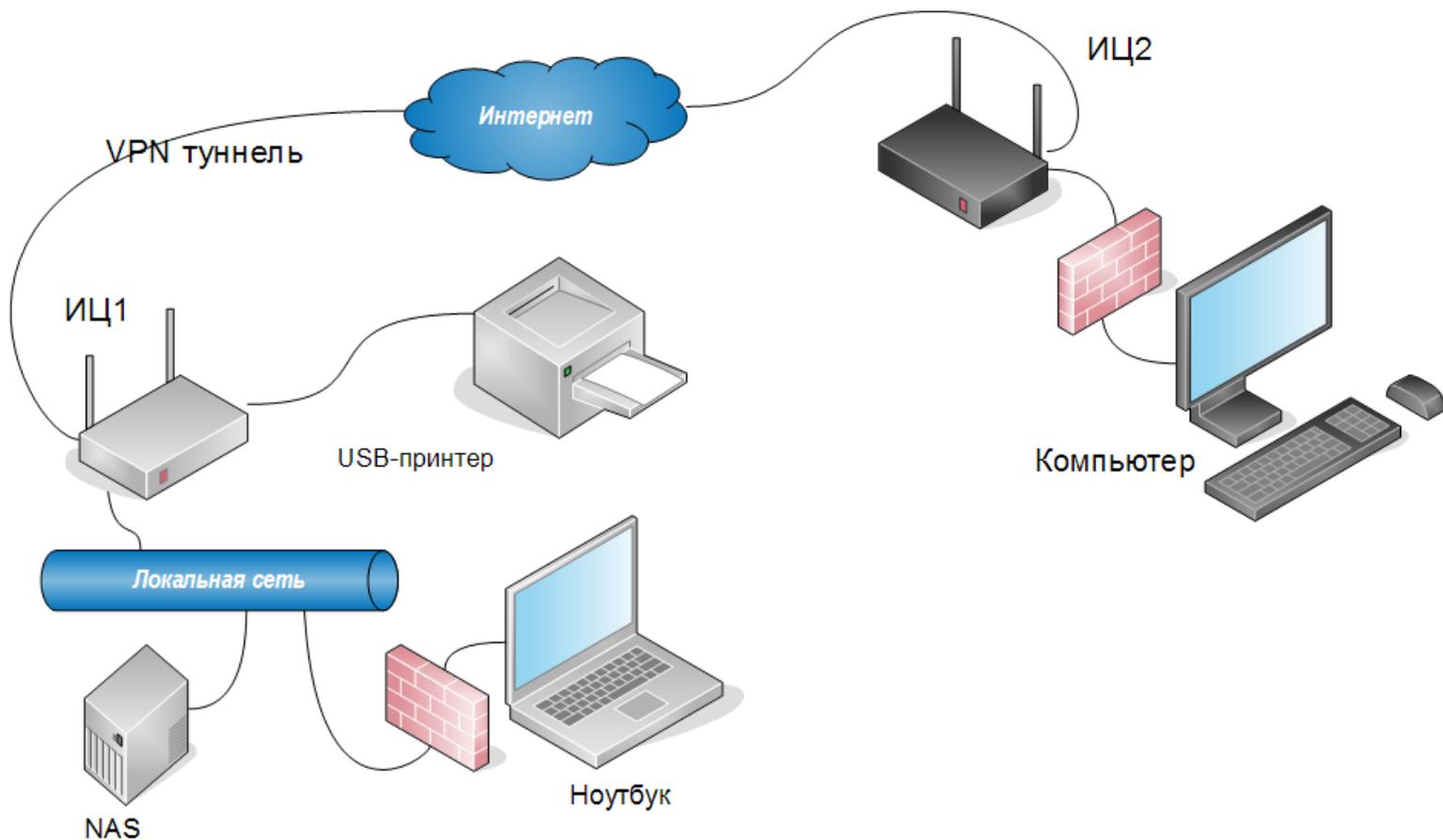


Настройка сетевого экрана в ОС Windows для подключений из сети за VPN-сервером Keenetic



В предлагаемой согласно статье Базы знаний <http://zyxel.ru/kb/4214> схеме объединения локальных сетей, доступ из сети за сервером к хостам в сети за клиентом PPTP может быть заблокирован политиками по умолчанию на файрволе. К примеру в операционной системе Windows по умолчанию блокируются входящие подключения (в том числе и зондирование ICMP), если адрес источника этого подключения не принадлежит к назначенной на интерфейсе компьютера сети.

Это означает, что Компьютер будет иметь доступ к USB-принтеру и хранилищу NAS, но на Ноутбуке обращения от него отбрасываются без соответствующей настройки сетевого экрана.

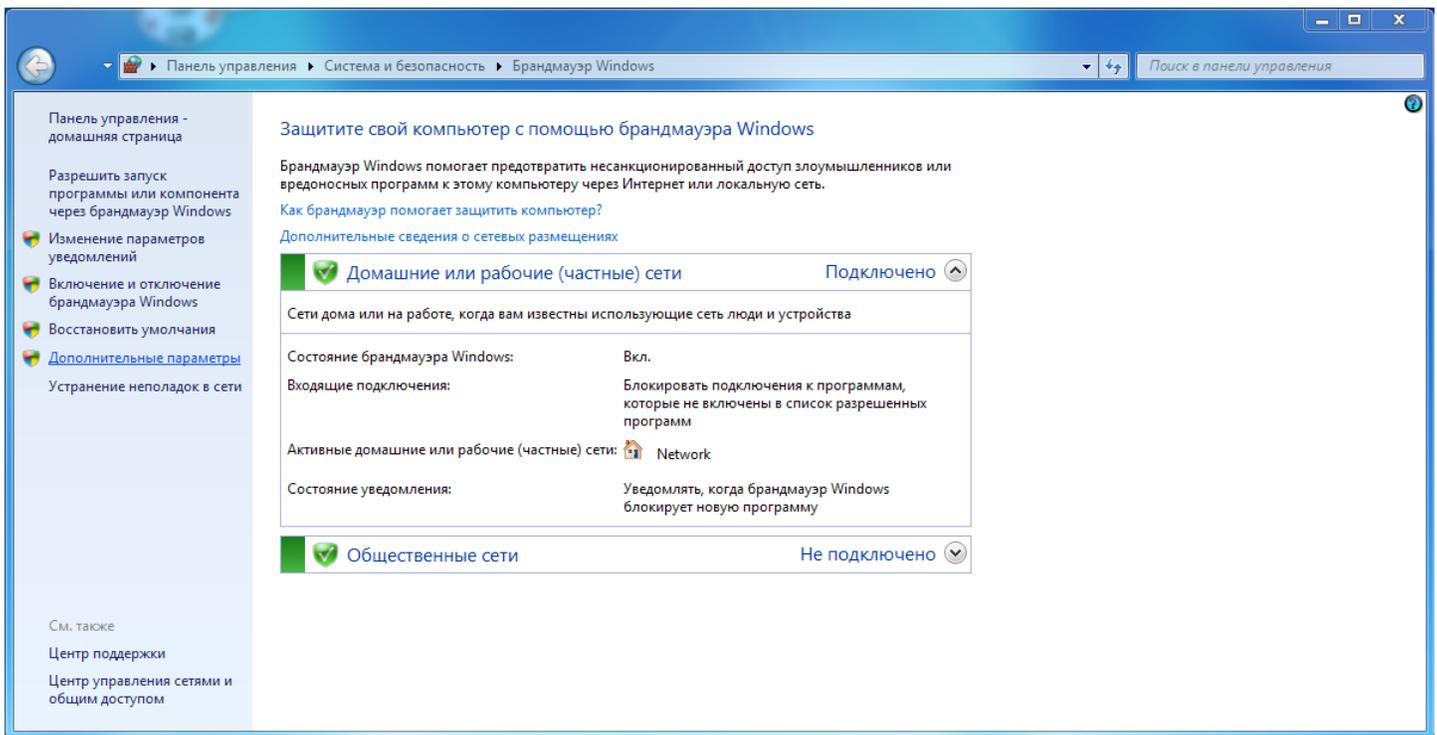
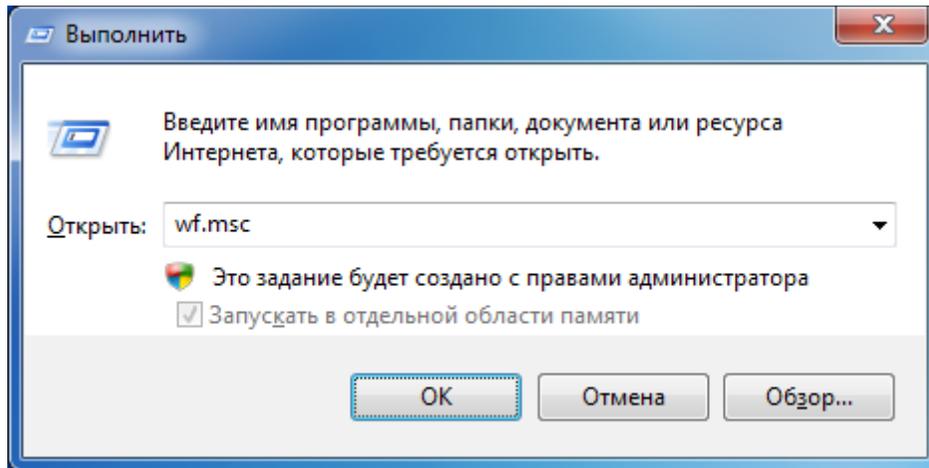
И наоборот, при обращении ноутбука из сети за ИЦ1 (VPN-клиентом) к Windows-компьютеру в сети за сервером ИЦ2, будет выполнена трансляция адреса NAT и действительный адрес отправителя сменится на адрес ИЦ2 полученный от сервера PPTP. То есть, обращение НЕ придёт от адреса хоста в той же сети, что и адрес назначения — и будет заблокировано брандмауэром Windows.

В обратном направлении, адрес отправителя входящего в сеть за ИЦ1 пакета (от Компьютера к Ноутбуку) не подменяется. Однако условие для блокировки по умолчанию на файрволе ноутбука снова выполняется — отправленный от 192.168.1.33 к 192.168.2.33 пакет будет

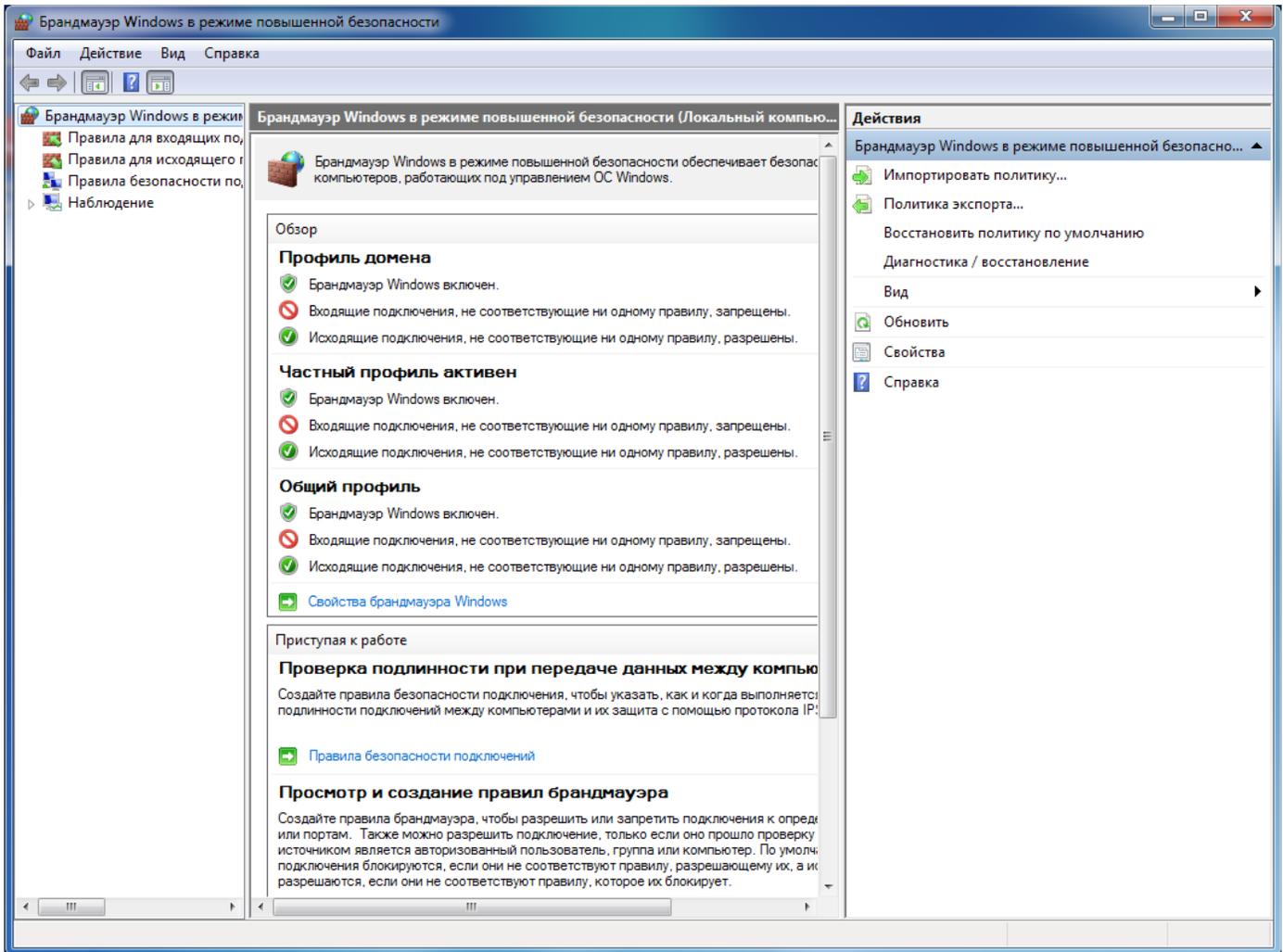
сброшен на компьютере 192.168.2.33.

Рассмотрим настройку Брандмауэра Windows, разрешающую подключения из удалённой сети к компьютерам в локальной сети. Для этого достаточно создать политику сетевого экрана, регулирующую входящие подключения.

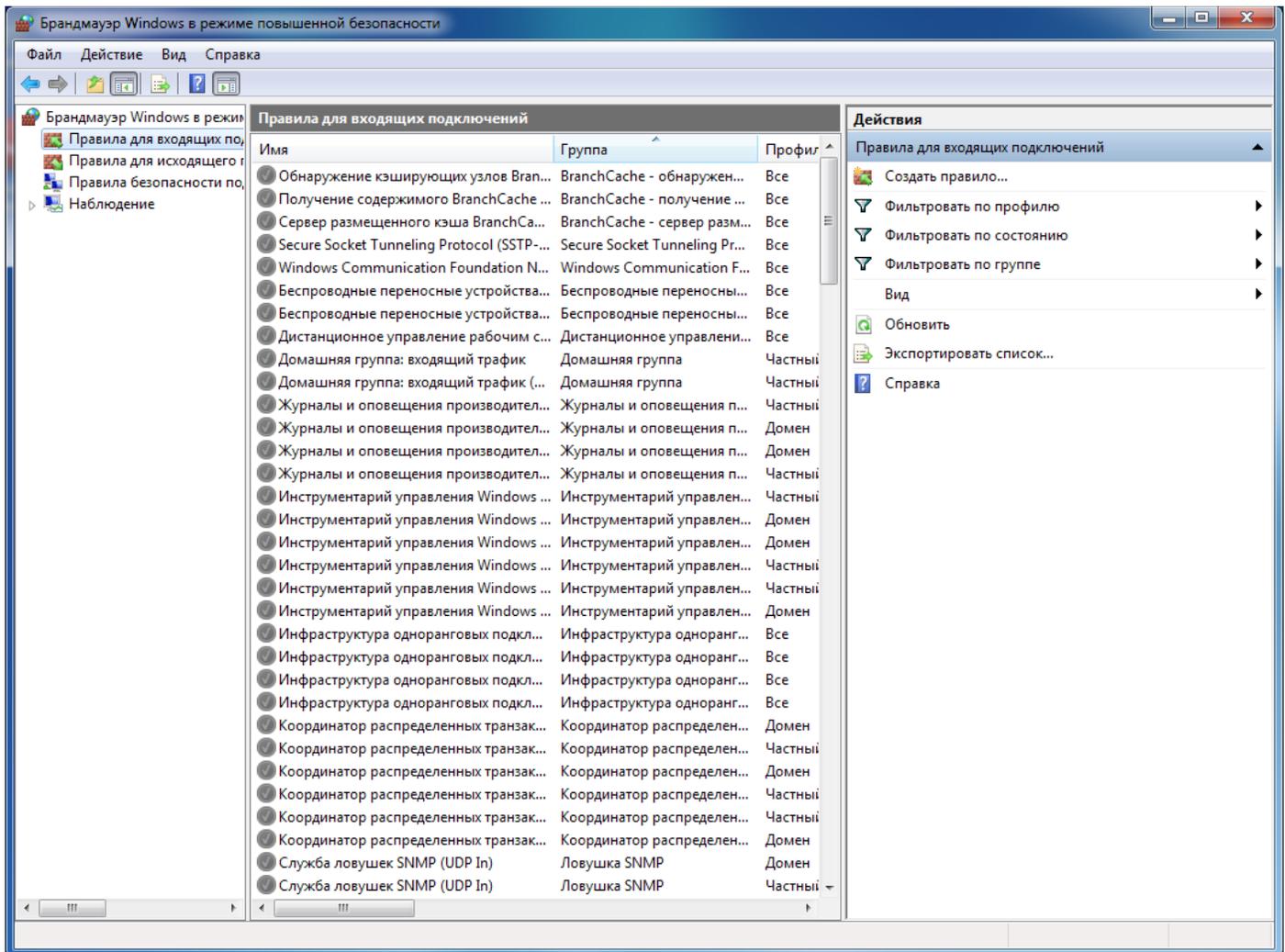
Приведённые далее скриншоты выполнены в операционной системе Windows 7.



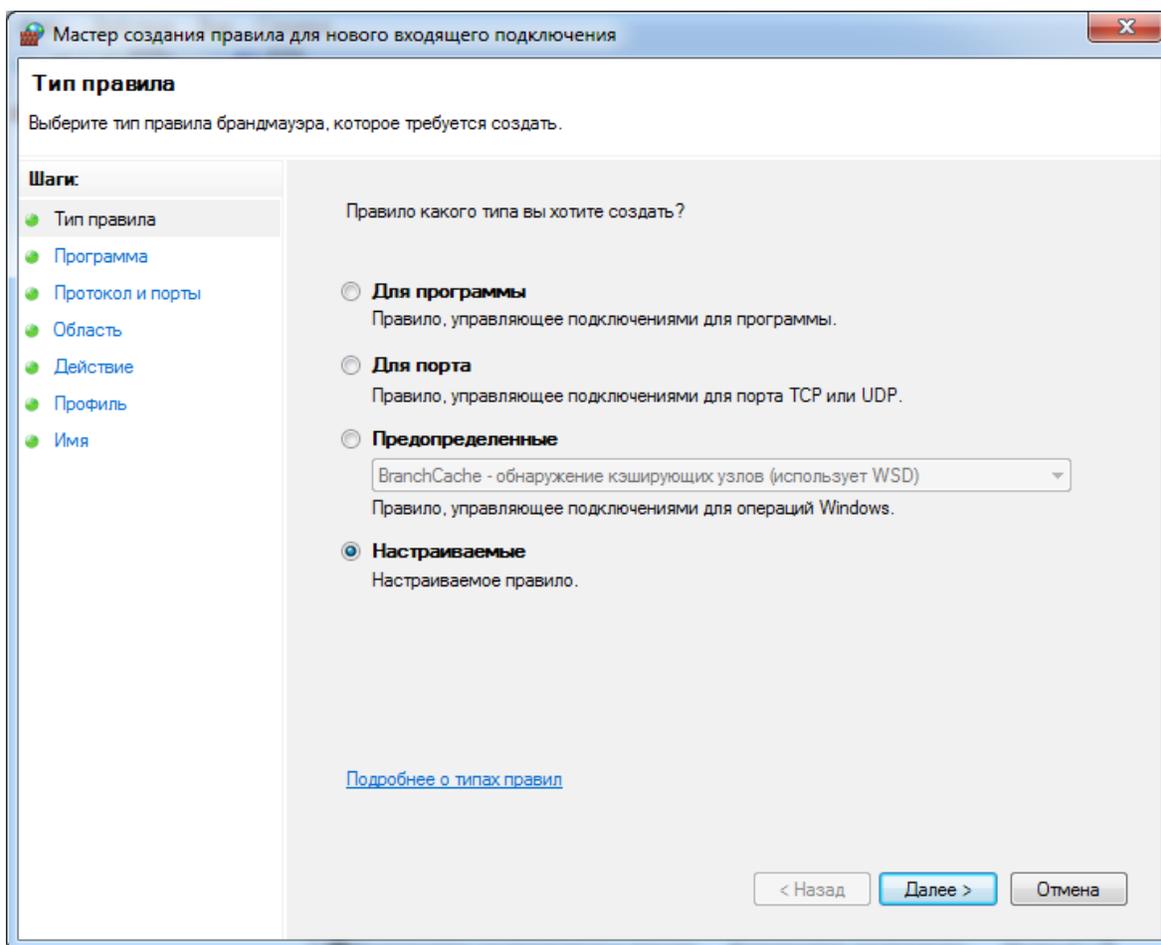
1. В строке командной строки Windows (**Win+R**) выполните команду *wf.msc*. Откроется окно апплета конфигурации службы Windows. Это же окно можно открыть через меню **Панель управления — Система и безопасность — Брандмауэр Windows** по кнопке **Дополнительные параметры**.



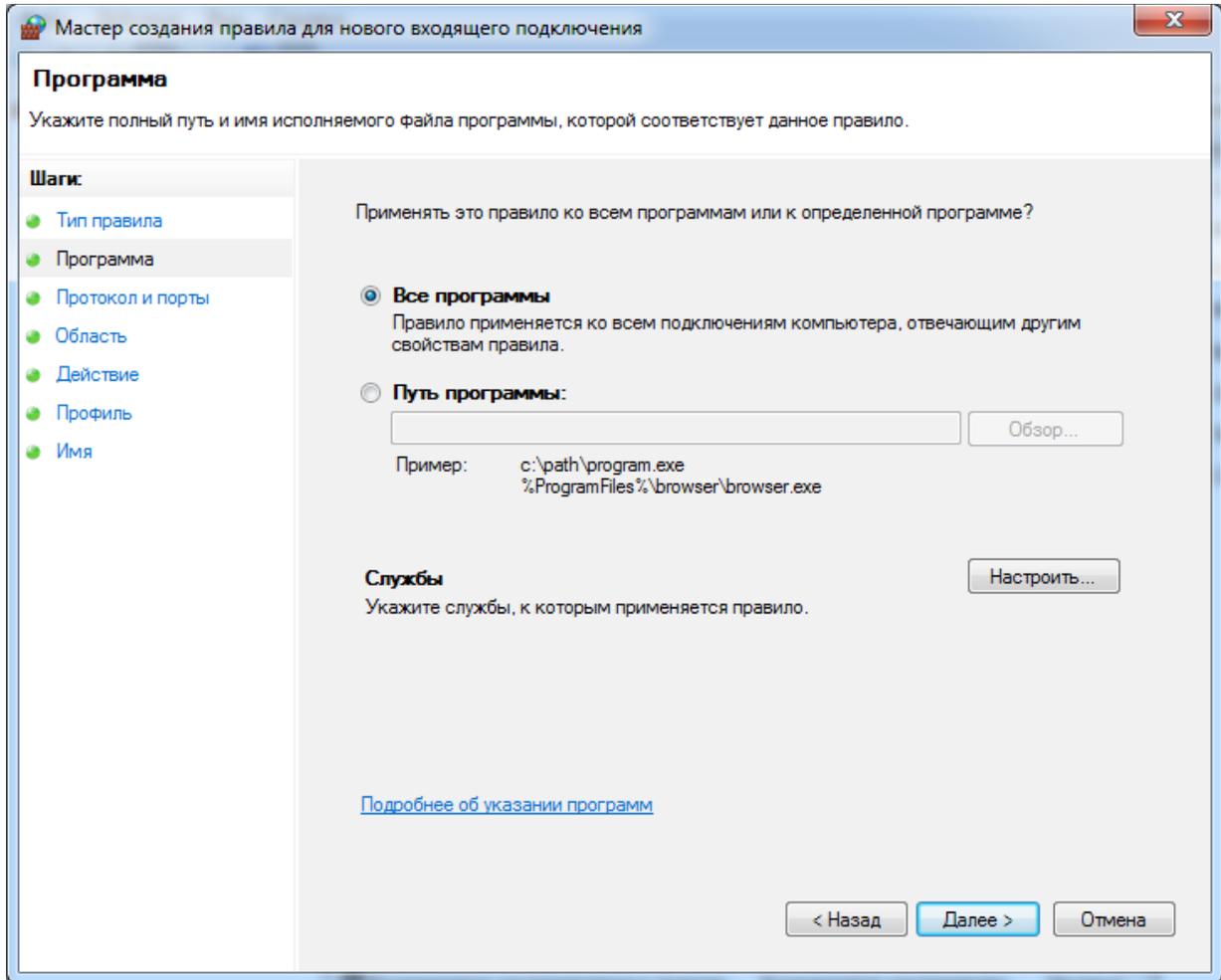
2. Выбрав в списке слева пункт **Правила для входящих подключений**, для добавления правила обработки трафика нужно нажать в правой панели **Создать правило...**



3. Откроется окно Мастера создания правила для нового подключения. В нём нужно указать тип правила — **Настраиваемые** и перейти к следующему шагу по кнопке **Далее**.



4. В пунктах **Программа** и **Протокол и порты** не требуется менять установки по умолчанию.



Мастер создания правила для нового входящего подключения

Протокол и порты

Укажите протоколы и порты, к которым применяется данное правило.

Шаги:

- Тип правила
- Программа
- Протокол и порты**
- Область
- Действие
- Профиль
- Имя

Укажите порты и протоколы, к которым применяется это правило.

Тип протокола: Любой

Номер протокола: 0

Локальный порт: Все порты

Пример: 80, 443, 5000-5010

Удаленный порт: Все порты

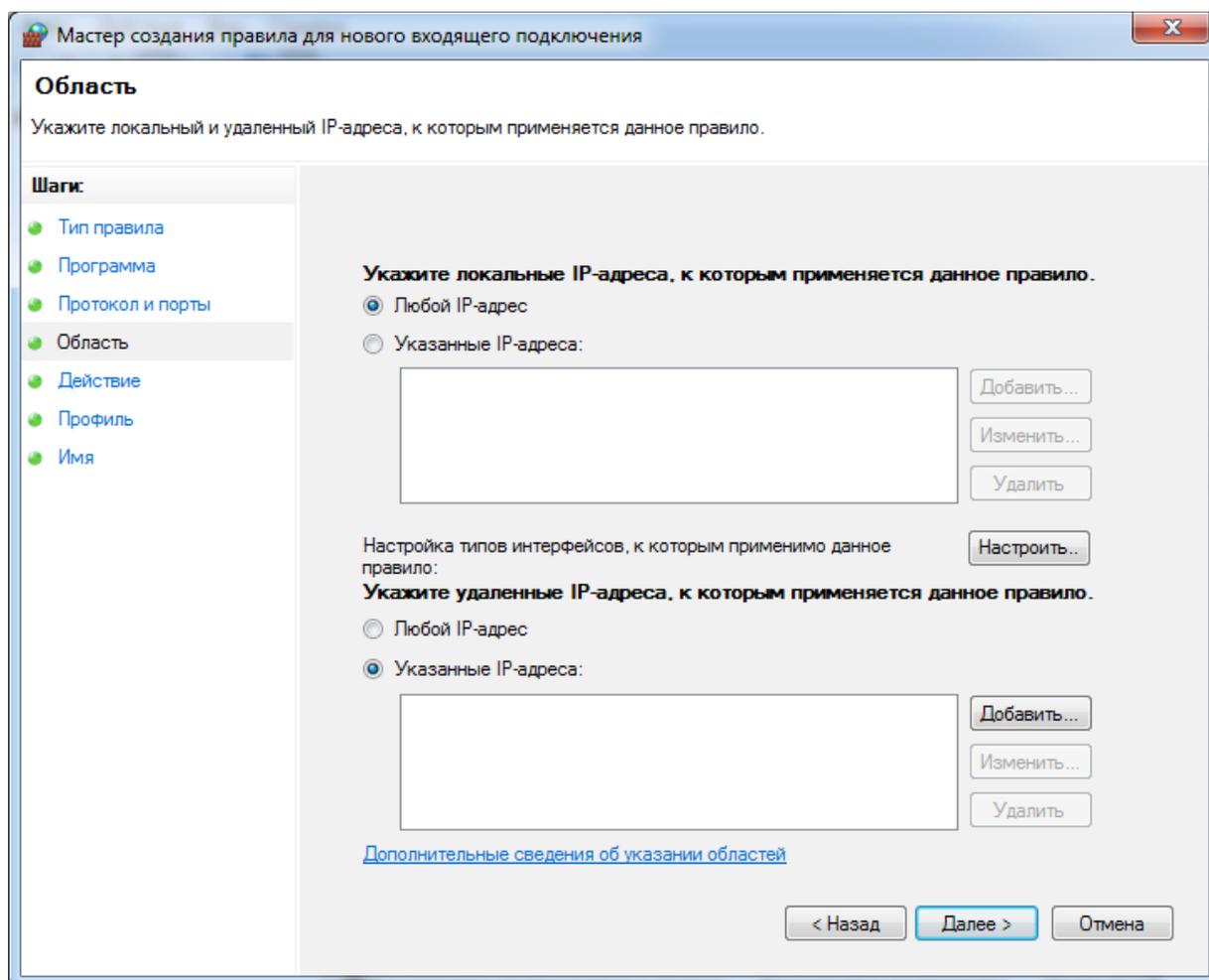
Пример: 80, 443, 5000-5010

Параметры протокола ICMP: Настроить...

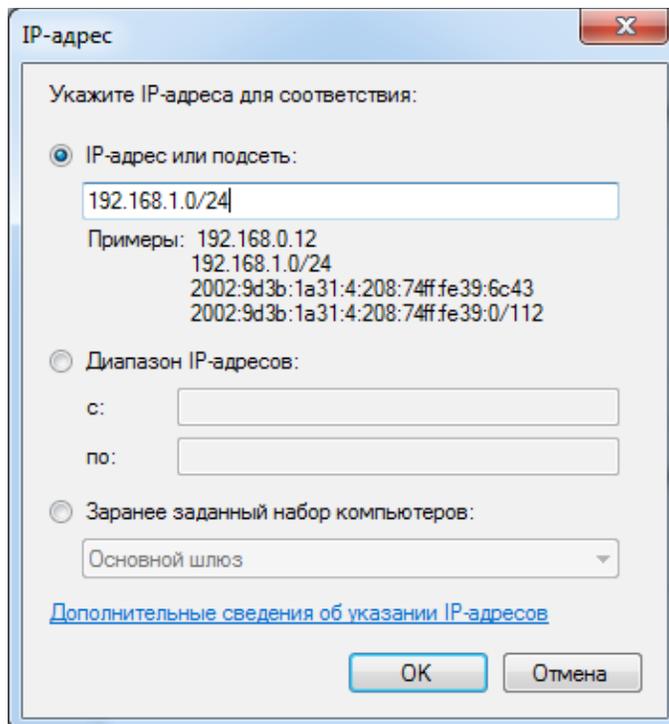
[Дополнительные сведения о протоколах и портах](#)

< Назад Далее > Отмена

В разделе **Область** следует установить переключатель **удаленные IP-адреса** в положение **Указанные** и нажать на кнопку **Добавить**.



5. В открывшемся окне, нужно указать адрес удалённой подсети и нажать **ОК**.



В случае если правилом требуется разрешить доступ с компьютера в локальной сети VPN-сервера (правило создаётся на компьютере в локальной сети клиента VPN), указывается подсеть на Домашнем интерфейсе сервера VPN.

Если правило создаётся на компьютере в локальной сети VPN-сервера (требуется для разрешения входящих подключений из сети за клиентом VPN), нужно указать подсеть, включающую адрес выданный клиенту от сервера (по умолчанию на интернет-центре это подсеть 172.16.1.0/24).

Можно указать несколько подсетей если к компьютеру требуется выполнять подключения из различных удалённых расположений. После ввода требуемых значений, в окне Мастера нужно нажать **Далее**.

The screenshot shows the 'Area' step of the Windows Firewall rule creation wizard. The window title is 'Мастер создания правила для нового входящего подключения'. The main heading is 'Область' (Area). Below it, the instruction reads: 'Укажите локальный и удаленный IP-адреса, к которым применяется данное правило.' (Specify local and remote IP addresses to which this rule applies).

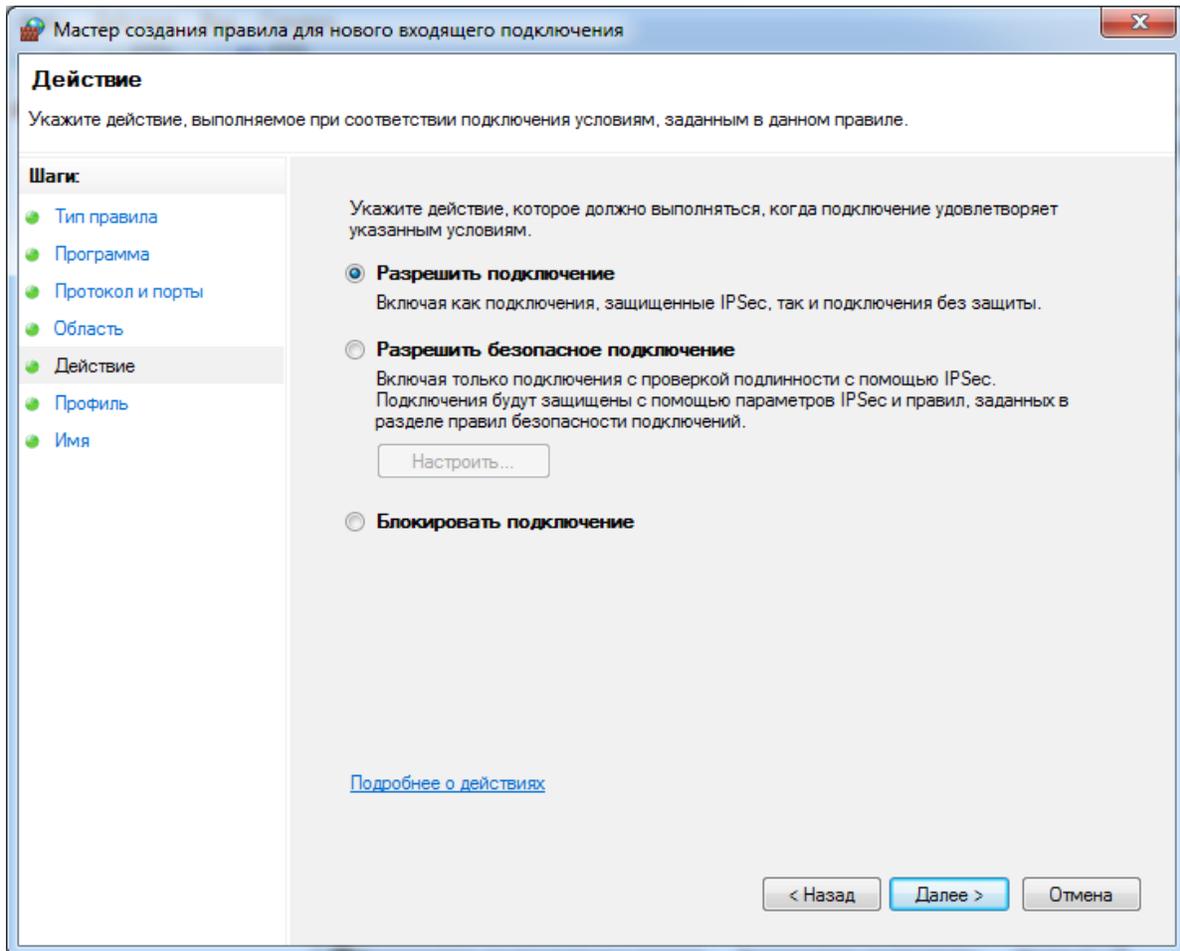
On the left, a 'Шаги' (Steps) sidebar lists: Тип правила, Программа, Протокол и порты, **Область**, Действие, Профиль, and Имя.

The main content area is divided into two sections:

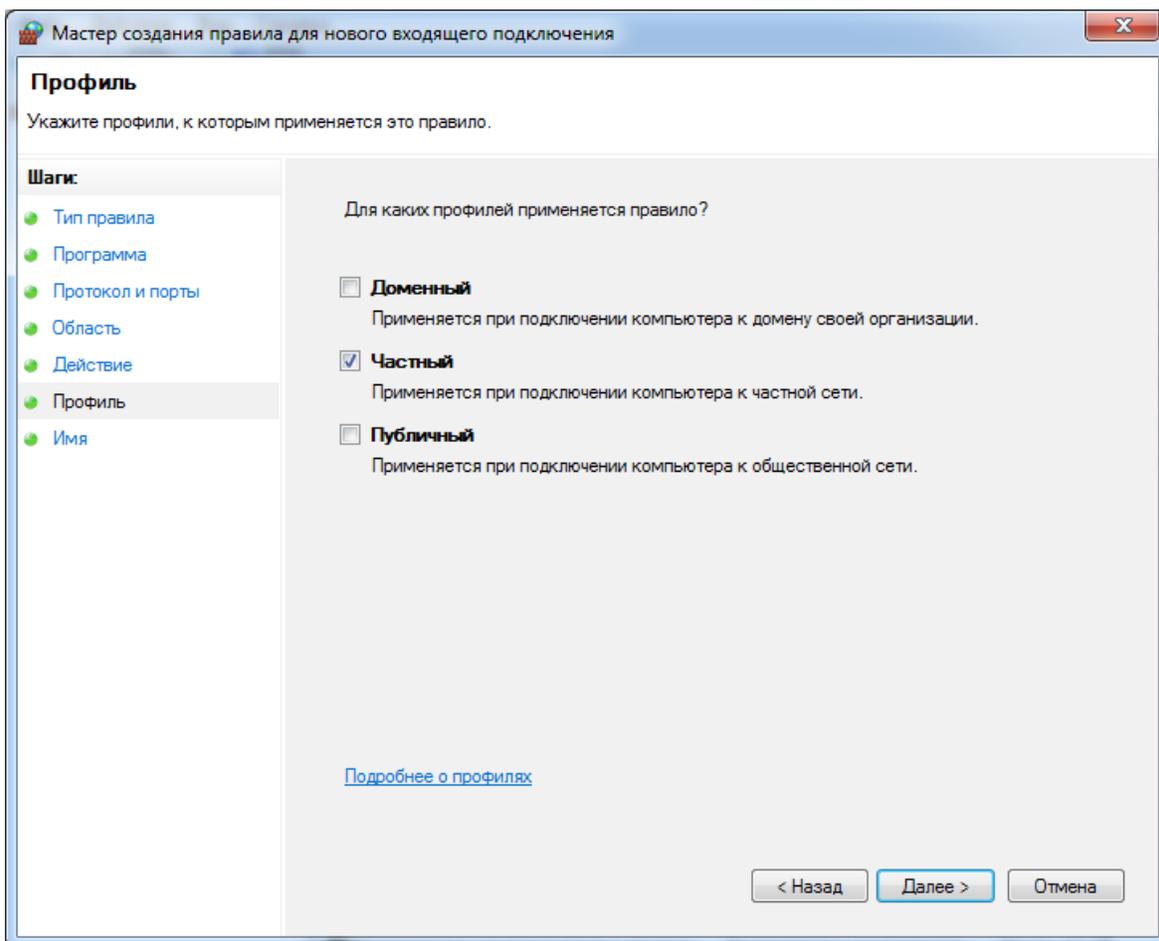
- Укажите локальные IP-адреса, к которым применяется данное правило.** (Specify local IP addresses to which this rule applies.)
 - Radio buttons for 'Любой IP-адрес' (Any IP address) and 'Указанные IP-адреса:' (Specified IP addresses:).
 - An empty text box for specifying local IP addresses.
 - Buttons: 'Добавить...' (Add...), 'Изменить...' (Change...), 'Удалить' (Delete).
- Настройка типов интерфейсов, к которым применимо данное правило:** (Interface type configuration for which this rule is applicable:)
- Укажите удаленные IP-адреса, к которым применяется данное правило.** (Specify remote IP addresses to which this rule applies.)
 - Radio buttons for 'Любой IP-адрес' (Any IP address) and 'Указанные IP-адреса:' (Specified IP addresses:).
 - A text box containing '192.168.1.0/24'.
 - Buttons: 'Добавить...' (Add...), 'Изменить...' (Change...), 'Удалить' (Delete).

At the bottom, there is a link: [Дополнительные сведения об указании областей](#) (Additional information about specifying areas). Navigation buttons at the bottom right are '< Назад' (Back), 'Далее >' (Next), and 'Отмена' (Cancel).

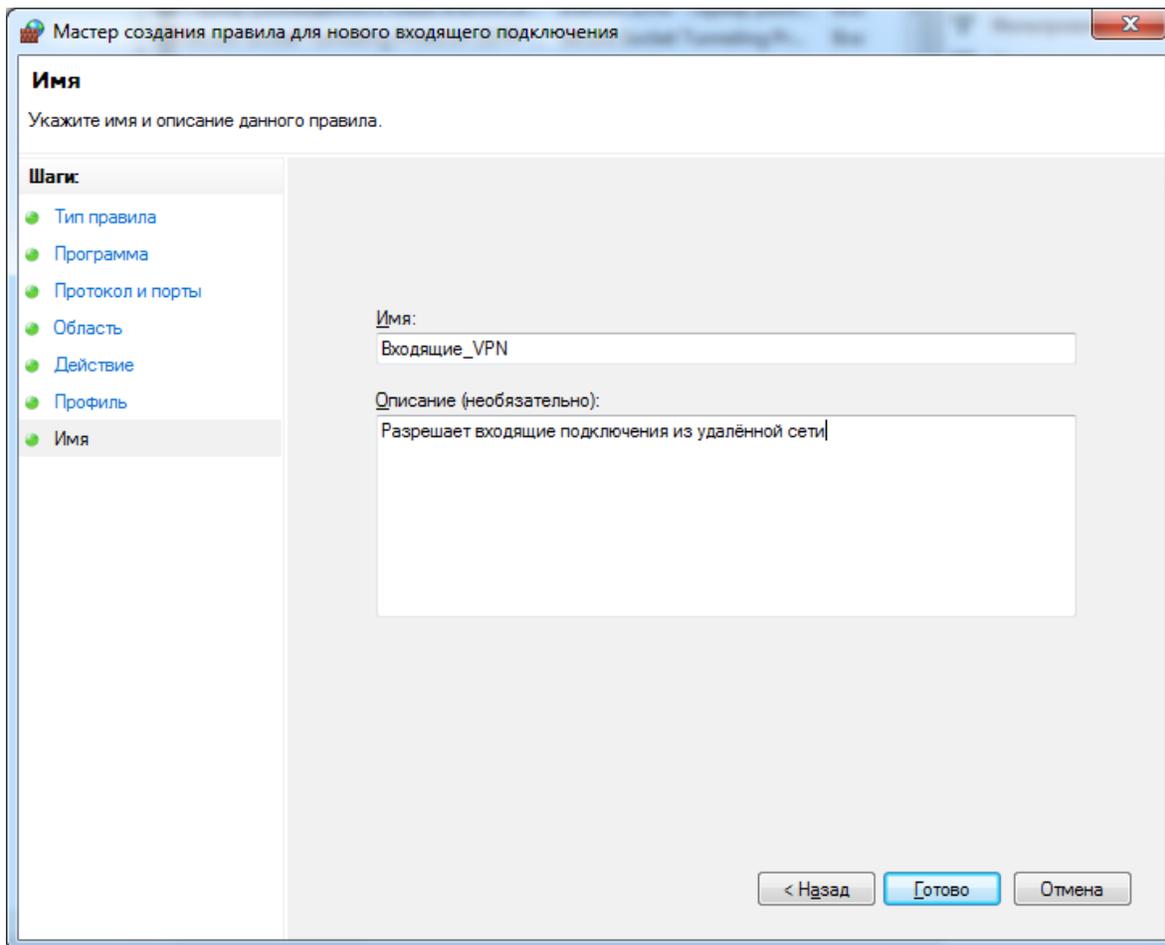
6. В следующем шаге, в разделе **Действие** оставим предустановленное значение **Разрешить подключение** и перейдём далее.



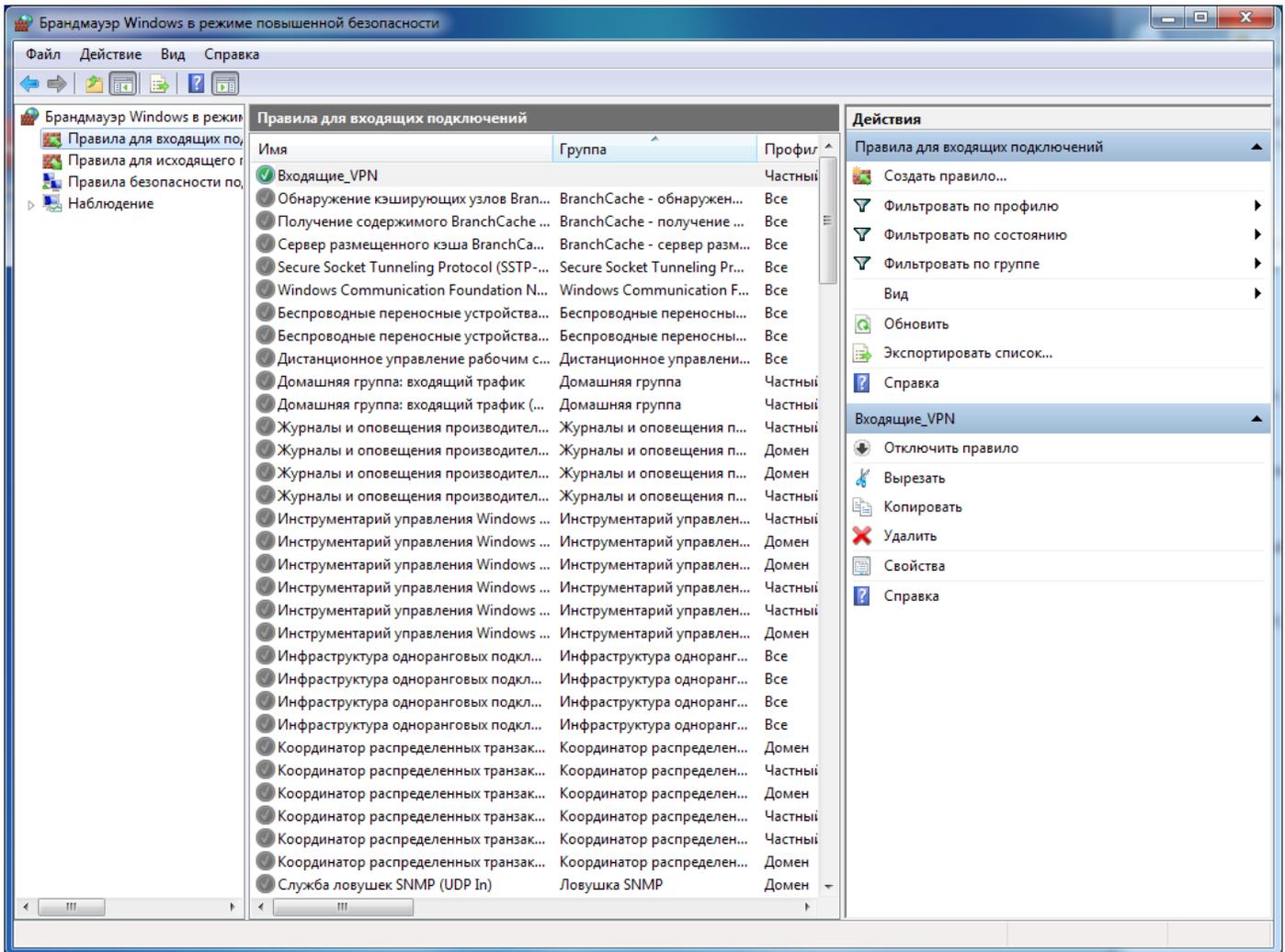
7. Раздел **Профиль** предоставляет возможность выбрать профиль, к которому будет относиться настроенное правило. Поскольку настройка выполняется для компьютера, подключенного в Домашней сети интернет-центра, достаточно оставить галочку напротив профиля **Частный**.



8. На завершающем шаге настройки, требуется указать имя правила и можно добавить поясняющее описание. По нажатию кнопки **Готово** мастер завершает работу.



9. Теперь, в окне представления **Правила для входящих подключений** отображается созданное правило. В последних версиях Windows для применения настройки дополнительных действий не требуется.



В случае если Windows-компьютер подключен к локальной сети ИЦ, являющегося VPN-сервером и к нему требуется выполнять подключения из удалённой сети (за клиентом), в разрешающем правиле межсетевого экрана следует указать подсеть из которой выдаются адреса VPN-клиентам на сервере. По умолчанию на интернет-центрах Keenetic под управлением NDMS v2 адреса при подключении к VPN-серверу выдаются клиентам из подсети частного диапазона 172.16.1.0/24.

ZyXEL Keenetic Ultra

Приложения

Файл подкачки | Сеть MS Windows | FTP | Права доступа | Клиент BitTorrent | Сервер DLNA | **Сервер VPN**

Сервер VPN (PPTP)

Сервер VPN позволяет получить доступ к устройствам вашей домашней сети с компьютеров и мобильных устройств с подключением к интернету вне дома. Подключения разрешены [пользователям системы](#) с правом доступа "vpn". Для доступа клиентов VPN-сервера в Интернет необходимо включить опцию "Транслировать адреса клиентов (NAT)".

Включить:

Одно подключение на пользователя:

Разрешить подключения без шифрования:

Транслировать адреса клиентов (NAT):

Доступ к сети: Home network (Wired and wireless hosts) (Home) ▾

Начальный адрес пула: 172.16.1.33

Размер пула адресов: 10

Имя пользователя	IP-адрес	Доступ разрешен
admin	Нет	Нет
net_1	172.16.1.2	Да
alexander	Нет	Да

Если компьютер, к которому требуется установить удалённое подключение, расположен в сети интернет-центра, являющегося клиентом VPN, в разрешающем правиле файрвола Windows потребуется указать подсеть адрес из которой установлен на интерфейсе подключающегося из-за VPN-сервера компьютера. Согласно схеме <http://zyxel.ru/sites/default/files/kb/KB-4214/4214-01.jpg> в статье БЗ-4214, это сеть 192.168.2.0/24.