

3.1.1.3 Настройка подключение к сетям VPN по предъявлению токена

Раздел содержит инструкцию по настройке доступа к сетям VPN по предъявлению токена.

Для настройки необходим компьютер с установленной операционной системой **Windows 2012 R2 Server Rus** и драйверами **Рутокен**, а также **дистрибутив этой ОС**.

Операционная система должна быть настроена как **Контроллер домена**. В системе должны быть установлены **Службы Сертификации**, **Служба Маршрутизация и удаленный доступ** (в брандмауэре Windows должно быть настроено разрешающее правило для этой службы), а пользователям выданы сертификаты типа **Пользователь со смарт-картой** или **Вход со смарт-картой**.

Все описанные далее действия производятся с правами администратора системы.

Для примера используется учетная запись **Admin**.

Этапы настройки подключения к сетям VPN по предъявлению токена:

1 этап: Настройка маршрутизации и удаленного доступа.

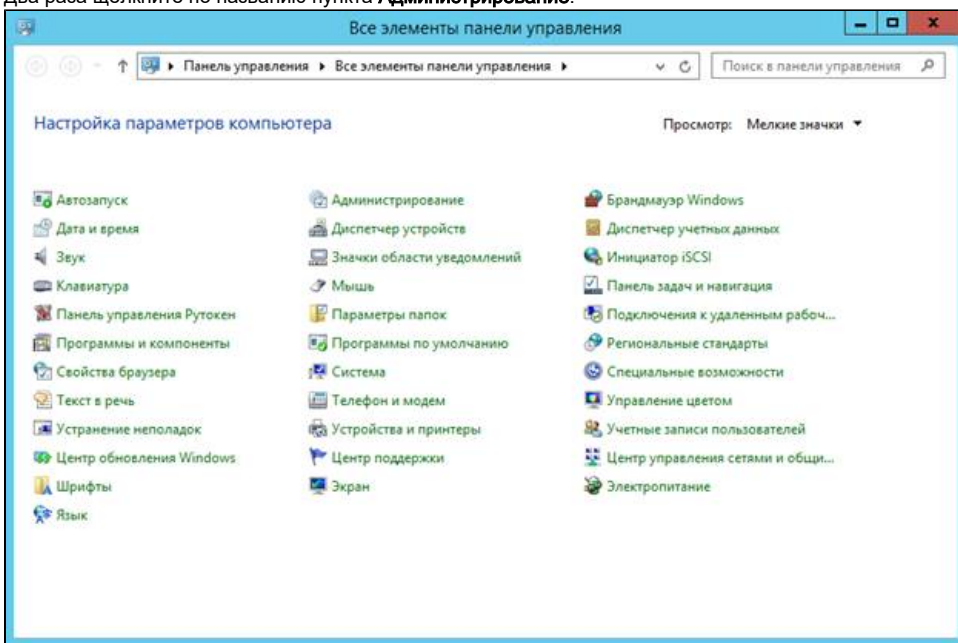
2 этап: Настройка учетных записей пользователей.

Настройка маршрутизации и удаленного доступа

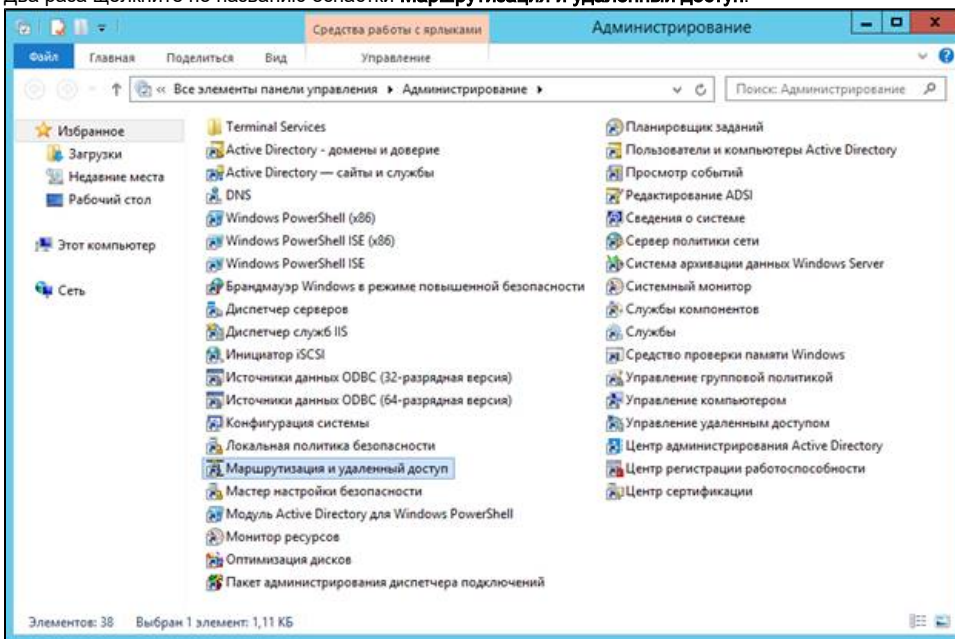
Перед настройкой маршрутизации и удаленного доступа необходимо убедиться, что на сервере установлены роли **Службы политики сети и доступа** и **Удаленный доступ**.

Для настройки маршрутизации и удаленного доступа:

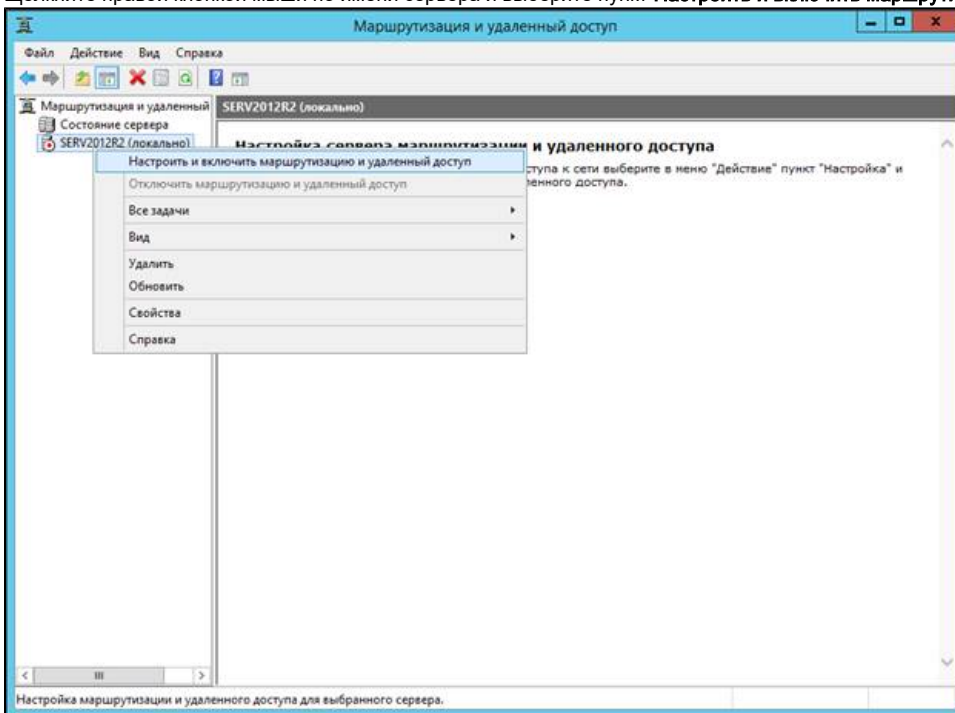
1. Откройте **Панель управления**.
2. Два раза щелкните по названию пункта **Администрирование**.



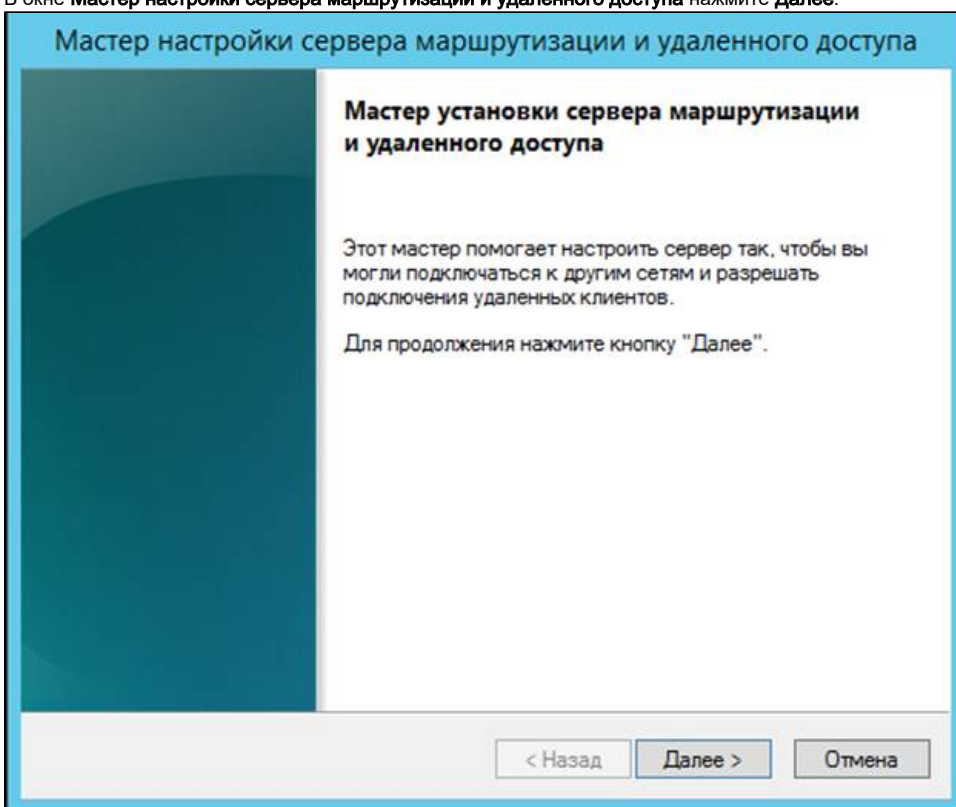
3. Два раза щелкните по названию оснастки **Маршрутизация и удаленный доступ**.



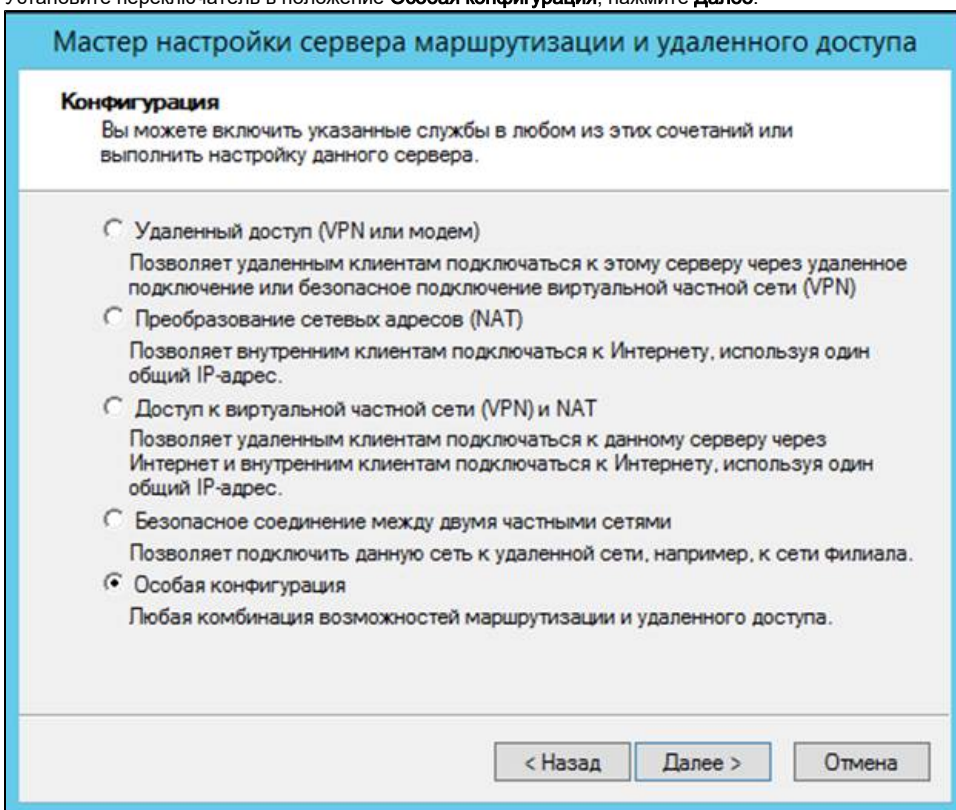
4. Щелкните правой кнопкой мыши по имени сервера и выберите пункт **Настроить и включить маршрутизацию и удаленный доступ**.



5. В окне **Мастер настройки сервера маршрутизации и удаленного доступа** нажмите **Далее**.



6. Установите переключатель в положение **Особая конфигурация**, нажмите **Далее**.



7. Установите флажок **Доступ к виртуальной частной сети (VPN)** и нажмите **Далее**.

Мастер настройки сервера маршрутизации и удаленного доступа

Настраиваемая конфигурация

После закрытия этого мастера вы можете настроить выбранные службы на консоли маршрутизации и удаленного доступа.

Выберите службы, которые вы хотите включить на данном сервере.

- ☒ Доступ к виртуальной частной сети (VPN)
- ☐ Удаленный доступ (через телефонную сеть)
- ☐ Подключения по требованию (для маршрутизации филиалов)
- ☐ Преобразование сетевых адресов (NAT)
- ☐ Маршрутизация локальной сети

< Назад Далее > Отмена

8. Убедитесь, что все необходимые функции сервера маршрутизации и удаленного доступа выбраны (поле **Сводка выбранных параметров**). Нажмите **Готово**.

Мастер настройки сервера маршрутизации и удаленного доступа

Завершение мастера сервера маршрутизации и удаленного доступа

Успешно завершена работа мастера сервера маршрутизации и удаленного доступа

Сводка выбранных параметров:

доступ к виртуальной частной сети (VPN)

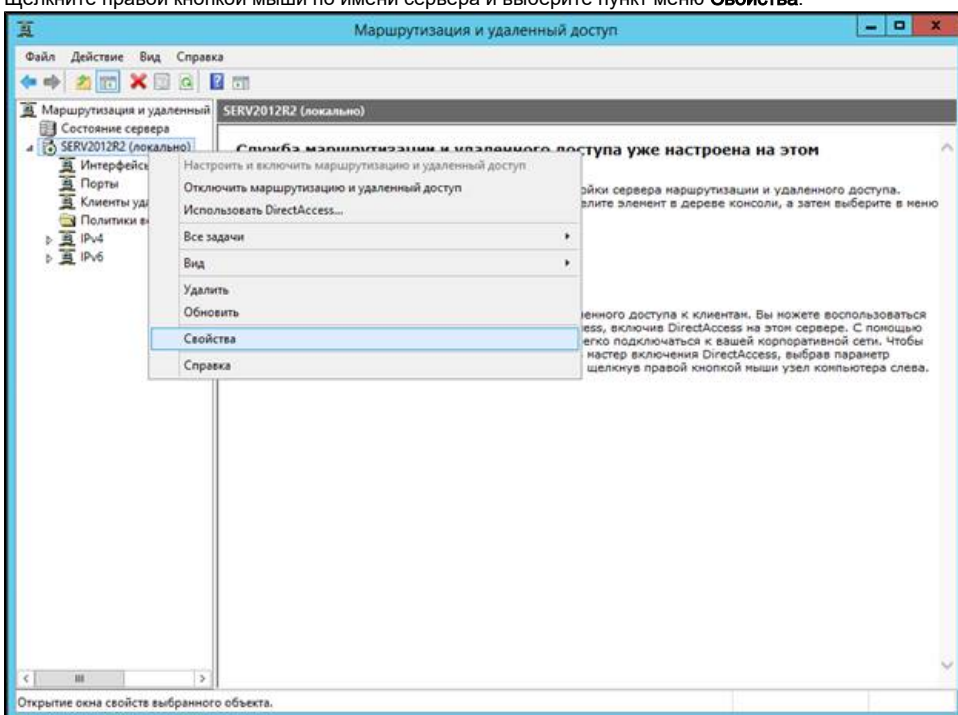
Закройте мастер и затем настройте выбранные службы на консоли маршрутизации и удаленного доступа.

Для закрытия мастера нажмите кнопку "Готово".

< Назад Готово Отмена

9. Нажмите **Запустить службу** и дождитесь завершения процесса запуска службы.

10. Щелкните правой кнопкой мыши по имени сервера и выберите пункт меню **Свойства**.



11. В окне со свойствами сервера перейдите на вкладку **Безопасность** и нажмите **Методы проверки подлинности**.

Свойства: SERV2012R2 (локально) ? X

IKEv2	PPP	Ведение журнала	
Общие	Безопасность	IPv4	IPv6



Так как установлен сервер политики сети (NPS), необходимо использовать его для настройки проверки подлинности и поставщиков учетных записей. Для этого создайте или измените политики запросов на подключение.

Методы проверки подлинности...

Пользовательская политика IPsec задает общий ключ для L2TP- и IKEv2-подключений. Чтобы настроить данный параметр, следует запустить службу маршрутизации и удаленного доступа. Инициаторы IKEv2, настроенные на проверку подлинности на этом сервере с помощью сертификата, не смогут выполнить подключение.

☐ Разрешить пользовательские политики IPsec для L2TP- и IKEv2-подключения

Общий ключ:

Привязка сертификата SSL

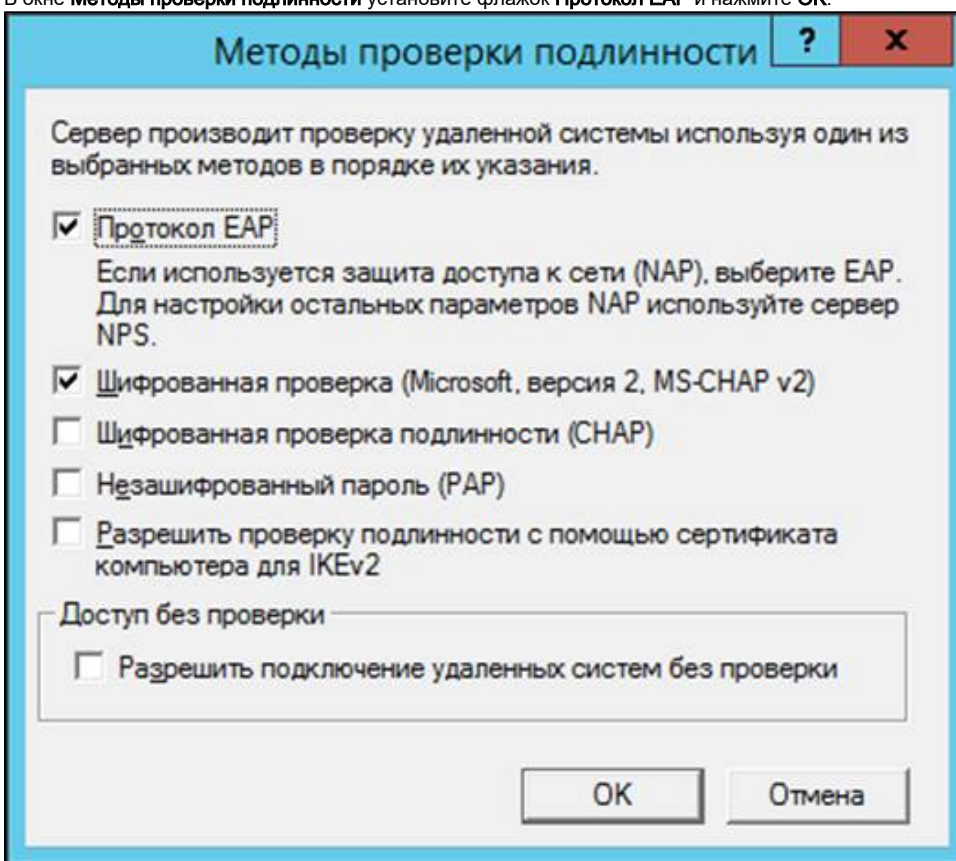
☐ Использовать HTTP

Выберите сертификат, который должен использовать SSTP-сервер для привязки SSL (веб-прослушиватель)

Сертификат: По умолчанию ▼ Просмотр

OK Отмена Применить

12. В окне **Методы проверки подлинности** установите флажок **Протокол EAP** и нажмите **OK**.



13. В нашем примере на компьютере не настроена служба DHCP. Поэтому удаленным клиентам сначала необходимо назначать IP-адреса из заданного диапазона. Перейдите на вкладку **IPv4** и установите переключатель в положение **статический пул адресов**.

14. Нажмите **Добавить**.

Свойства: SERV2012R2 (локально) ? X

IKEv2	PPP	Ведение журнала	
Общие	Безопасность	IPv4	IPv6

☒ Включить пересылку IPv4

Назначение IPv4-адресов

Сервер может назначать IPv4-адреса, используя:

☐ протокол DHCP

☒ статический пул адресов

С	По	Число	IP-адрес	Маска

☒ Включить широковещание при разрешении имен

15. Введите начало и конец диапазона IP-адресов, нажмите **ОК**.

Новый диапазон IPv4-адресов

?

✕

Введите начальный IP-адрес и либо конечный IP-адрес, либо количество адресов в непрерывном диапазоне.

Начальный IP-адрес: 192 . 168 . 60 . 110

Конечный IP-адрес: 192 . 168 . 60 . 120

Количество адресов: 11

ОК

Отмена

16. Нажмите ОК.

Свойства: SERV2012R2 (локально) ? X

IKEv2		PPP		Ведение журнала	
Общие	Безопасность	IPv4	IPv6		

☒ Включить пересылку IPv4

Назначение IPv4-адресов

Сервер может назначать IPv4-адреса, используя:

☐ протокол DHCP

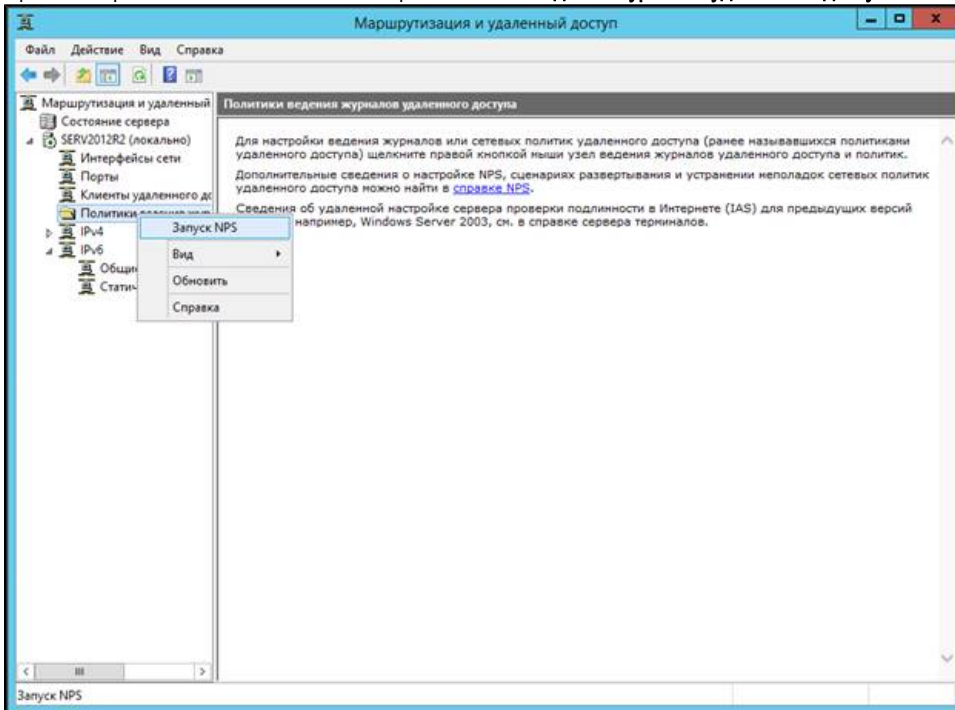
☒ статический пул адресов

С	По	Число	IP-адрес	Маска
192.168....	192.168...	11	192.168...	255.255...

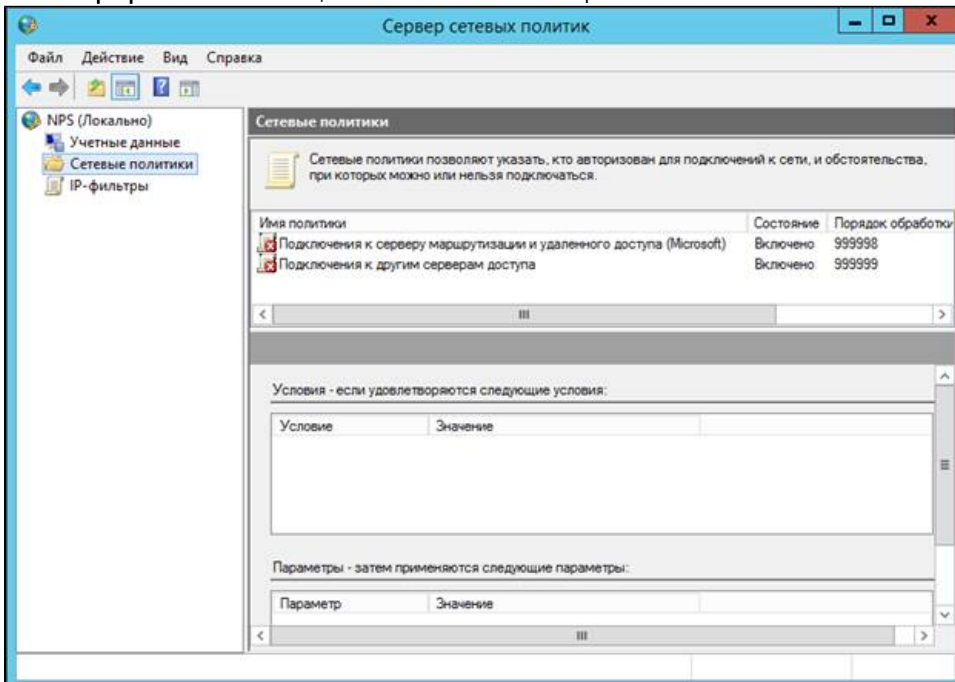
☒ Включить широковещание при разрешении имен

17. Щелкните правой кнопкой мыши на категории **Политики ведения журналов удаленного доступа**. Выберите пункт **Обновить**.

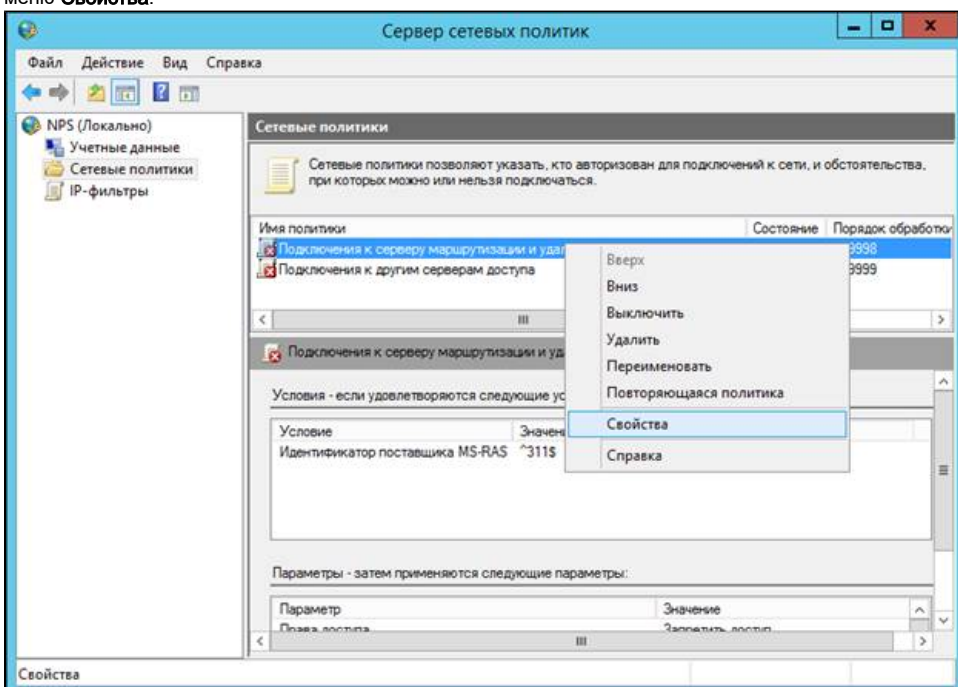
18. Щелкните правой кнопкой мыши на категории **Политики ведения журналов удаленного доступа**. Выберите пункт **Запуск NPS**.



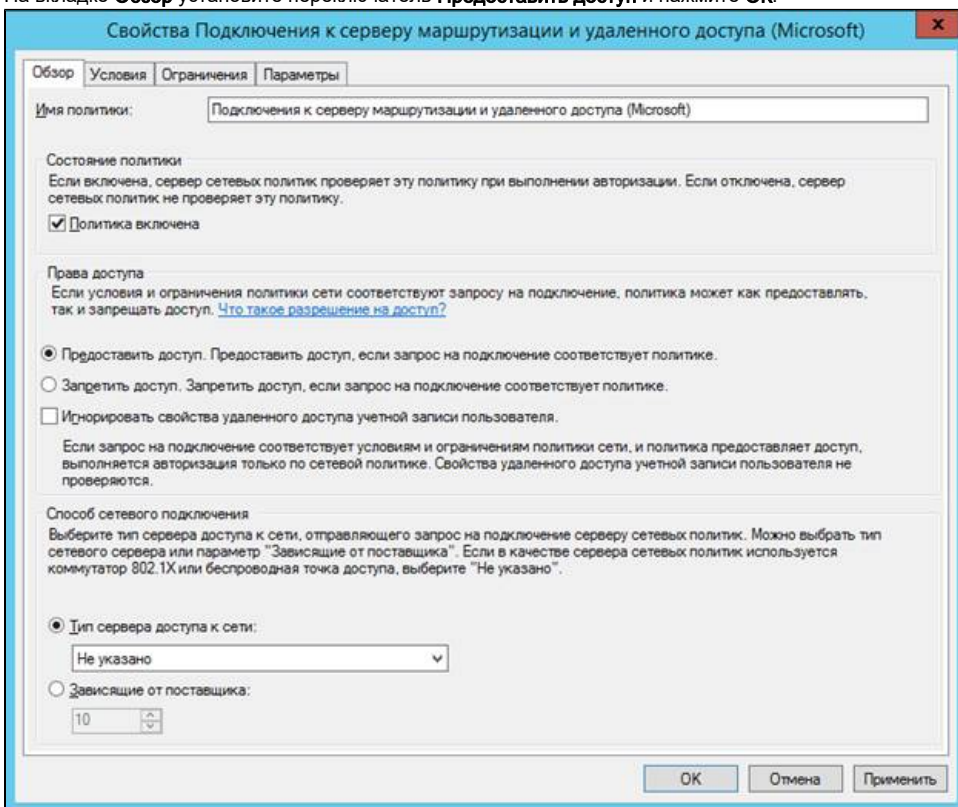
19. В окне **Сервер сетевых политик** щелкните по названию категории **Сетевые политики**.



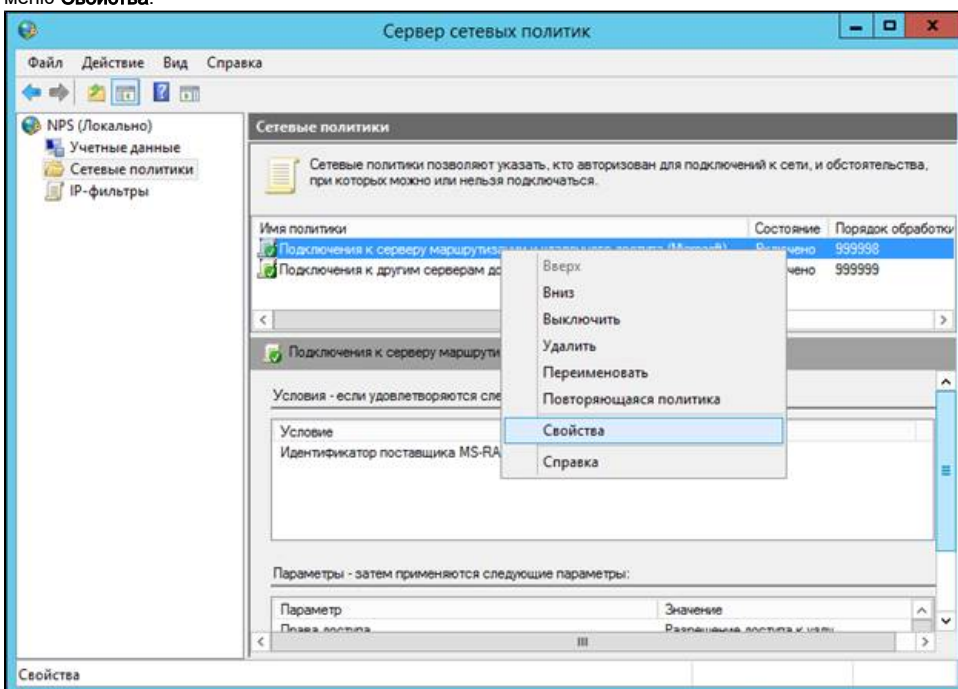
20. Кликните правой кнопкой мыши по строке **Подключение к серверу маршрутизации и удаленного доступа (Microsoft)** и выберите пункт меню **Свойства**.



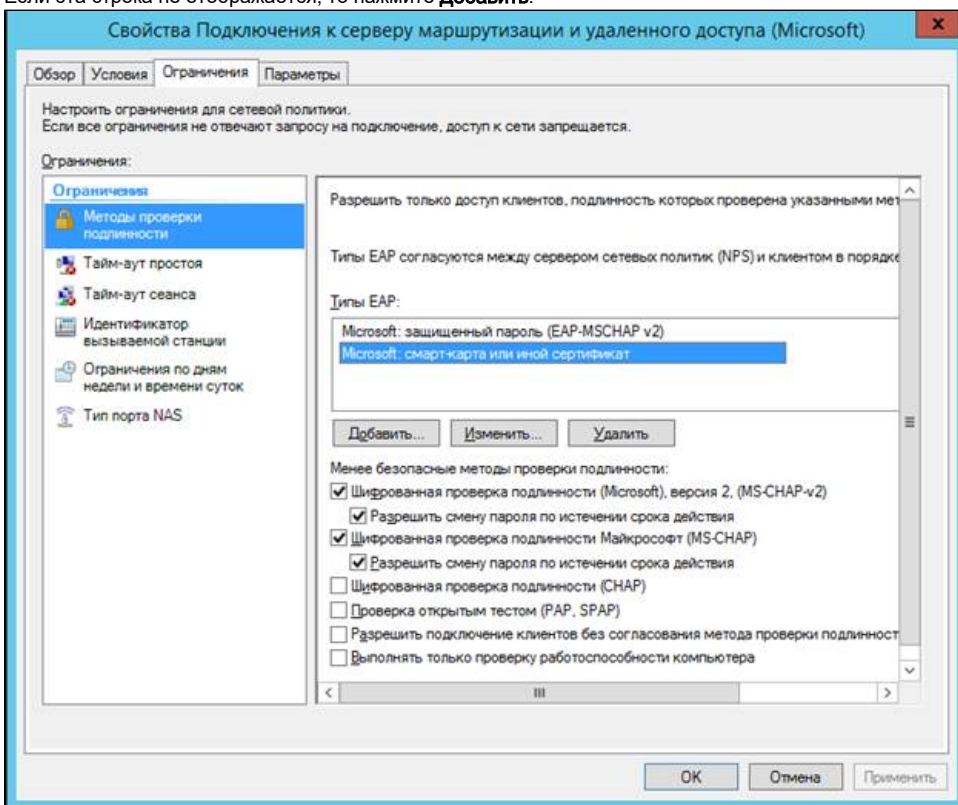
21. На вкладке **Обзор** установите переключатель **Предоставить доступ** и нажмите **ОК**.



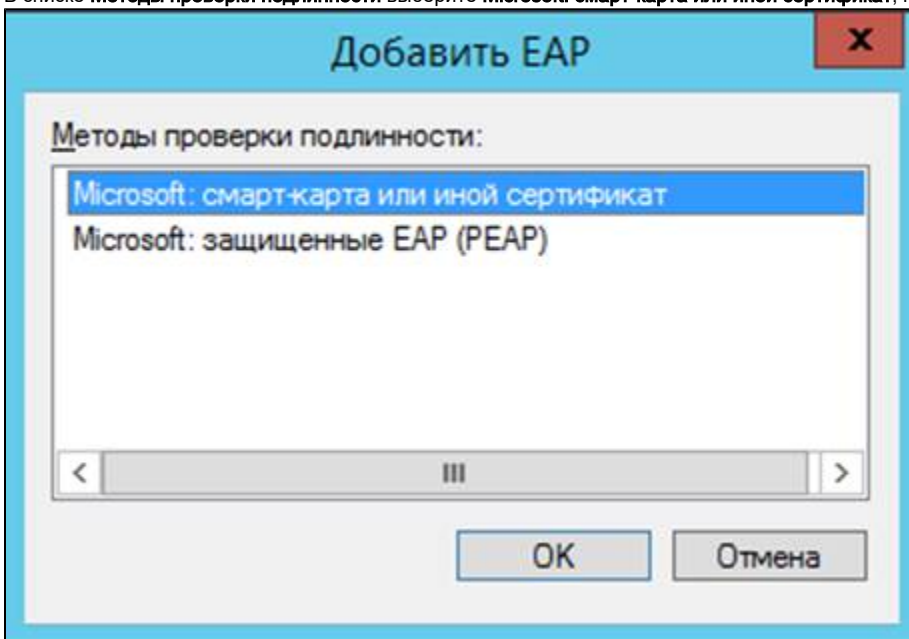
22. Кликните правой кнопкой мыши на строке **Подключение к серверу маршрутизации и удаленного доступа (Microsoft)** и выберите пункт меню **Свойства**.



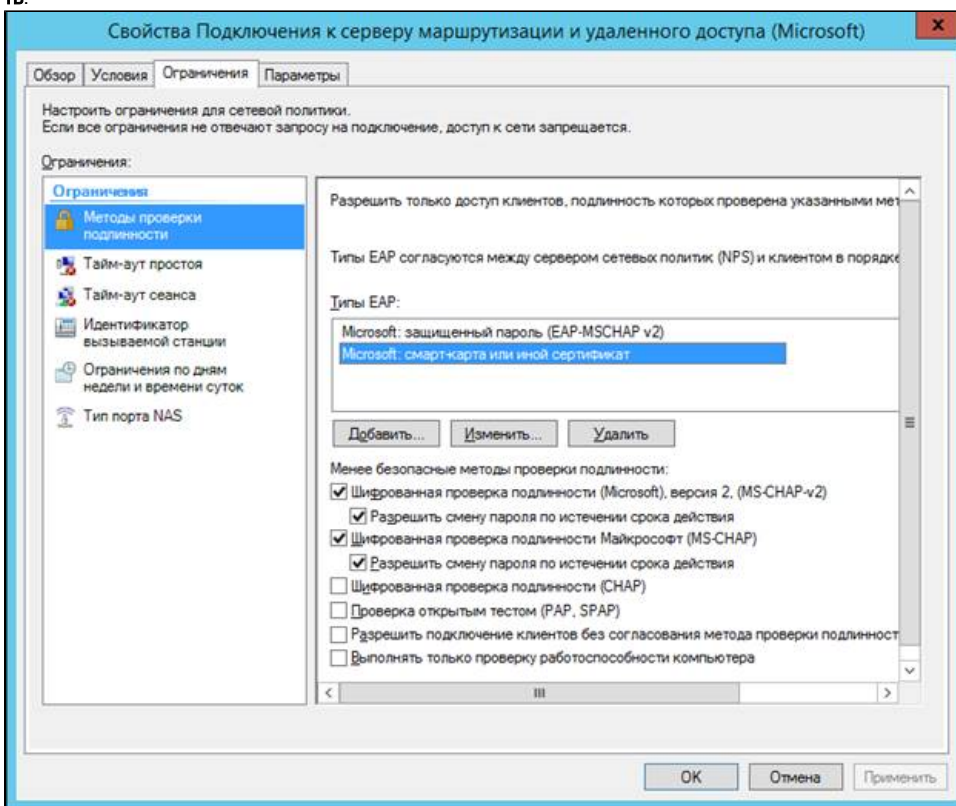
23. На вкладке **Ограничения** в левой части окна щелкните по названию ограничения **Методы проверки подлинности**.
24. В правой части окна в списке **Типы EAP** должна отображаться строка **Microsoft: смарт-карта или иной сертификат**.
25. Если эта строка не отображается, то нажмите **Добавить**.



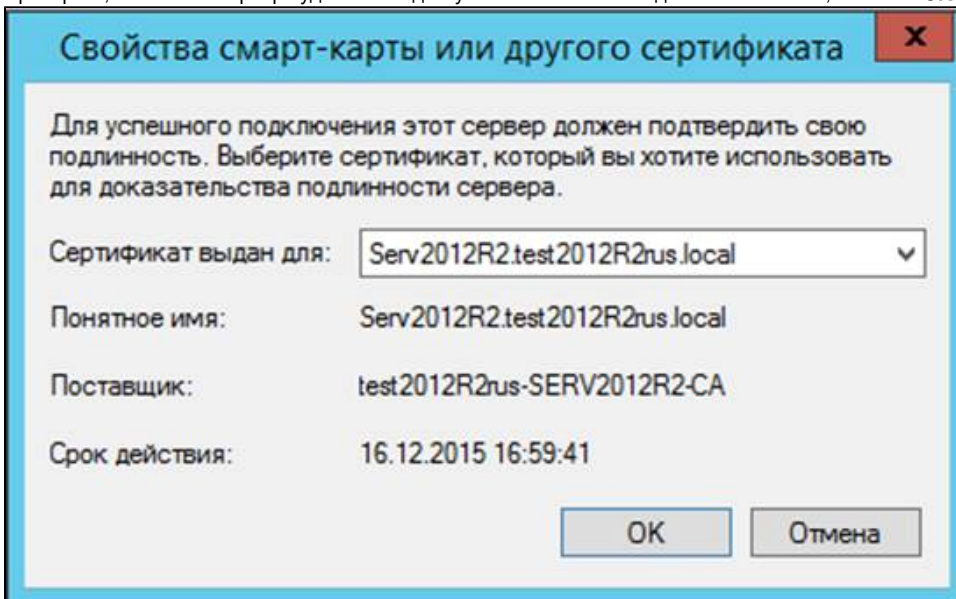
26. В списке **Методы проверки подлинности** выберите **Microsoft: смарт-карта или иной сертификат**, нажмите **ОК**.



27. Далее укажите сервер для аутентификации. Для этого щелкните по строке **Microsoft: смарт-карта или иной сертификат** и нажмите **Изменить**.



28. Проверьте, чтобы имя сервера удаленного доступа соответствовало действительности, нажмите **ОК**.



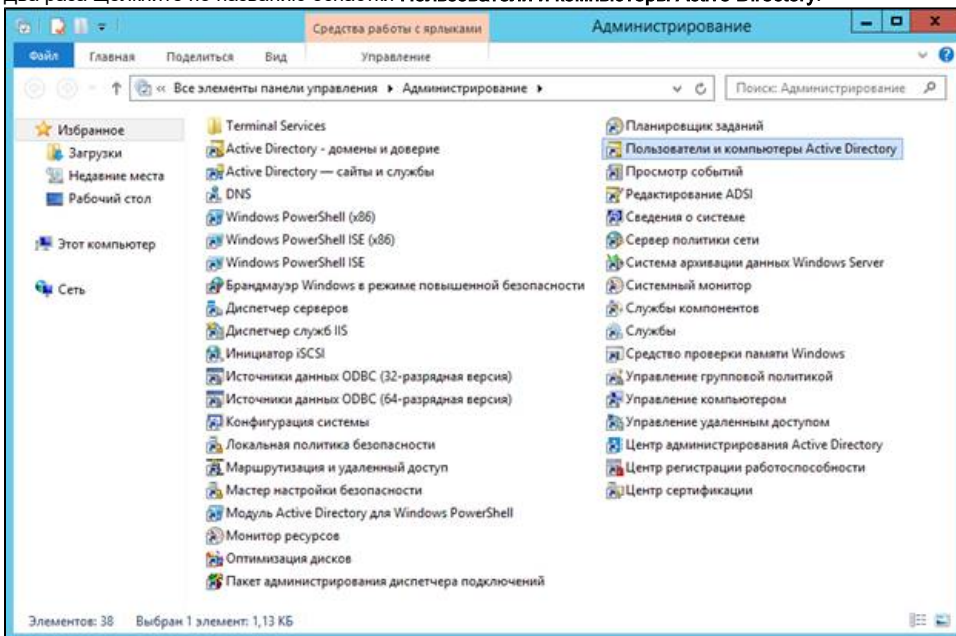
29. Закройте оснастку **Сервер сетевых политик**.

Настройка учетных записей пользователей

После настройки сервера удаленного доступа пользователям необходимо дать права на подключение к VPN.

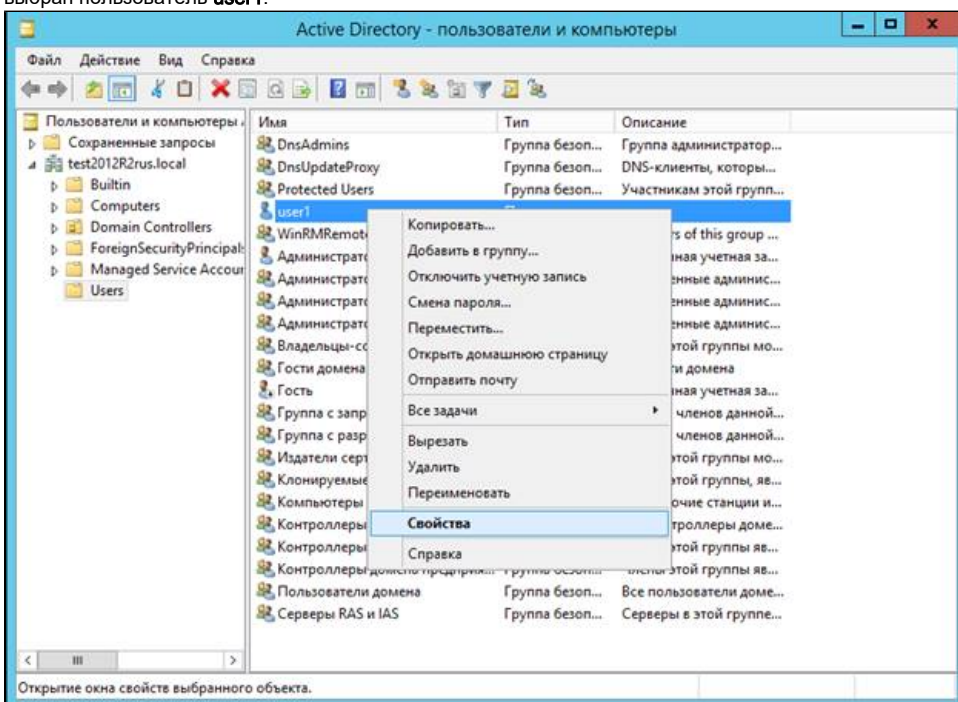
Для настройки учетных записей пользователей:

1. Зайдите в **Панель управления**.
2. Два раза щелкните по названию пункта **Администрирование**.
3. Два раза щелкните по названию оснастки **Пользователи и компьютеры Active Directory**.



4. В окне **Active Directory - пользователи и компьютеры** щелкните по названию папки **Users**.

5. В правой части окна, в строке с именем пользователя щелкните правой кнопкой мыши и выберите пункт **Свойства**. В данном примере выбран пользователь **user1**.



6. В окне **Свойства:[Имя пользователя]** перейдите на вкладку **Входящие звонки**.

7. Установите переключатель в положение **Разрешить доступ** и нажмите **ОК**.

The screenshot shows the 'Свойства: user1' (Properties: user1) dialog box with the 'Удаленное управление' (Remote control) tab selected. The dialog has a title bar with a question mark and a close button. Below the title bar is a tabbed interface with tabs: 'Профиль служб удаленных рабочих столов', 'COM+', 'Общие', 'Адрес', 'Учетная запись', 'Профиль', 'Телефоны', 'Организация', 'Член групп', 'Входящие звонки', 'Среда', 'Сеансы', and 'Удаленное управление'. The 'Удаленное управление' tab is active, showing several sections with radio buttons and checkboxes. The 'Права доступа к сети' (Network access rights) section has three radio buttons: 'Разрешить доступ' (selected), 'Запретить доступ', and 'Управление доступом на основе политики сети NPS'. Below this is a checkbox 'Проверять код звонящего:' followed by an empty text box. The 'Ответный вызов сервера' (Server callback) section has three radio buttons: 'Ответный вызов не выполняется' (selected), 'Устанавливается вызывающим (только для RAS)', and 'Всегда по этому номеру:' followed by an empty text box. The 'Назначить статические IP-адреса' (Assign static IP addresses) section has a checkbox and a text box 'Определите IP-адреса, разрешенные для этого входящего подключения.' followed by a button 'Статические IP-адреса...'. The 'Использовать статическую маршрутизацию' (Use static routing) section has a checkbox and a text box 'Определите маршруты, работающие с входящим подключением.' followed by a button 'Статические маршруты...'. At the bottom are four buttons: 'ОК', 'Отмена', 'Применить', and 'Справка'.

8. Закройте оснастку **Пользователи и компьютеры Active Directory**.

Настройка сервера завершена. Теперь необходимо настроить удаленное подключение к виртуальной частной сети (VPN) [на клиентском компьютере](#).