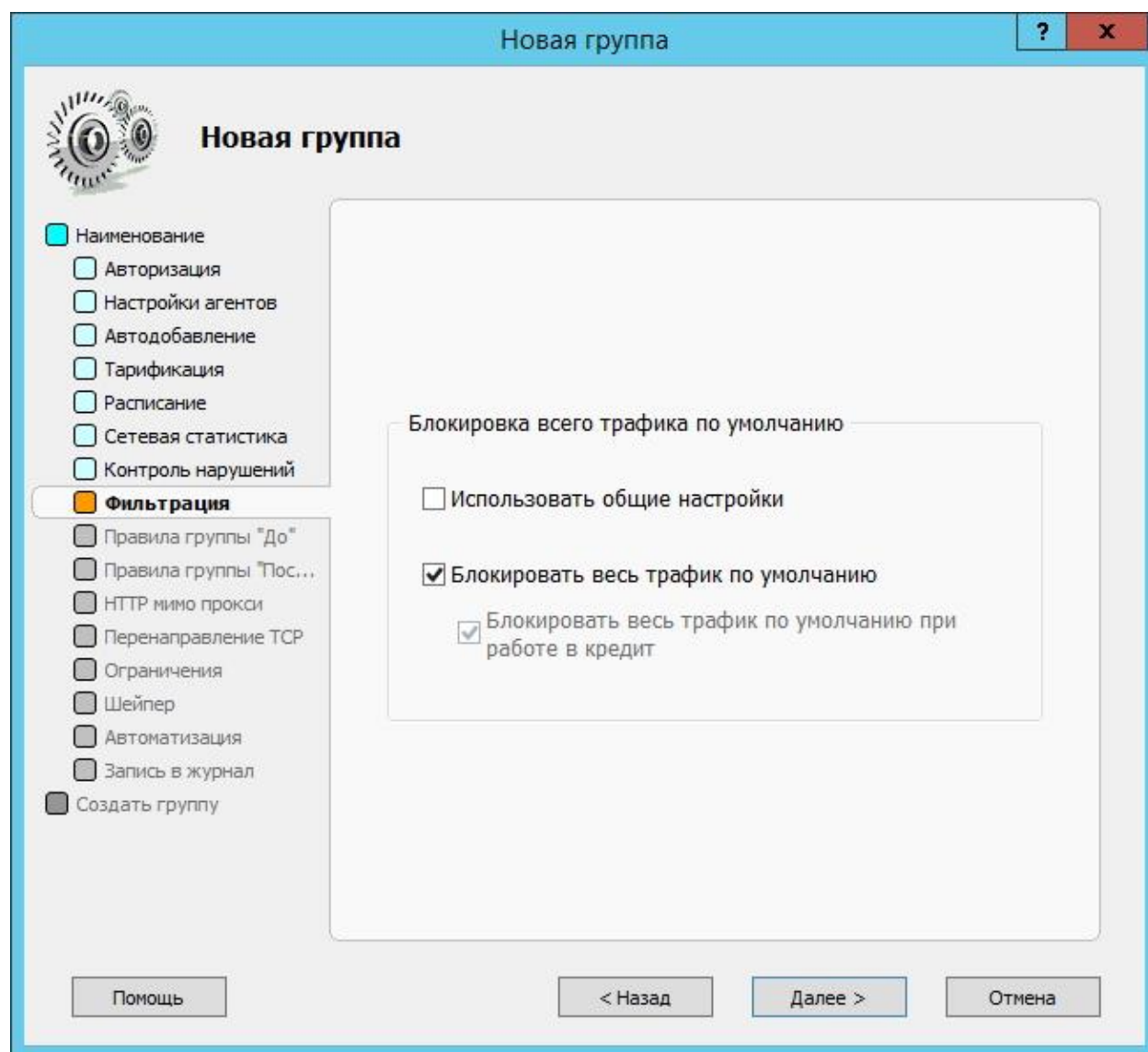


НАСТРОЙКА РАЗРЕШАЮЩИХ ФИЛЬТРОВ ДЛЯ ГРУППЫ, ГДЕ ВСЕ ЗАПРЕЩЕНО

Чтобы жестко ограничить доступ к сети интернет какой-то группе пользователей:

1. Создайте группу с фильтром на запрещение. Для этого при создании группы на вкладке «Фильтрация» установите галку «Блокировать весь трафик по умолчанию».



2. Создайте фильтр на разрешение (в примере создается фильтр на разрешение SMTP по 25 порту).

Новое правило

Наименование

Имя
SMTP
введите уникальное имя

Запретить правило

Описание

Помощь < Назад Далее > Отмена

Новое правило

Наименование

Тип трафика

Тип правила

Разрешение + "действия"
Комбинированное правило - кроме разрешения данного трафика также описываются различные другие действия.

Запрет
Трафик, подпадающий 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).

1 - Баннеры

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

Только "действия"

Помощь < Назад Далее > Отмена

В поле «порт назначения» вписываются порты удаленного сервера, в нашем примере это 25 порт, стандартный для почты (SMTP). Можете выбрать протокол из списка шаблонов.

Новое правило

Наименование
Тип трафика
Тип правила
 IP адрес
 IP протокол
 Расширенная фильтр...
 Дополнительно
 Расписание
 Тарификация
 Шейпер
 Роутинг
 Сохранить данные
 Готово

Подсказка - выберите протокол из списка шаблонов
SMTP client (TCP/25)

Протокол
TCP

Тип (номер) IP протокола
6 (1-255)

TCP/UDP порты источника
 Порт / диапазон портов
-
 Динамические порты

TCP/UDP порты назначения
 Порт / диапазон портов
25 -
 Динамические порты

Помощь < Назад Далее > Отмена

Новое правило

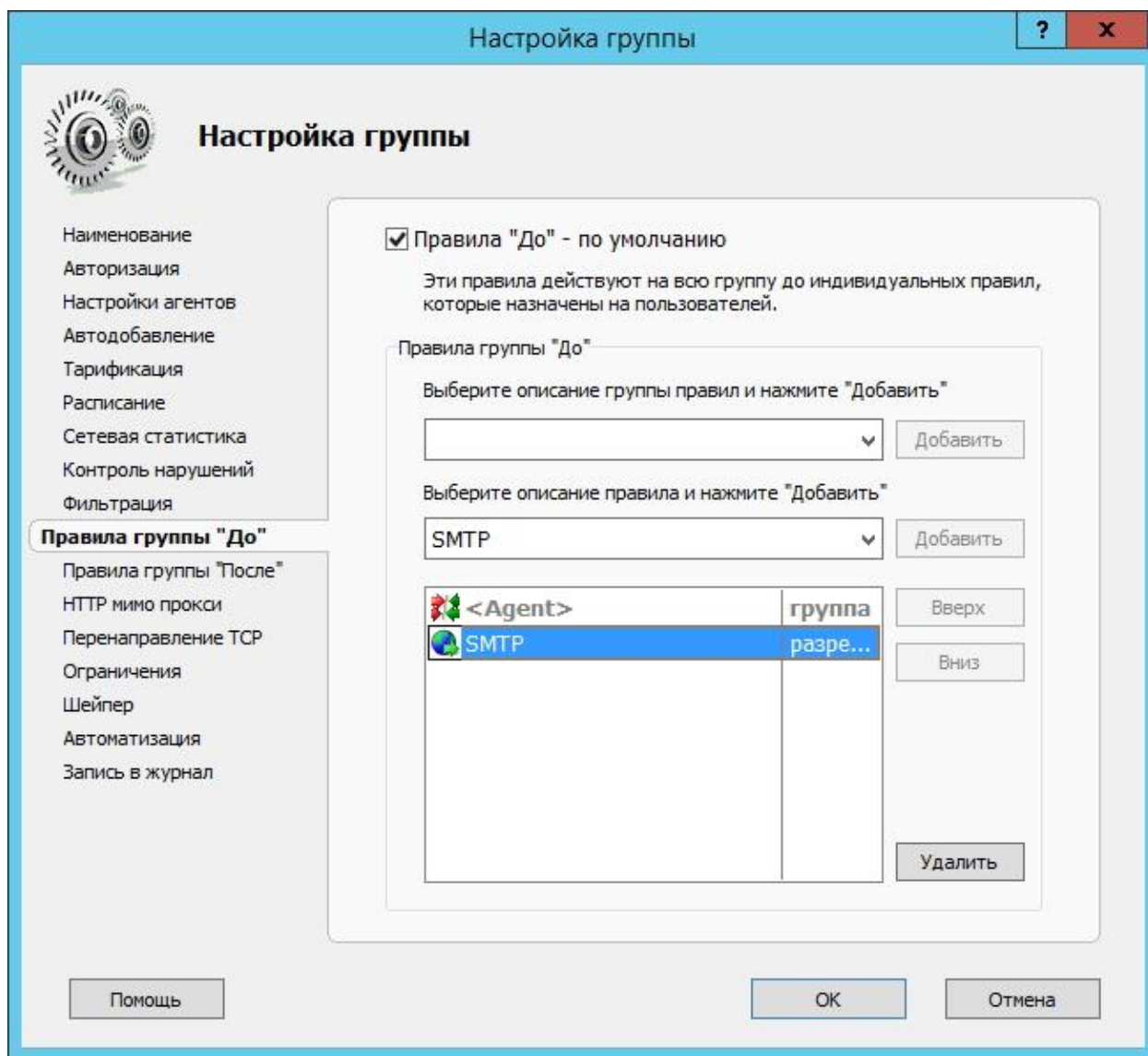
Наименование
Тип трафика
Тип правила
 IP адрес
 IP протокол
 Расширенная фильтр...
 Дополнительно
 Расписание
 Тарификация
 Шейпер
 Роутинг
 Сохранить данные
 Готово

Новое описание правила создано.

Создать еще
Этот мастер будет вызван повторно.

Помощь < Назад Готово Отмена

Примените данное правило к группе пользователей. Это делается в свойствах группы.



Обратите внимание, что для полноценной работы почты надо добавить еще 2 фильтра на разрешение по портам 110 и 143.

Подобным образом можно сделать и наоборот - запретить только почту (соответственно при создании группы не нужно устанавливать галку «Блокировать весь трафик по умолчанию» и фильтры надо создавать на запрещение).

Соответственно можно создать несколько групп с разными запрещающими или разрешающими фильтрами, которые будут действовать только на пользователей данной группы.

Приложение

Таблица наиболее часто используемых протоколов

Название	Протокол	транспортный протокол	Порт	Примечание
Почта	SMTP	TCP	25	В этих фильтрах можно еще добавить имя хоста. Но в этом случае Вам необходимо учесть, что если DNS внешний, то необходимо открыть еще порты DNS см.таб.
	POP3	TCP	110	
	IMAP	TCP	143	
DNS		UDP	53	
DHCP		UDP	67	
		UDP	68	
FTP	FTP-DATA	TCP	20	
	FTP	TCP	21	
WWW		TCP	80	
Proxy (TI)	HTTP	TCP	8080	
	Socks	TCP	1080	
ICQ	IP сети			Примечание
	205.188.0.0/255.255.0.0			ICQ работает с разными портами, поэтому лучше разрешать диапазон сетей.
	64.12.0.0/255.255.0.0			

Для настройки фильтров по другим протоколам, если не знаете порт и тип транспортного протокола, воспользуйтесь сетевой статистикой в программе.