3.1.3.3. Настройка доступа 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 2019 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 доступа к сетям VPN по предъявлению токена:

1 этап: Настройка маршрутизации и удаленного доступа.

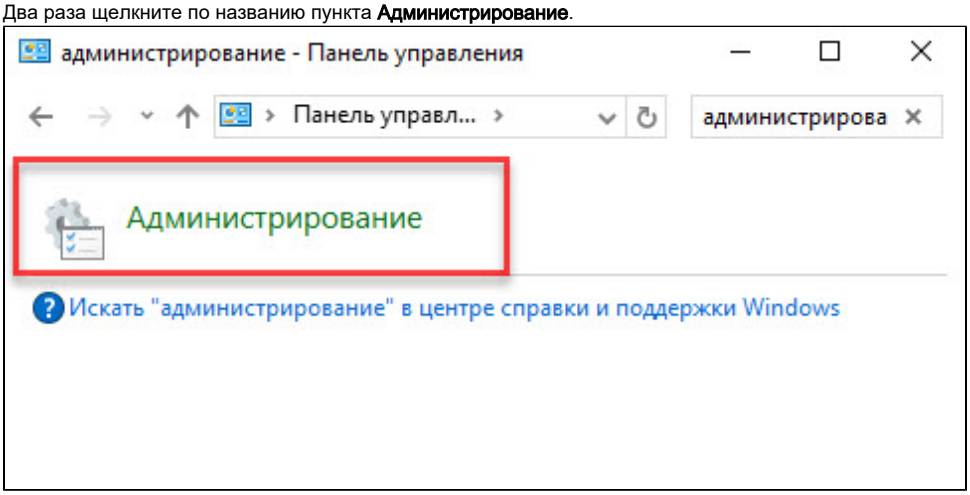
2 этап: Настройка учетных записей пользователей.

Настройка маршрутизации и удаленного доступа

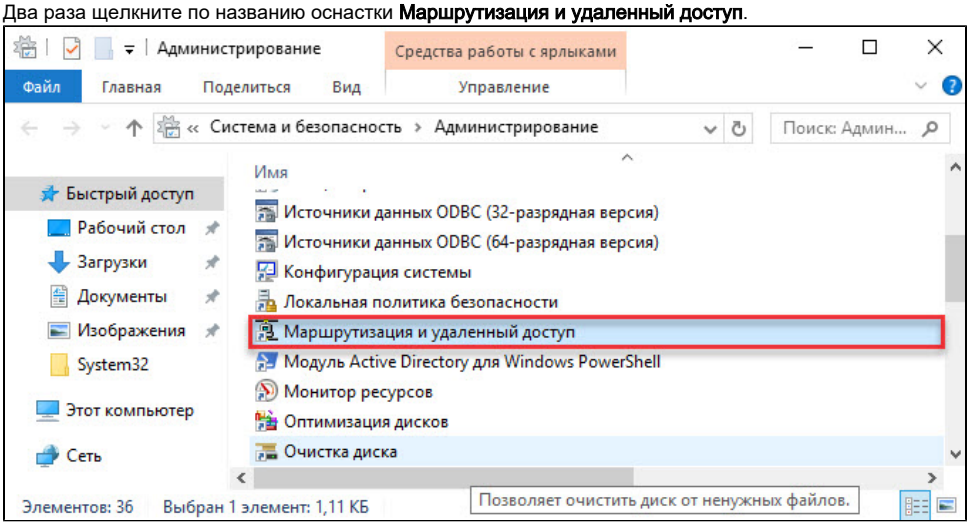
Перед настройкой маршрутизации и удаленного доступа необходимо убедиться, что на сервере установлены роли **Службы политики сети и доступа** и **Удаленный доступ**.

Для настройки маршрутизации и удаленного доступа:

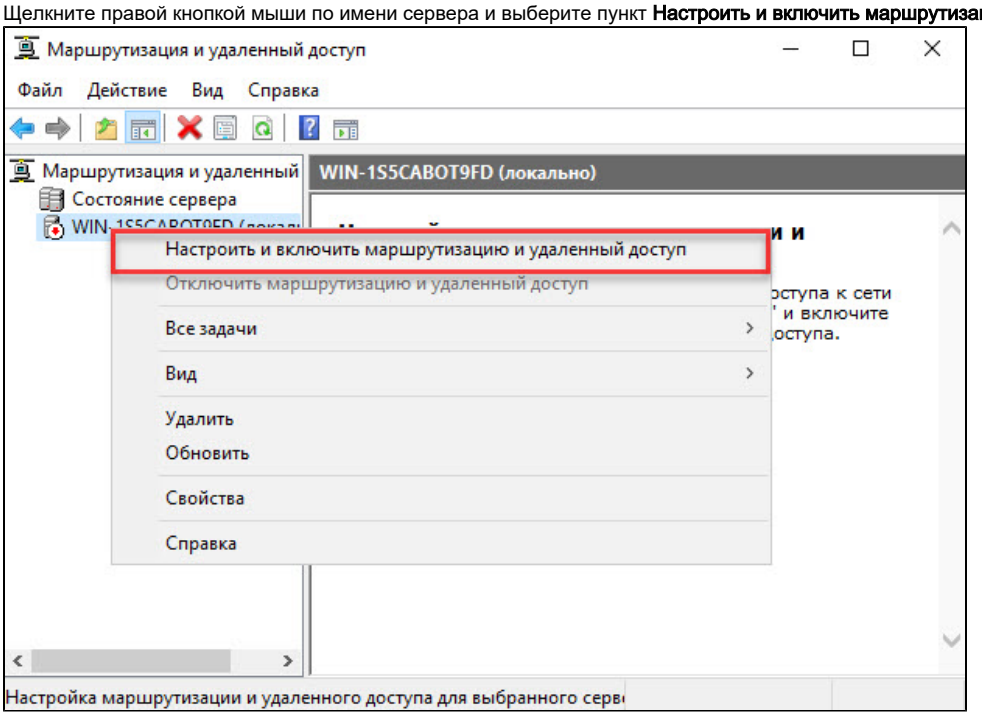
1. Откройте **Панель управления**.
2. В поле поиска введите слово "администрирование".
3. Два раза щелкните по названию пункта **Администрирование**.



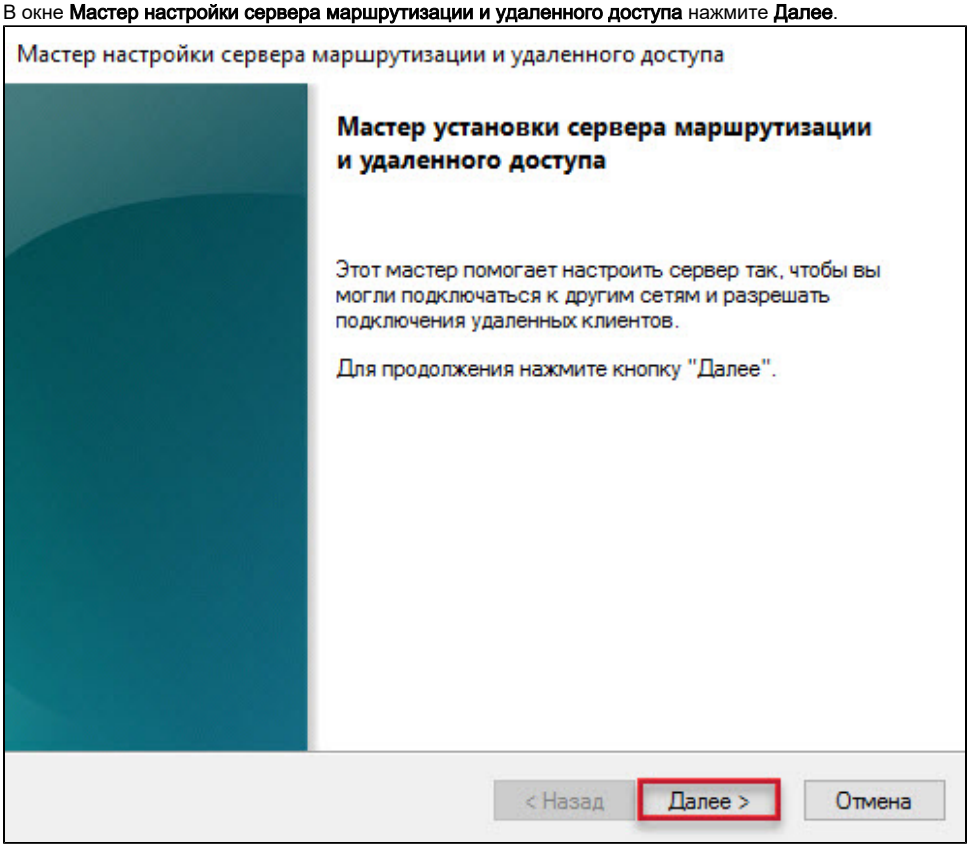
4. Два раза щелкните по названию оснастки **Маршрутизация и удаленный доступ**.



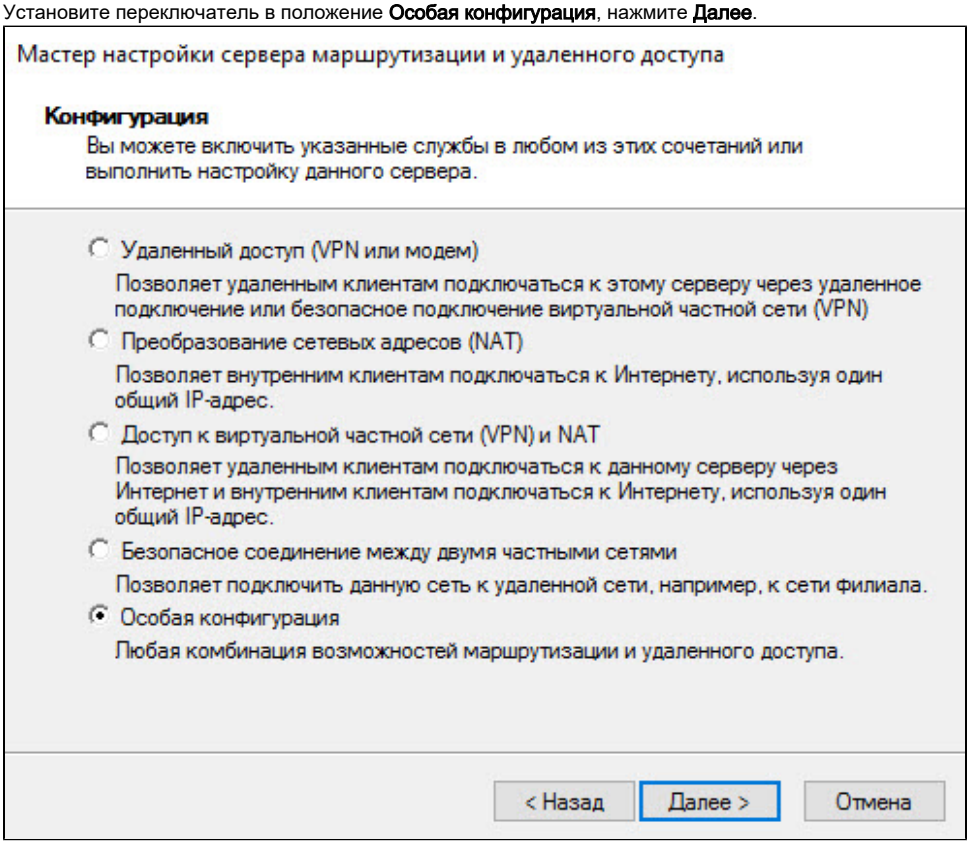
5. Щелкните правой кнопкой мыши по имени сервера и выберите пункт **Настроить и включить маршрутизацию и удаленный доступ**.



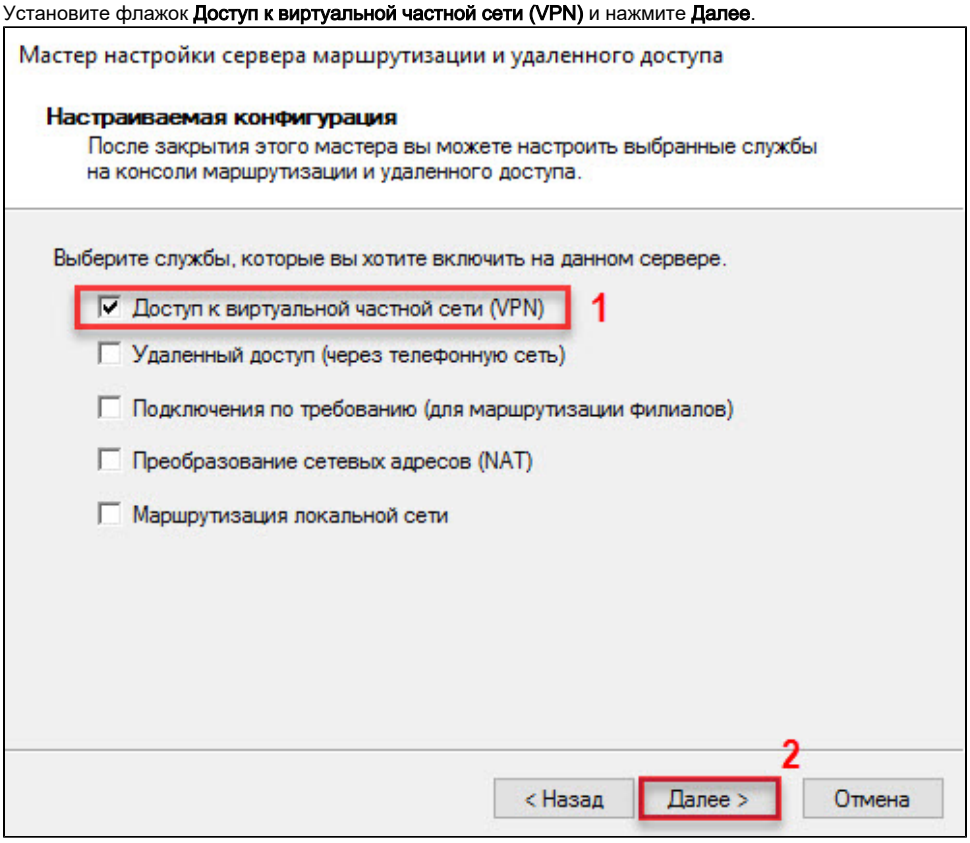
6. В окне **Мастер настройки сервера маршрутизации и удаленного доступа** нажмите **Далее**.



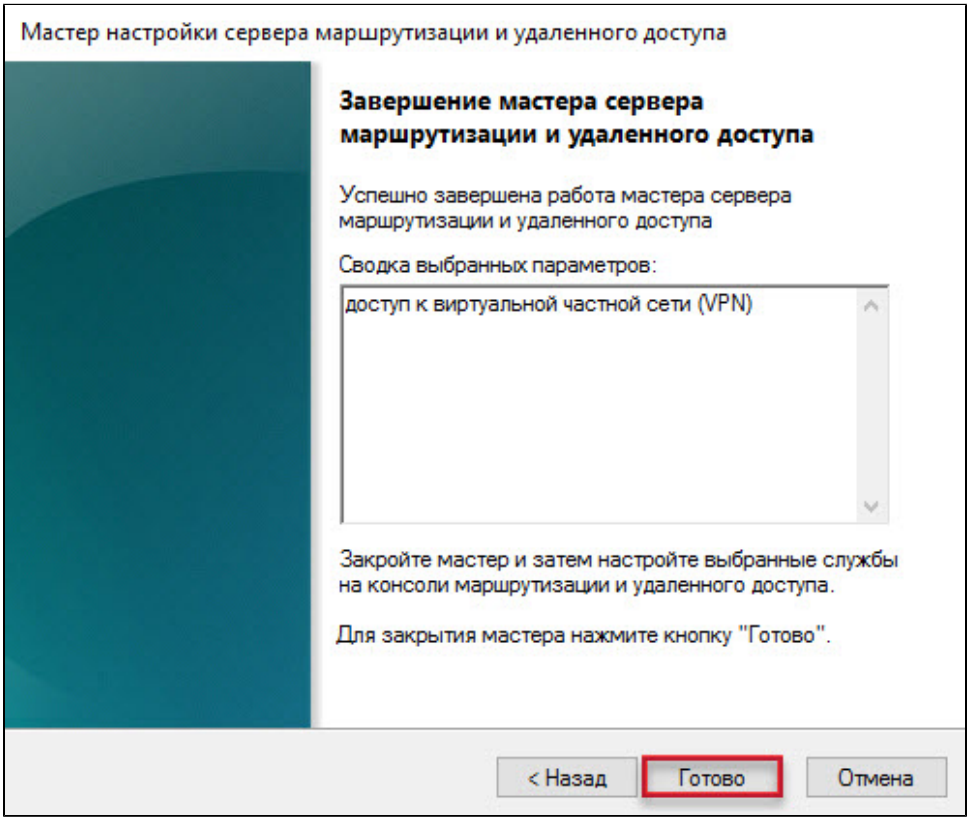
7. Установите переключатель в положение **Особая конфигурация**, нажмите **Далее**.



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

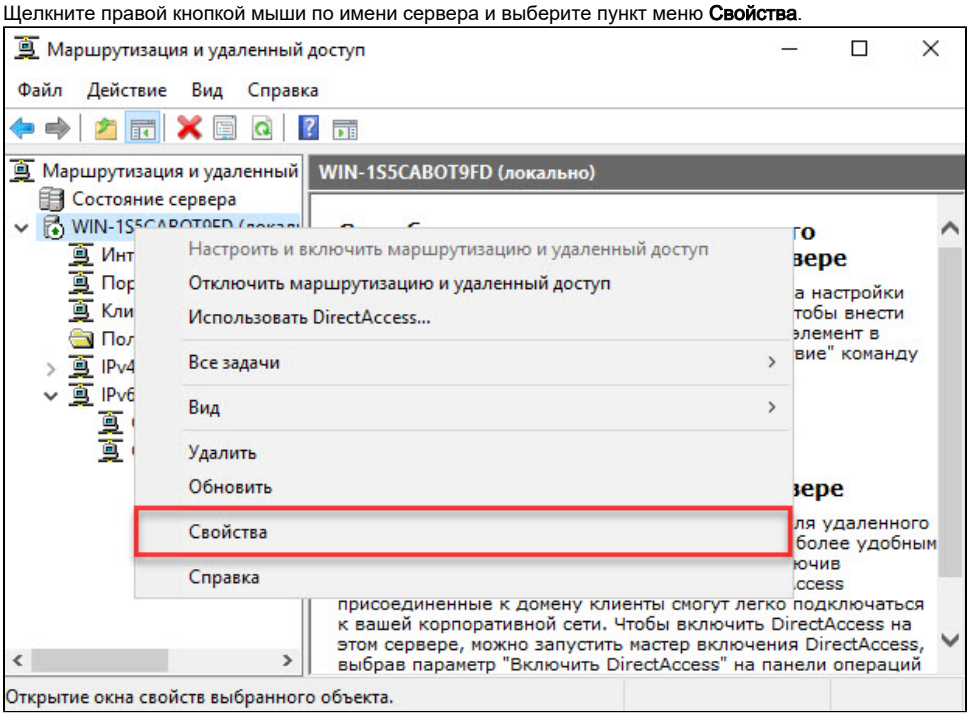


9. Убедитесь, что все необходимые функции сервера маршрутизации и удаленного доступа выбраны (поле **Сводка выбранных параметров**). Нажмите **Готово**.

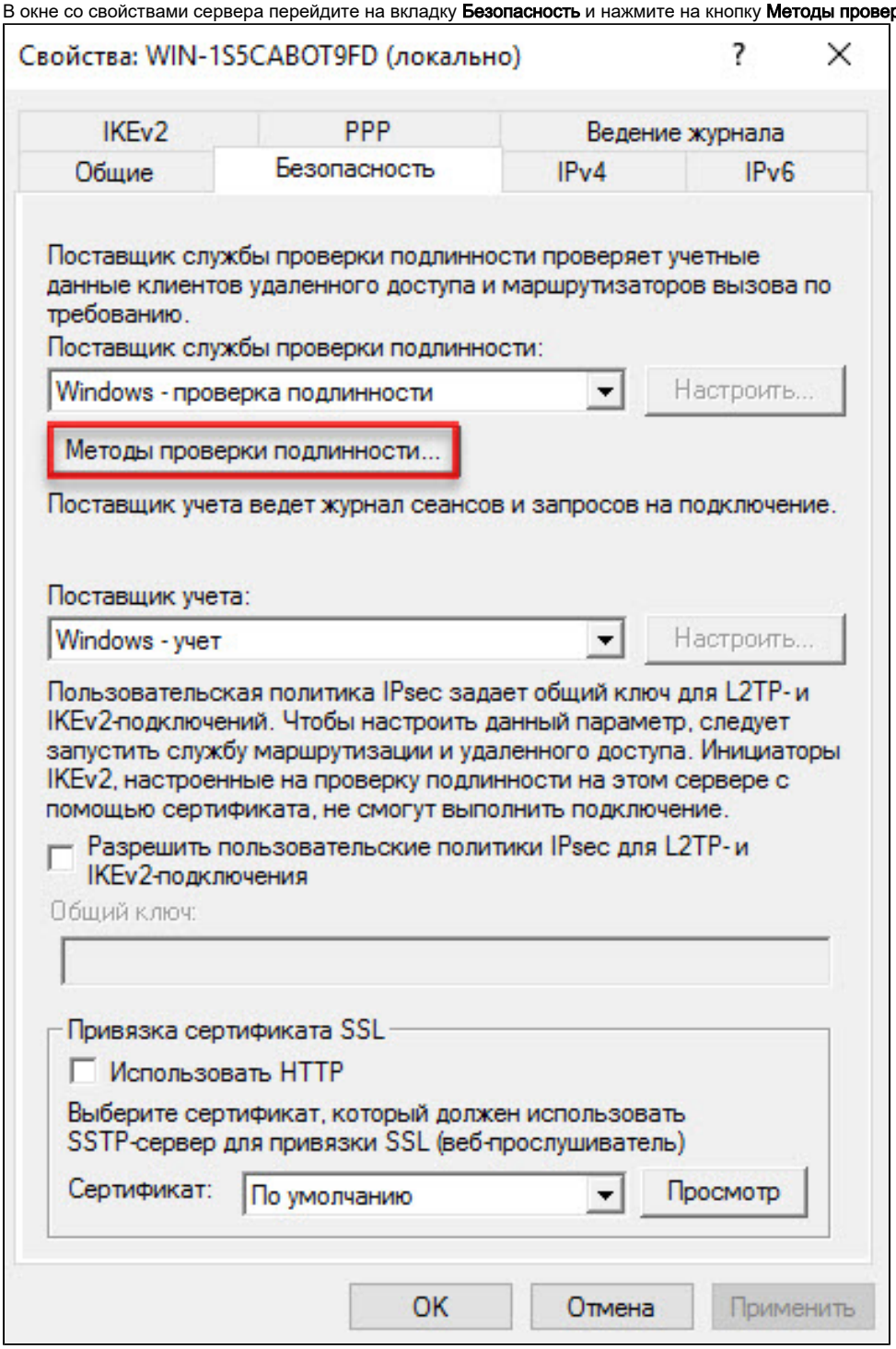


10. Нажмите **Запустить службу** и дождитесь завершения процесса запуска службы.

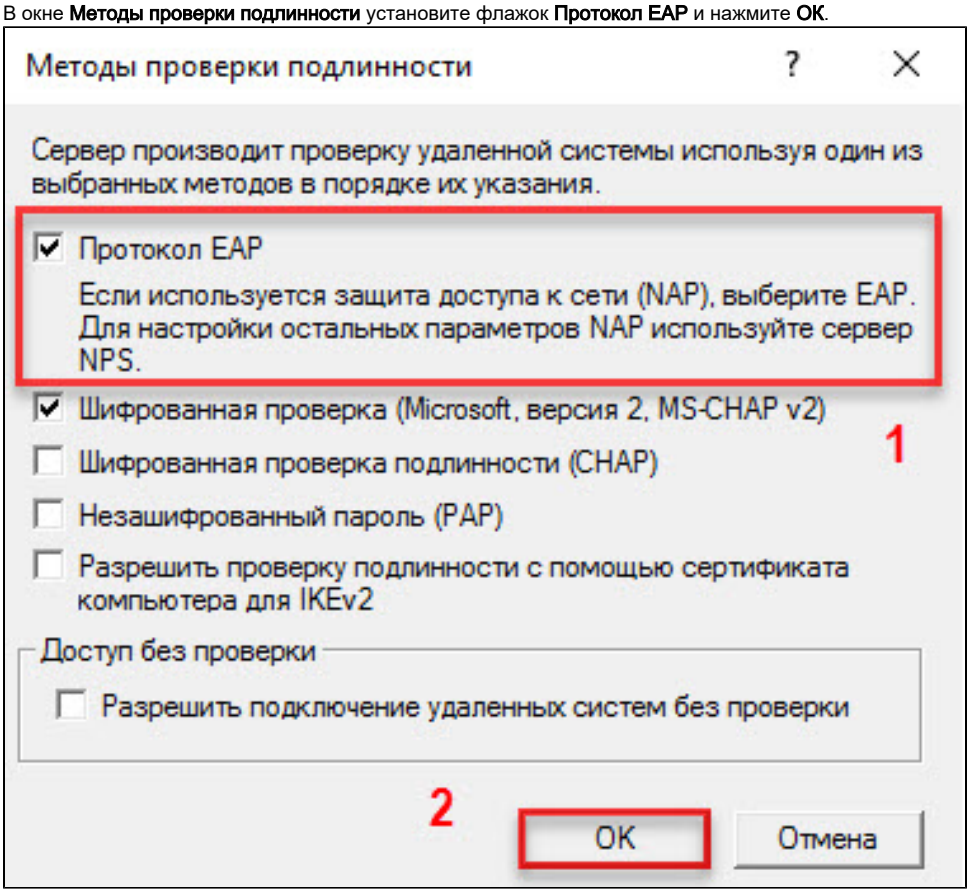
11. Щелкните правой кнопкой мыши по имени сервера и выберите пункт меню **Свойства**.



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

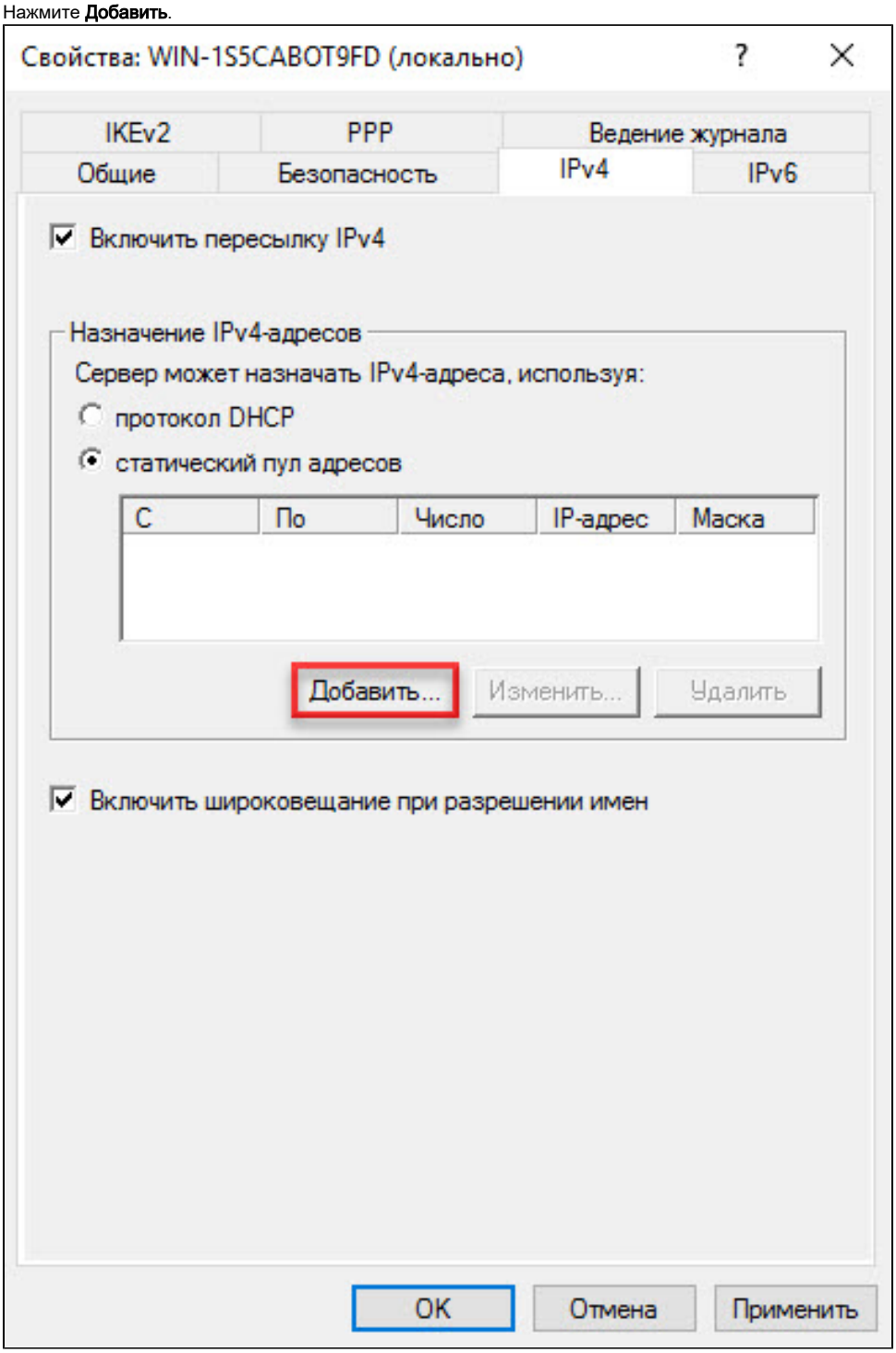


13. В окне **Методы проверки подлинности** установите флажок **Протокол EAP** и нажмите **OK**.

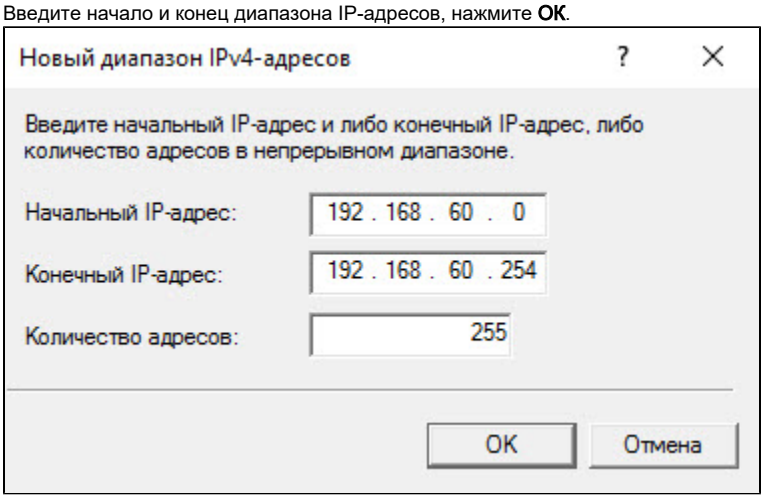


14. В нашем примере на компьютере не настроена служба DHCP. Поэтому удаленным клиентам сначала необходимо назначить IP-адреса из заданного диапазона. Перейдите на вкладку **IPv4** и установите переключатель в положение **статистический пул адресов**.

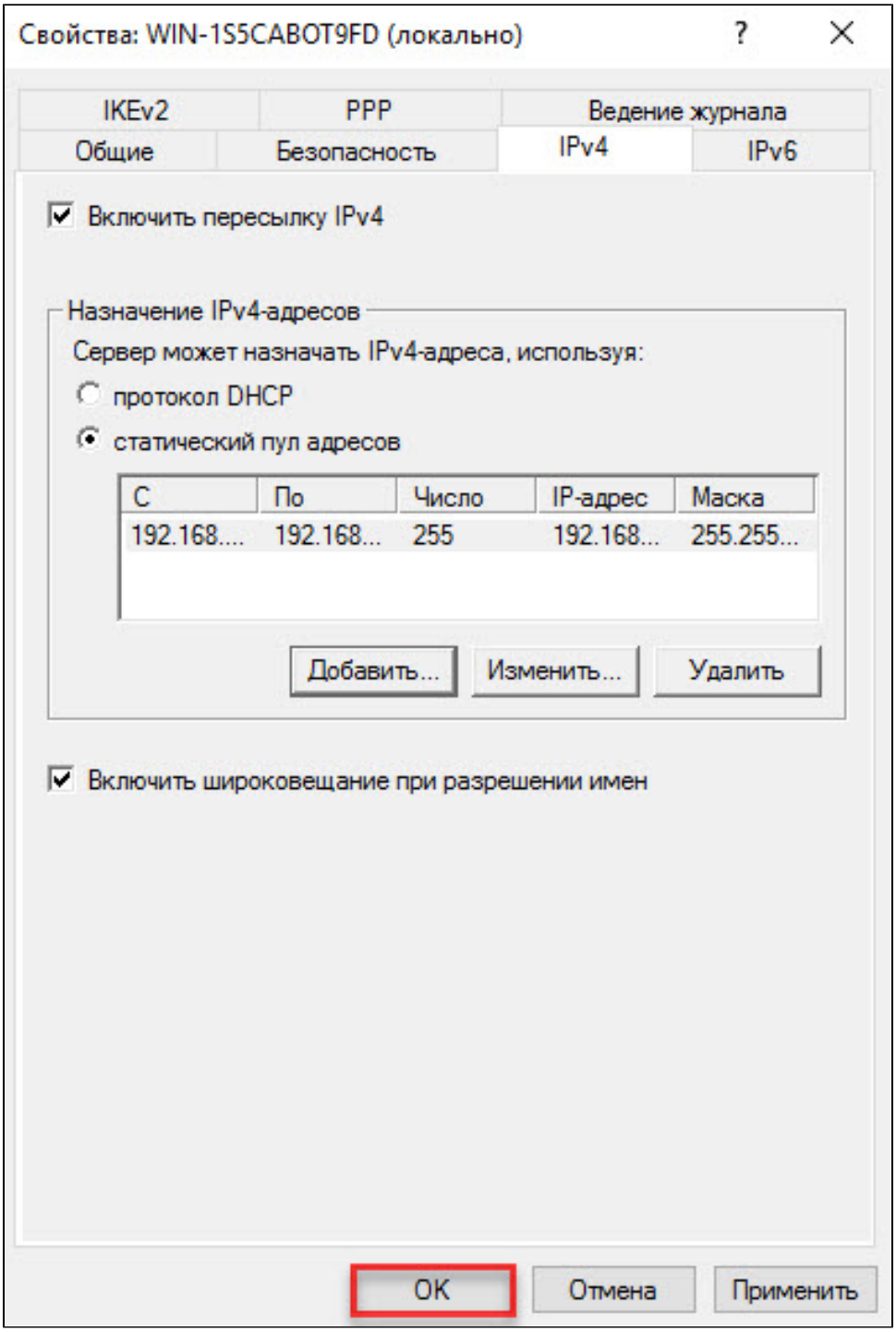
15. Нажмите **Добавить**.



16. Введите начало и конец диапазона IP-адресов, нажмите **OK**.

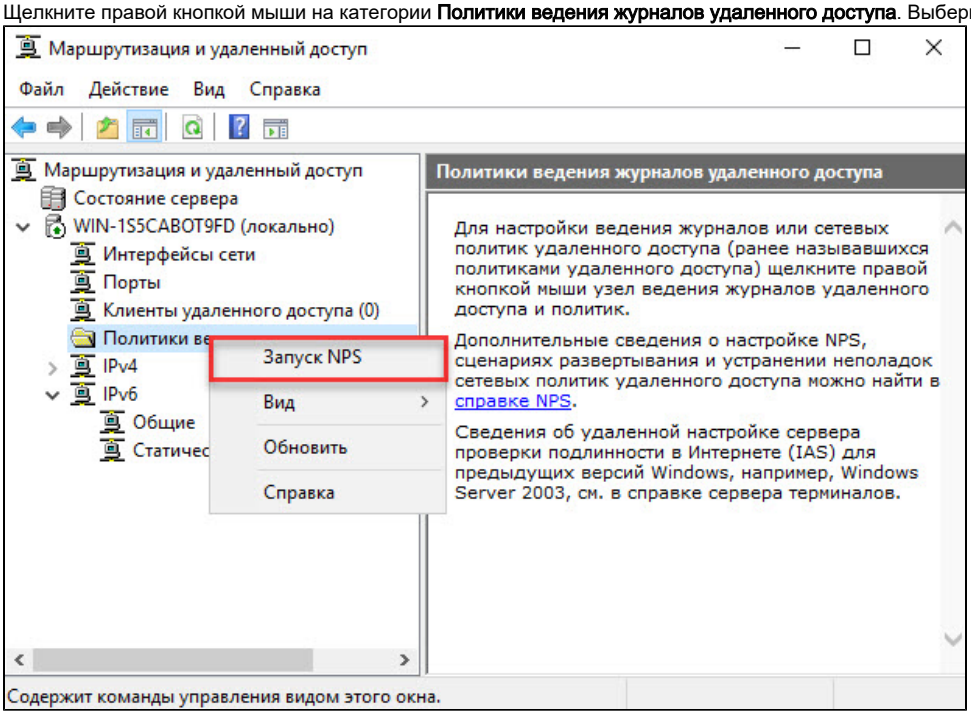


17. Нажмите **OK**.

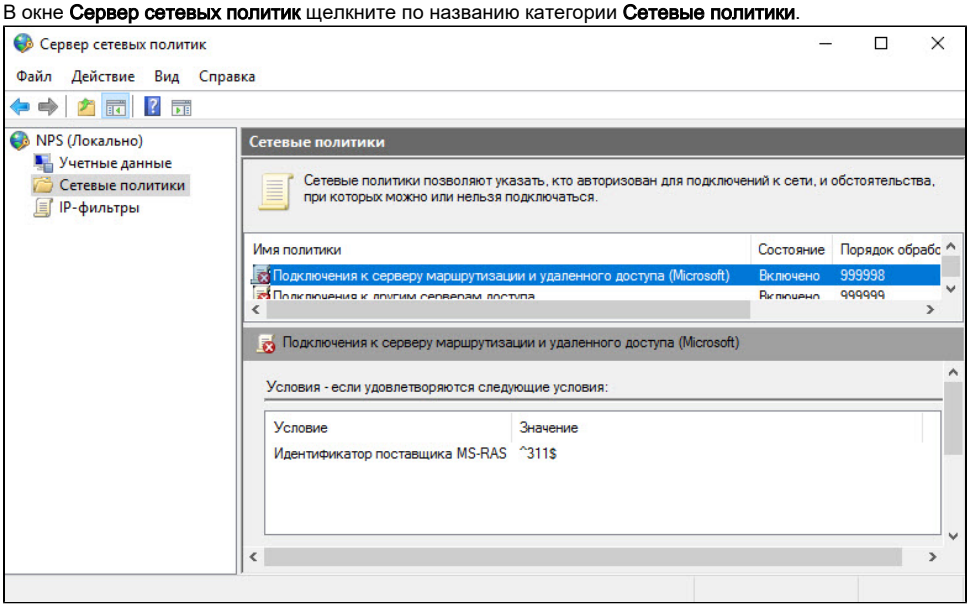


18. Щелкните правой кнопкой мыши на категории **Политики ведения журналов удаленного доступа**. Выберите пункт **Обновить**.

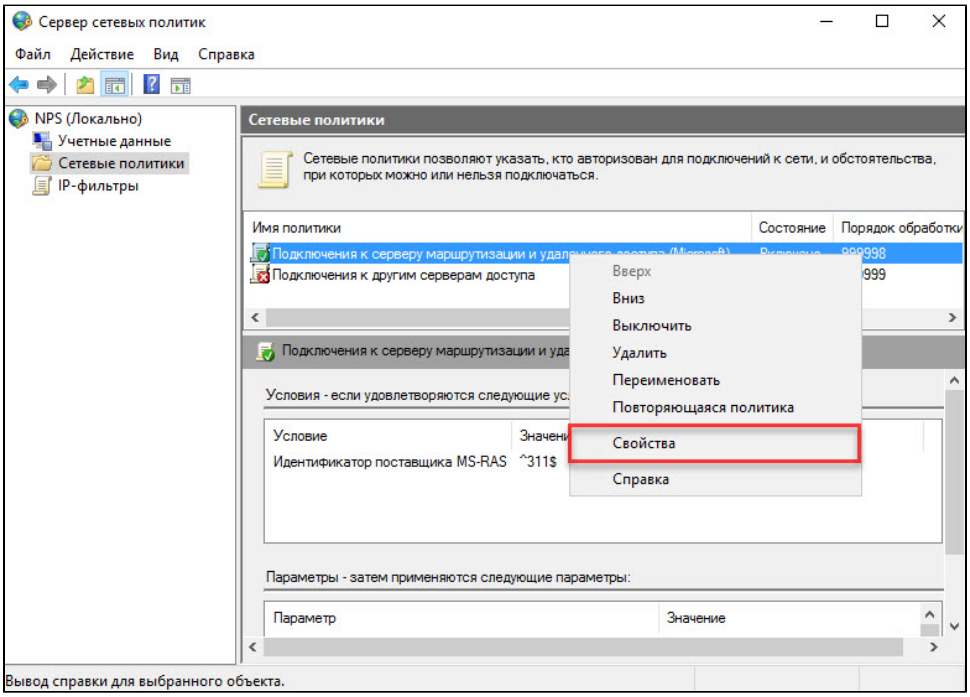
19. Щелкните правой кнопкой мыши на категории **Политики ведения журналов удаленного доступа**. Выберите пункт **Запуск NPS**.



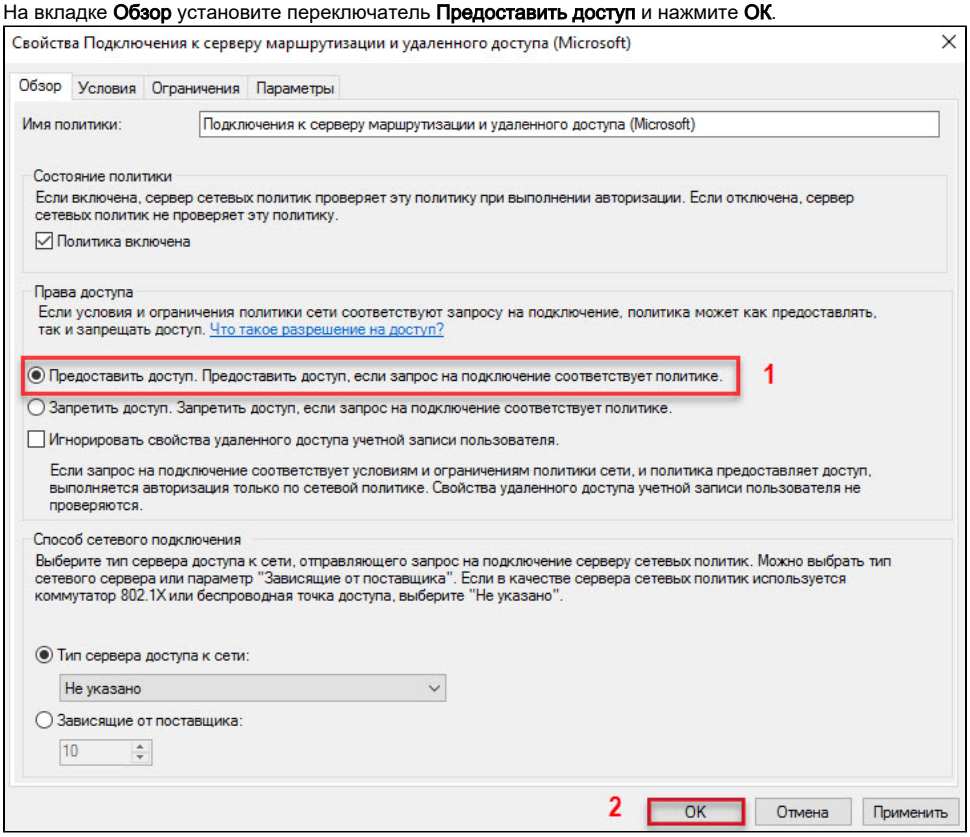
20. В окне **Сервер сетевых политик** щелкните по названию категории **Сетевые политики**.



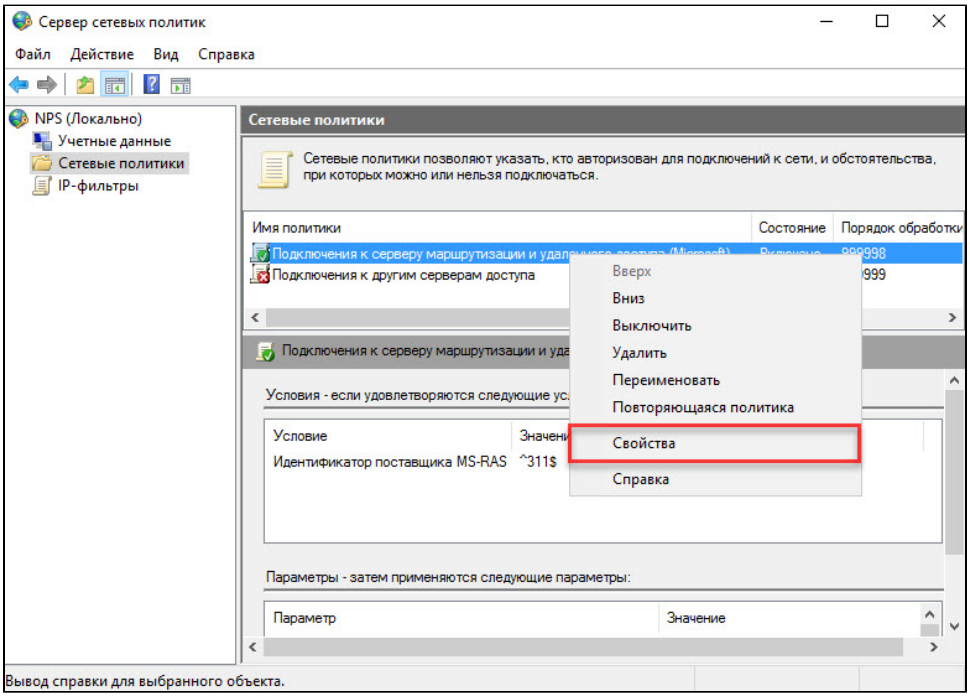
21. Кликните правой кнопкой мыши по строке **Подключение к серверу маршрутизации и удаленного доступа (Microsoft)** и выберите пункт меню **Свойства**.



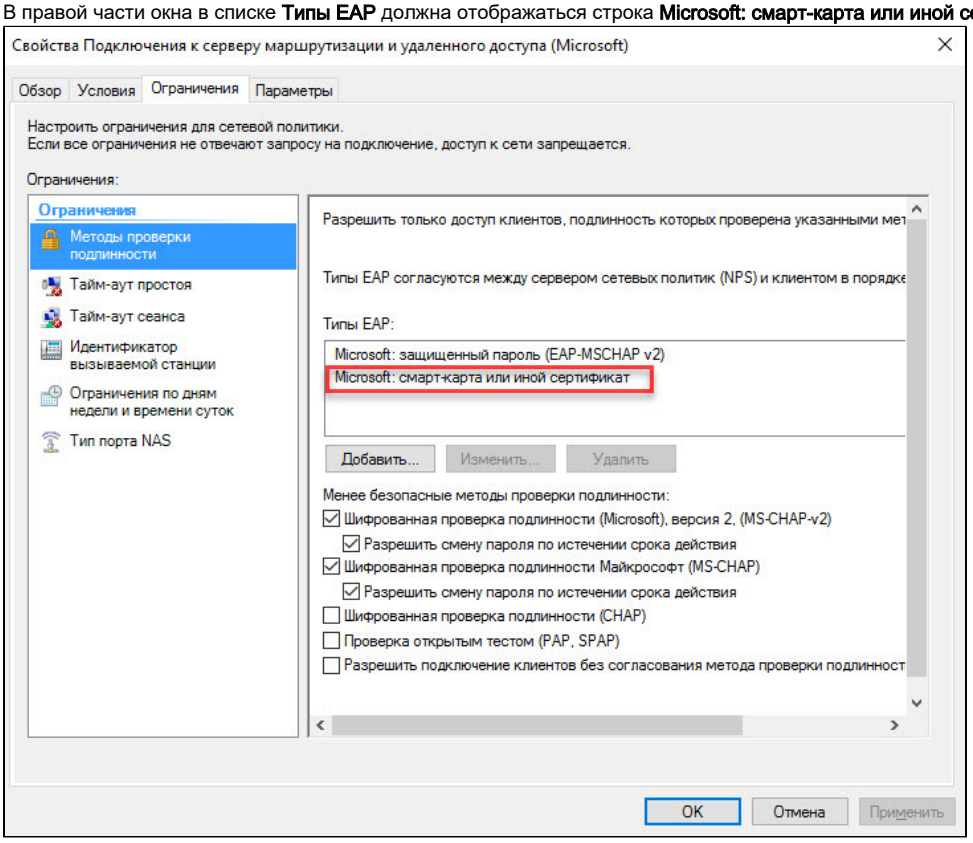
22. На вкладке **Обзор** установите переключатель **Предоставить доступ** и нажмите **OK**.



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

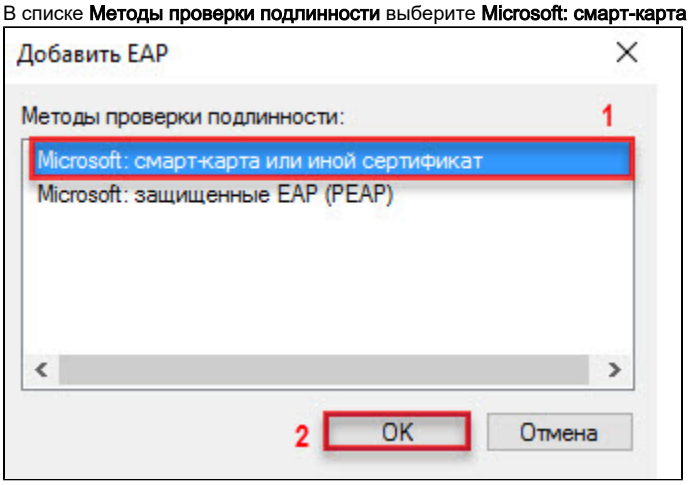


24. На вкладке **Ограничения** в левой части окна щелкните по названию ограничения **Методы проверки подлинности**.
25. В правой части окна в списке **Типы EAP** должна отображаться строка **Microsoft: смарт-карта или иной сертификат**.

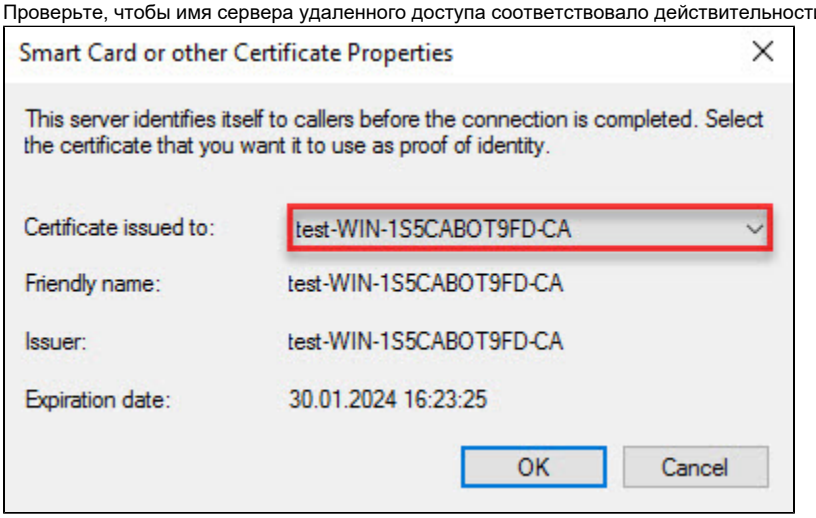


26. Если эта строка не отображается, то нажмите **Добавить**.

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



28. Далее укажите сервер для аутентификации. Для этого щелкните по строке **Microsoft: смарт-карта или иной сертификат** и нажмите **Измени ть**.
29. Проверьте, чтобы имя сервера удаленного доступа соответствовало действительности.



30. Нажмите **OK**.
31. Закройте оснастку **Сервер сетевых политик**.

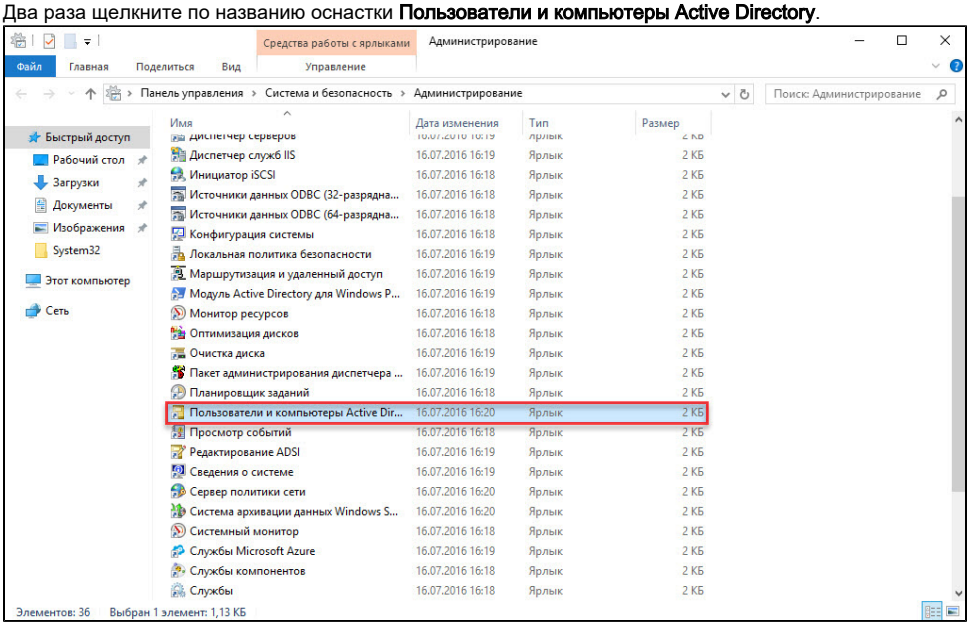
Настройка учетных записей пользователей

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

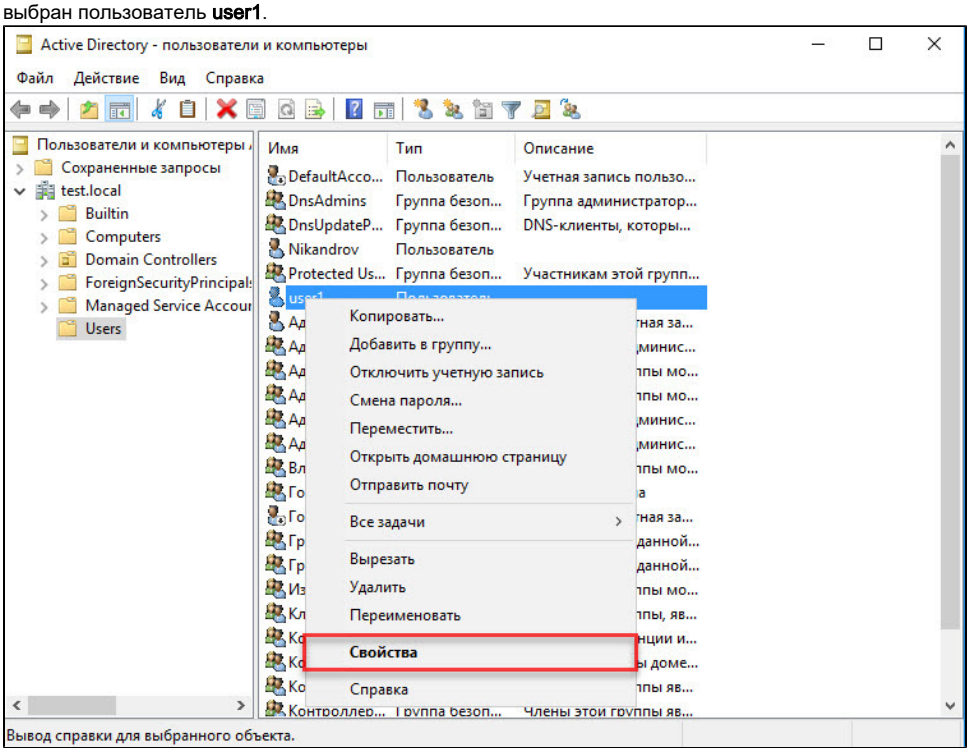
Для настройки учетных записей пользователей:

1. Зайдите в **Панель управления**.
2. В поле для поиска введите слово "администрирование".
3. Два раза щелкните по названию пункта **Администрирование**.

4. Два раза щелкните по названию оснастки **Пользователи и компьютеры Active Directory**.

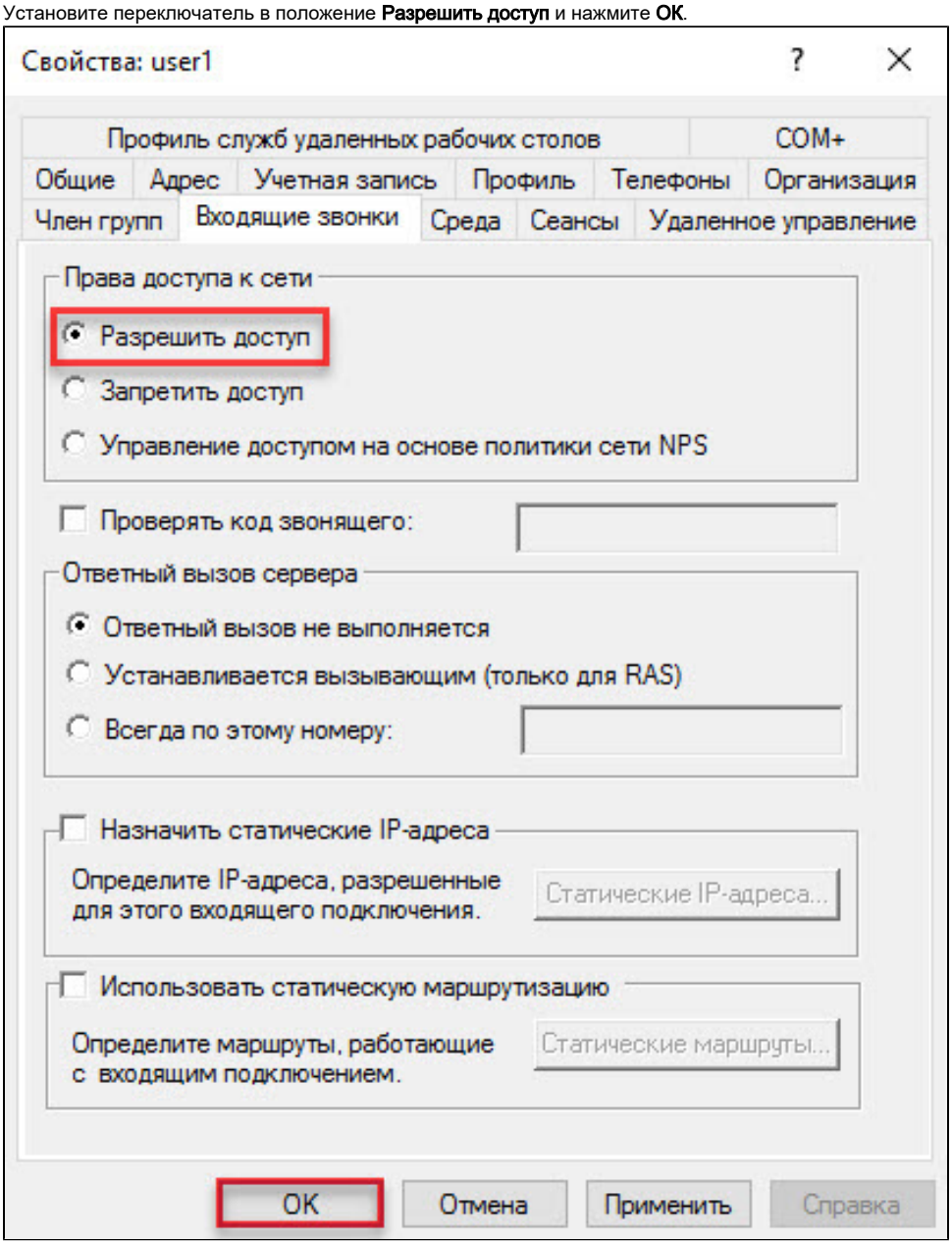


5. В окне **Active Directory - пользователи и компьютеры** щелкните по названию папки **Users**.
6. В правой части окна, в строке с именем пользователя щелкните правой кнопкой мыши и выберите пункт **Свойства**. В данном примере выбран пользователь **user1**.



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

8. Установите переключатель в положение **Разрешить доступ** и нажмите **OK**.



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

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