5. При появлении запроса на выбор размещения компьютера введите Home (домашний).

### Настройка протокола TCP/IP

Теперь на компьютере CLIENT1 следует настроить свойства протокола TCP/IP – а именно, указать статический IP-адрес 131.107.0.3 для публичных соединений (через Интернет).

**Настройка свойств протокола TCP/IP**

1. На компьютере CLIENT1 нажмите кнопку Start и выберите пункт Control Panel (панель управления).

2. Последовательно выберите пункты Network and Internet (сеть и подключения к Интернету), Network and Sharing Center (центр управления сетями и общим доступом) и Manage network connections (управление сетевыми подключениями).

3. Щелкнув правой кнопкой мыши запись Local Area Connection (подключение по локальной сети), выберите команду Properties. Если на экране появится диалоговое окно с запросом на разрешения, необходимые для выполнения данной операции, нажмите кнопку Continue (продолжить).

4. Во диалоговом окне Local Area Connection Properties (свойства подключения по локальной сети) выберите запись Internet Protocol Version 4 (TCP/IPv4) и нажмите кнопку Properties.

5. Установите переключатель в положение Use the following IP address. В поле IP address (IP-адрес) введите 131.107.0.3, а в поле маски подсети – 255.255.0.0.

6. Последовательно нажмите кнопки **OK** и **Close**.

Далее необходимо включить в файл hosts запись компьютера VPN1. Именно так делается в рабочих средах, когда корпоративный VPN-сервер получает общедоступное имя узла.

**Настройка файла hosts**

1. На компьютере CLIENT1 нажмите кнопку , последовательно выберите пункты и (стандартные), затем щелкните правой кнопкой мыши пункт **Command Prompt** (командная строка) и выберите команду .

2. В диалоговом окне User Account Control (контроль учетных записей) нажмите кнопку Continue.

3. Введите нижеследующую команду в командной строке, а затем нажмите клавишу ВВОД:

```
notepad %windir%\system32\drivers\etc\hosts
```

4. Добавьте новой строкой в конец документа следующий текст:

```
131.107.0.2        vpn1.contoso.com
```

5. Сохраните и закройте файл hosts.

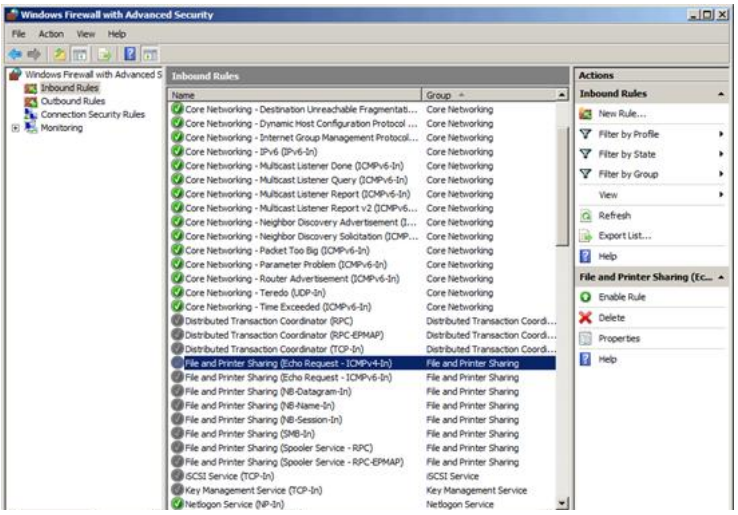
Чтобы удостовериться в наличии связи между компьютерами CLIENT1 и VPN1, выполните команду ping на компьютере CLIENT1.

**Проверка сетевого подключения при помощи команды ping**

1. На компьютере VPN1 нажмите кнопку Start, выберите сначала Administrative Tools, а затем – Windows Firewall with Advanced Security (брандмауэр Windows в режиме повышенной безопасности).

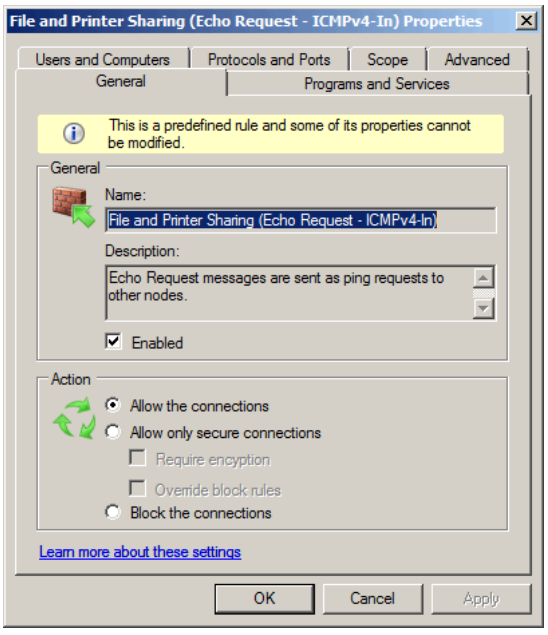
2. Выберите пункт Inbound Rules (правила входящих) в дереве консоли.

**Рисунок 13. Оснастка Windows Firewall with Advanced Security.**



3. Прокрутите область сведений до записи File and Printer Sharing (Echo Request - ICMPv4-In) (общий доступ к файлам и принтерам (эхо-запрос - входящий трафик ICMPv4)), связанной с профилем Public (общий), и дважды щелкните её. Убедитесь в том, что данное правило введено в действие.

**Рисунок 14. Диалоговое окно File and Printer Sharing (Echo Request - ICMPv4-In).**




4. Установив флажок **Enabled** (включено) во вкладке General (общие), нажмите кнопку OK.

5. В окне команд на компьютере CLIENT1 введите команду ping vpn1.contoso.com, а затем нажмите клавишу ВВОД.

6. Убедитесь в том, что проверка связи с компьютером VPN1 прошла успешно.

В рамках задач, поставленных перед рассматриваемой лабораторией тестирования, данное соединение свидетельствует о том, что удаленный пользователь в состоянии подключиться к VPN-серверу организации через Интернет.

7. Закройте окно команд.

### 7. Имитация ошибки подключения по протоколу PPTP

После выполнения вышеописанных процедур инфраструктуру лаборатории тестирования можно считать завершенной. В этом разделе описывается способ настройки лаборатории тестирования, при котором попытки VPN-подключения по протоколу PPTP будут завершаться ошибками. Так мы имитируем сценарий, встречающийся в рабочих средах, когда сервер удаленного доступа находится под защитой брандмауэра, который блокирует соединения по протоколу PPTP. В нашем случае в качестве брандмауэра сетевого периметра будет выступать брандмауэр Windows в режиме повышенной безопасности, установленный на компьютере VPN1.

#### Настройка VPN-подключения по протоколу PPTP

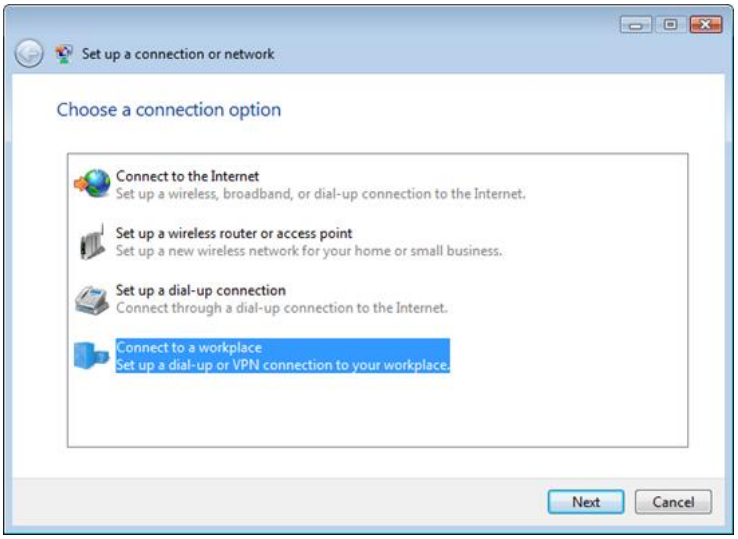
Создадим подключение по протоколу PPTP.

### Настройка VPN-подключения по протоколу PPTP

1. На компьютере CLIENT1 нажмите кнопку Start и выберите пункт Control Panel.

2. Последовательно выберите пункты Network and Internet, Network and Sharing Center и Set up a connection or network (установка подключения или сети).

**Рисунок 15. Диалоговое окно Set up a connection or network.**




3. Выберите пункт Connect to a workplace (подключение к рабочему месту) и нажмите кнопку Next.

4. Выберите пункт Use my Internet connection (VPN) (использовать мое подключение к Интернету (VPN)).

5. Установите параметр I'll set up an Internet connection later (отложить настройку подключения к Интернету).

6. Введите адрес vpn1.contoso.com в поле Internet address (адрес в Интернете) и нажмите кнопку Next.

> **Примечание**
> Интернет-адрес должен совпадать с именем субъекта, который согласно настоящему руководству должен был быть настроен ранее. Это необходимо для организации SSTP-подключения, речь о котором пойдет ниже.

7. При появлении диалогового окна Type your user name and password (введите имя пользователя и пароль) введите следующие данные:

   а) в поле User name (имя пользователя) введите user1;
   б) в поле Password введите P@ssword;

   в) установите флажок Remember this password (сохранить пароль);

   г) в поле Domain (домен) введите contoso.

8. Последовательно нажмите кнопки **Create** (создать) и **Close**.

### Проверка подключения по протоколу PPTP

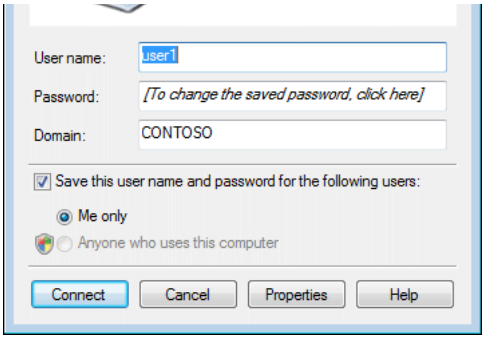
На данном этапе следует проверить подключение по протоколу PPTP на предмет работоспособности. VPN-подключение по протоколу PPTP, настроенное на компьютере CLIENT1, должно обеспечивать возможность успешного соединения с компьютером VPN1.

**Проверка подключения по протоколу PPTP**

1. На компьютере CLIENT1 откройте окно Network and Sharing Center, а затем выберите пункт Manage network connections.

2. Дважды щелкнув запись VPN Connection (VPN-подключение), нажмите кнопку Connect (подключить).

**Рисунок 16. Диалоговое окно VPN Connection.**




3. Убедитесь в том, что соединение было успешно установлено. Для этого, щелкнув правой кнопкой мыши запись VPN Connection, выберите пункт Status (состояние). В области Media State (состояние носителя) должно быть указано состояние Connected (подключено).

4. Нажмите кнопку **Disconnect** (отключить) в диалоговом окне VPN Connection Status (состояние VPN-подключения).

### Настройка брандмауэра Windows в режиме повышенной безопасности

PPTP-трафик состоит из трафика, передаваемого через TCP-порт 1723 для поддержки туннеля, и через IP-порт 47 по протоколу GRE для туннелирования данных. Наша задача состоит в том, чтобы настроить брандмауэр Windows в режиме повышенной безопасности так, чтобы он блокировал трафик по протоколу GRE, поступающий на компьютер VPN1. Так мы сможем смоделировать сценарий, при котором сервер удаленного доступа находится под защитой брандмауэра, блокирующего PPTP-подключения.

**Настройка брандмауэра Windows в режиме повышенной безопасности на блокирование подключений по протоколу PPTP**

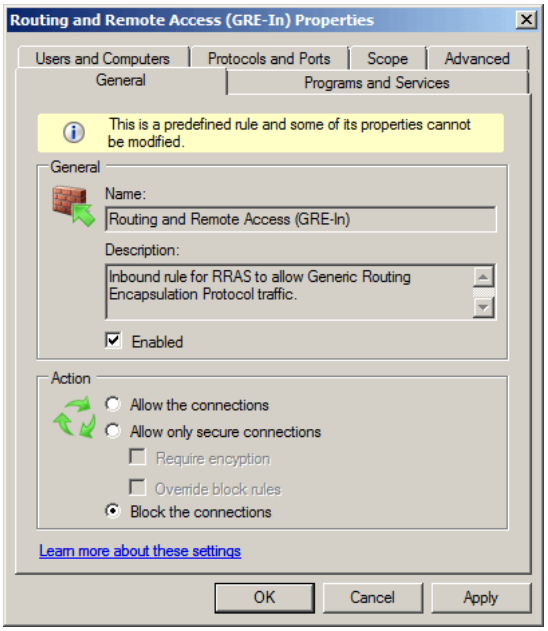
1. На компьютере VPN1 нажмите кнопку Start, выберите сначала Administrative Tools, а затем – Windows Firewall with Advanced Security.

2. Выберите пункт Inbound Rules в дереве консоли.

3. Прокрутите область сведений и дважды щелкните запись Routing and Remote Access (GRE-In) (маршрутизация и удаленный доступ (GRE – входящий)).

4. Установите переключатель в области Action (действие) в положение Block the connections (блокировать подключения) и нажмите кнопку OK.

Рисунок 17. Диалоговое окно Routing and Remote Access (GRE-In) Properties.




### Проверка подключения по протоколу PPTP

Теперь нужно убедиться в том, что подключения к компьютеру VPN1 по протоколу PPTP действительно блокируются.

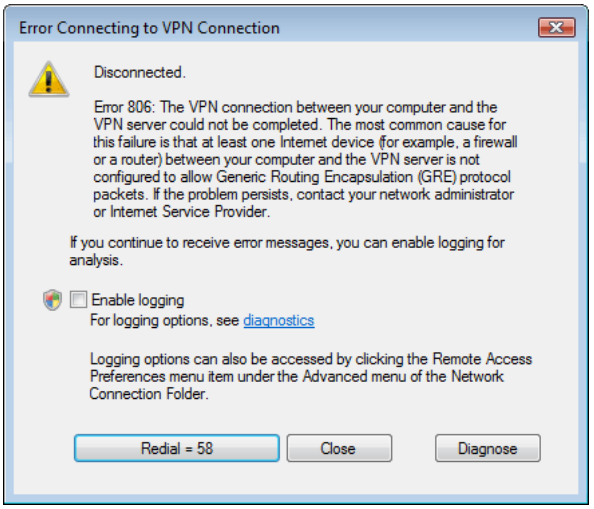
**Проверка подключения по протоколу PPTP**

1. На компьютере CLIENT1 откройте окно Network and Sharing Center, а затем выберите пункт Manage network connections.

2. Дважды щелкнув запись VPN Connection, нажмите кнопку Connect.

3. Убедитесь в том, что установить соединение не удалось. На экране должно появиться диалоговое окно приблизительно следующего содержания:

**Рисунок 18. Ошибка VPN-подключения по протоколу PPTP.**




4. Нажмите кнопку Close.

## 8. Настройка SSTP-подключения

Для организации SSTP-подключений VPN-клиент должен установить сертификат от корневого ЦС, выдавшего сертификат компьютера VPN-серверу. В ходе проверки подлинности на основе SSL VPN-клиент при помощи своего собственного сертификата проверяет сертификат проверки подлинности сервера.

### Получение сертификата от доверенного корневого ЦС

Корневой сертификат можно получить методом автоматической подачи заявки (если клиент является участником домена Active Directory) или путем подачи заявки через Интернет от веб-сайта ЦС, выдающего сертификаты. В нашем случае компьютер CLIENT1 должен получить у компьютера VPN1 сертификат от корневого ЦС методом подачи заявки через Интернет.

**Получение сертификата компьютера у VPN1**

1. На компьютере CLIENT1 нажмите кнопку Start и выберите пункт Internet Explorer.

2. Когда откроется обозреватель Internet Explorer, введите адрес http://vpn1.contoso.com/certsrv вместо текущего URL-адреса и нажмите клавишу ВВОД.

3. В случае вывода оповещения фильтра фишинга выберите пункт Turn off automatic Phishing Filter и нажмите кнопку OK.

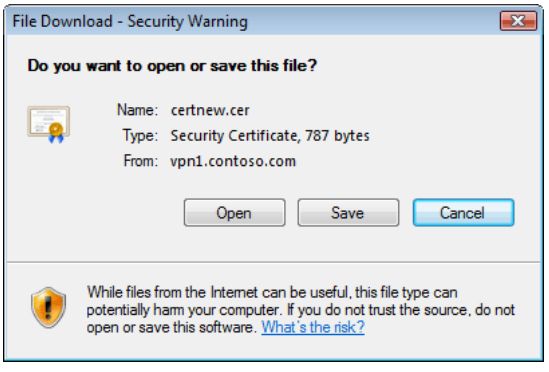
4. В области Select a task на начальной странице выберите пункт Download a CA certificate, certificate chain, or CRL (загрузка сертификата ЦС, цепочки сертификатов или CRL).

5. В случае вывода оповещения о панели информации нажмите кнопку Close.

6. Выберите пункт Download CA certificate (загрузка сертификата ЦС).

7. Нажмите кнопку **Open** в диалоговом окне File Download (загрузка файла).

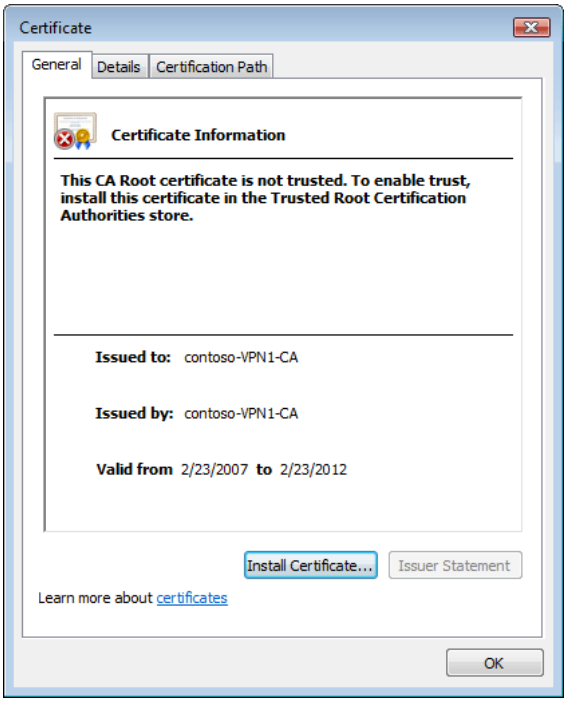
**Рисунок 19. Диалоговое окно File Download при загрузке сертификата безопасности.**




8. В диалоговом окне оповещения системы безопасности нажмите кнопку Allow (разрешить).

9. Click Install Certificate (установить сертификат).

**Рисунок 20. Диалоговое окно Certificate.**




10. При появлении окна Certificate Import Wizard (мастер импорта сертификатов) нажмите кнопку Next.

11. Чтобы согласиться с предложенным по умолчанию хранилищем, нажмите кнопку **Next** в диалоговом окне Certificate Store.

12. Нажмите кнопку Finish.

13. В диалоговом окне подтверждения нажмите кнопку OK.

14. Чтобы закрыть диалоговое окно **Certificate** (сертификат), нажмите кнопку OK.

Теперь установленный сертификат компьютера необходимо переместить в нужное хранилище. По умолчанию устанавливаемые сертификаты автоматически помещаются в хранилище Current User, Intermediate Certification Authority (текущий пользователь, промежуточный центр сертификации). Требуется переместить сертификат в хранилище Local Computer, Trusted Root Certification Authority (локальный компьютер, доверенный корневой центр сертификации) на компьютере CLIENT1. В первую очередь следует настроить консоль MMC с оснастками сертификатов пользователя и компьютера.

**Настройка консоли MMC**

1. На компьютере CLIENT1 нажмите кнопку Start, выберите All Programs, Accessories, а затем – Run (выполнить).

2. Введите команду mmc в поле Open и нажмите кнопку OK.

3. В диалоговом окне User Account Control нажмите кнопку Continue.

4. При появлении оснастки Console1 откройте меню File и выберите команду Add/Remove Snap-in.

5. В списке Available snap-ins выберите пункт Certificates и нажмите кнопку Add.

6. Чтобы согласиться с предложенным по умолчанию параметром My user account, нажмите кнопку Finish.

7. Нажмите кнопку Add, выберите пункт Computer account, а затем нажмите кнопку Next.

8. Чтобы согласиться с предложенным по умолчанию параметром Local computer, нажмите кнопку Finish в диалоговом окне Select Computer.

9. Чтобы закрыть диалоговое окно Add or Remove Snap-ins, нажмите кнопку OK.

Следующая задача заключается в том, чтобы переместить установленный сертификат из хранилища, в которое он был помещен по умолчанию. Так как сертификат не предусматривает привязки по закрытому ключу, его можно перенести в новое хранилище путем копирования и последующей вставки.

**Перемещение сертификата**

1. В области дерева консоли MMC, которая была только что создана на компьютере CLIENT1, последовательно дважды щелкните записи Certificates - Current User и Intermediate Certification Authorities (промежуточные центры сертификации), а затем выберите пункт Certificates.

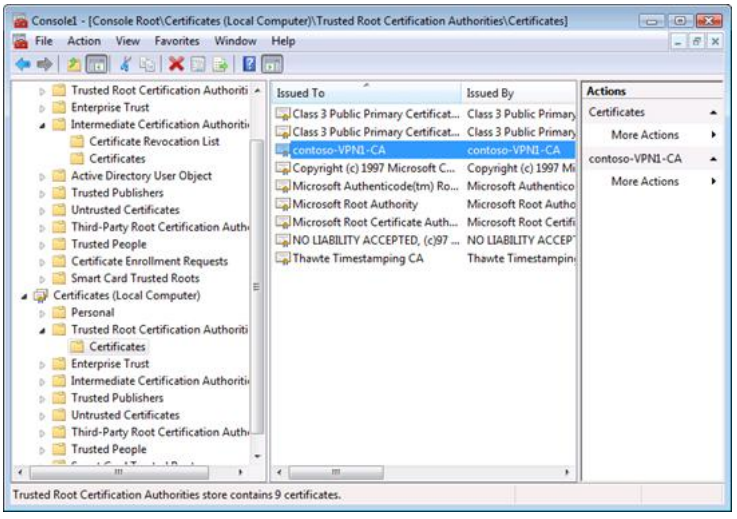
2. Щелкните правой кнопкой мыши запись сертификата contoso-VPN1-CA в средней области просмотра, а затем выберите команду Copy (копировать).

3. В области дерева консоли последовательно дважды щелкните записи Certificates (Local Computer) и Trusted Root Certification Authorities (доверенные корневые центры сертификации), а затем выберите пункт Certificates.

4. Щелкните правой кнопкой мыши в средней области просмотра и выберите команду Paste (вставить).

5. Чтобы убедиться в том, что сертификат размещен в хранилище, обновите экран.

**Рисунок 21. Новое хранилище загруженного сертификата.**




## Настройка и тестирование VPN-подключения по протоколу SSTP

Теперь, когда сертификат от корневого ЦС, выдавшего сертификат компьютера VPN-сервера, находится в хранилище сертификатов Trusted Root Certification Authorities на компьютере CLIENT1, нам осталось настроить подключение по протоколу SSTP и проверить его работоспособность.

**Настройка и тестирование подключения по протоколу SSTP**

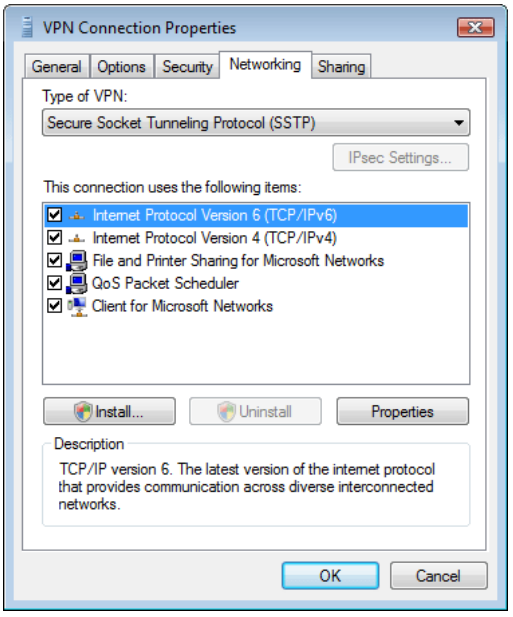
1. На компьютере CLIENT1 откройте окно Network and Sharing Center, а затем выберите пункт Manage network connections.

2. Дважды щелкнув запись VPN Connection, нажмите кнопку Properties.

3. Откройте вкладку Networking.

4. Выберите пункт Secure Socket Tunneling Protocol (SSTP) в раскрывающемся списке Type of VPN (тип VPN) и нажмите кнопку OK.

**Рисунок 22. Диалоговое окно VPN Connection Properties.**




5. Нажмите кнопку **Connect** (подключить) в диалоговом окне Connect VPN Connection (установить VPN-подключение).

Компьютер CLIENT1 должен успешно подключиться к компьютеру VPN1 по протоколу SSTP. Проверьте, доступен ли файловый сервер организации при обращении к нему с удаленного узла.

6. Нажмите кнопку Start, а затем последовательно выберите пункты All Programs, **Accessories** и **Run**.

7. Введите команду \\dc1.contoso.com\corpdata в поле Open и нажмите кнопку OK.

8. Откройте файл VPNTest двойным щелчком мыши, добавьте в него новый текст и сохраните.

9. Закройте файл VPNTest.

---

Пошаговая инструкция. Источни:к www.microsoft.com

« Пред. След. »

Вернуться



Go to top