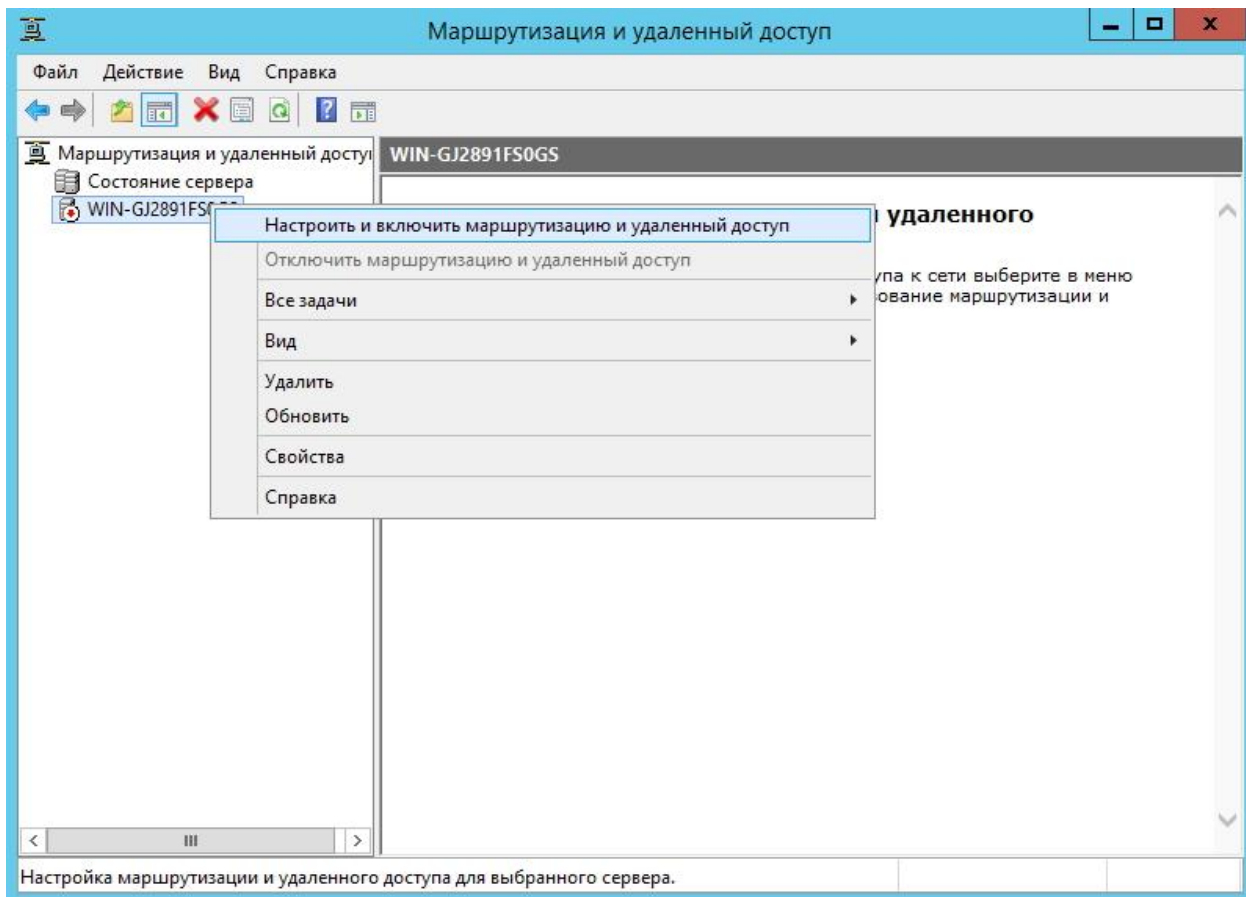


НАСТРОЙКА VPN СЕРВЕРА

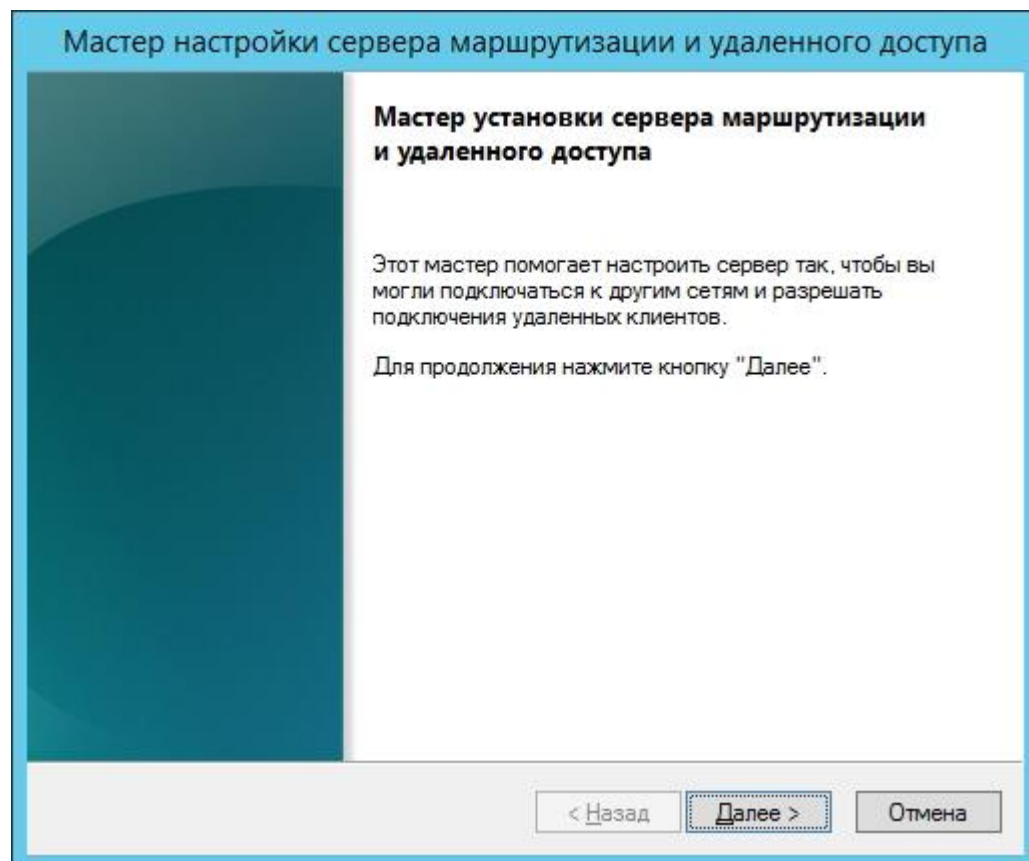
VPN PPTP-сервер для защищенного подключения клиентов может быть настроен только на серверных версиях Windows на одном компьютере с Traffic Inspector. Он настраивается как сервер удаленного доступа (RAS-сервер) в службе RRAS (Маршрутизация и удаленный доступ). Эта справка предназначена для опытных пользователей.

1. Создание VPN сервера.

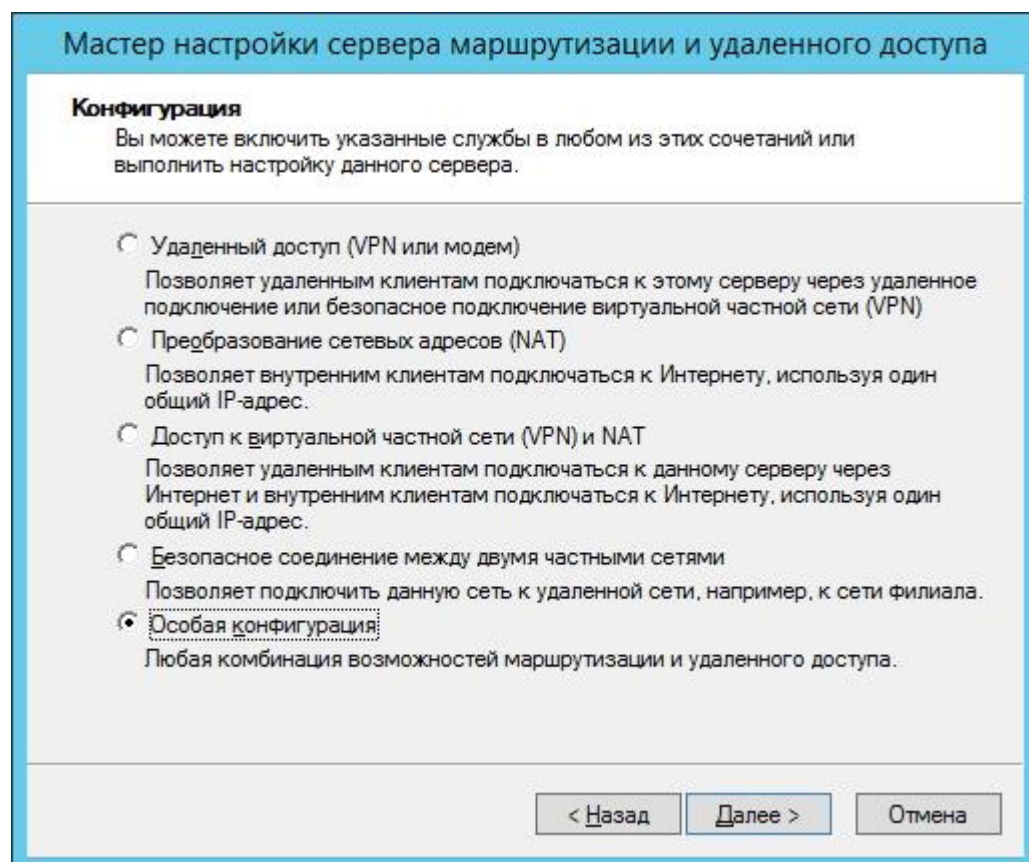
Откройте службу «Маршрутизация и удаленный доступ». Выберите свой сервер. После этого в контекстном меню выберите пункт «Настроить и включить маршрутизацию и удаленный доступ».



Нажимаем «Далее».



In the following menu, we select the item «Special configuration».



В следующем окне выбираем «Доступ к виртуальной частной сети», «Преобразование сетевых адресов», «Маршрутизация локальной сети» и нажимаем «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

Нажимаем «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:

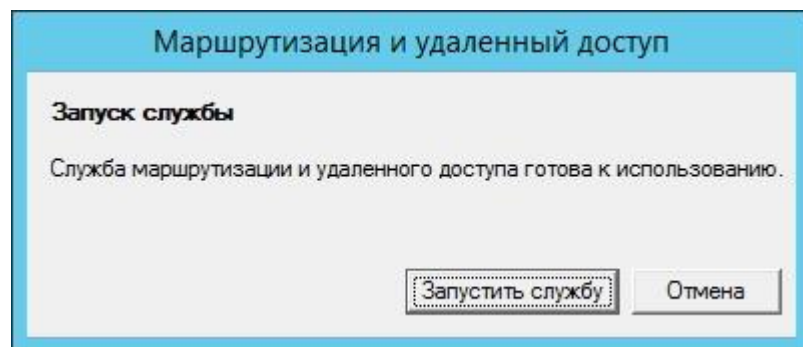
- доступ к виртуальной частной сети (VPN)
- NAT
- Маршрутизация локальной сети

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

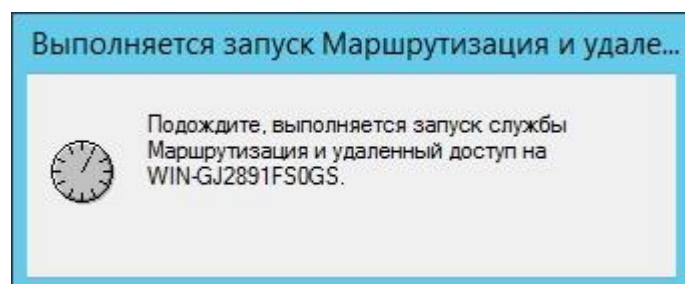
Для закрытия мастера нажмите кнопку "Готово".

< Назад Готово Отмена

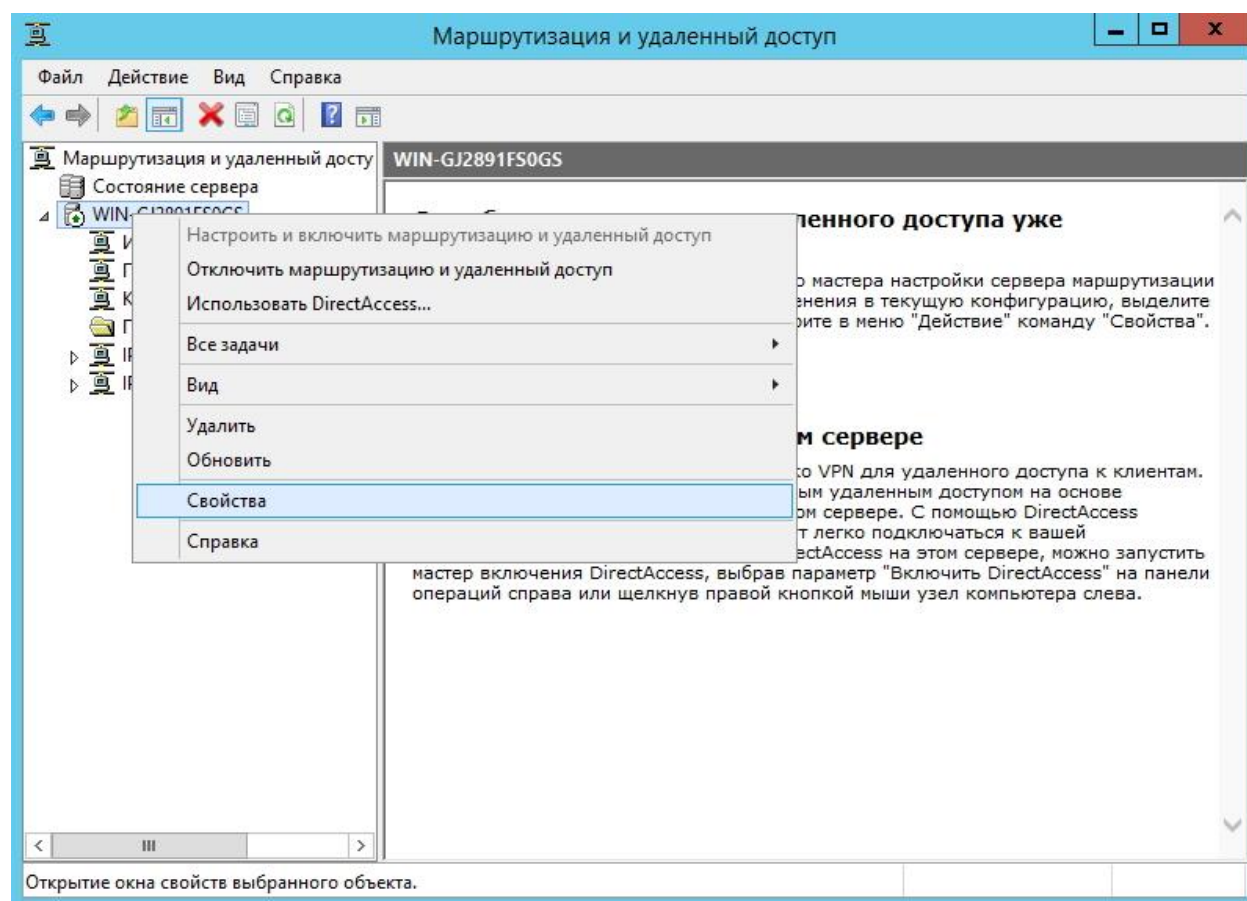
В появившемся окне нажимаем «Запустить службу».



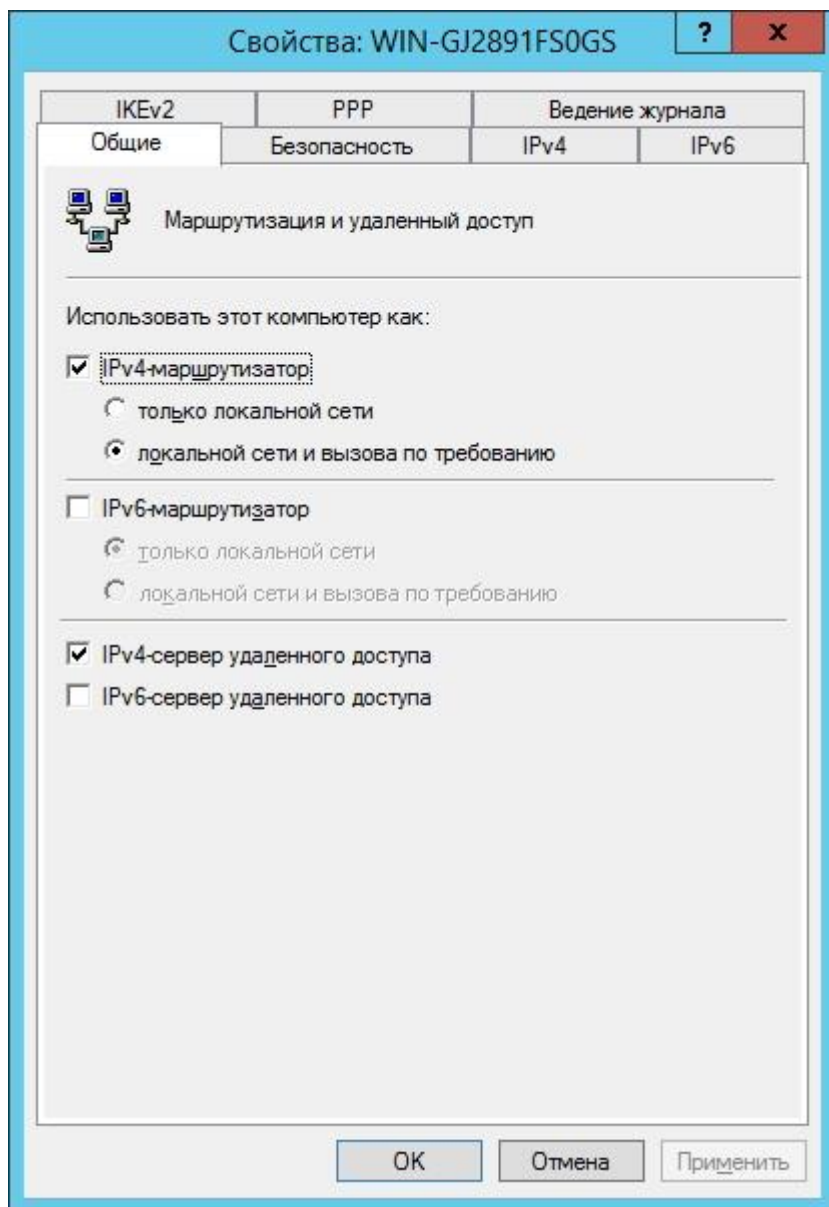
После чего запустится «Маршрутизация и удаленный доступ».



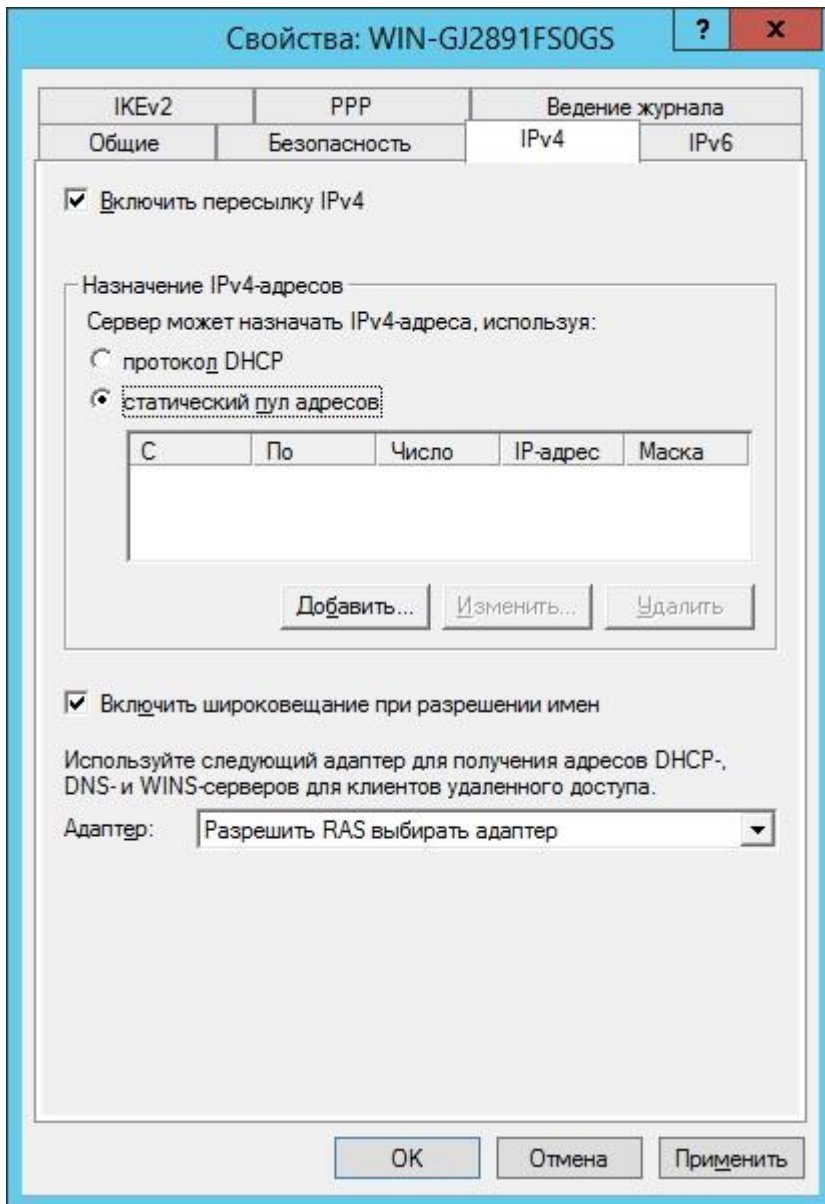
Заходим в свойства сервера.



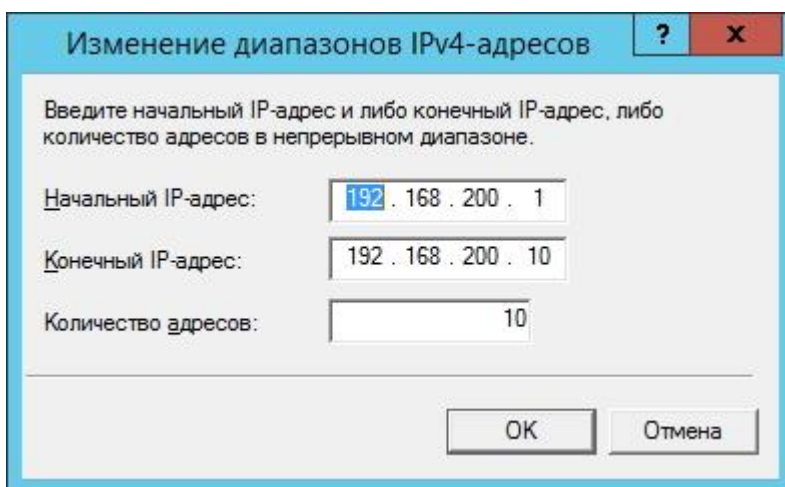
Выставляем настройки на вкладке «Общие» так, как показано на рисунке.



Переходим во вкладку IPv4 и выбираем статический пул адресов.



Нажимаем кнопку «Добавить» и назначаем пул адресов (в данном случае выбрана подсеть «192.168.200.1 - 192.168.200.10», состоящая из 10 адресов. Причем сервер получает адрес 192.168.200.1).



Переходим во вкладку «Ведение журнала» и указываем «Вести журнал ошибок и предупреждений».

Общие

Безопасность

IPv4

IPv6

IKEv2

PPP

Ведение журнала

Выберите типы событий, которые вы хотите регистрировать:

- вести только журнал ошибок
 - вести журнал ошибок и предупреждений
 - вести журнал всех событий
 - Не записывать в журнал никаких событий
- Записывать дополнительные сведения о маршрутизации и удаленном доступе (используется для отладки)

Чтобы просмотреть сведения в данных журналах, откройте папку %windir%\tracing.

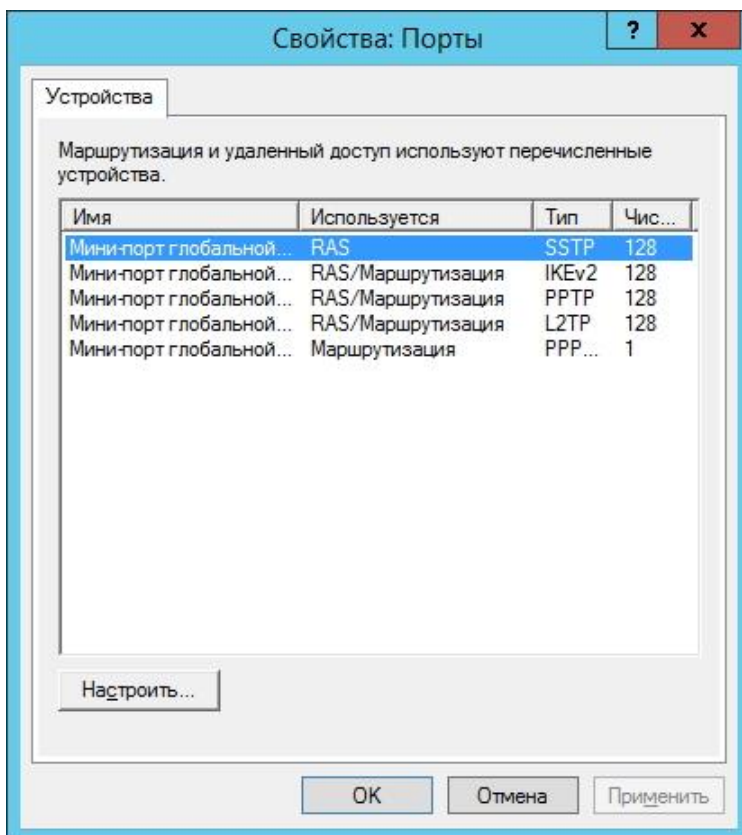
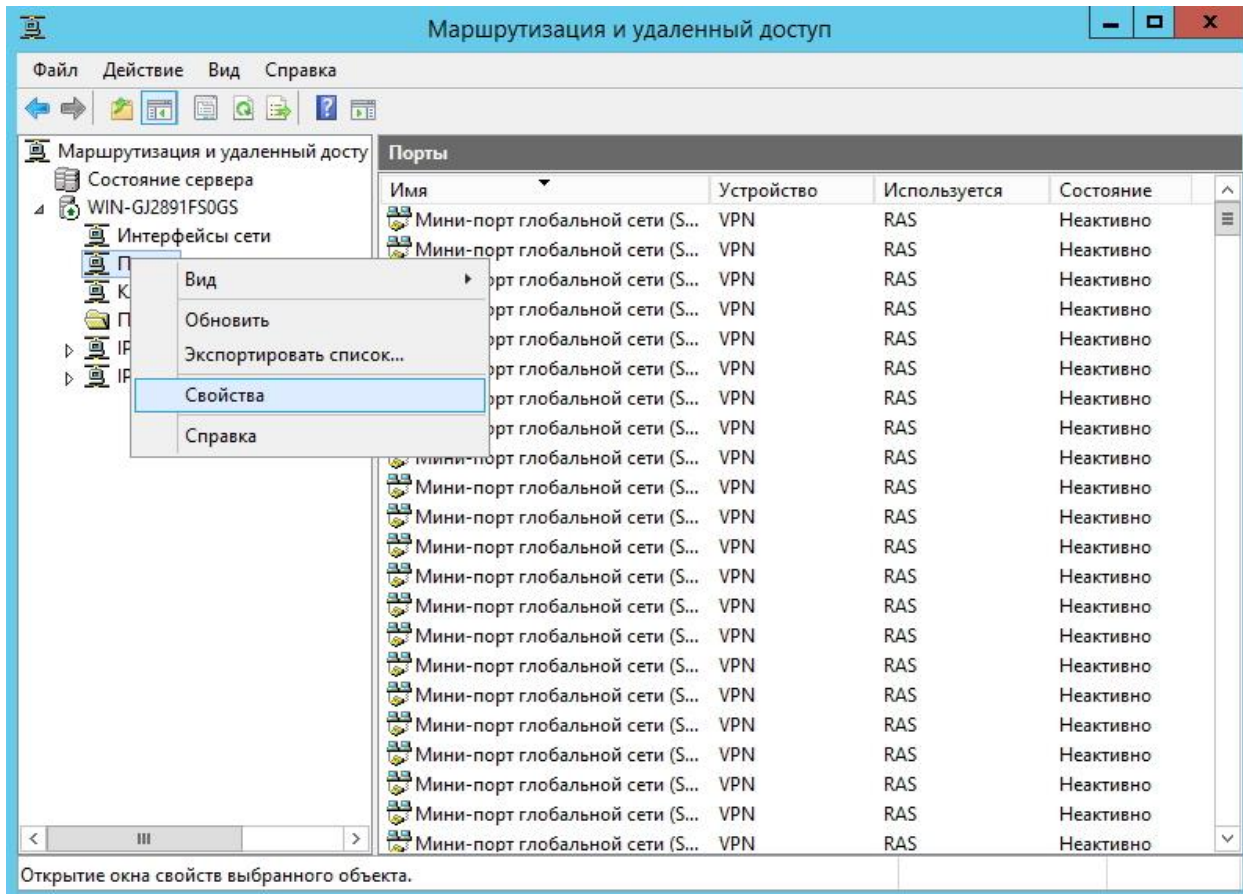
ОК

Отмена

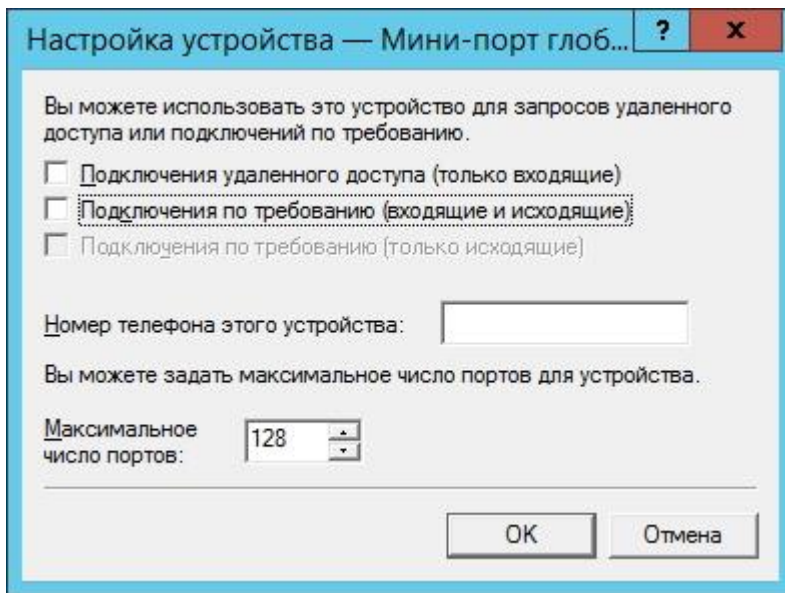
Применить

2. Конфигурация портов.

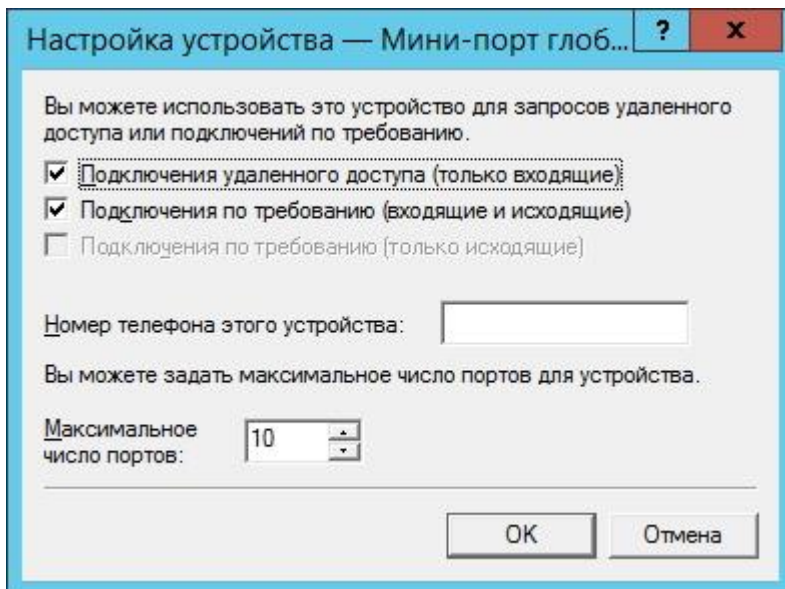
Зайдите в свойства раздела «Порты» консоли «Маршрутизация и удаленный доступ».



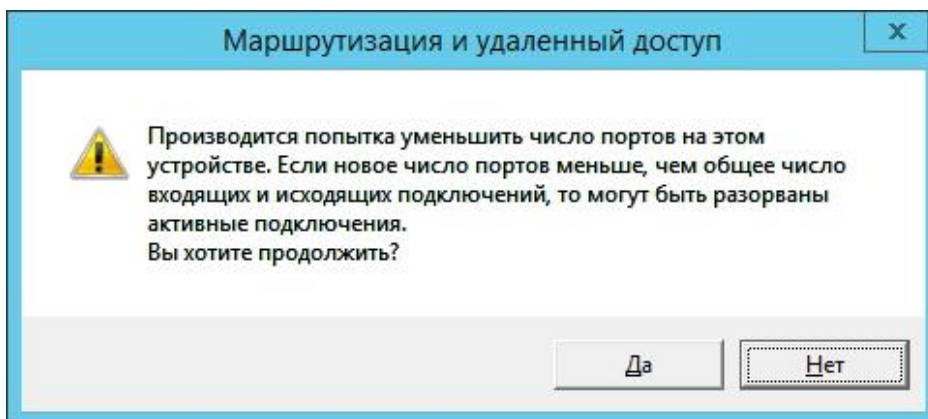
Для стабильной работы сервера рекомендуется удалить ненужные порты и создать необходимое количество портов. Для этого необходимо в настройках портов SSTP, PPOE, L2TP, IKEv2 снять использование портов для удаленных подключений. Настройки отключенных портов должно выглядеть так (на примере L2TP):



Создаем необходимое количество портов RPTP (в данном случае 10). Для этого указываем настройки мини-порта RPTP как на рисунке:



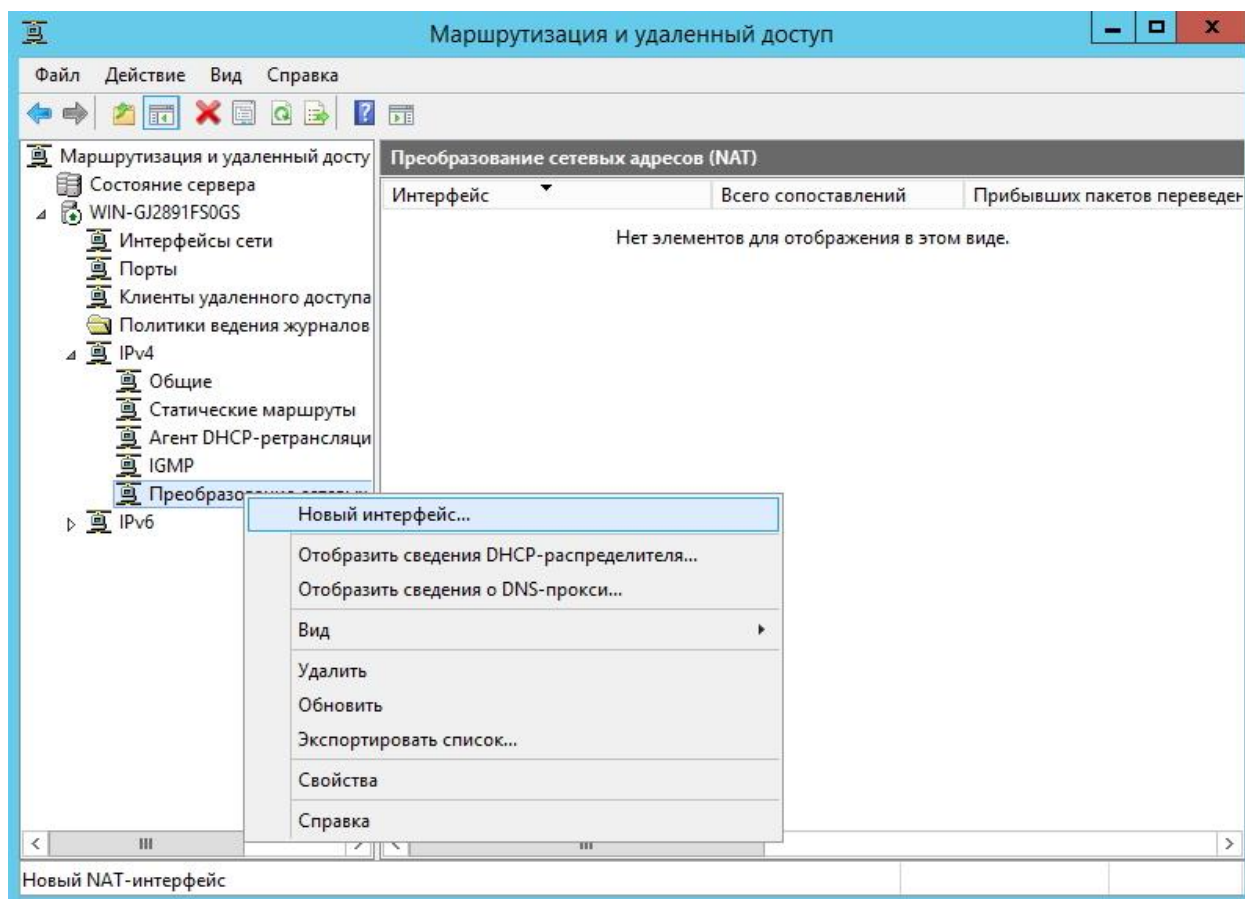
Утвердительно отвечаем на предупреждение о сокращении количества портов.



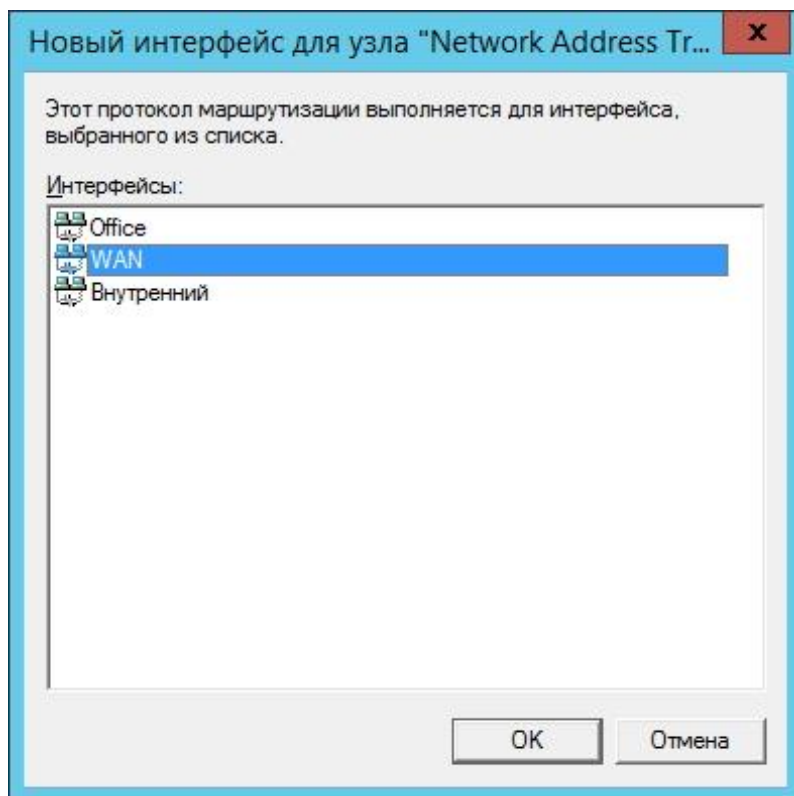
Получится примерно так, как на следующем рисунке.

3. Настройка NAT.

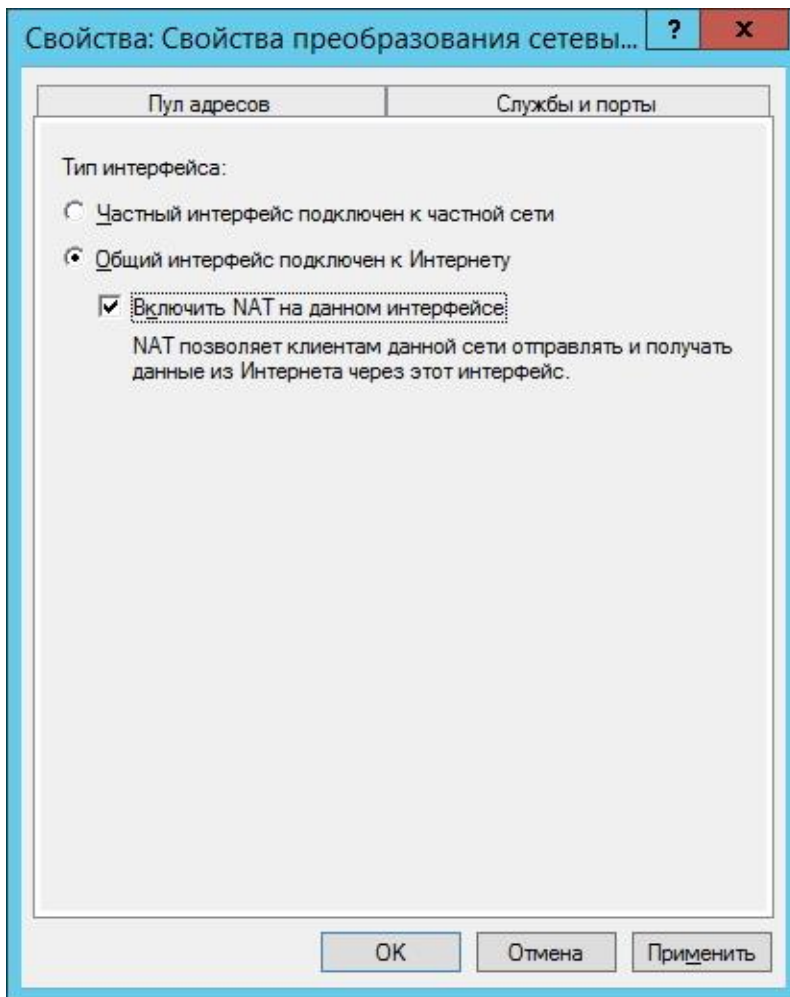
Переходим в «Преобразование сетевых адресов (NAT)» и добавляем новый интерфейс.



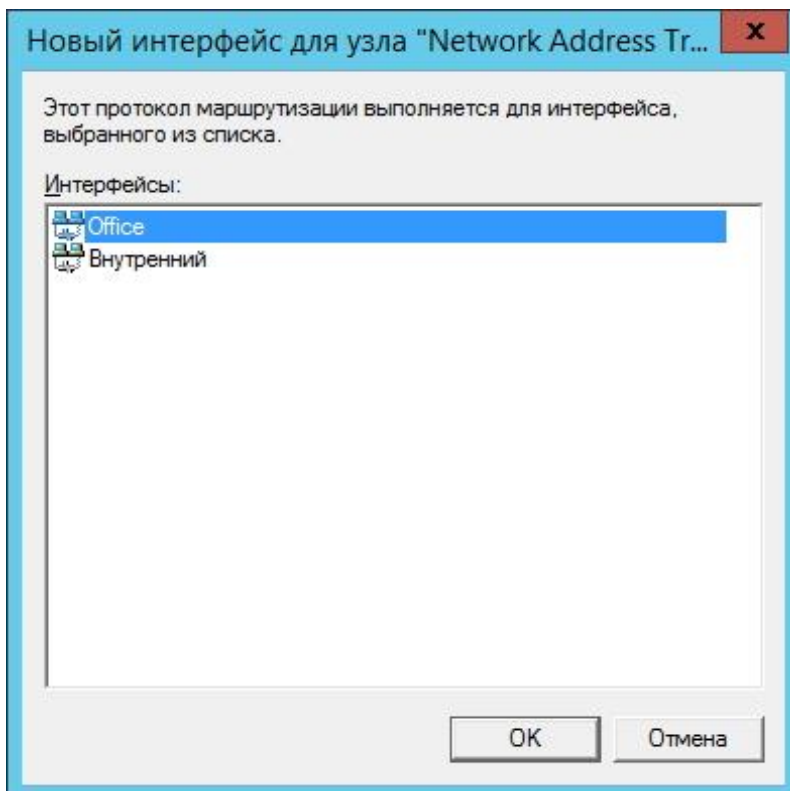
Выбираем подключение к Интернету.



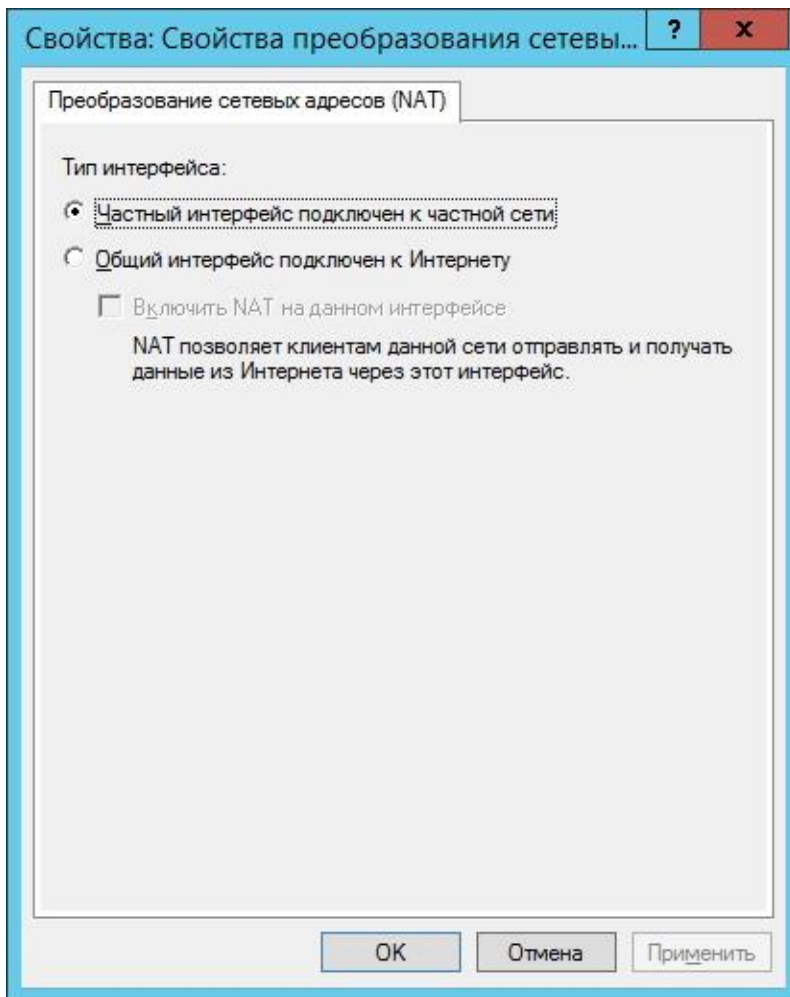
Помечаем его как «Общий интерфейс подключен к Интернету» и включаем NAT:



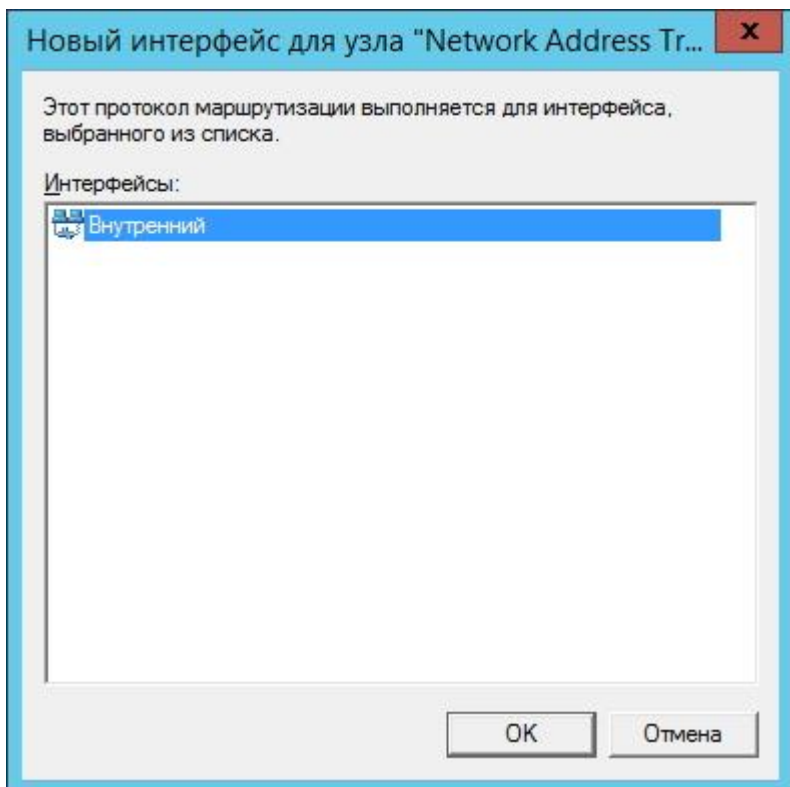
После этого добавляем интерфейс локальной сети:

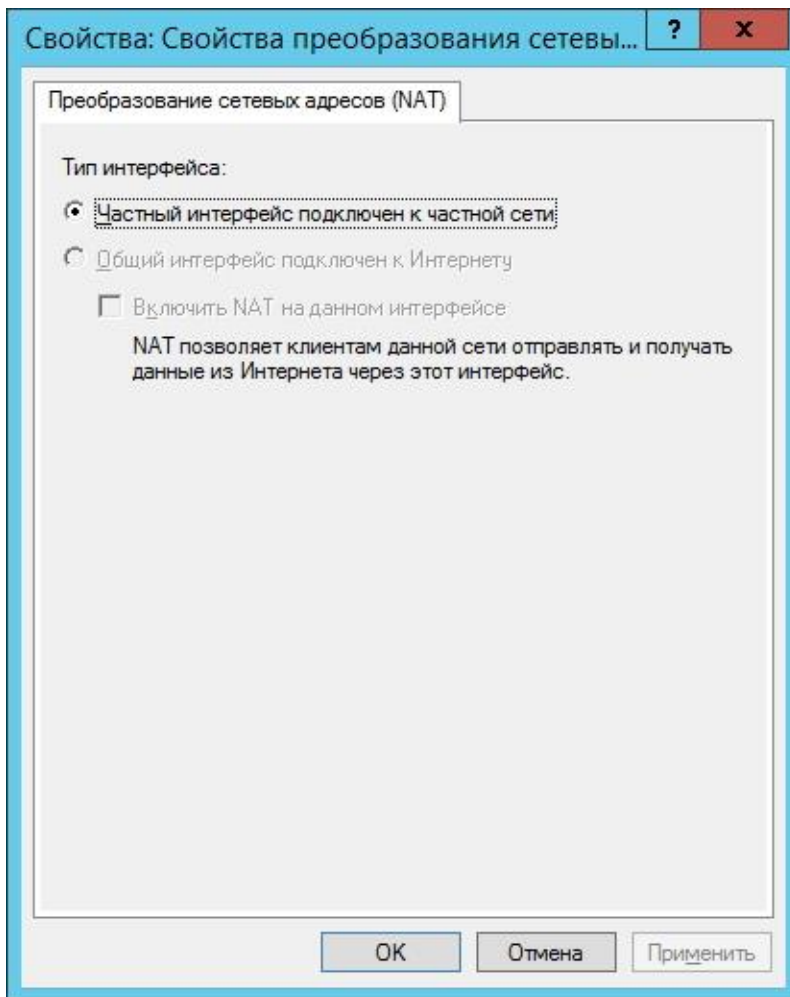


В свойствах указываем его как частный интерфейс:

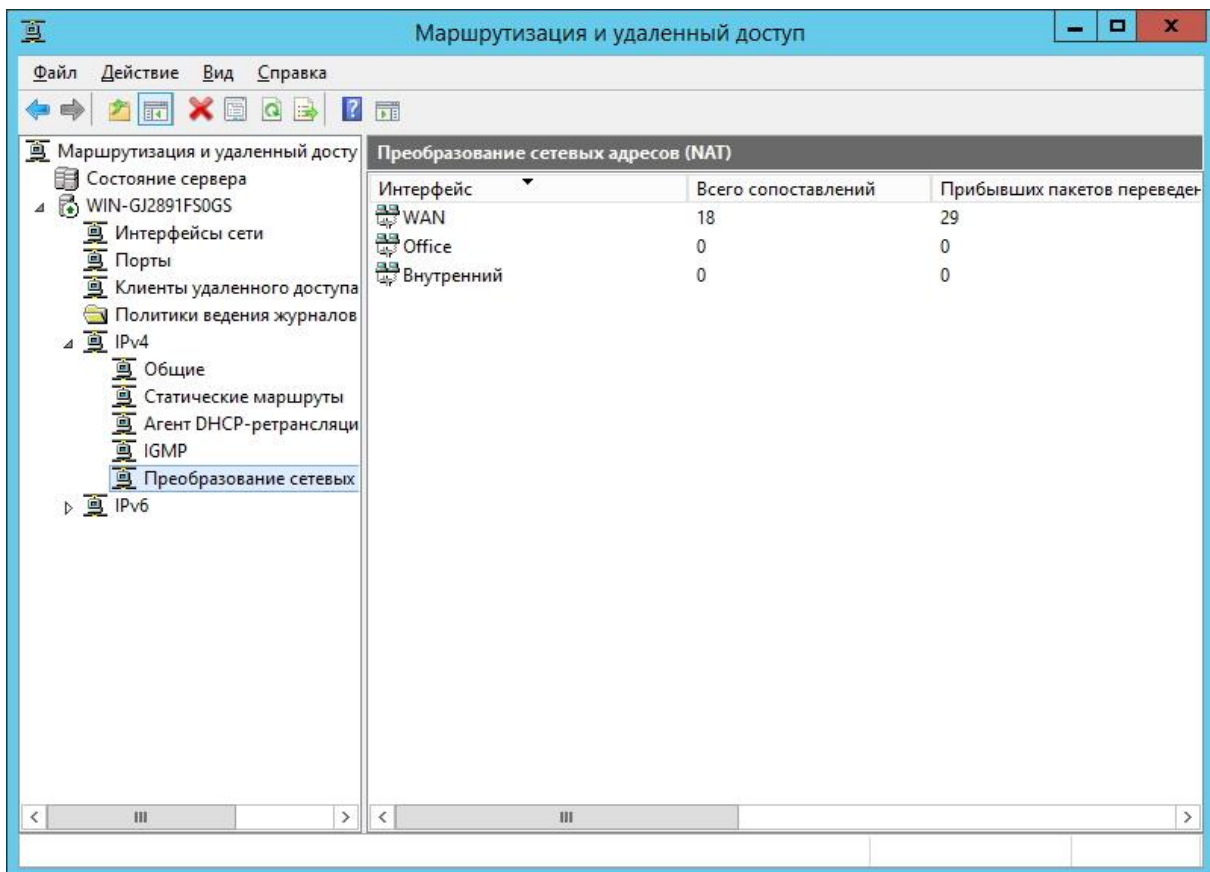


Добавляем Внутренний интерфейс: как частный интерфейс сети.



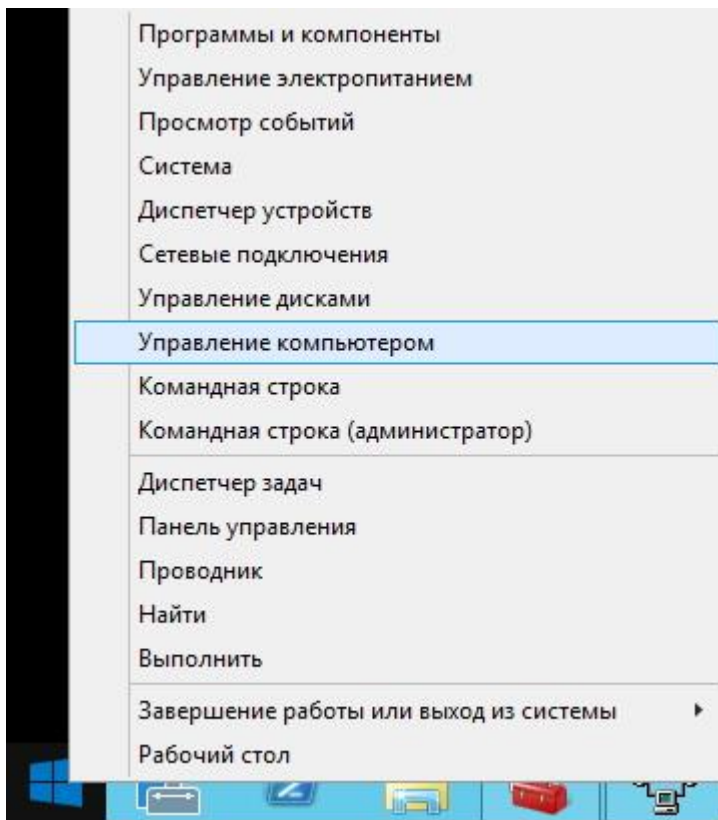


В разделе консоли «Преобразование сетевых адресов» увидим такую картину:

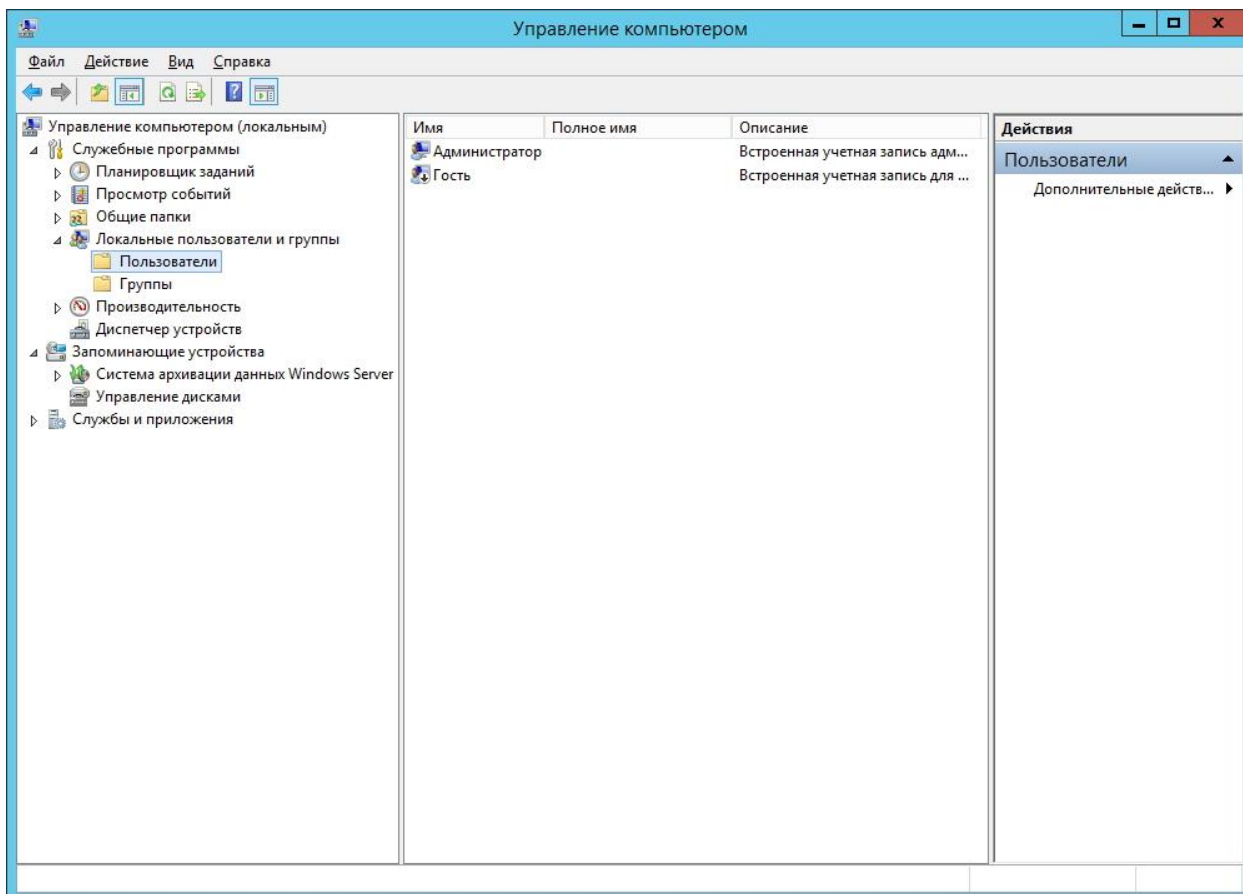


4. Настройка клиентов.

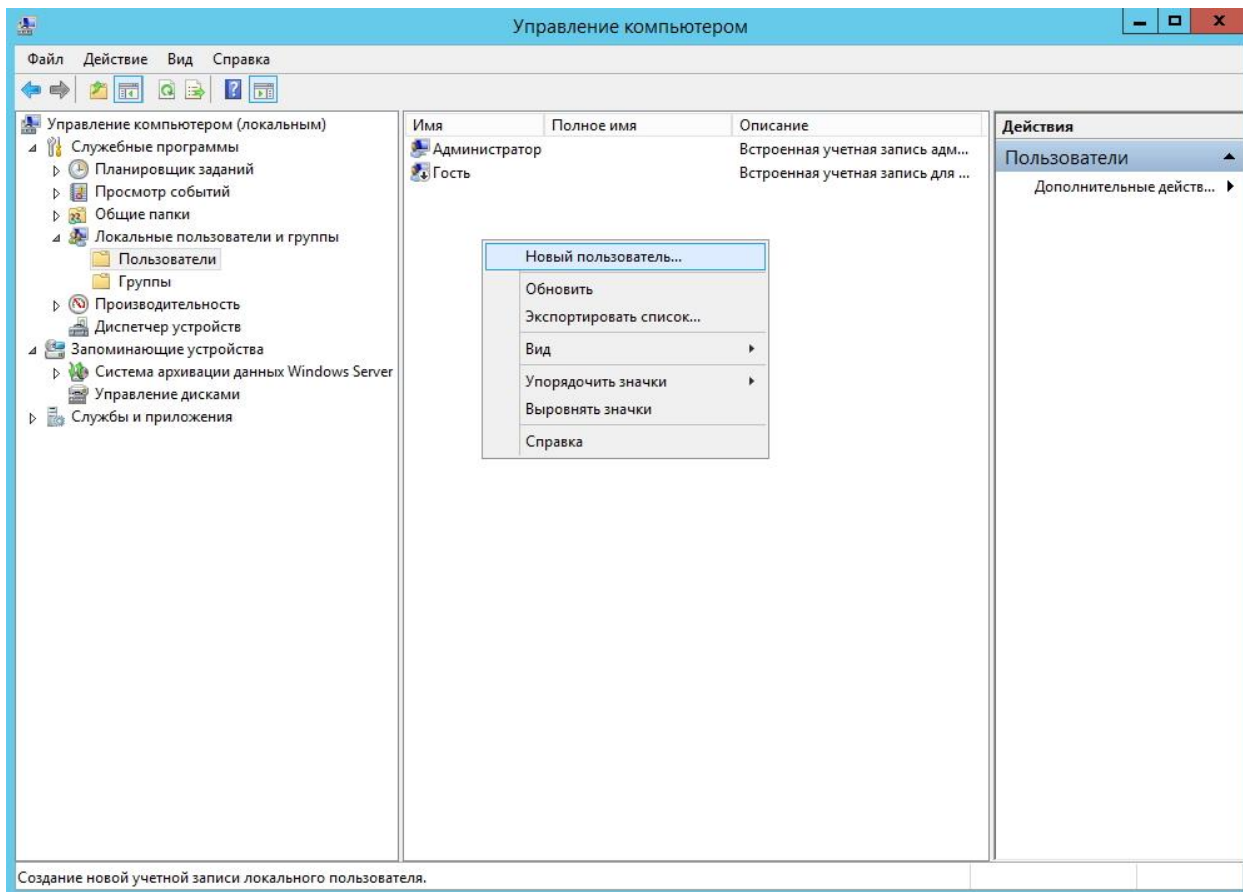
Запускаем управление компьютером.



Переходим в «Локальные пользователи и группы - Пользователи».



И добавляем нового пользователя.



Задаем логин пользователя и пароль как на следующем рисунке.

Новый пользователь

Пользователь: VPN

Полное имя:

Описание:

Пароль: ●●●●●●●●

Подтверждение: ●●●●●●●●

Требуется смена пароля при следующем входе в систему

Запретить смену пароля пользователем

Срок действия пароля не ограничен

Отключить учетную запись

Справка Создать Закрыть

Переходим в свойства пользователя на вкладку «входящие звонки» и осуществляем настройку в соответствии со следующим рисунком (Также здесь можно назначить пользователю статический IP).

Свойства: VPN



Удаленное управление

Общие | Членство в группах | Профиль | Среда | Сеансы

Профиль служб удаленных рабочих столов

Входящие звонки

Права доступа к сети

- Разрешить доступ
- Запретить доступ
- Управление доступом на основе политики сети NPS

Проверять код звонящего:

Ответный вызов сервера

- Ответный вызов не выполняется
- Устанавливается вызывающим (только для RAS)
- Всегда по этому номеру:

Назначить статические IP-адреса

Определите IP-адреса, разрешенные для этого входящего подключения.

Статические IP-адреса...

Использовать статическую маршрутизацию

Определите маршруты, работающие с входящим подключением.

Статические маршруты...

OK

Отмена

Применить

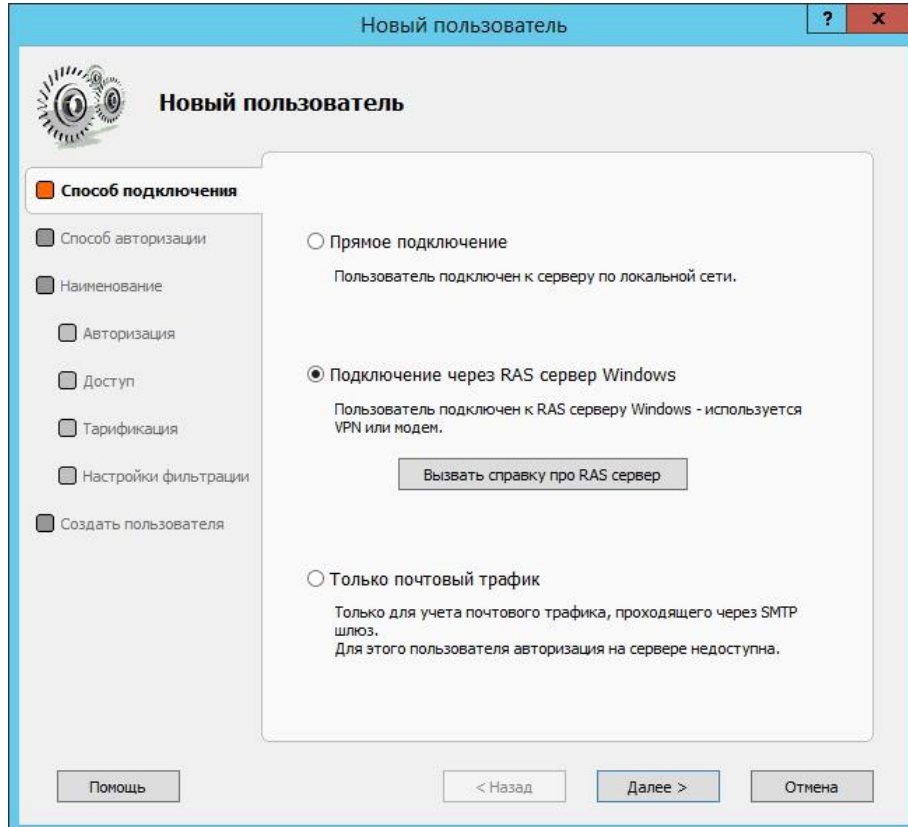
Справка

5. Настройка Traffic Inspector.

В конфигураторе Traffic Inspector в настройке служб ставим галочку «Используется RAS сервер».



Заводим в программе нового клиента и указываем способ подключения «Подключение через RAS сервер Windows».



Все остальные настройки не отличаются от настроек всех остальных клиентов программы. В данном случае использована авторизация по IP.

Новый пользователь

Новый пользователь

Способ подключения

Способ авторизации

Наименование

Авторизация

Доступ

Тарификация

Настройки фильтрации

Создать пользователя

Учетная запись (логин) Windows

Загрузить данные из Active Directory

Имя пользователя и его E-Mail адреса будут добавлены из учетной записи домена

Учетная запись (логин) Traffic Inspector

Имя

Пароль

IP адрес пользователя или диапазон адресов

192.168.200.2 - . . .

MAC адрес

Определить

Помощь < Назад Далее > Отмена

Новый пользователь

Новый пользователь

Способ подключения

Способ авторизации

Наименование

Авторизация

Доступ

Тарификация

Настройки фильтрации

Создать пользователя

Отображаемое имя

VPN

Если не задано, то в качестве отображаемого имени будет использоваться параметр авторизации.


Пользователь запрещен

Все параметры по умолчанию

Примечания

Помощь < Назад Далее > Отмена

Новый пользователь



Новый пользователь

- Способ подключения
- Способ авторизации
- Наименование
- Авторизация**
- Доступ
- Тарификация
- Настройки фильтрации
- Создать пользователя

Параметры авторизации пользователя

Логин

Пароль


IP адрес
192. 168. 200. 2 - . . .

MAC

Вносить MAC и IP в ARP таблицу стека TCP/IP

Создать резервирование в DHCP

Новый пользователь



Новый пользователь

- Способ подключения
- Способ авторизации
- Наименование
- Авторизация
- Доступ**
- Тарификация
- Настройки фильтрации
- Создать пользователя

Тип доступа

Безлимитный
Пользователь работает независимо от значения баланса

Автоотключение
Доступ с блокировкой при наличии отрицательного баланса.
Может работать в кредит.

Ограничения на доступ по датам

С даты
15.01.2014

По дату
. .

Новый пользователь

Новый пользователь

- Способ подключения
- Способ авторизации
- Наименование
- Авторизация
- Доступ
- Тарификация**
- Настройки фильтрации
- Создать пользователя

Использовать тариф по умолчанию

Default

Основной счет пользователя

Настройка по умолчанию

Настройка задает счет пользователя, состояние которого отображается по умолчанию - в агенте и т.д.

Использовать счет пользователя

Использовать коллективный счет

Блокировать остановку работы

Запрещает быструю операцию перевода пользователя в состояние СТОП в мониторе работы.

Помощь < Назад Далее > Отмена

Новый пользователь

Новый пользователь

- Способ подключения
- Способ авторизации
- Наименование
- Авторизация
- Доступ
- Тарификация
- Настройки фильтрации**
- Создать пользователя

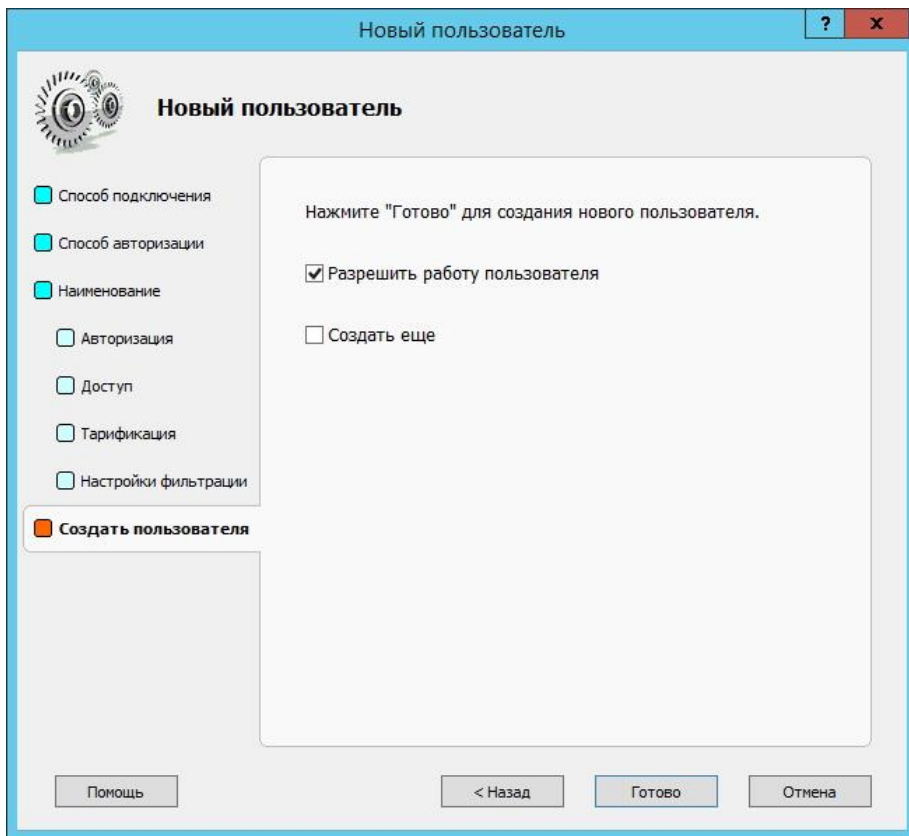
Установить индивидуальный минимальный уровень фильтрации для пользователя (F1-F4)

1 - Баннеры

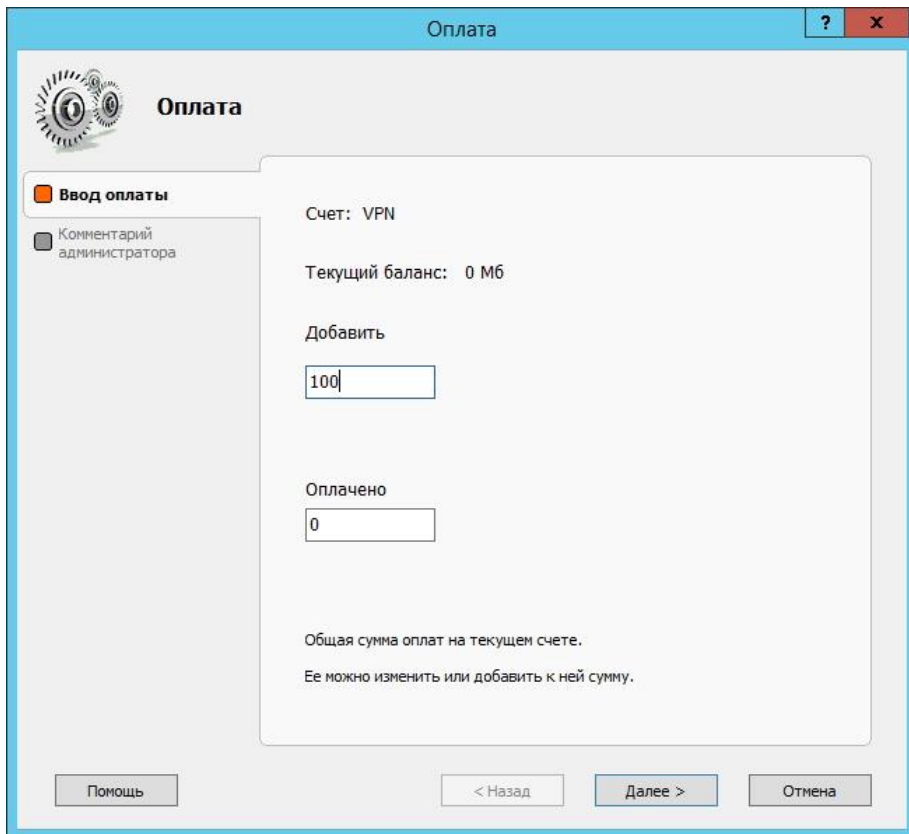
Отключить запрещающие IP правила и внутренний сетевой экран

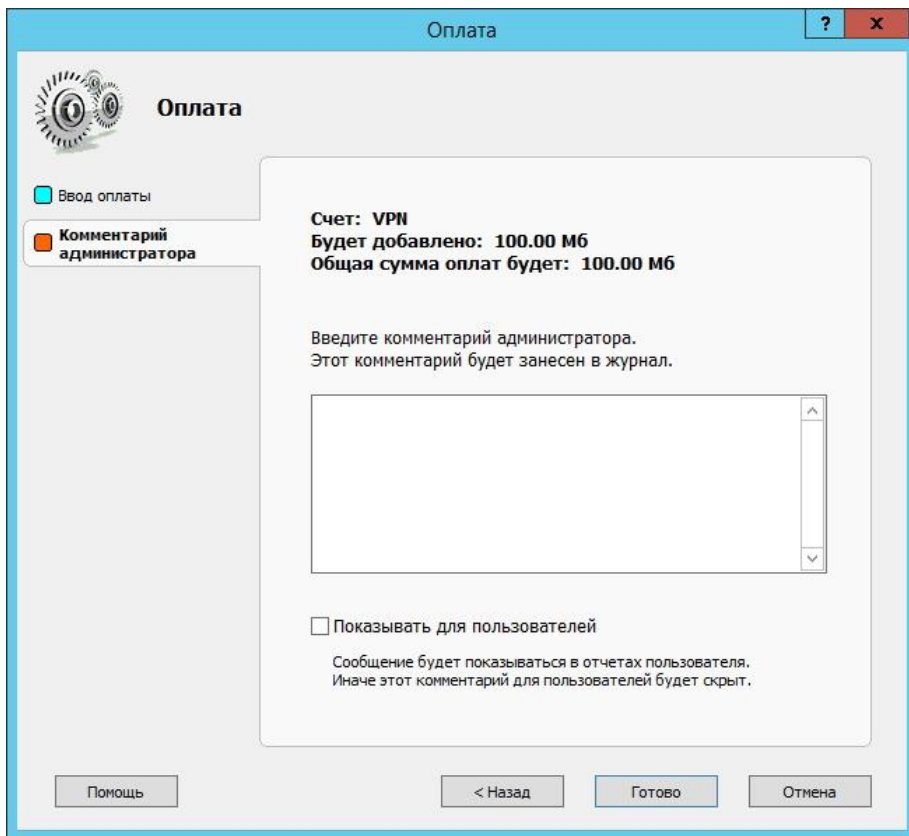
Для этого пользователя не будут действовать IP правила на запрещение и отключается внутренний сетевой экран. Позволяет при удаленном доступе в случае ошибок настройки не потерять контроль за сервером.

Помощь < Назад Далее > Отмена

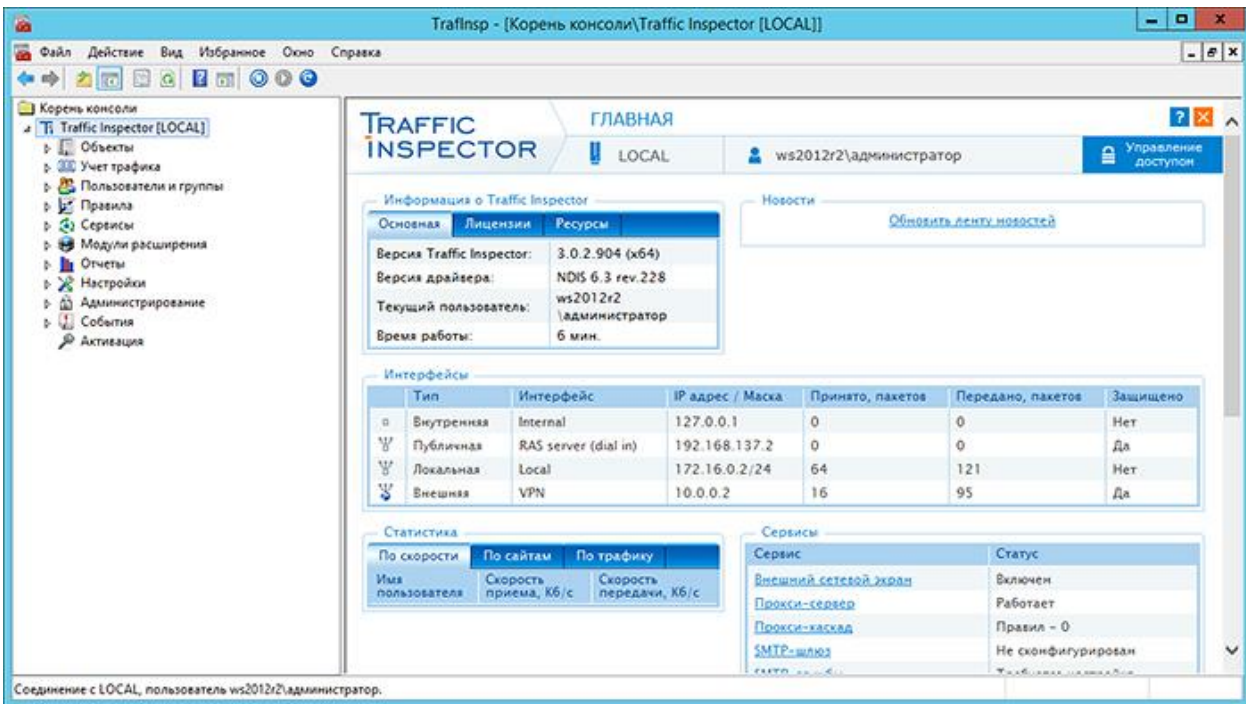


Начисляем баланс клиенту в мониторе работы, если это необходимо.





После подключения VPN в главном окне Traffic Inspector появляется новая сеть «RAS server (dial in)».



На этом настройка завершена.