МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное
учреждения высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«__29__» _____ 2017 г.

КОНТРОЛЬ СЕТЕВОЙ АКТИВНОСТИ ЧЕРЕЗ VPN

Методические указания к лабораторной работе
для студентов укрупненной группы специальностей и
направлений подготовки 10.00.00 «Информационная безопасность»

Курск 2017

УДК 621.(076.1)

Составитель: М.О. Таныгин

Рецензент

Кандидат технических наук, доцент кафедры
«Информационная безопасность» И.В. Калуцкий

Контроль сетевой активности через VPN [Текст] : методические указания к лабораторной работе/ Юго-Зап. гос. ун-т; сост.: М.О. Таныгин. – Курск, 2017. – 32 с.: ил. 30. – Библиогр.: с. 32.

Содержат сведения по вопросам лабораторной работы по основам мониторинга безопасности инфокоммуникационных систем и сетей. Указывается порядок выполнения лабораторной работы, правила оформления отчета.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по специальности.

Предназначены для студентов укрупненной группы специальностей и направлений подготовки 10.00.00 «Информационная безопасность».

Текст печатается в авторской редакции

Подписано в печать 24.11.17. Формат 60x84 1/16.
Усл.печ. л. 1,86. Уч.-изд. л. 1,68. Тираж 100 экз. Заказ. Бесплатно. 2140
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

Краткая теория

Как известно, технология VPN служит для организации прямого безопасного соединения между клиентами (конечным пользователем и корпоративным офисом) или двумя локальными сетями через общедоступный интернет-канал. С помощью VPN удаленные пользователи могут обращаться к серверам предприятия и связываться с различными офисами своей компании.

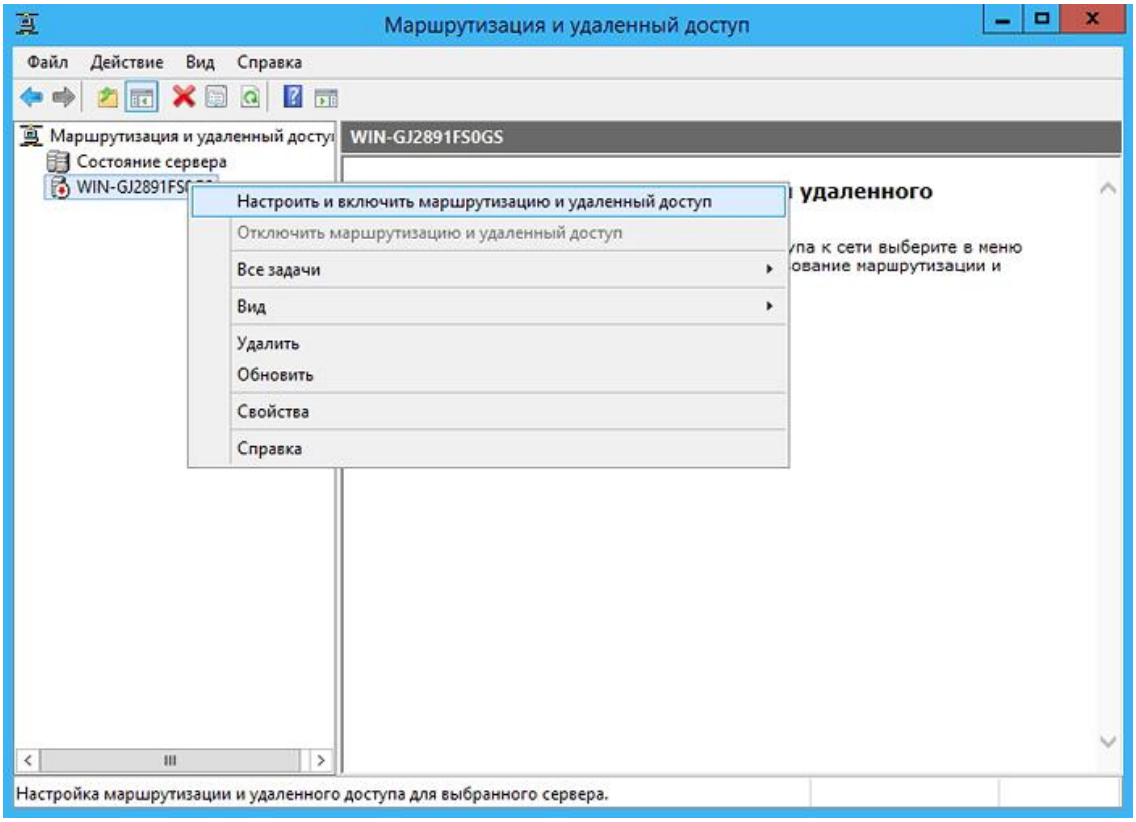
Для VPN не нужны выделенные линии, поэтому пользоваться ею может каждый, кто располагает доступом к Интернету. Как только соединение установлено, сотрудник может работать со всеми сетевыми ресурсами, как если бы он находился в офисе. Но, пожалуй, важнейшее преимущество этой технологии заключается в том, что, несмотря на общедоступную инфраструктуру, прямое соединение VPN (так называемый VPN-туннель) защищено столь надежно, что украсть данные или получить несанкционированный доступ к географически распределенной сети практически невозможно.

Организация VPN-туннеля может обеспечить высокую скорость и безопасность подключения в корпоративной сети, гарантированную полосу пропускания, а также экономию средств на сетевой инфраструктуре. Вместе с тем, проблема сетевой безопасности остается актуальной и для VPN. Traffic Inspector восполняет этот пробел, позволяя оперативно контролировать работу пользователей в Интернете и подключения к корпоративному серверу, в том числе задавать квоты на трафик, ограничивать доступ к определенным ресурсам, настраивать различные уровни фильтрации для пользователей и многое другое. При этом от системного администратора не требуется каких-либо специальных знаний — вся настройка выполняется в Консоли управления Windows (MMC) с помощью удобных пошаговых мастеров.

Выполнение работы
Настройка VPN-сервера

Итак, теперь мы знаем общий порядок настройки и можем переходить к описанию конкретных действий. Для примера мы взяли систему Windows Server 2012, но все то же самое применимо и для более ранних версий (Windows 2003 и 2008).

В службе **Маршрутизация и удаленный доступ** щелкните правой кнопкой мыши свой сервер и выберите пункт **Настроить и включить маршрутизацию и удаленный доступ.**

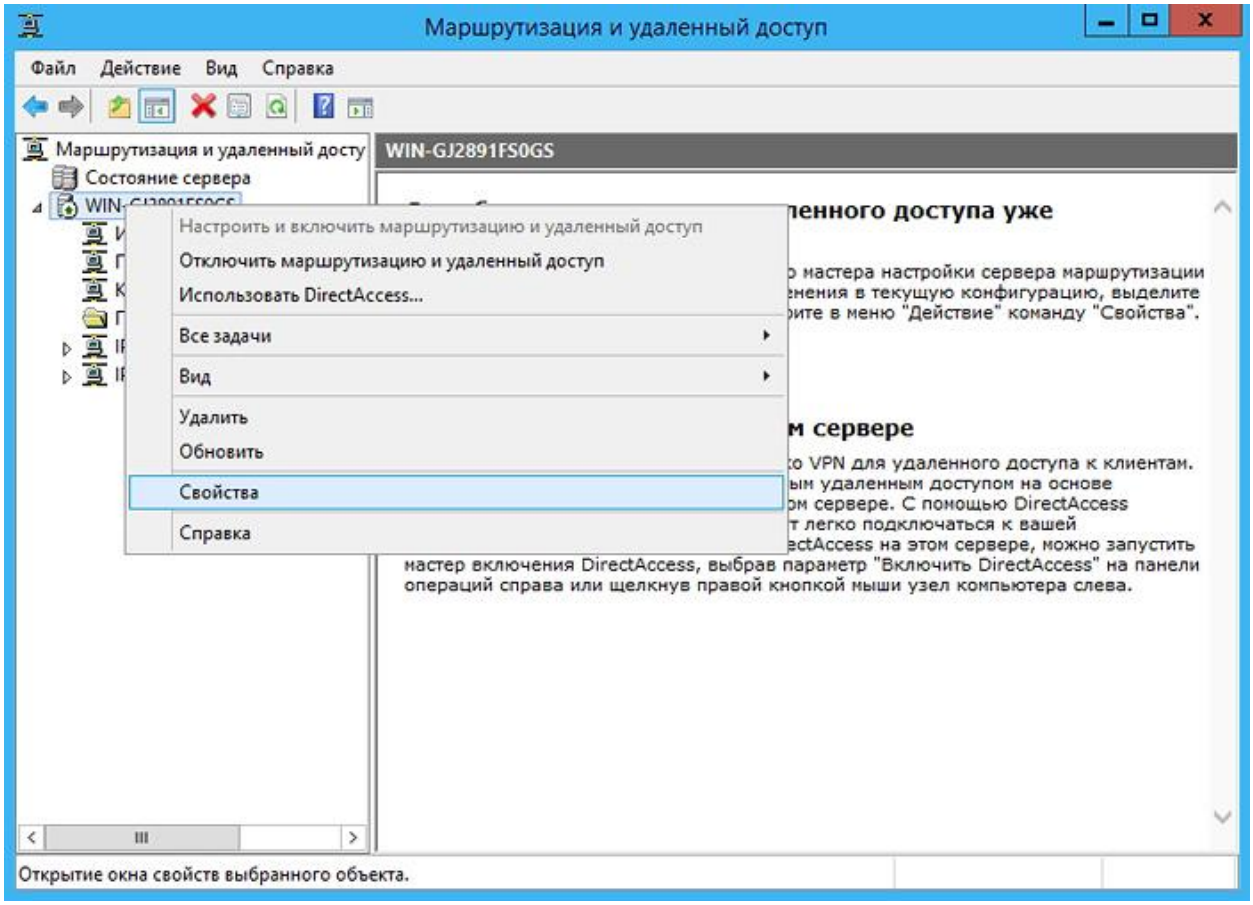


В открывшемся мастере установки сервера маршрутизации и удаленного доступа нажмите **Далее** и выберите вариант **Особая конфигурация.**

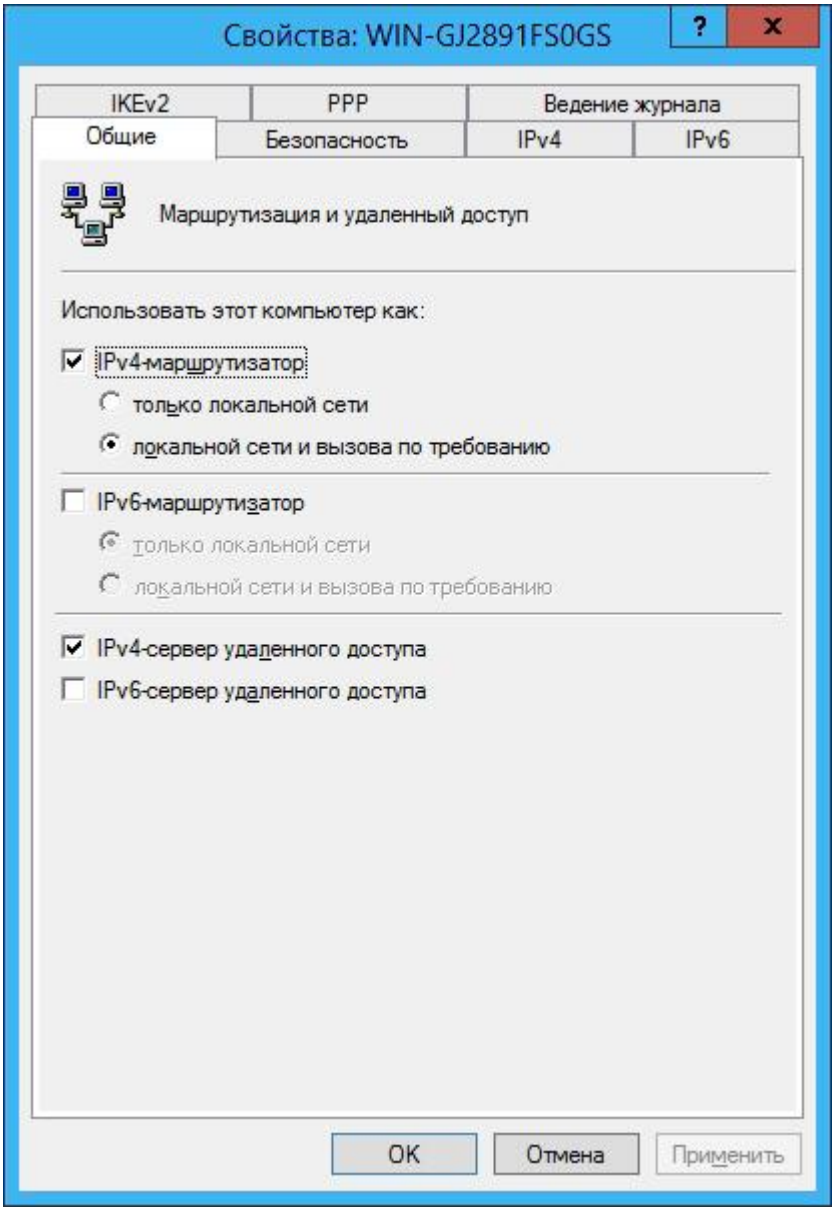
В следующем окне выберите **Доступ к виртуальной частной сети (VPN), Преобразование сетевых адресов (NAT), Маршрутизация локальной сети** и нажмите **Далее.**

В последнем окне мастера нажмите кнопку **Готово** и запустите службу.

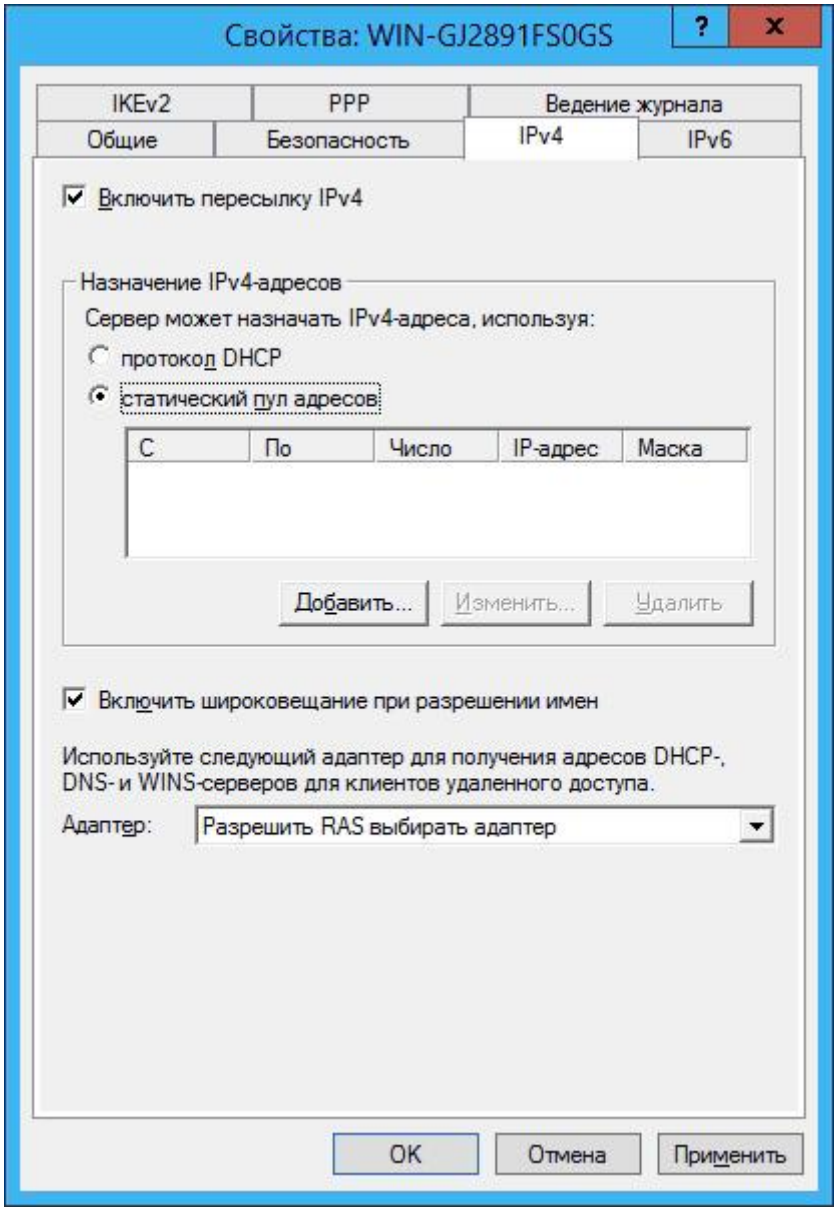
Теперь зайдите в свойства сервера:



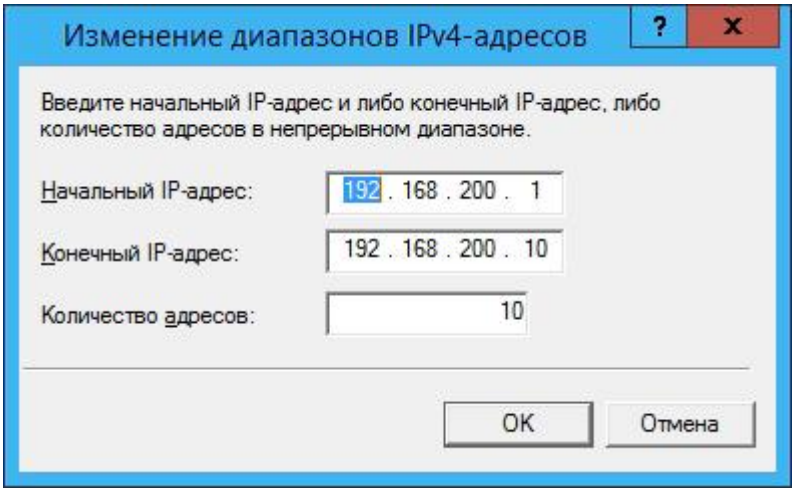
и на вкладке **Общие** задайте следующие параметры:



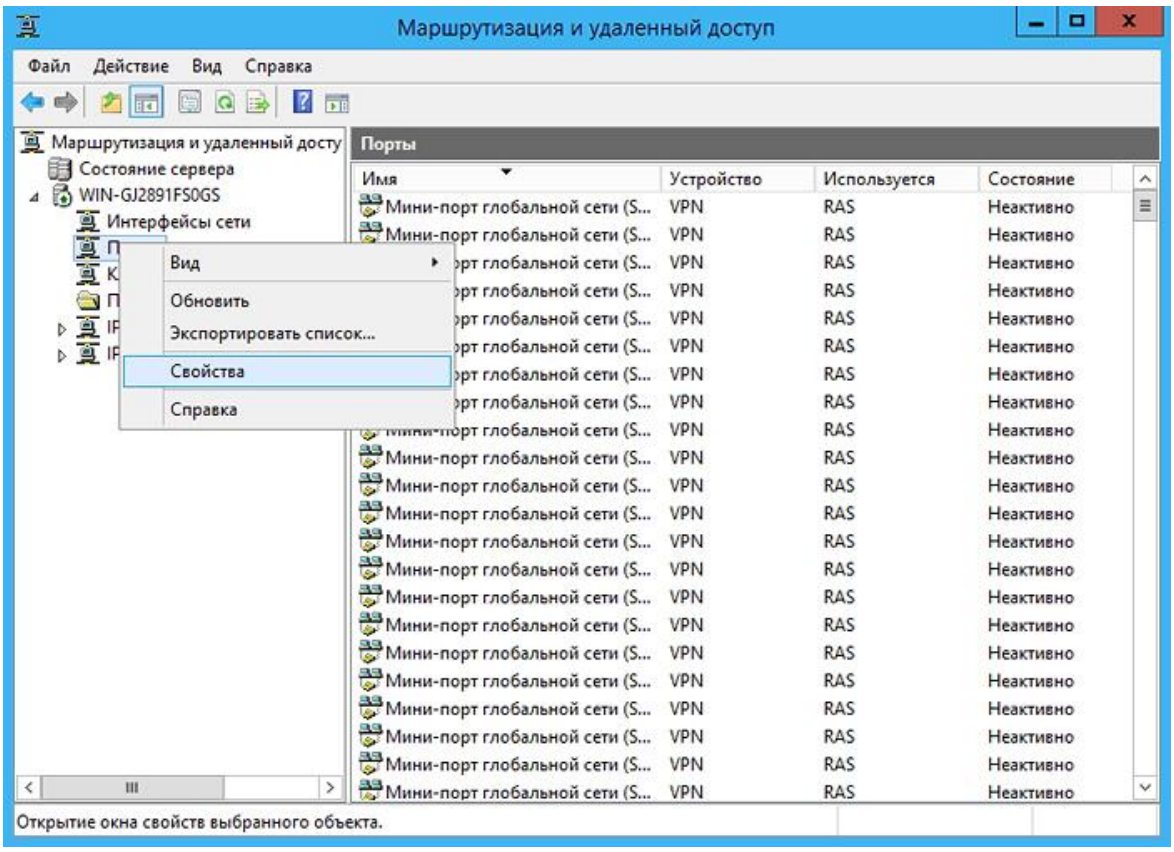
Перейдите на вкладку **IPv4** и выберите статический пул адресов: 4



Нажмите кнопку **Добавить** и назначьте 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):

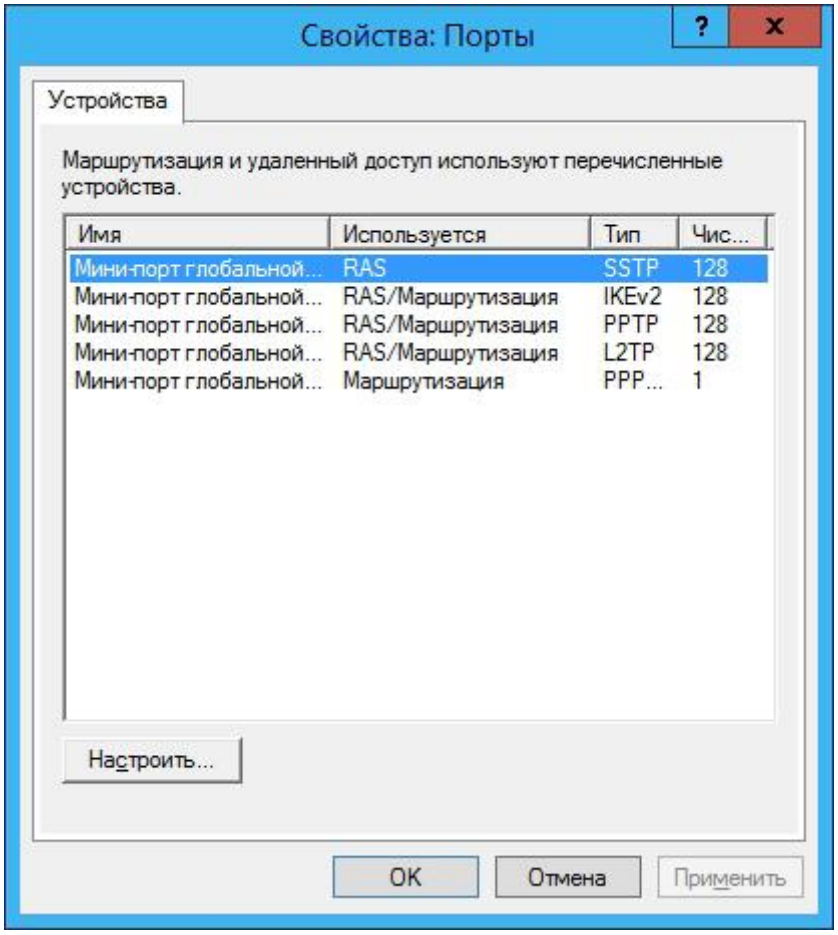


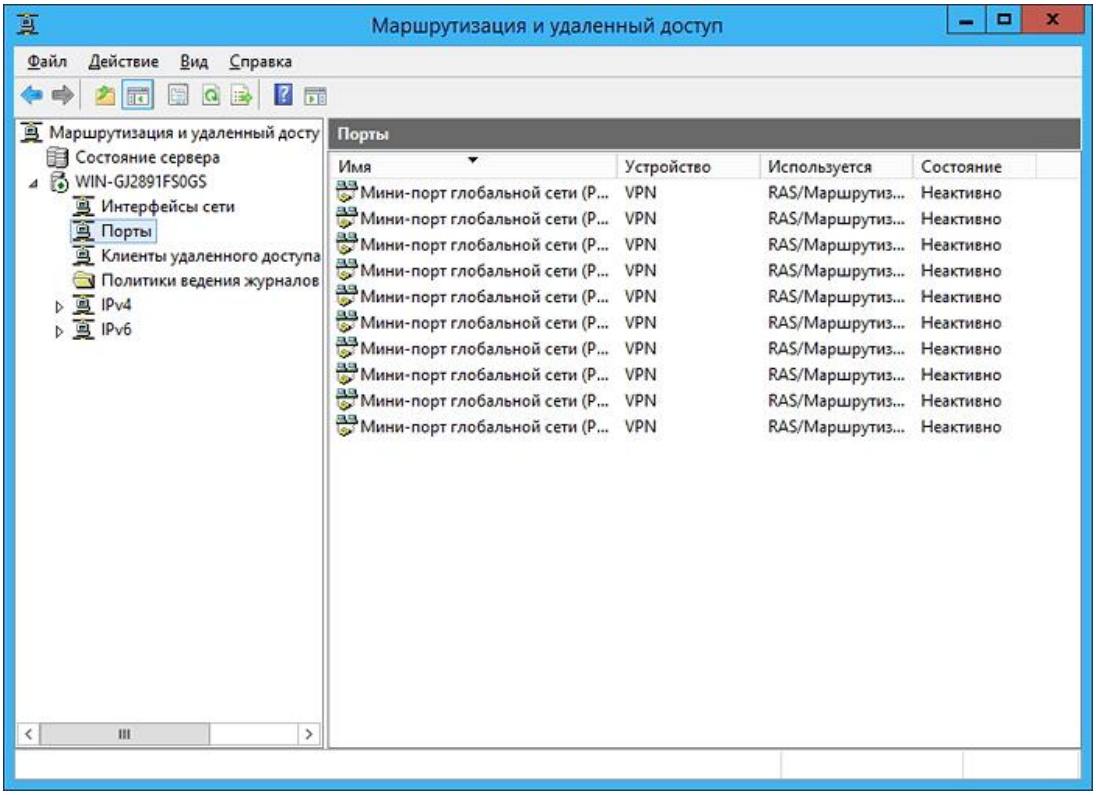
Перейдите на вкладку **Ведение журнала** и установите флажок в поле **Вести журнал ошибок и предупреждений.** Щелкните правой кнопкой мыши **Порты** и выберите пункт **Свойства**:



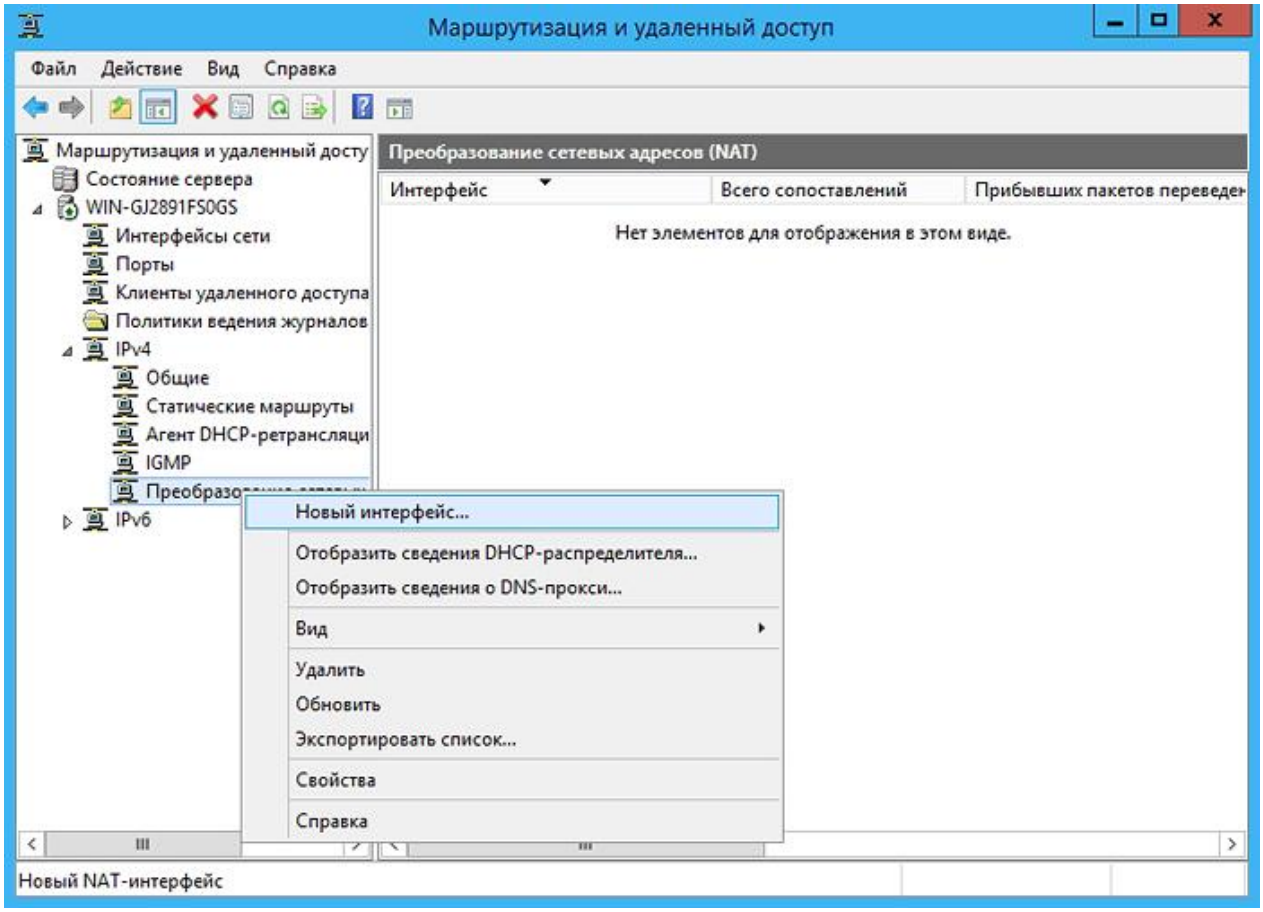
Для стабильной работы сервера рекомендуется удалить ненужные порты (SSTP, PPOE, L2TP, IKEv2) и создать

необходимое количество портов PPTP (в нашем случае нужно 10 таких портов):



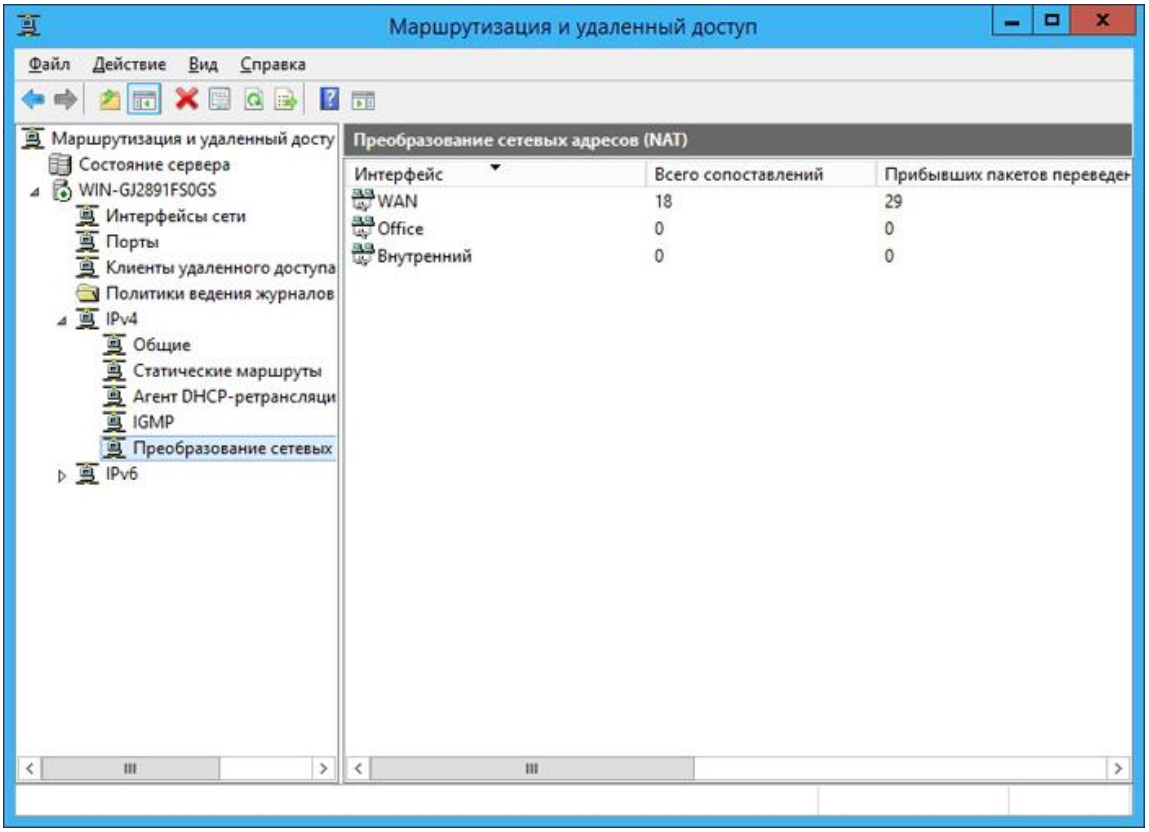


Перейдите к элементу **Преобразование сетевых адресов (NAT)** и добавьте новый интерфейс:



Выберите подключение к Интернету и установите флажки в полях **общий интерфейс подключен к интернету** и **Включить NAT на данном интерфейсе**.

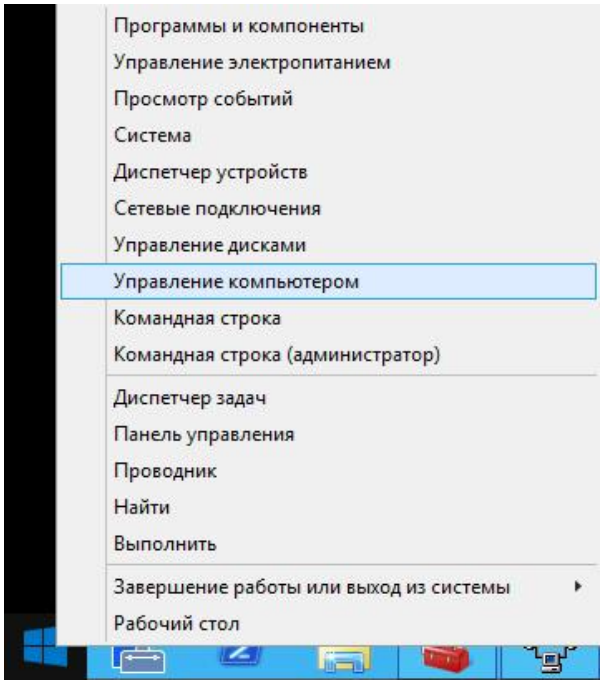
Затем пометьте интерфейс локальной сети как **«Частный интерфейс подключен к частной сети»**, а внутренний интерфейс — **как Частный интерфейс подключен к частной сети**. Получится примерно следующее:



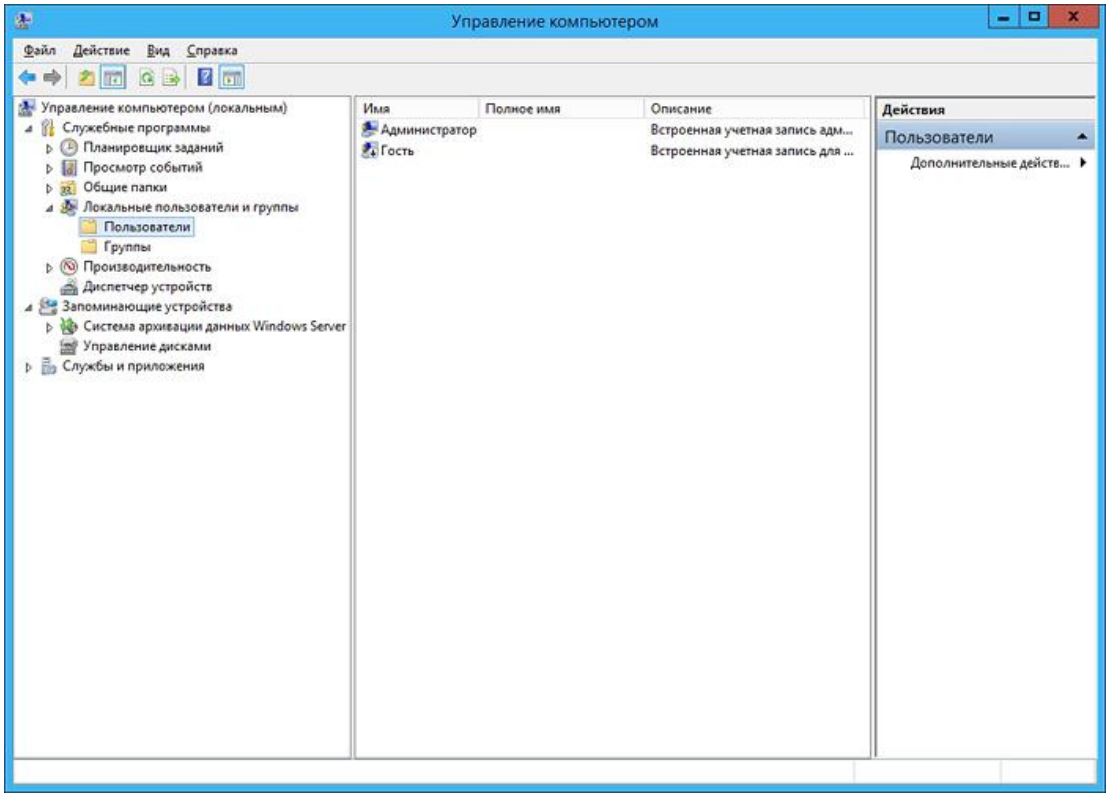
На этом настройка VPN-сервера в головном офисе завершена, и можно переходить к настройке VPN-клиентов в филиале.

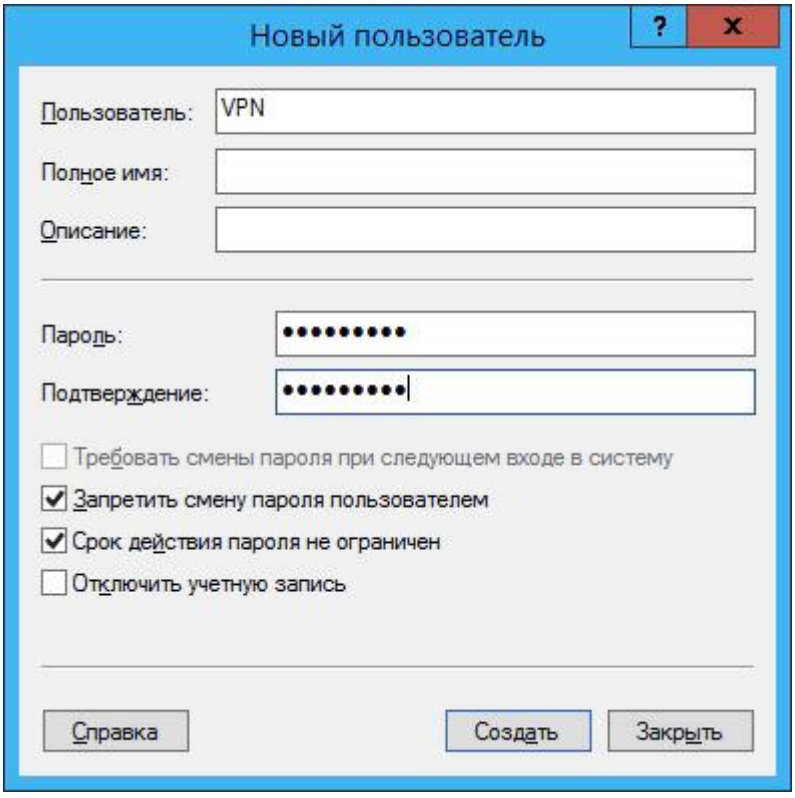
Настройка VPN-клиентов

На серверной стороне запустите управление компьютером:

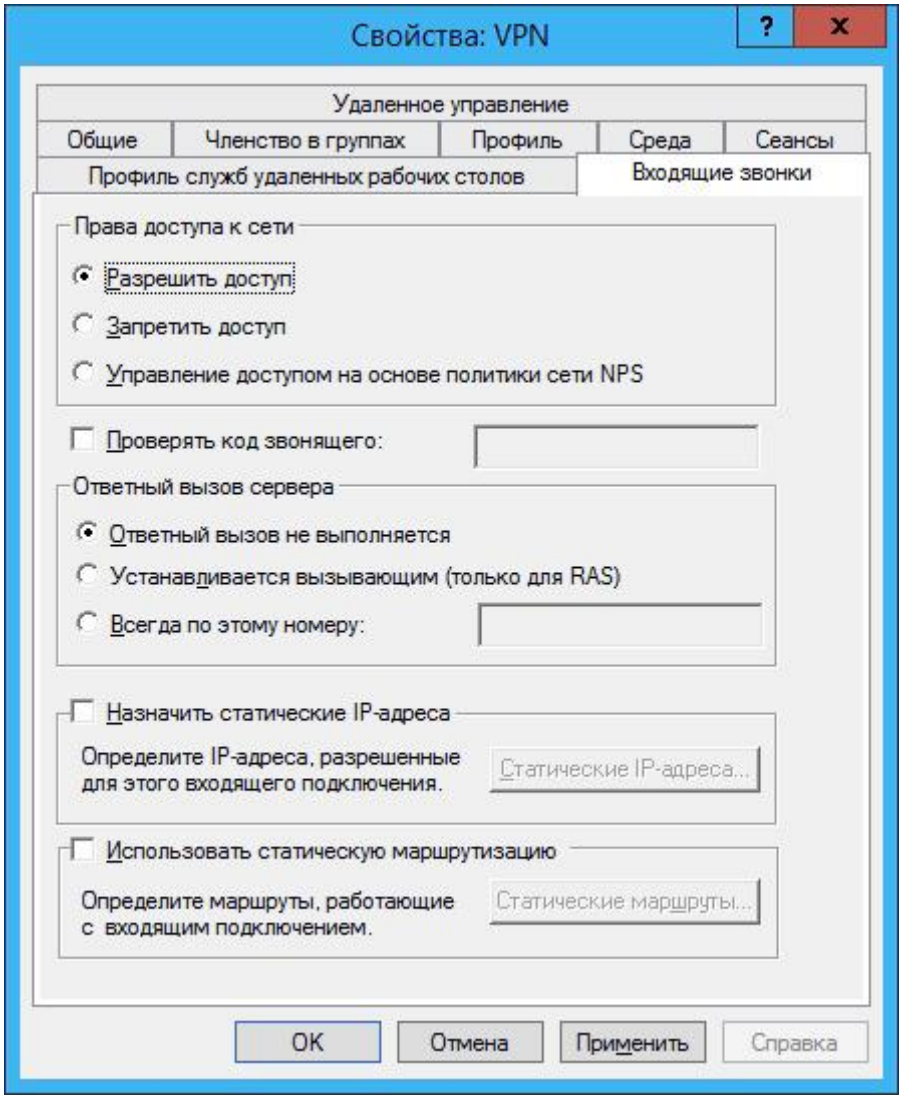


и в разделе **Локальные пользователи и группы — Пользователи** добавьте нового пользователя и укажите его учетные данные:

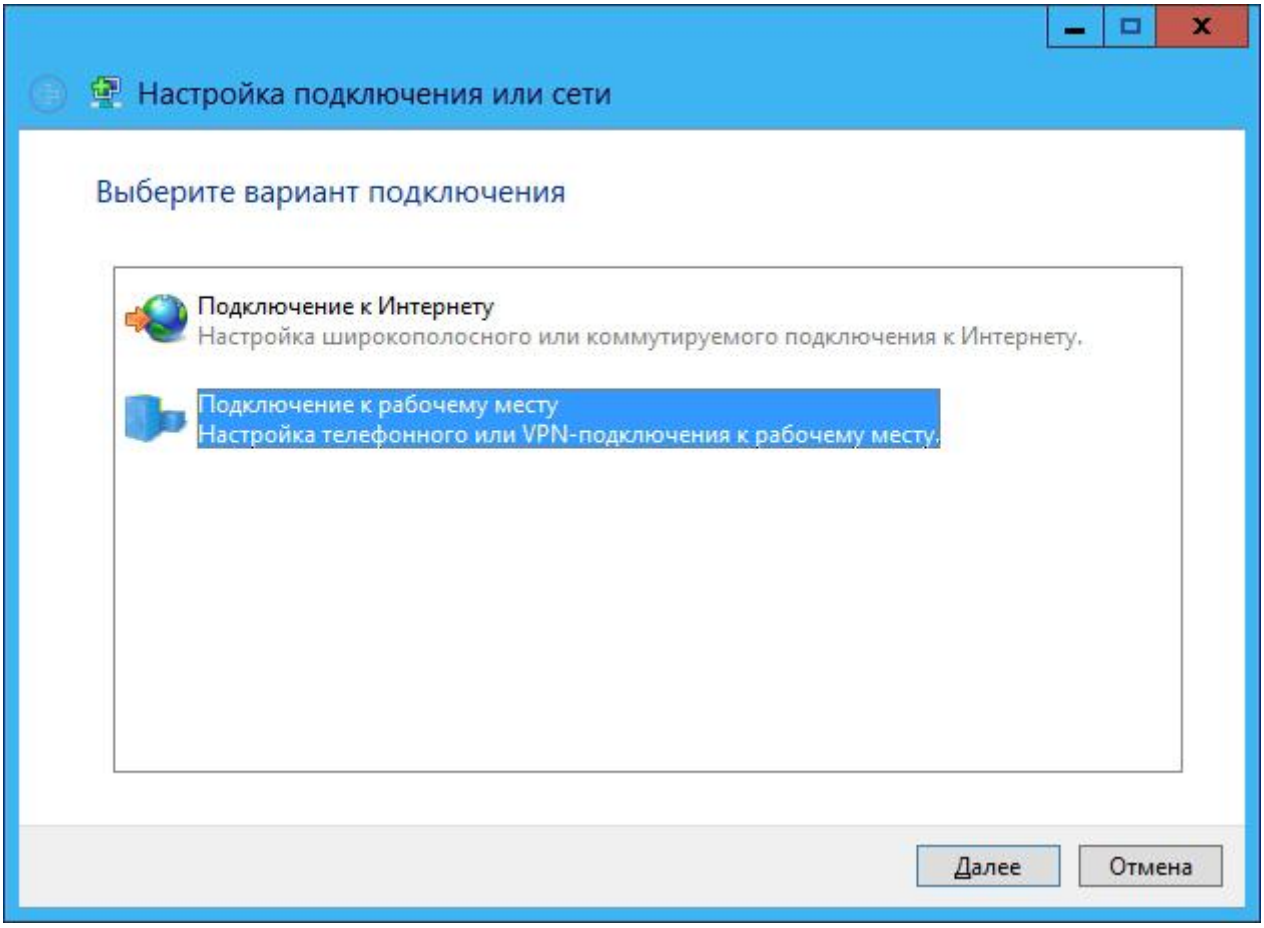




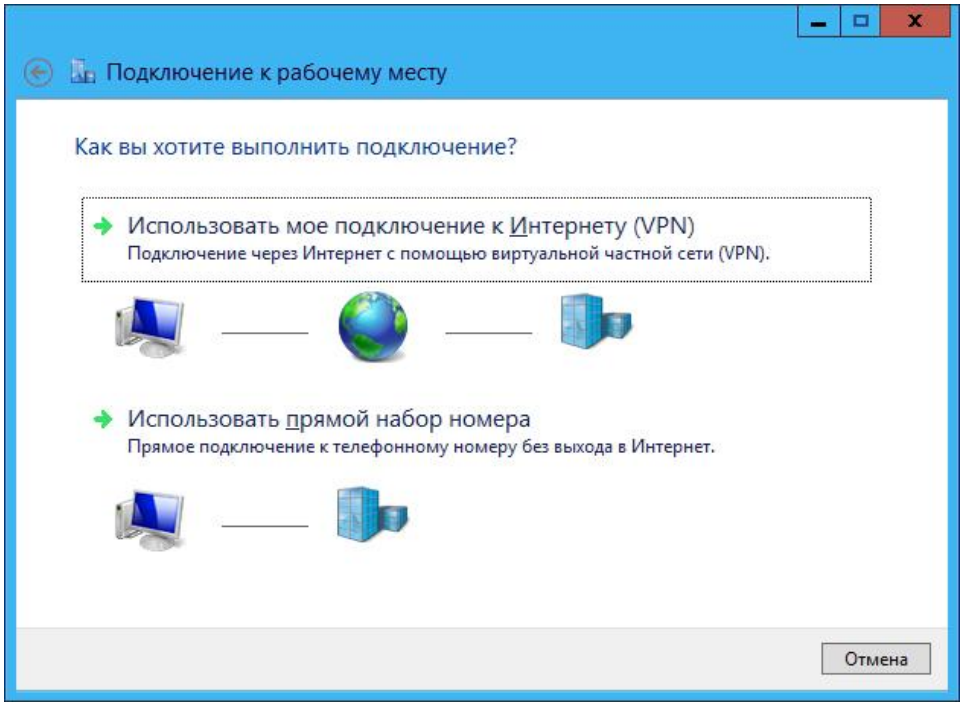
Перейдите в свойства пользователя на вкладку **Входящие звонки** и укажите настройки, как показано на рисунке (пользователю можно также назначить статический IP):



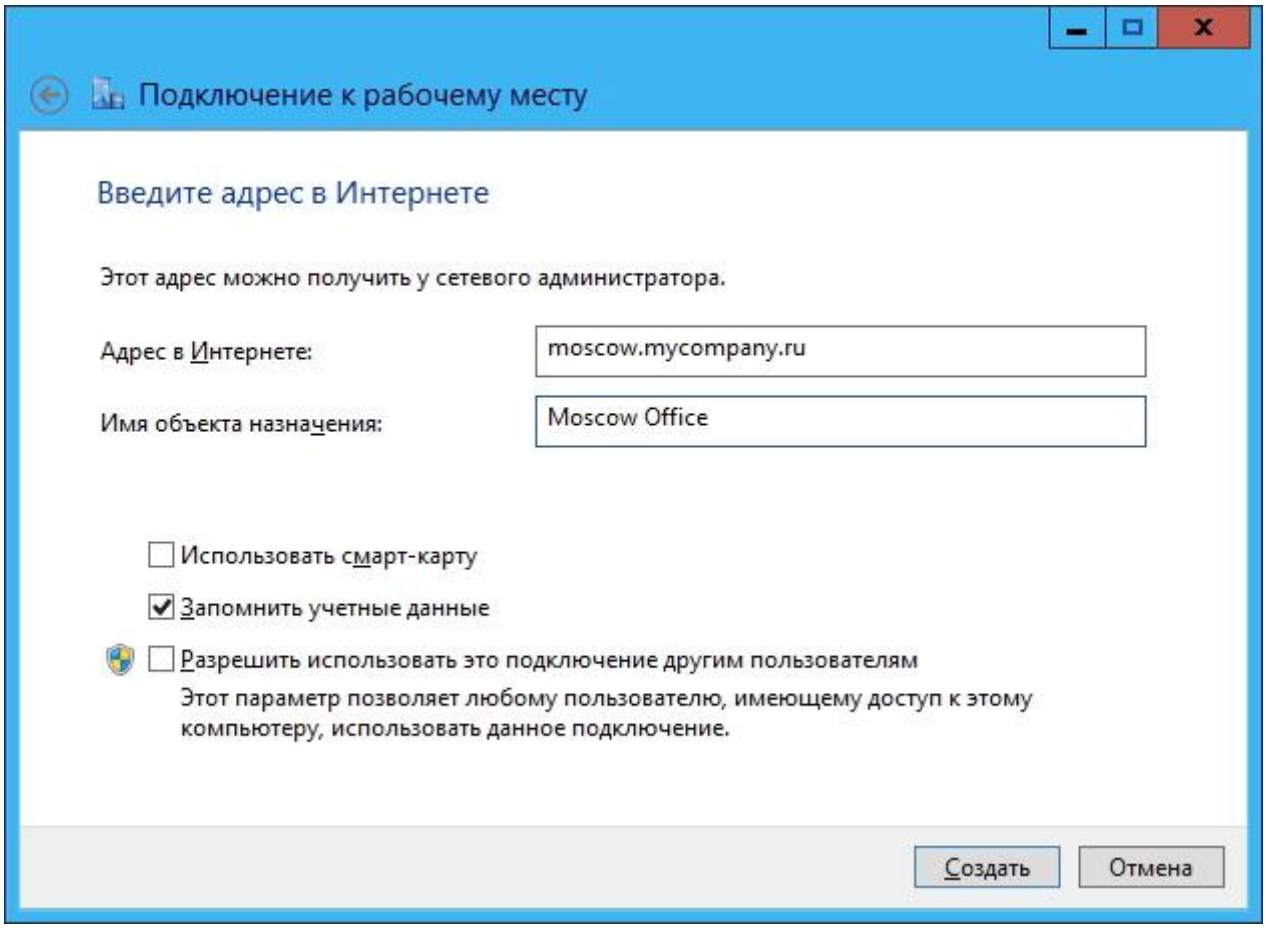
Теперь на стороне клиента создайте VPN-подключение средствами операционной системы (в качестве примера возьмем ОС Windows 8). Для этого в Центре управления сетями и общим доступом выберите вариант **Настройка нового подключения или сети** и в открывшемся мастере настройки выберите **Подключение к рабочему месту**:



Выберите **Использовать мое подключение к Интернету (VPN)** и нажмите **Далее**:



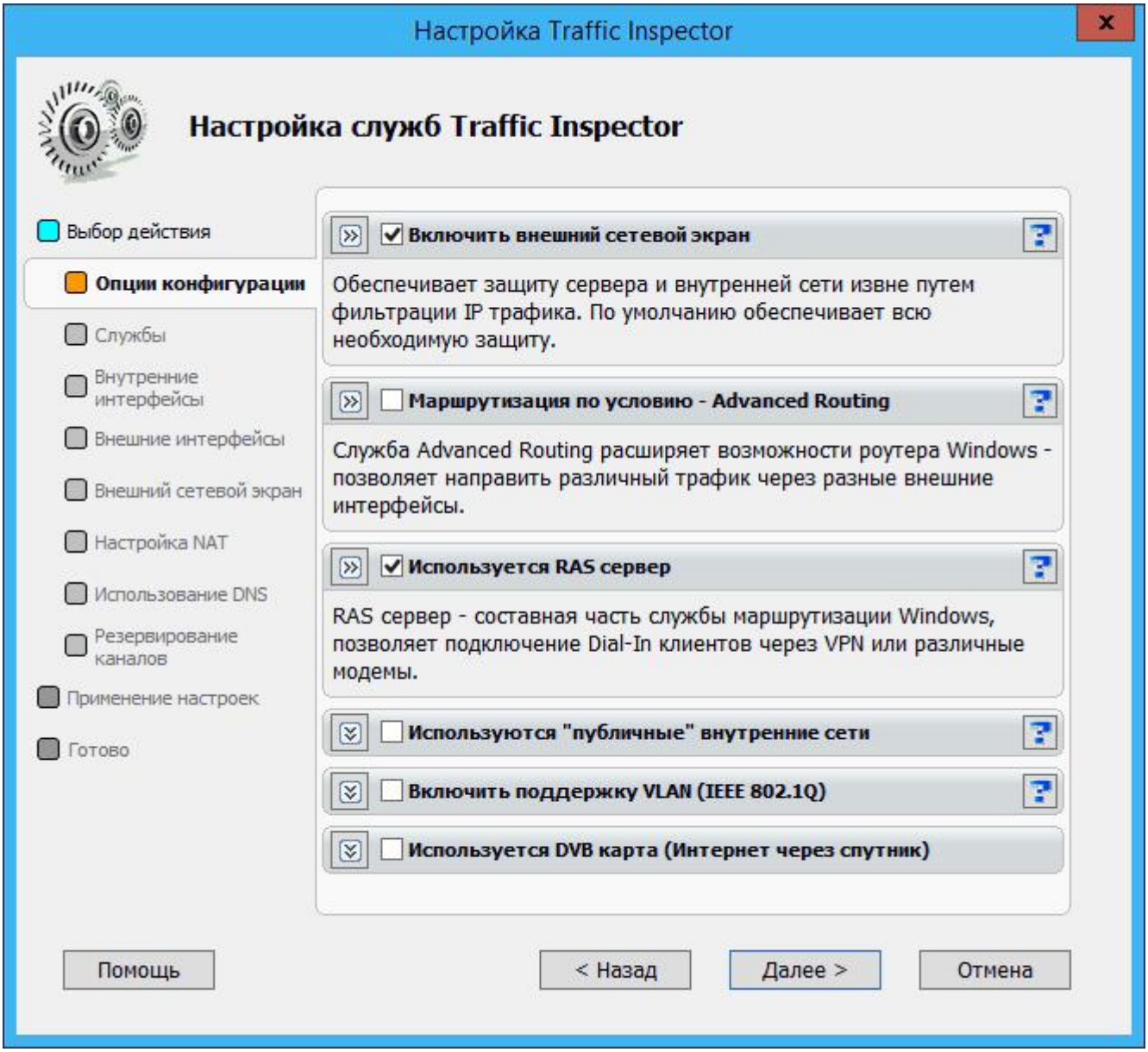
Затем введите URL или IP-адрес VPN-сервера, укажите название его местоположения и нажмите кнопку **Создать**:



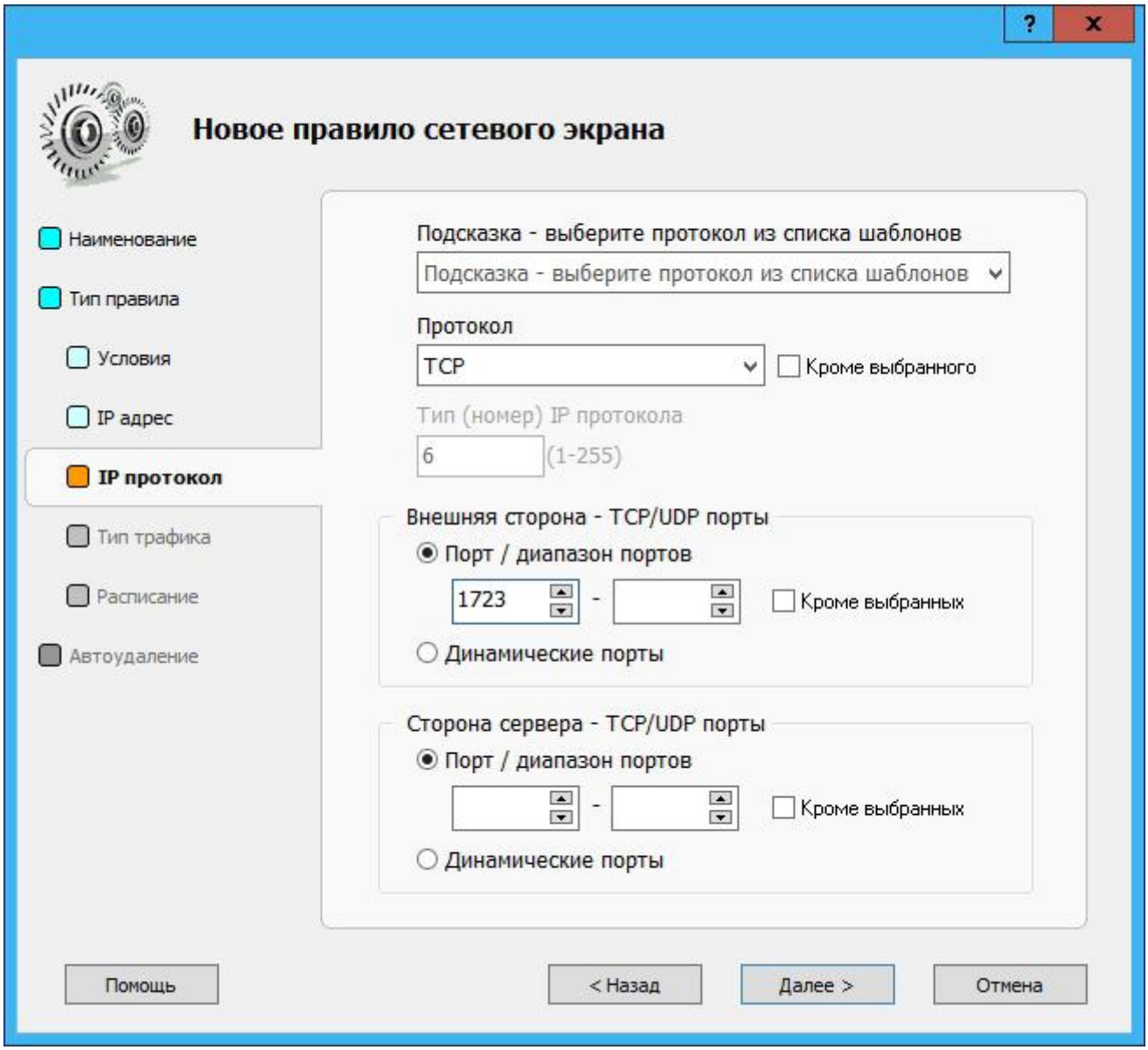
Настройка Traffic Inspector на VPN-сервере

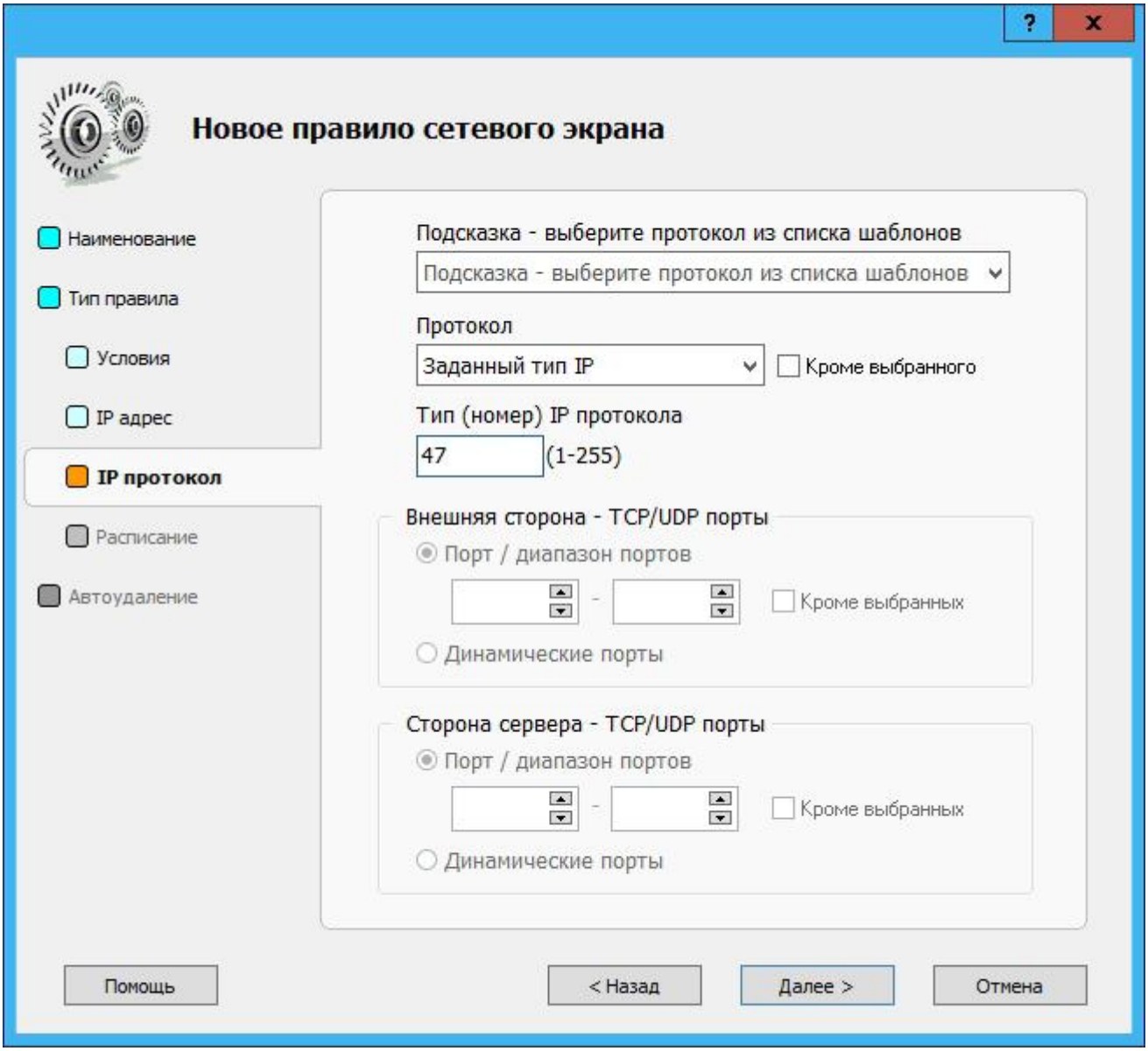
После настройки VPN-сервера и клиентов можно переходить к установке и конфигурированию самого Traffic Inspector'а. Обратите внимание, что Traffic Inspector устанавливается только на этом этапе, поэтому работоспособность VPN необходимо проверить заранее стандартными средствами Windows (ping, netstat, tracert и т. д.).

В конфигураторе **Traffic Inspector** в настройках служб установите флажок **Используется RAS сервер**:



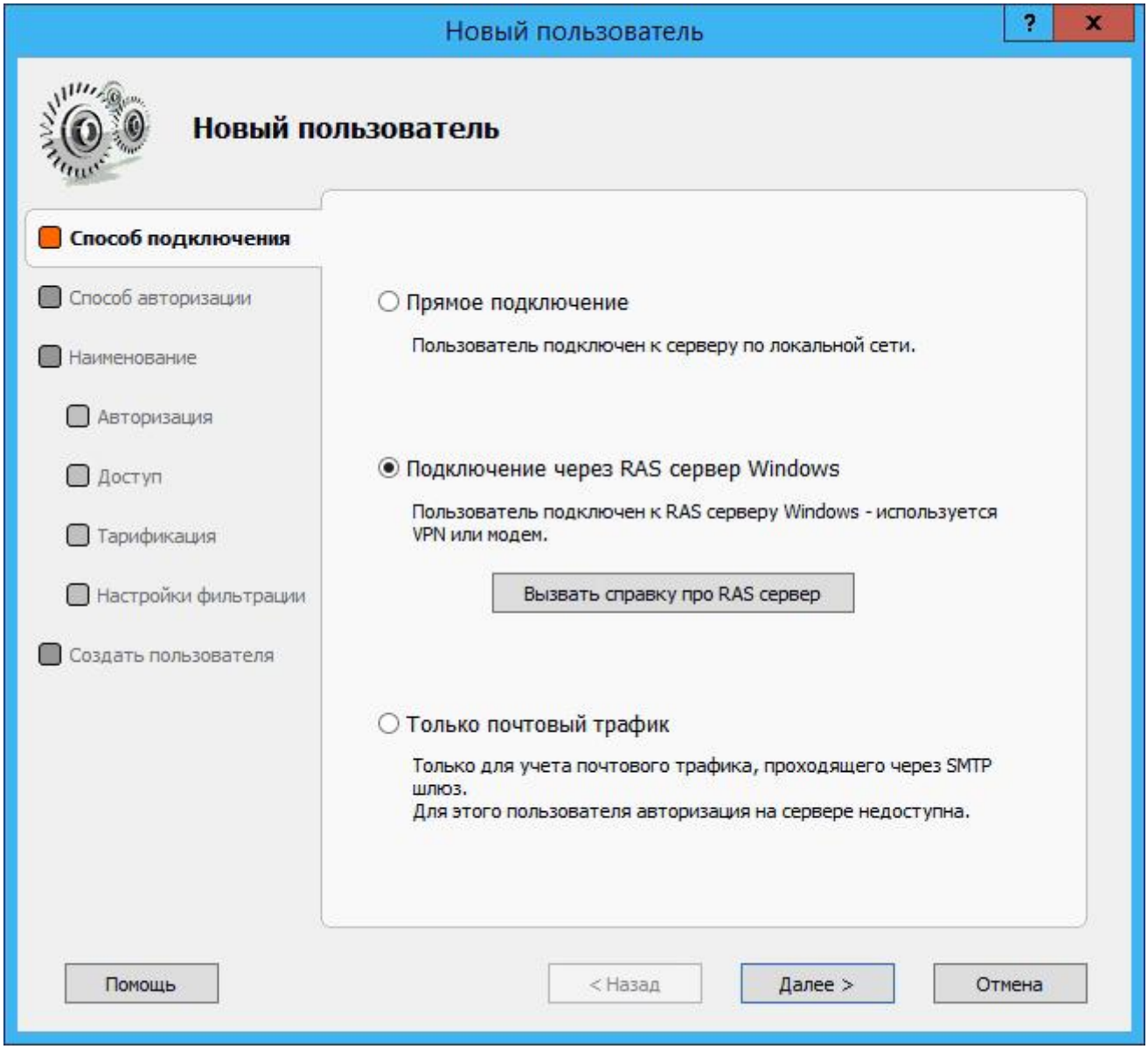
В разделе **Правила внешнего сетевого экрана** в Traffic Inspector создайте два правила — в одном правиле разрешите подключение по TCP на порт 1723 для внешних клиентов, а во втором правиле разрешите подключения по протоколу GRE (вариант **Заданный тип IP**, номер **47**):



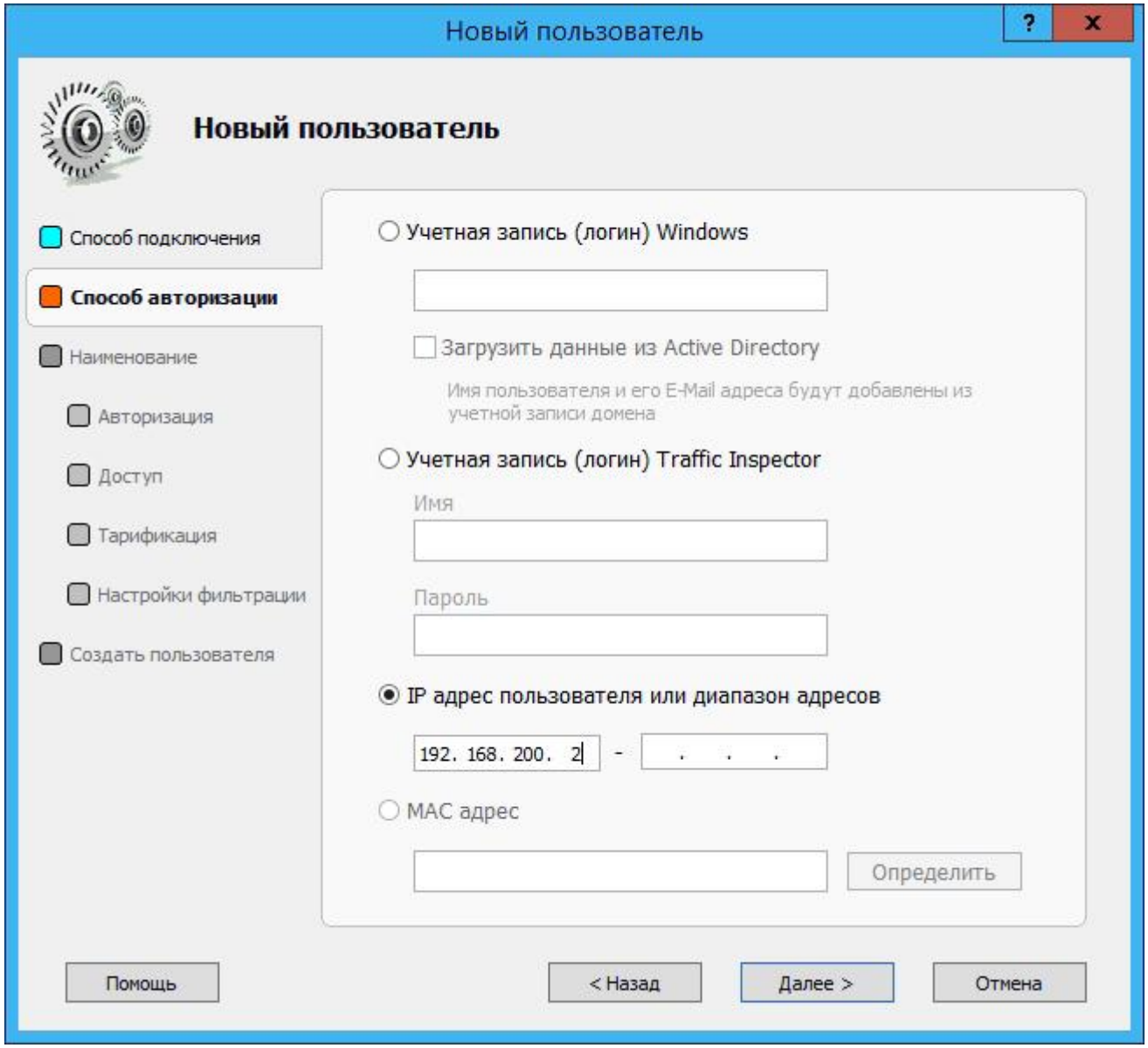


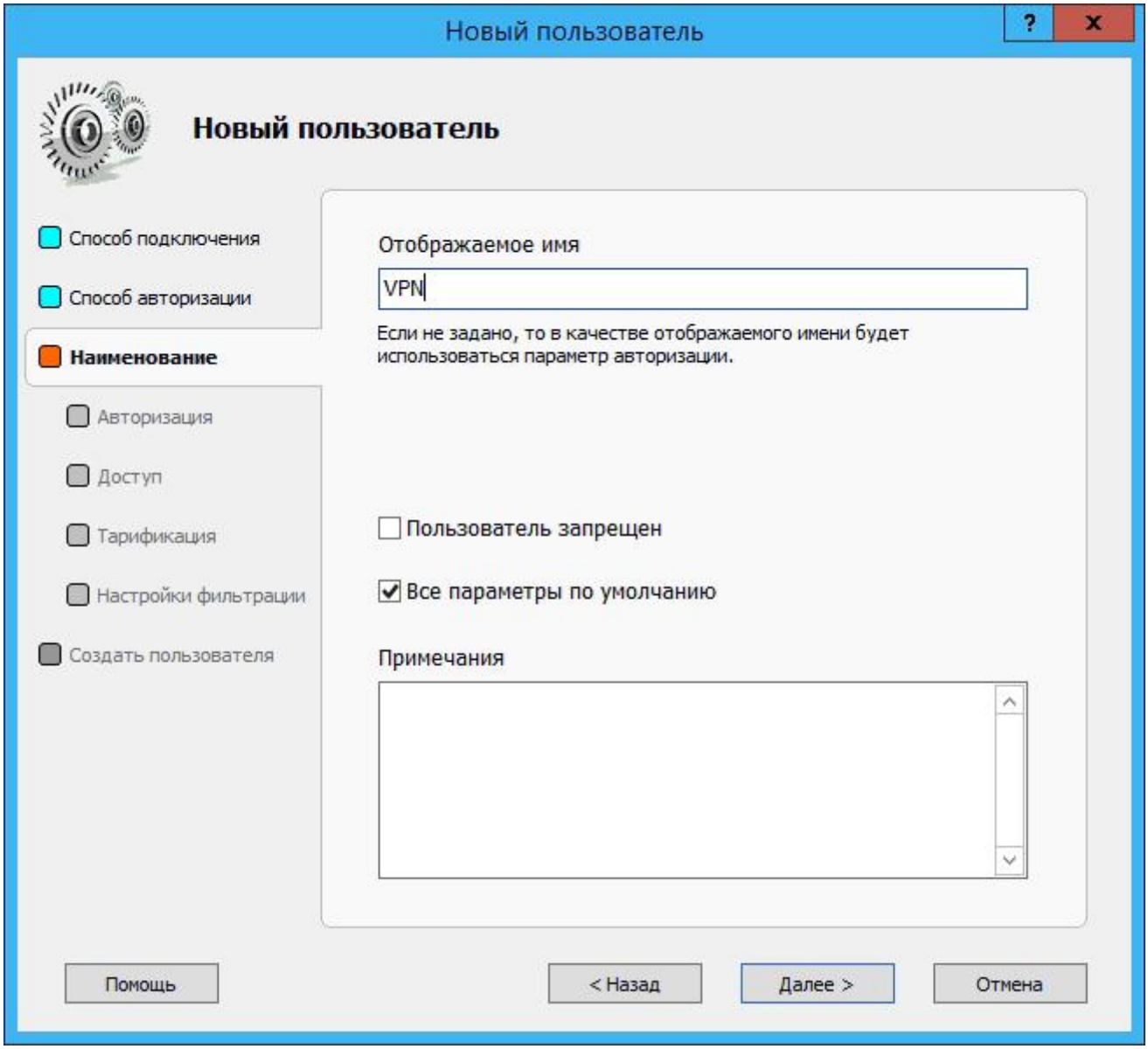
Остальные параметры можно не изменять и оставить значения по умолчанию.

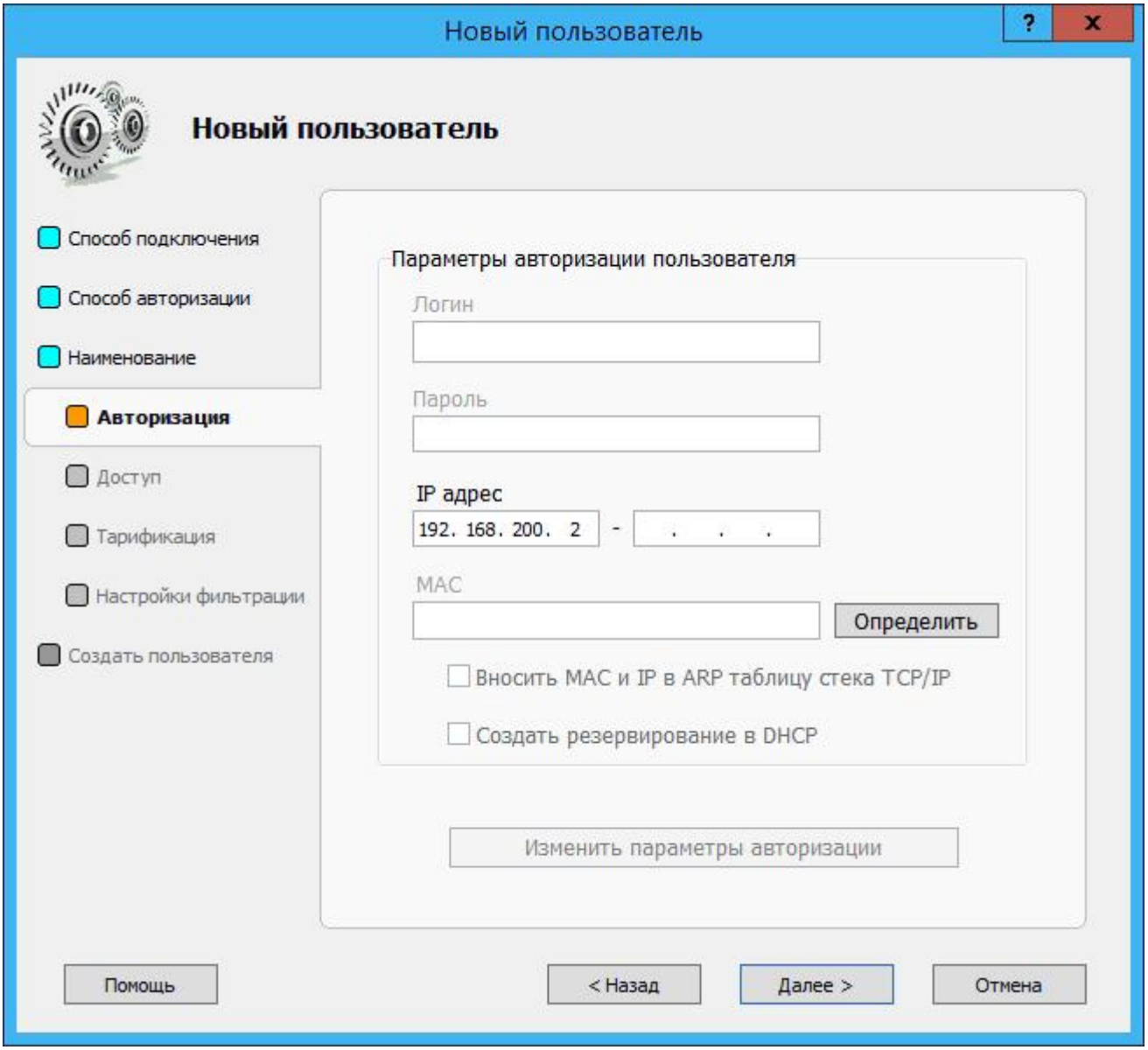
Добавьте в программу нового клиента и укажите способ подключения **Подключение через RAS сервер Windows**:



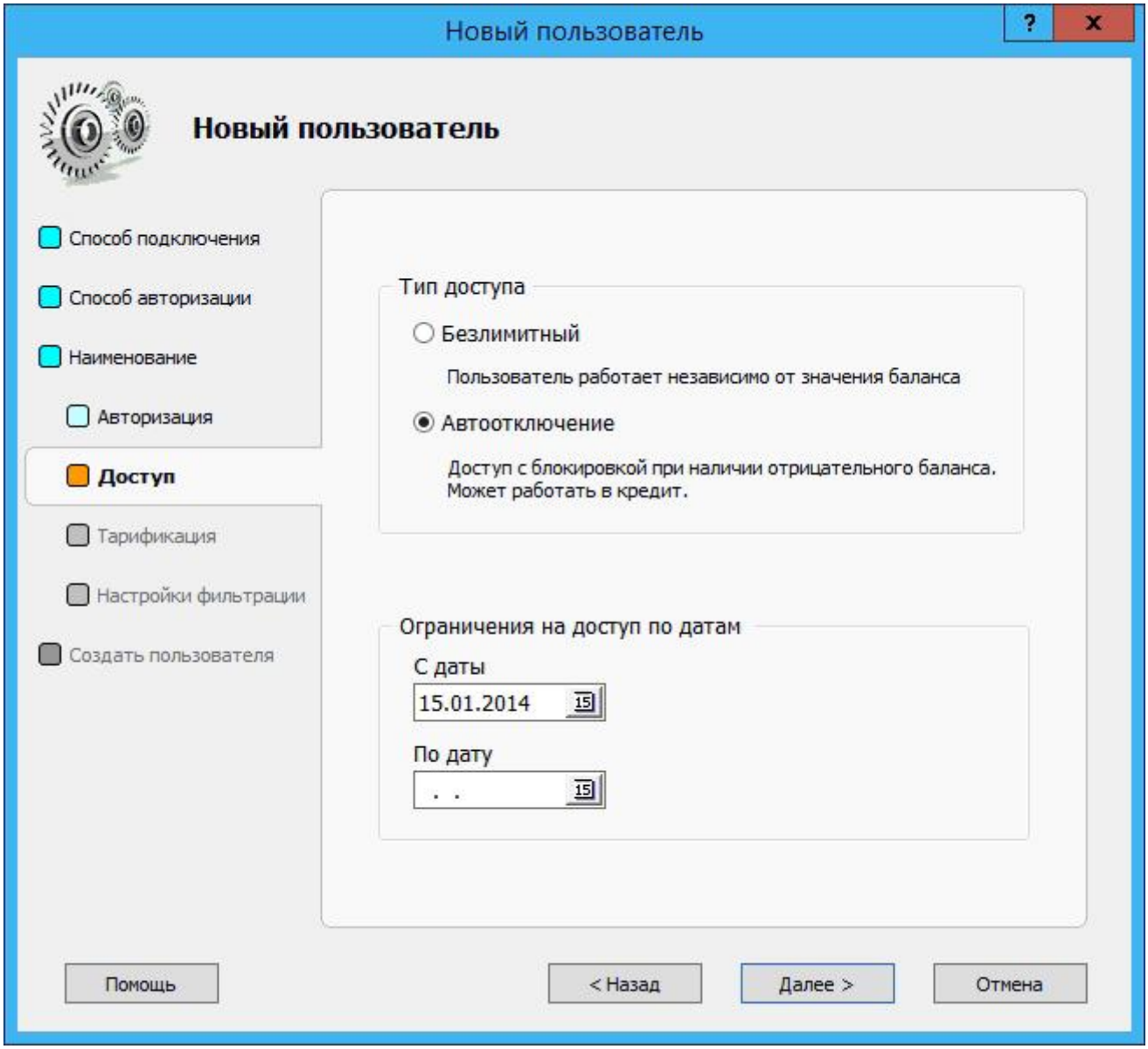
Остальные настройки аналогичны настройкам клиентов программы. В данном случае использована авторизация по IP:

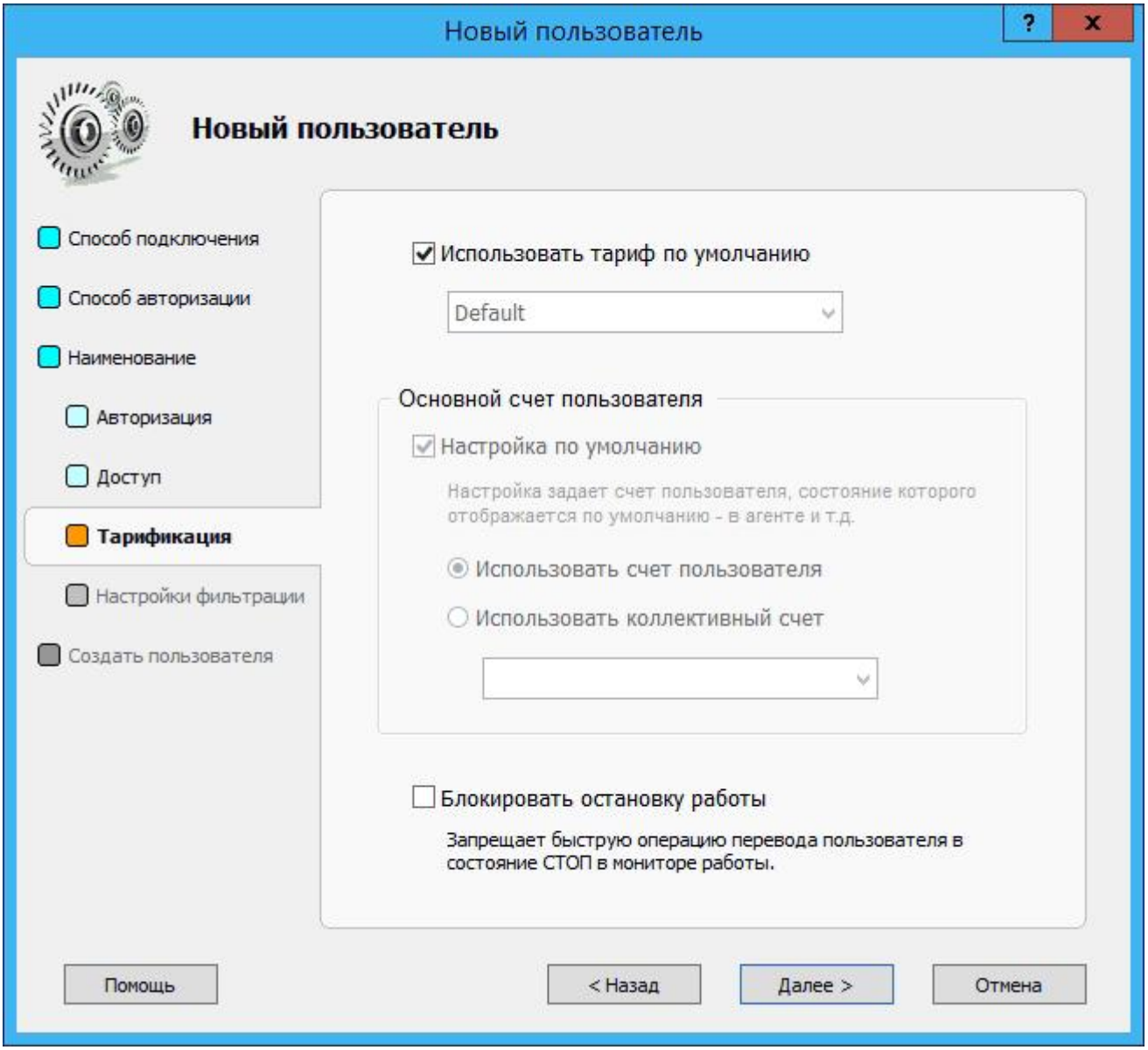

Новый пользователь
Новый пользователь
Способ подключения
Способ авторизации
Наименование
Авторизация
Доступ
Тарификация
Настройки фильтрации
Создать пользователя
Учетная запись (логин) Windows
Загрузить данные из Active Directory
Имя пользователя и его E-Mail адреса будут добавлены из учетной записи 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

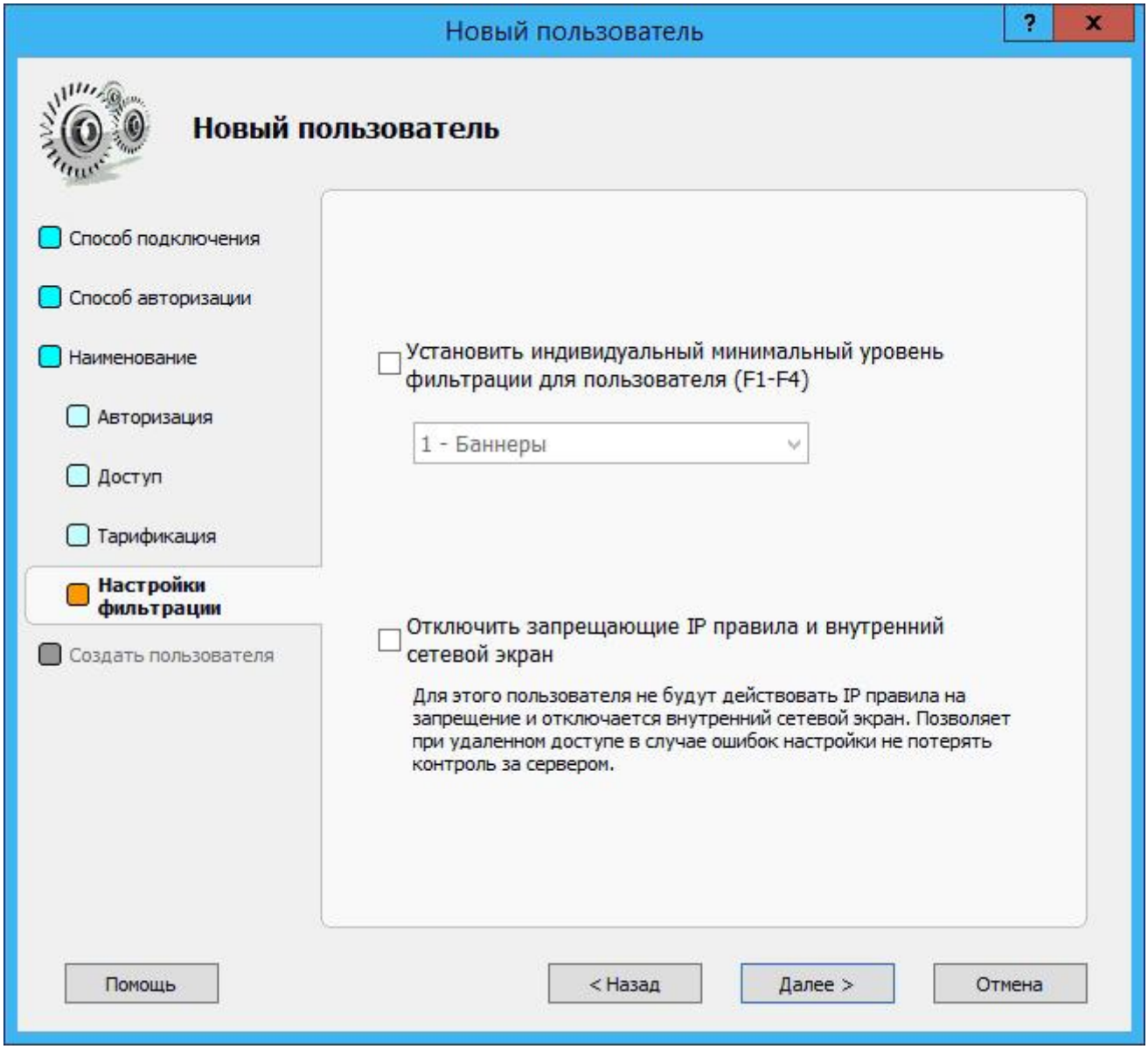


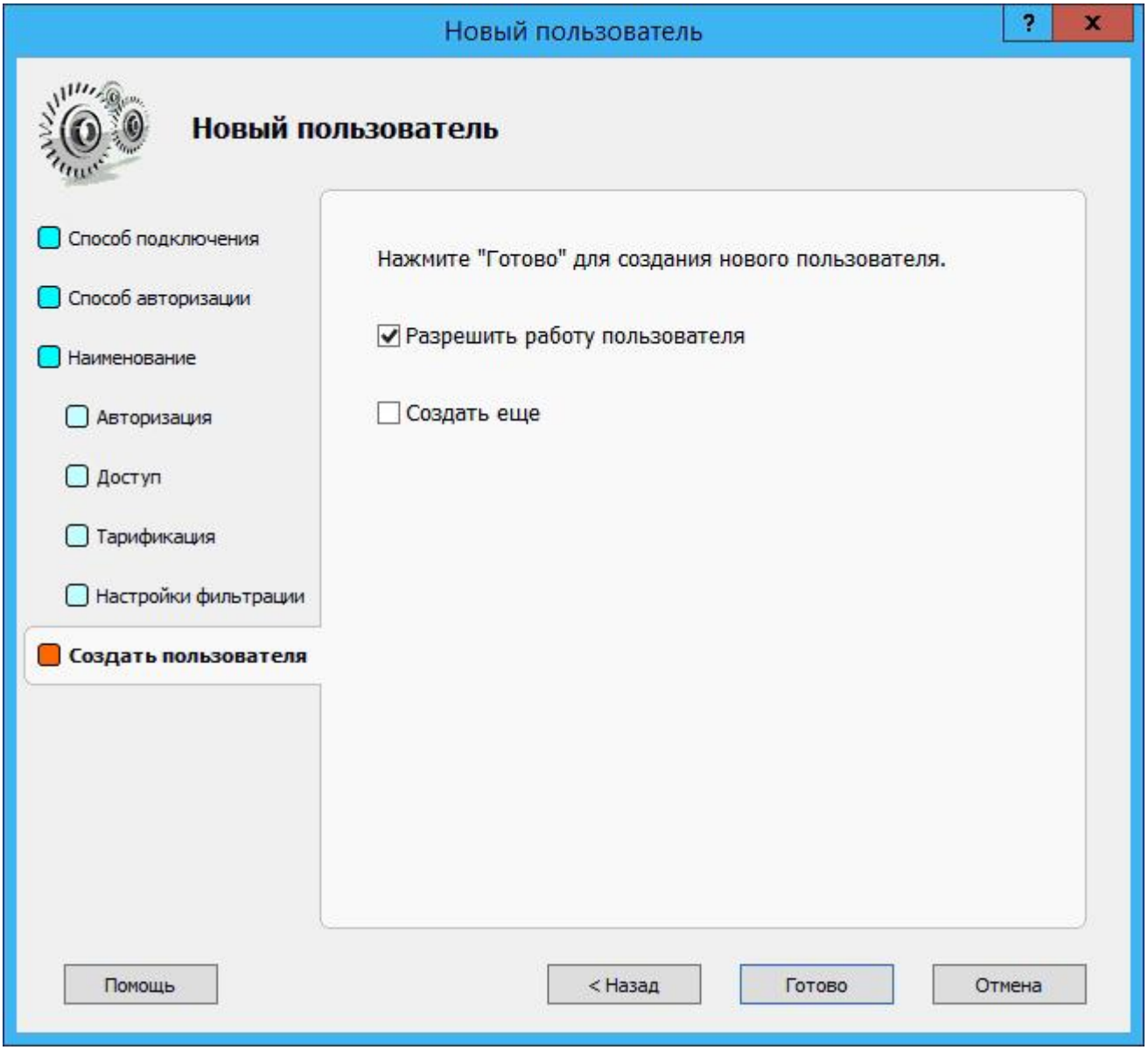
При необходимости можно настроить автоматическое отключение клиента в случае превышения допустимого баланса или же запретить доступ к серверу в определенные дни:


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
. .
Помощь
< Назад
Далее >
Отмена

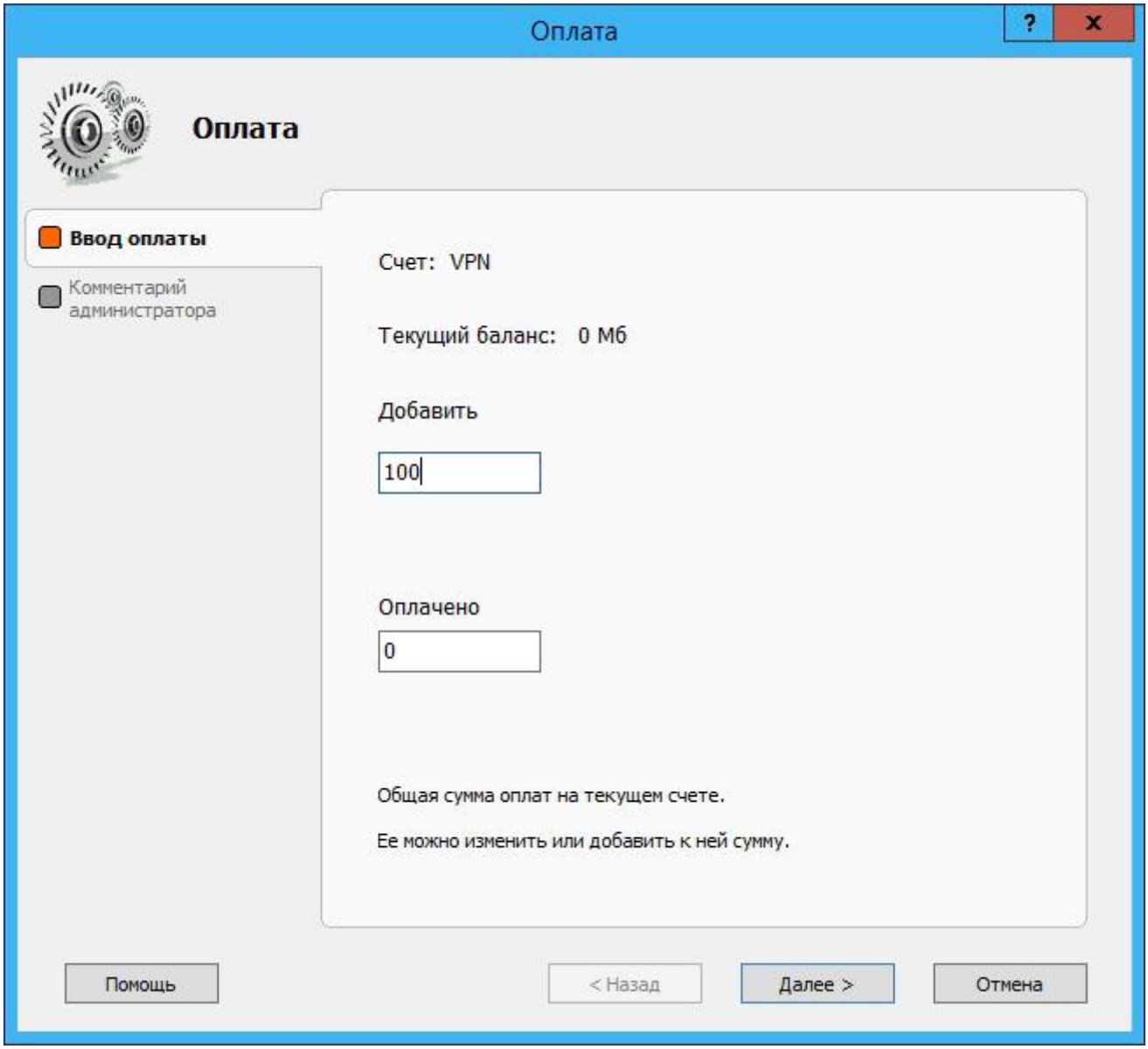


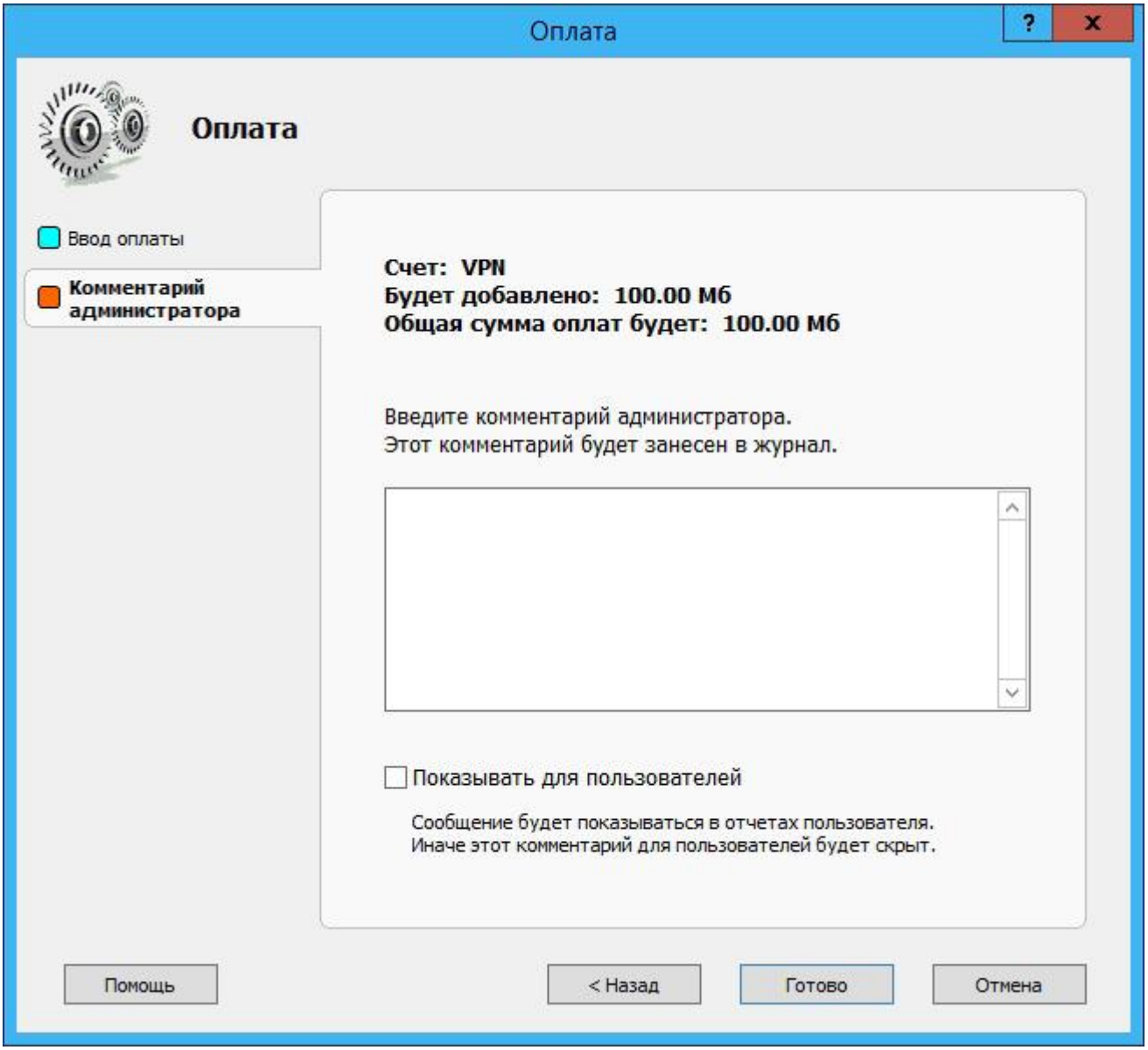
В Traffic Inspector предусмотрены 4 уровня фильтрации трафика для пользователей — баннеры, мультимедиа, графика и только текст. Чтобы выбрать один из них, поставьте флажок в поле **Установить индивидуальный минимальный уровень фильтрации для пользователя**:


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

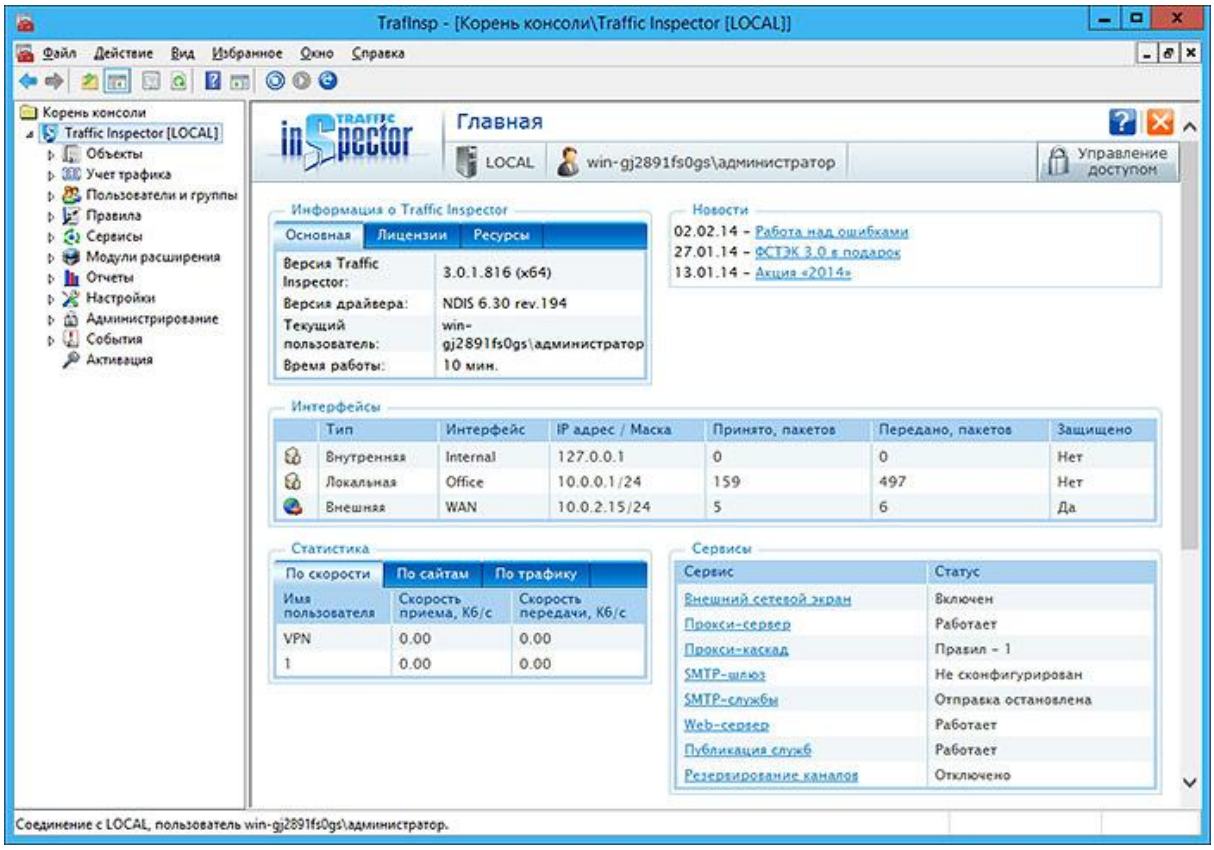


Кроме того, пользователю можно выделить определенную квоту трафика (например, 100 МБ):


Оплата
Оплата
Ввод оплаты
Комментарий администратора
Счет: VPN
Текущий баланс: 0 Мб
Добавить
100
Оплачено
0
Общая сумма оплат на текущем счете.
Ее можно изменить или добавить к ней сумму.
Помощь
< Назад
Далее >
Отмена



После окончания настройки в главном окне Traffic Inspector появится новая сеть RAS server (dial in):



Задание

1. Организовать виртуальную сеть, состоящую из одой серверной и двух клиентских машин
2. Создать и настроить VPN-сервер на серверной машине
3. Настроить VPN подключения к серверу
4. Установить Traffic Inspector на сервере
5. Назначить правила отдельным пользователям и их группам (настроить учет и тарификацию дневного и вечернего трафика).
6. Проверить работу правил и корректность настроек

Контрольные вопросы

1. Что такое виртуальная частная сеть?
2. Какие средства существуют у операционных систем для организации контроля сетевой активности пользователей?
3. Какие функции у приложения Traffic Inspector
4. Какую сетевую активность можно наблюдать с помощью VPN – туннеля?

5. Можно ли из внешней сети обнаружить активность приложения Traffic Inspector?

Библиография

1. Баканов В.М. Сетевые технологии: Учебное пособие. - М.: МГУПИ, 2008. - 105 с. [Электронный ресурс]: http://window.edu.ru/resource/182/58182
2. Комагоров В.П. Архитектура сетей и систем телекоммуникации: учебное пособие / В.П. Комагоров; Томский политехнический университет. - Томск: Изд-во Томского политехнического университета, 2011. - 154 с. [Электронный ресурс]: http://window.edu.ru/resource/074/79074
3. Олифер В. Г., Компьютерные сети. Принципы, технологии, протоколы [Текст] : учебник для вузов / В. Г. Олифер, Н. А. Олифер. - 4-е изд. - Санкт-Петербург : Питер, 2015. - 943 с. - (Учебник для вузов). - Библиогр.: с. 917 . - Алф. указ.: с. 918