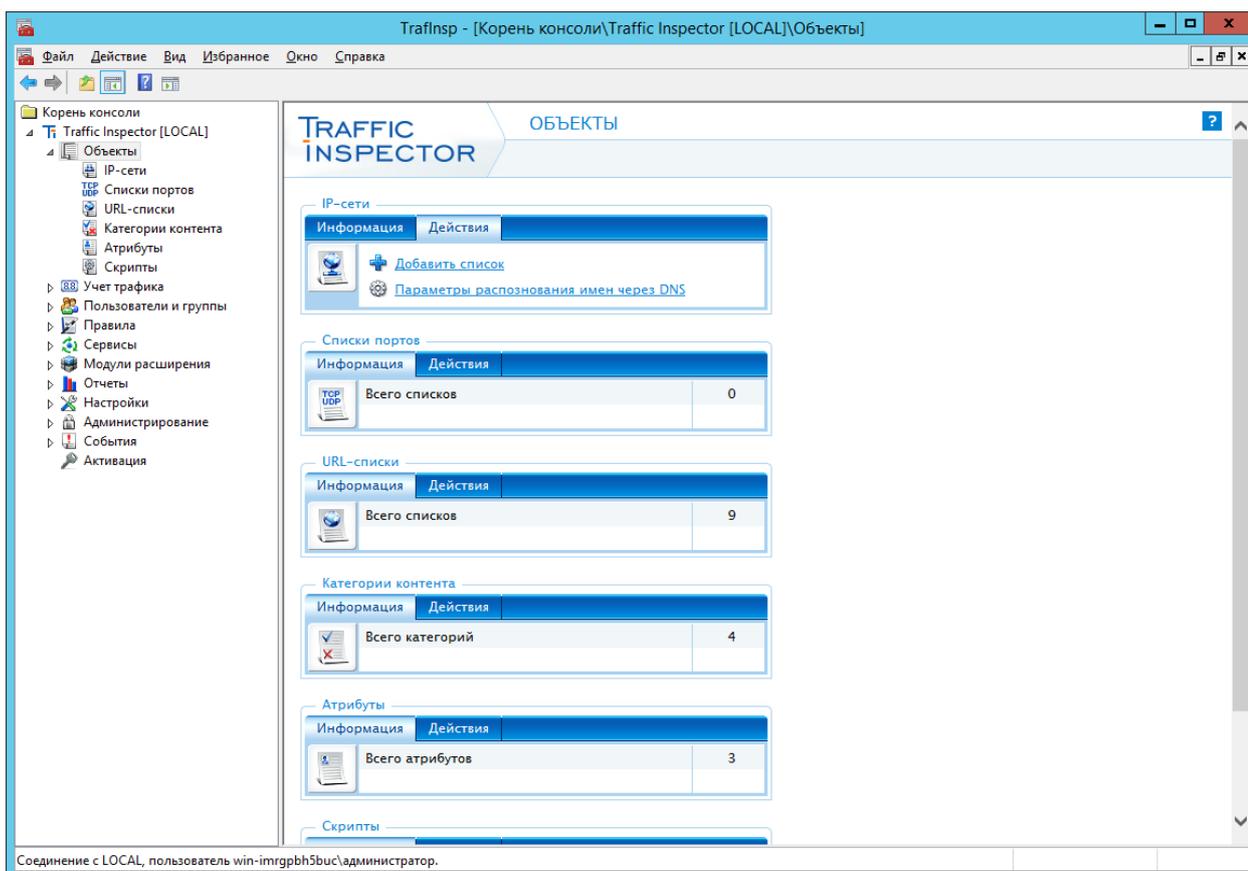


НАСТРОЙКА ЧЕРНОГО СПИСКА РЕСУРСОВ ДЛЯ ОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЙ

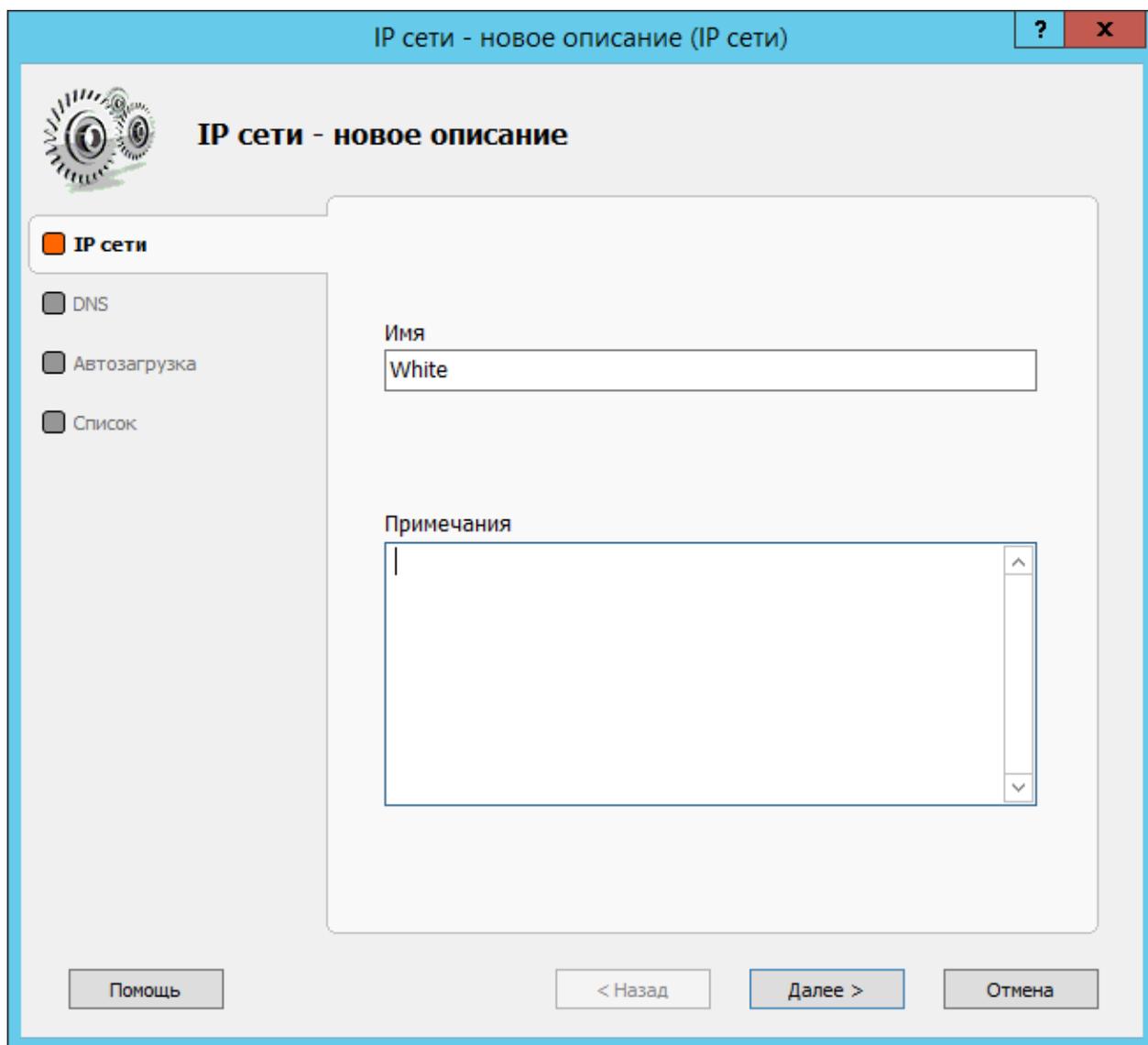
Такой подход позволяет использовать доступ в интернет по строго определённым целям, а с другой стороны гарантирует отсутствие доступа к нежелательной информации. Сначала необходимо сформировать правило разрешающее доступ к определенным сайтам. А потом создать правило, которое запретит весь остальной трафик.

1. Настройка «черного» списка запрещенных ресурсов

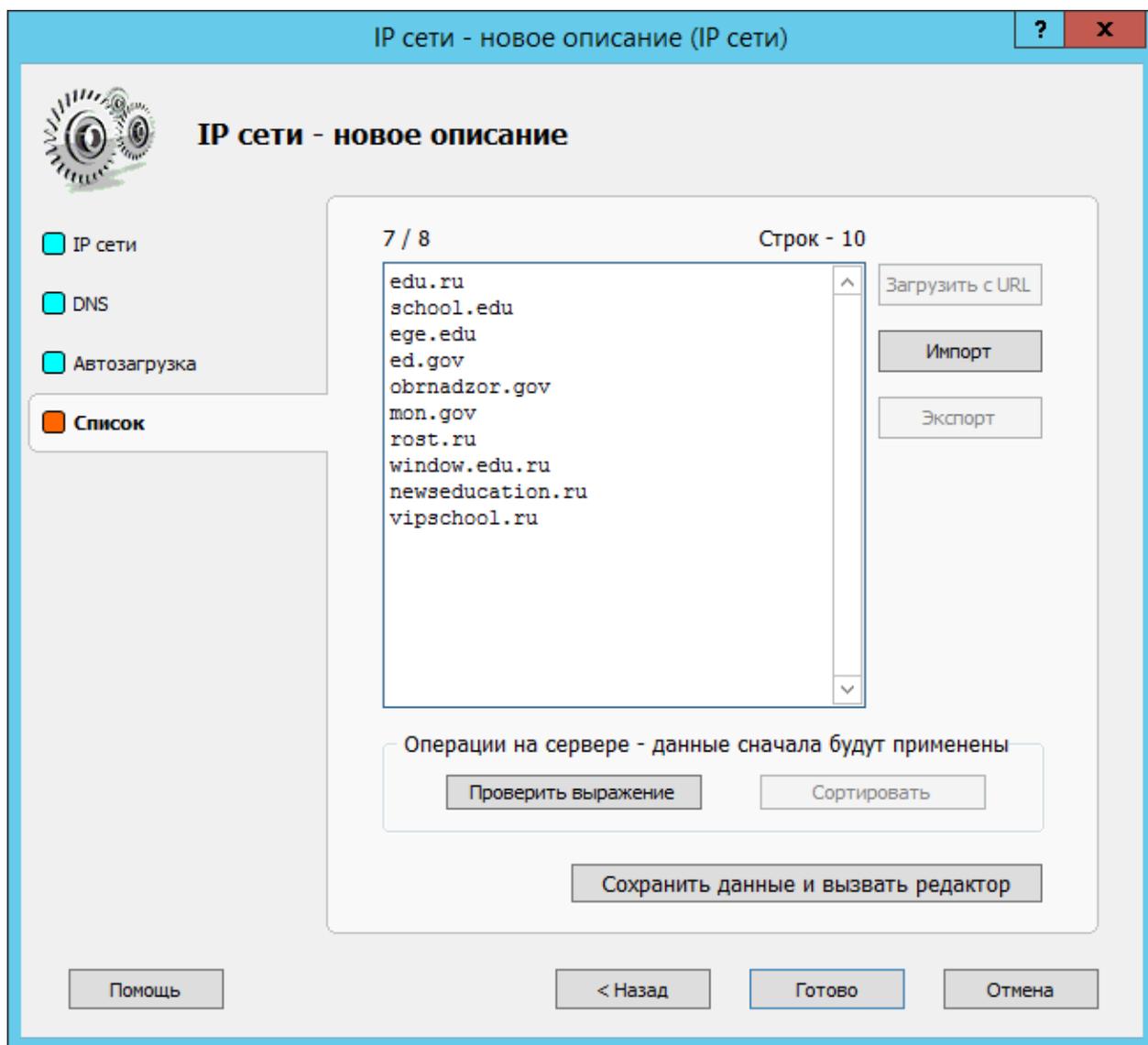
1.1 Сначала необходимо сформировать список разрешенных сайтов. Для этого необходимо подготовить перечень сайтов, доступ к которым будет разрешен. Сделать это можно с помощью **«IP-списка»**. Для этого в консоли управления **Traffic Inspector** откройте раздел **«Объекты»** и в блоке **«IP-сети»** нажмите ссылку **«Добавить список»**.



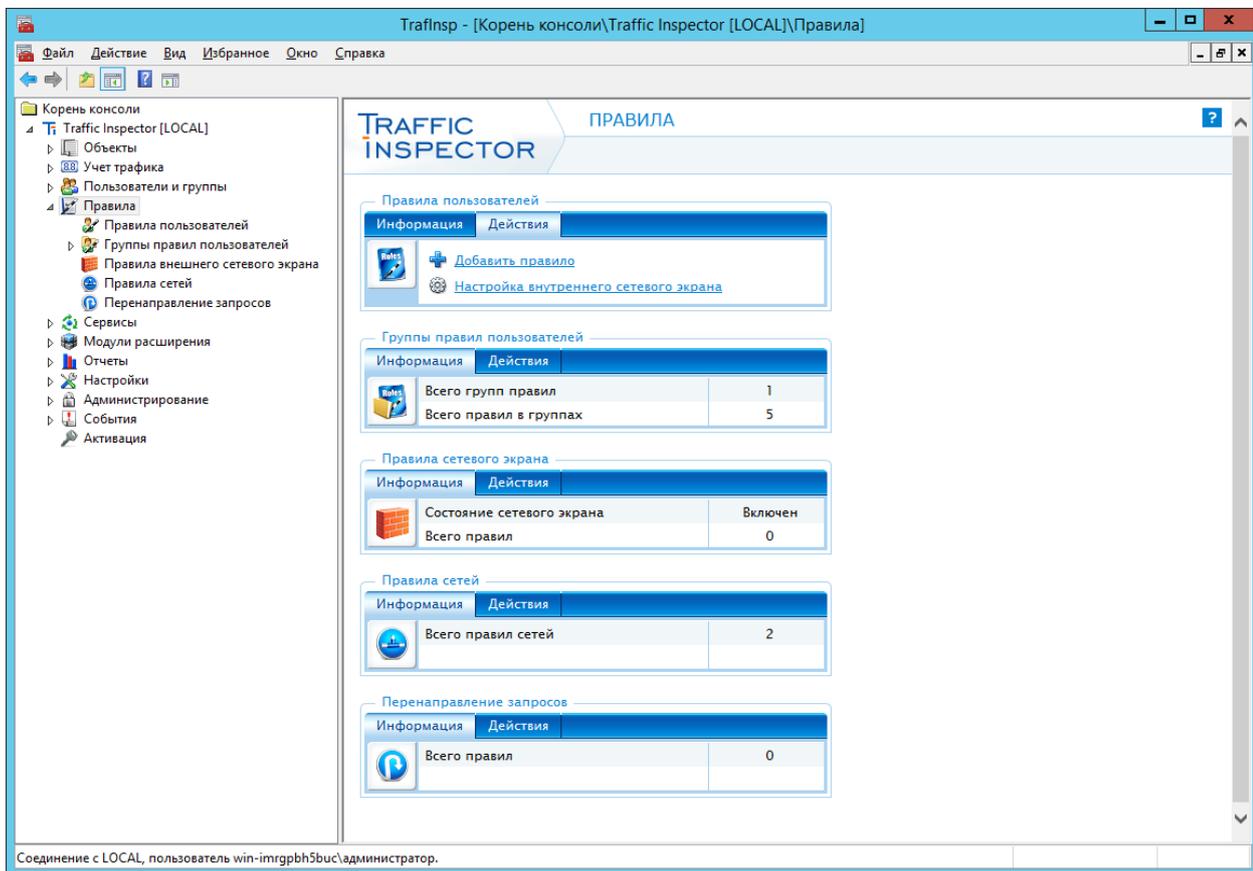
1.2 В открывшемся окне введите **«Имя»** списка и нажмите кнопку **«Далее»**.



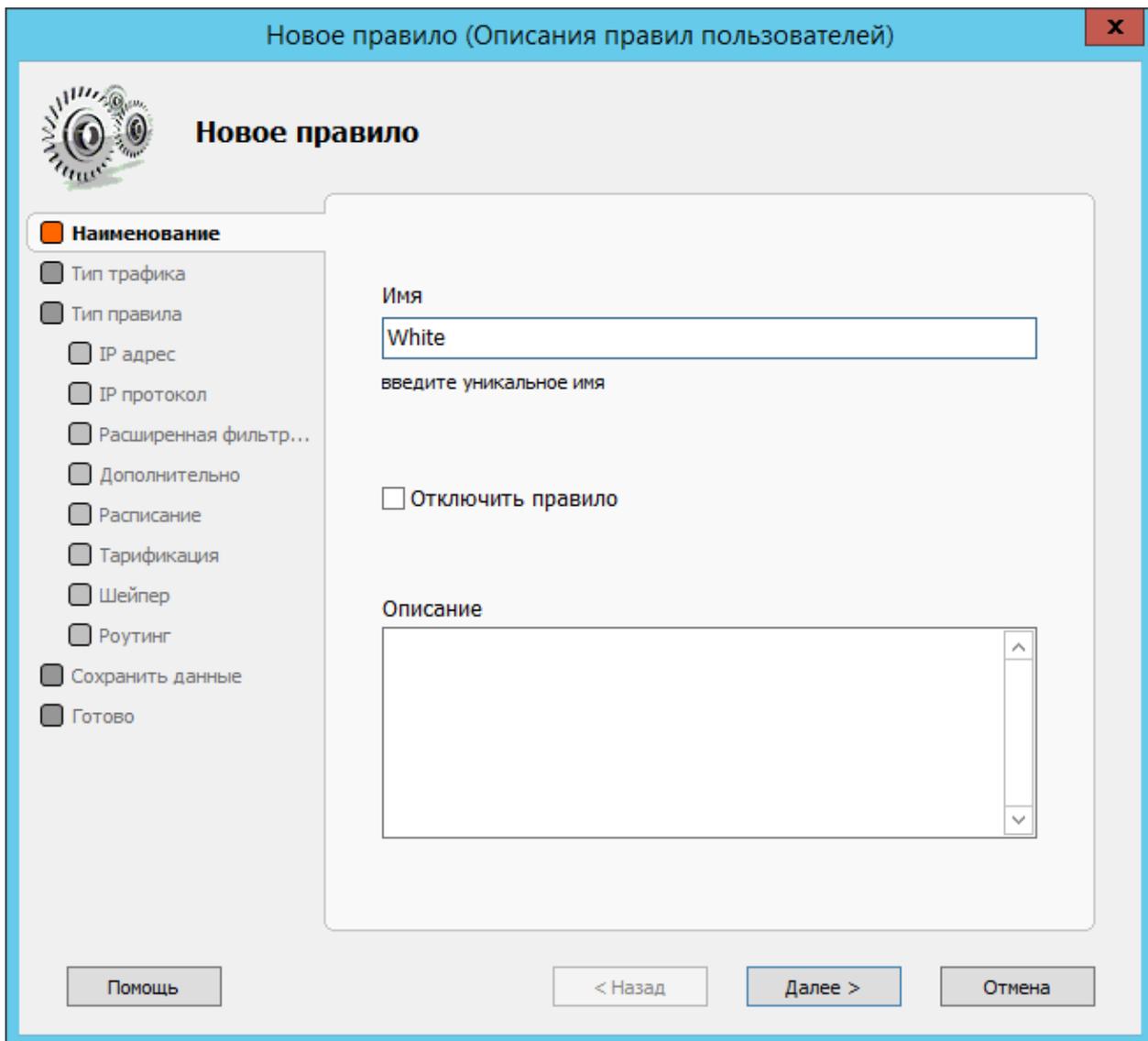
1.3 Перейдите на вкладку **«Список»** и внесите доменные имена или ip-адреса сайтов, доступ к которым будет разрешен. Нажмите кнопку **«Готово»**.



1.4 Создайте правило, которое будет разрешать доступ к сайтам из списка. Для этого откройте раздел **«Правила»** консоли управления, и в блоке **«Правила пользователей»** нажмите ссылку **«Добавить правило»**.



1.5 Введите наименование правила и нажмите кнопку «Далее».



1.6 На вкладке тип правила выберите значение **«Разрешение+Действие»**. Нажмите кнопку **«Далее»**.

The screenshot shows a window titled "Новое правило (Описания правил пользователей)" with a close button (X) in the top right corner. The window is divided into a left sidebar and a main content area.

Left Sidebar:

- Наименование (checkbox)
- Тип трафика (checkbox)
- Тип правила (checkbox, highlighted)**
 - IP адрес (checkbox)
 - IP протокол (checkbox)
 - Расширенная фильтр... (checkbox)
 - Дополнительно (checkbox)
 - Расписание (checkbox)
 - Тарификация (checkbox)
 - Шейпер (checkbox)
 - Роутинг (checkbox)
 - Сохранить данные (checkbox)
 - Готово (checkbox)

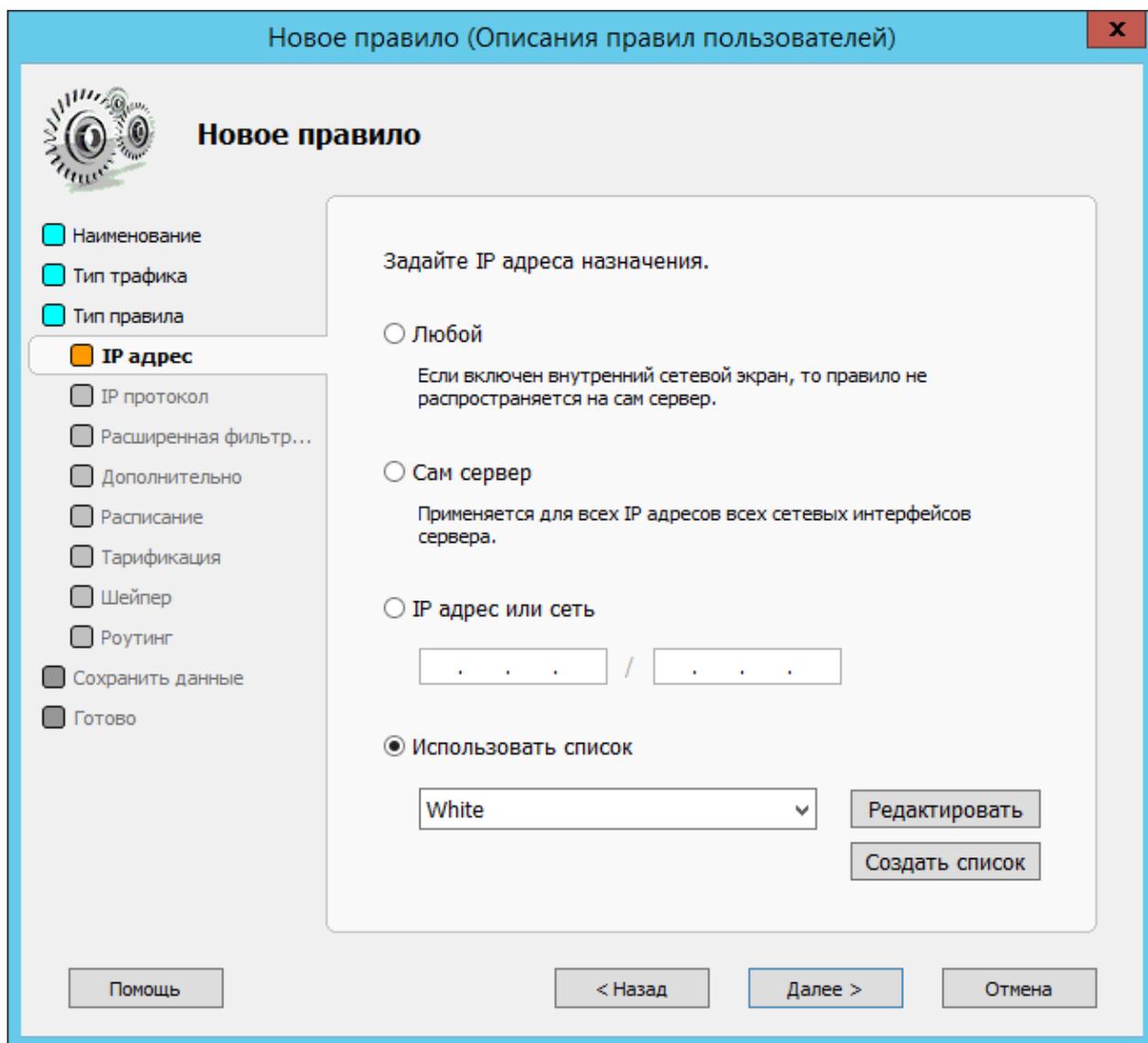
Main Content Area:

- Разрешение + "действия"**
Комбинированное правило - кроме разрешения данного трафика также описываются различные другие действия.
- Запрет**
Трафик, попадающий под заданное условие, будет заблокирован. Для трафика через HTTP прокси возможно задание дополнительных действий.
- Управляемое пользователем**
Имеет смысл, если данное правило применено для пользователя. Задайте уровень правила (F1-F4).

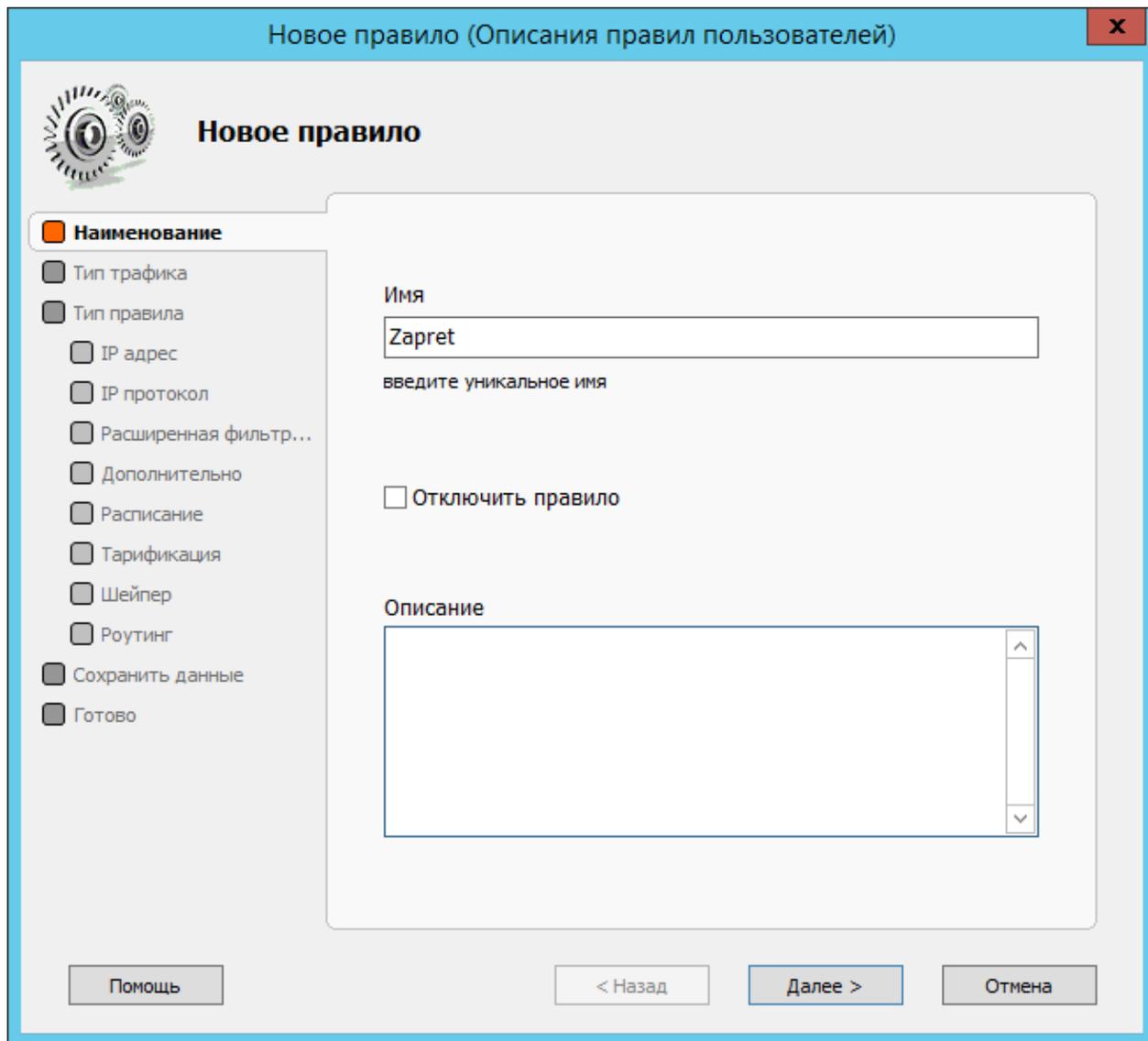
Пользователь сам задает свой уровень фильтрации. Правило применяется, если уровень правила (F1-F4) не более уровня пользователя.
- Только "действия"**

Buttons at the bottom: Помощь, < Назад, Далее >, Отмена.

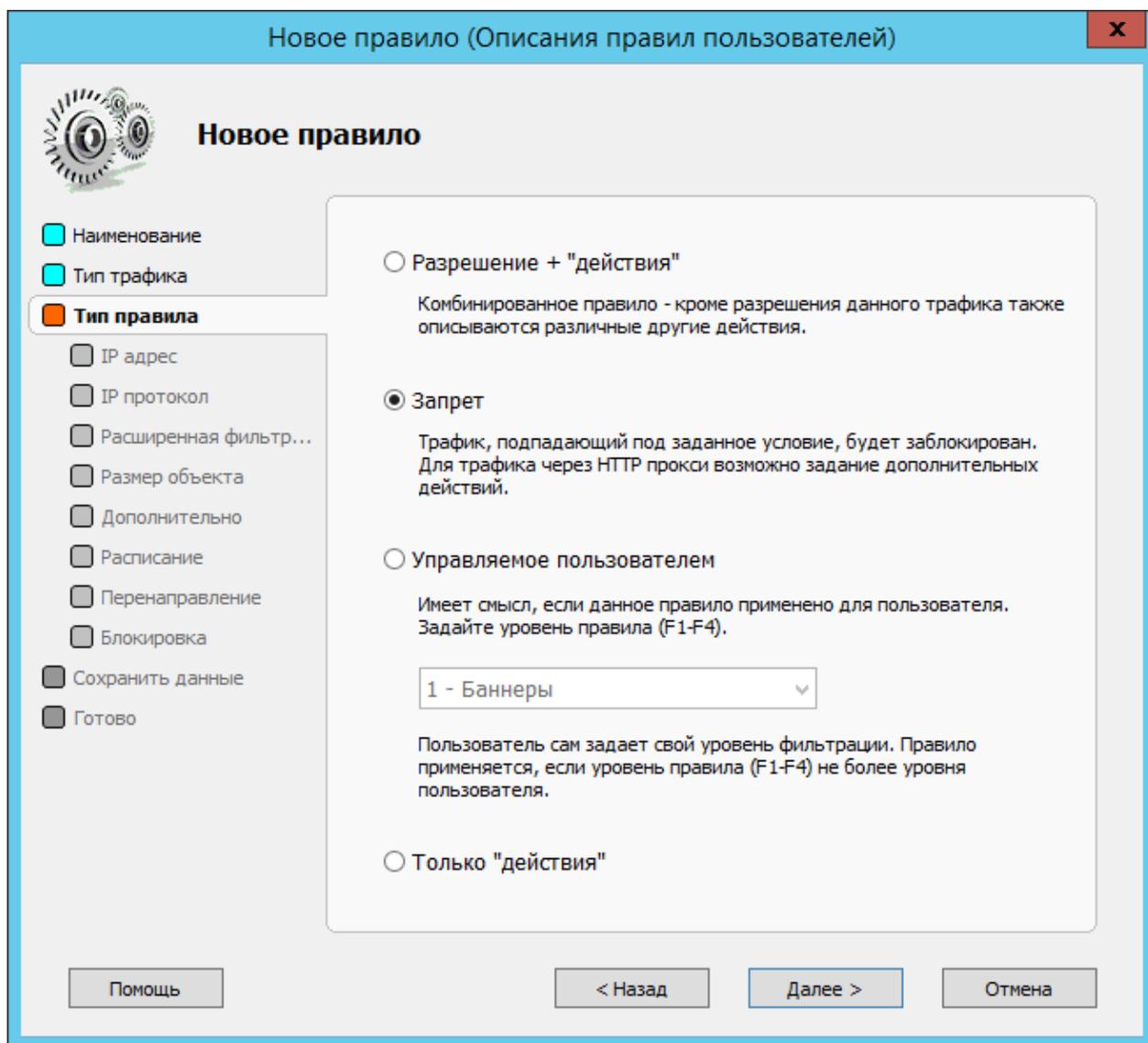
1.7 После этого на вкладке **«IP-адрес»** поставьте отметку **«Использовать список»** и выбрать список **«White»**. Нажмите кнопку **«Далее»**. Все остальные параметры мастера создания нового правила можно оставить без изменения.



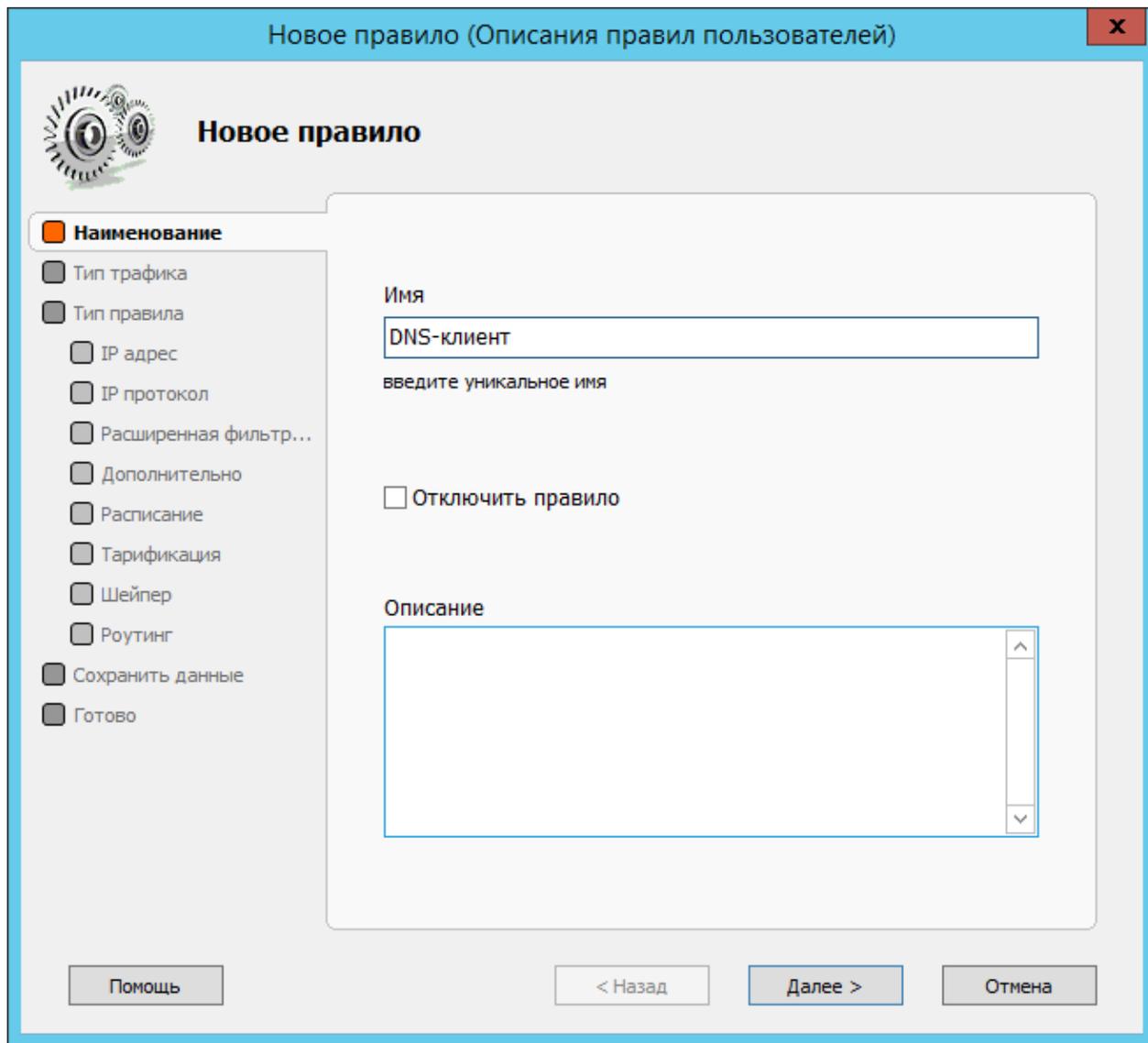
1.8 Создайте новое правило на запрет всего трафика. Для этого вызовите мастер создания нового правила и введите его имя. Нажмите кнопку **«Далее»**.



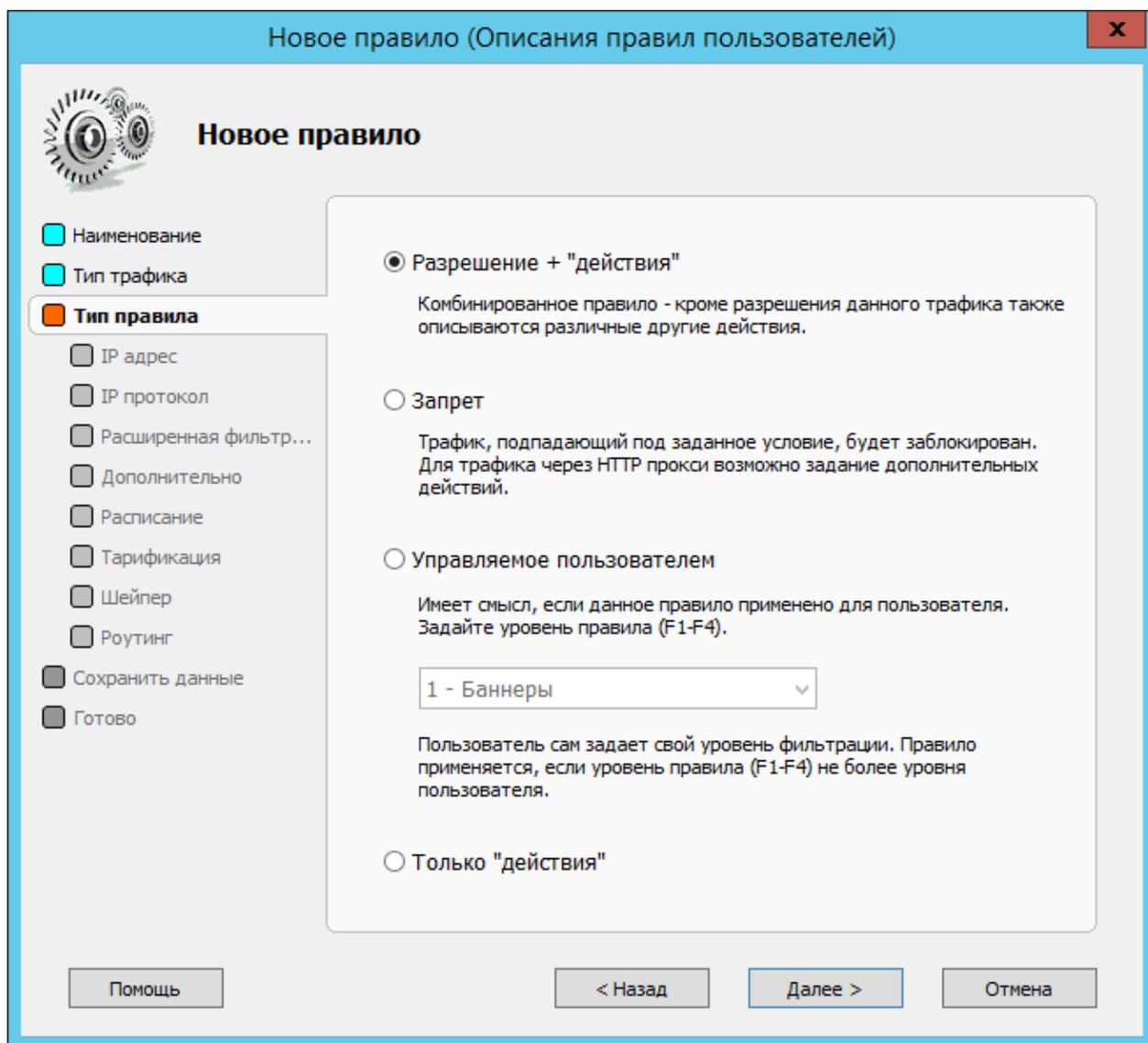
1.9 На вкладке тип правила выберите значение **«Запрет»**. Нажмите кнопку **«Далее»**. Все остальные параметры мастера создания нового правила можно оставить без изменения.



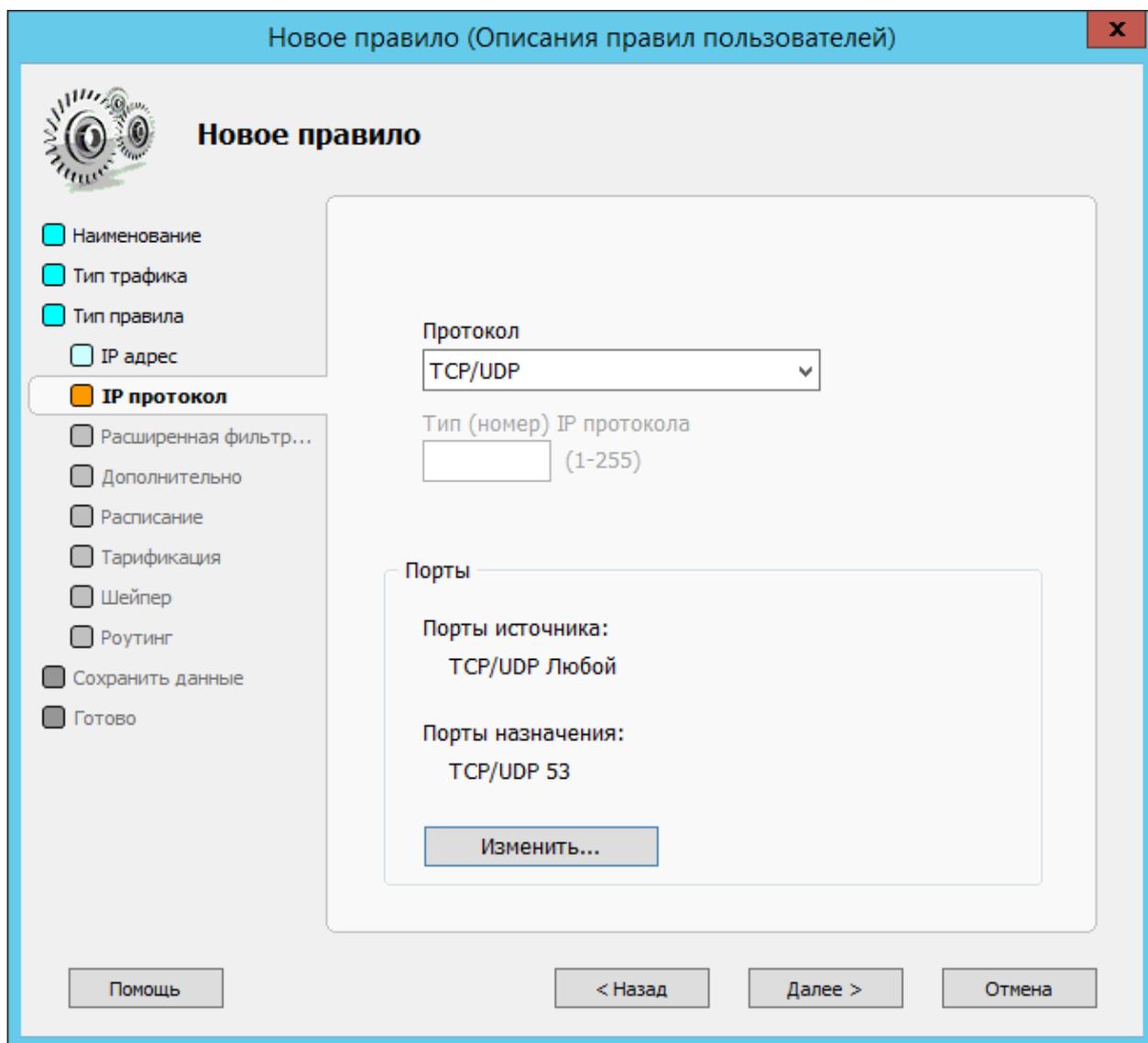
1.10 Создайте новое правило, которое разрешит использование клиентом DNS. Если этого не сделать, то запрещающее правило, которое мы создаем в дальнейшем заблокирует все обращения к DNS серверам. В результате чего загружать сайты по доменным именам будет невозможно. Задайте **«Имя»** правила DNS-клиент. Нажмите кнопку **«Далее»**.



1.11 На вкладке тип правила выберите значение **«Разрешение+Действие»**.
Нажмите кнопку **«Далее»**.



1.11 На вкладке «IP-протокол» выберите «Протокол» «TCP\UDP» и в разделе «Порты назначения» укажите 53 порт. Нажмите кнопку **«Далее»**. Все остальные параметры мастера создания нового правила можно оставить без изменения.



1.12 Назначьте созданные ранее правила группе пользователей в следующем порядке: первое – White, второе – DNS-клиенты, третье – zapret. Для этого зайдите в свойства группы и назначьте эти правила на вкладке **«Правила группы До»**.



Настройка группы

- Наименование
- Авторизация
- Настройки агентов
- Тарификация
- Расписание
- Сетевая статистика
- Контроль нарушений
- Фильтрация

Правила группы "До"

- Правила группы "После"
- HTTP мимо прокси
- Перенаправление TCP
- Ограничения
- Шейпер
- Автоматизация
- Запись в журнал

Правила "До" - по умолчанию

Эти правила действуют на всю группу до индивидуальных правил, которые назначены на пользователей.

Правила группы "До"

Выберите описание группы правил и нажмите "Добавить"

Добавить

Выберите описание правила и нажмите "Добавить"

White Добавить

White	разре...	Вверх
DNS-клиент	разре...	Вниз
Zapret	запрет	
		Удалить

Помощь

ОК

Отмена

1.13 Также возможно настроить работу отдельного пользователя по белому списку. Назначьте созданные ранее правила пользователю в следующем порядке: первое – White, второе – DNS-клиенты, третье – zapret. Для этого зайдите в свойства пользователя и назначьте эти правила на вкладке «Правила».



Настройки пользователя

- Наименование
- Авторизация
- Доступ
- Опции авторизации
- Настройки агентов
- Тарификация
- Расписание
- Сетевая статистика
- Контроль нарушений
- Настройки фильтрации

Правила

- HTTP мимо прокси
- Перенаправление TCP
- Ограничения
- Шейпер
- SMTP
- Автоматизация
- Запись в журнал

Правила "До" - по умолчанию

Выберите описание группы правил и нажмите "Добавить"

Добавить

Выберите описание правила и нажмите "Добавить"

Добавить

White	разре...	Вверх
DNS-клиент	разре...	Вниз
Zapret	запрет	

Удалить

Правила "После" - по умолчанию

Помощь

ОК

Отмена