

Что такое Firewall

С системой портов тесно связана такая система защиты, как Firewall — программа, которая обеспечивает санкционированность всей информации, приходящей или уходящей с компьютера. К примеру, при отправке почты используется порт 25, а при получении — порт 110. С этими портами работает почтовая программа. Если же какая-нибудь другая программа — например, вирус-«троян» — попытается запросить этот порт, то Firewall не даст ей это сделать (в принципе, «трояну» ничего не стоит замаскироваться под почтовую программу, но это сложнее — прим. ред.). Кроме того, Firewall вообще не позволяет осуществлять связь с удаленным компьютером, если это не разрешено пользователем. Перед началом использования программы необходимо произвести ее настройку — указать номеров портов, через которые может идти обмен данными, и программ, которые с этими портами работают. В современных «файерволлах» настройка может проходить и автоматически.

Иными словами, если с компьютера отправляется пакет данных, то Firewall посмотрит, какая программа его отправляет, по какому порту, и на какой порт. Обеспечение информационной безопасности и защита от проникновения «извне» также тесно связаны с управлением системой портов. На компьютере постоянно запущено множество программ. И не исключено, что при обращении к какому-либо порту некая программа возьмет и ответит на запрос, да еще и проигнорировав положенную авторизацию доступа. Это так называемая «дыра» — за что программистов обычно нещадно ругают. В другом случае, операционная система, принимая данные по какому-либо порту, может попросту «повиснуть» — опять-таки из-за ошибки в своем программном коде. Так, до появления Service Pack 3 для Windows NT, пакеты, адресованные на 139 порт компьютера с этой операционной системой, приводили либо к перезагрузке ОС, либо к ее «зависанию» (кстати, «дыры» могут появляться и по иным причинам — не только из-за системы портов, просто «дыра через порт» — самый распространенный вариант).

Порты компьютера можно просканировать — то есть послать ему пакеты данных, адресованные на все порты подряд, и ждать ответа хоть от какого-нибудь из них. Если отклик есть, значит, с этим портом можно попробовать «договориться» — в частности, заставить программу, которая им заведует, работать в своих целях. «Прослушать» порты можно, например, с помощью программы Internet Maniac. С такого сканирования и поиска «дыр» в программном обеспечении обычно начинается любая хакерская атака, поэтому многие провайдеры, банковские системы и другие большие сетевые представительства

отслеживают подобные действия и принимают адекватные меры в адрес того, кто это делает.

Вот так сканируются порты. Это пример — а при настоящей хакерской атаке можно было бы и «дыру» отловить, да и самому попасться — зависит от опыта обеих сторон.

Использование Firewall позволяет в определенной степени свести «на нет» риск от несанкционированного сканирования портов. Эта программа не дает возможности получить с портов, не входящих в список разрешенных, какой-либо ответ, так как вообще не пропускает к ним подобного рода запросы. Но Firewall не сможет помочь, если атака ведется с помощью вполне законного доступа — скажем, в вашей почте окажется письмо, содержащее вирус.

Как правильно настроить firewall? (В том числе, чтобы проходило ping-тестирование)

Сетевой экран — это программа, установленная на пользовательском компьютере и предназначенная для защиты от несанкционированного доступа к компьютеру. Другое распространенное название сетевого экрана — файрвол или файервол образовано транслитерацией английского термина firewall. Иногда сетевой экран называют еще брандмауэром (нем. brandmauer) — это немецкий эквивалент слова firewall. Основная задача сетевого экрана — не пропускать (фильтровать) пакеты, не подходящие под критерии, определённые в конфигурации сетевого экрана.

Здесь мы опишем, как выполнить требуемые настройки для сетевых экранов:

1. Настройка сетевого экрана Windows XP [Microsoft Firewall](#)
2. Настройка сетевого экрана Windows 7

(О настройке сетевого экрана Windows Vista читайте здесь - <http://technet.microsoft.com/en-us/library/cc749323.aspx>)

Настройка сетевого экрана Microsoft Firewall

Если вы хотите использовать на своем компьютере сетевой экран Microsoft Firewall, его надо включить. Сетевой экран Microsoft Firewall включается следующим образом. В главном меню Windows выбрать Settings ==> Control Panel (см. Рис. 1), затем в открывшемся окне <Control Panel> найти и открыть окно сетевого экрана двойным щелчком

по значку Windows Firewall (см. Рис. 2).



Рис. 1



Рис. 2

Во вкладке General окна <Windows Firewall> включить опцию On (recommended) и, таким образом, включить работу сетевого экрана Microsoft Firewall (см. Рис. 3). Далее выполняется настройка сетевого экрана. Чтобы настройки соответствовали требованиям Регламента, надо разрешить следующее сетевые взаимодействия:

разрешить ping-тестирование вашего компьютера;

разрешить доступ к вашему компьютеру по протоколу HTTP для программ пакета BotikTools.



Рис. 3

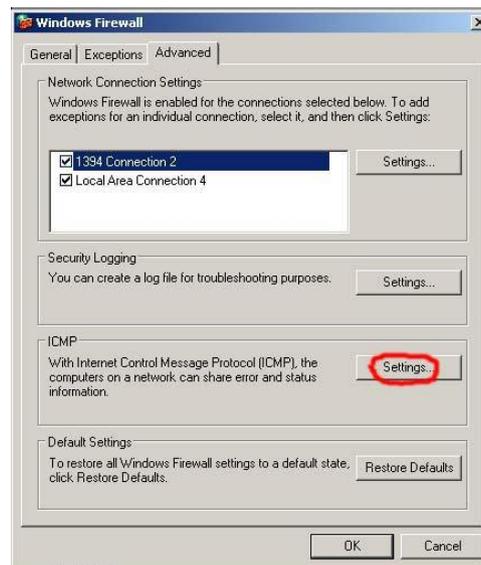


Рис. 4

Настройка разрешения ping-тестирования

Во вкладке Advanced окна <Windows Firewall> (см. Рис. 4) щелкнуть Settings в разделе ICMP (отмечено красным на Рис. 4). В открывшемся окне <ICMP Settings> установить флаг Allow incoming echo request (см. Рис. 5) и щелкнуть ОК. Теперь ваш компьютер доступен для ping-тестирования.

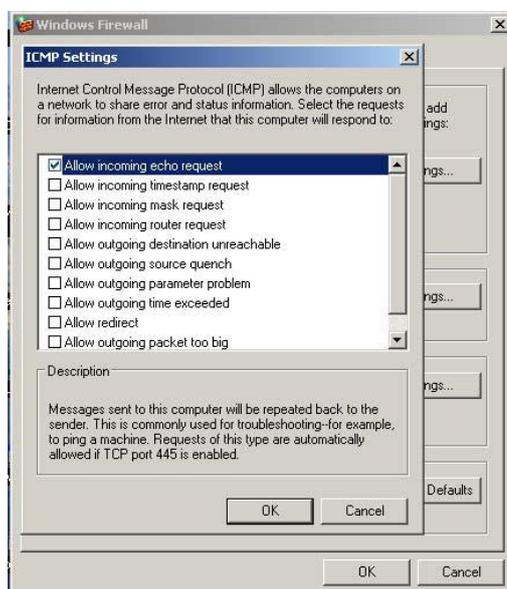


Рис. 5

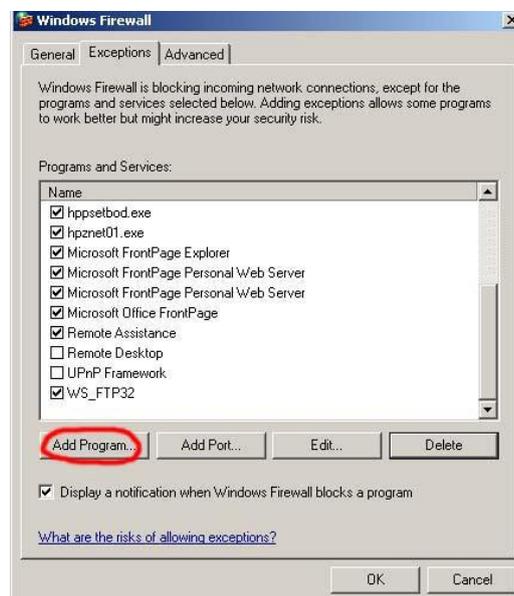


Рис. 6

Настройка разрешения доступа по протоколу HTTP

Сетевой экран блокирует входящие сетевые соединения с программами, которые установлены на вашем компьютере. Тем самым обеспечивается защита от несанкционированного доступа. Для корректной работы некоторых программ необходимо сделать исключение и разрешить возможность таких соединений. Эти программы перечислены во вкладке Exceptions (Исключения).

В окне <Windows Firewall> выберите вкладку Exceptions (см. Рис. 6). Здесь перечислены программы и сервисы, которым разрешены входящие соединения по протоколу HTTP. Для этого щелкните Add Program... (на Рис. 6 отмечено красным). В открывшемся окне <Add a Program> (см. Рис. 7) щелкните Browse, чтобы указать путь к программе.



Рис. 7

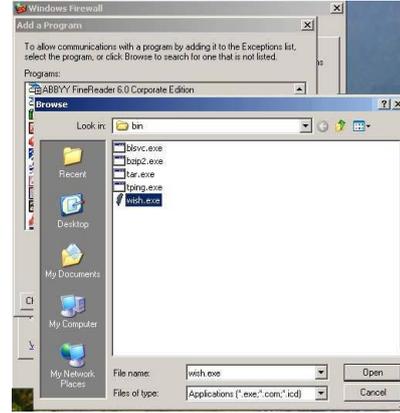


Рис. 8

На Рис. 8 показано стандартное окно <Browse> папки C:\Program Files\BotikTools\bin, в которой хранится программа wish.exe. Отметив программу wish.exe, щелкните Open в окне <Browse> и, таким образом, введите путь к программе wish.exe в поле Path окна <Add a Program>. В окне <Add a Program> щелкните ОК, чтобы добавить программу wish.exe в список Exceptions. Теперь сетевой экран разрешит доступ по протоколу HTTP программам.

Сетевой экран Microsoft Firewall настроен.

Настройка сетевого экрана в Windows 7

Открыть окно Мой компьютер -> Администрирование и для настройки брандмауэра выбрать режим "Брандмауэр Windows в режиме повышенной безопасности" (см. Рис. 21)

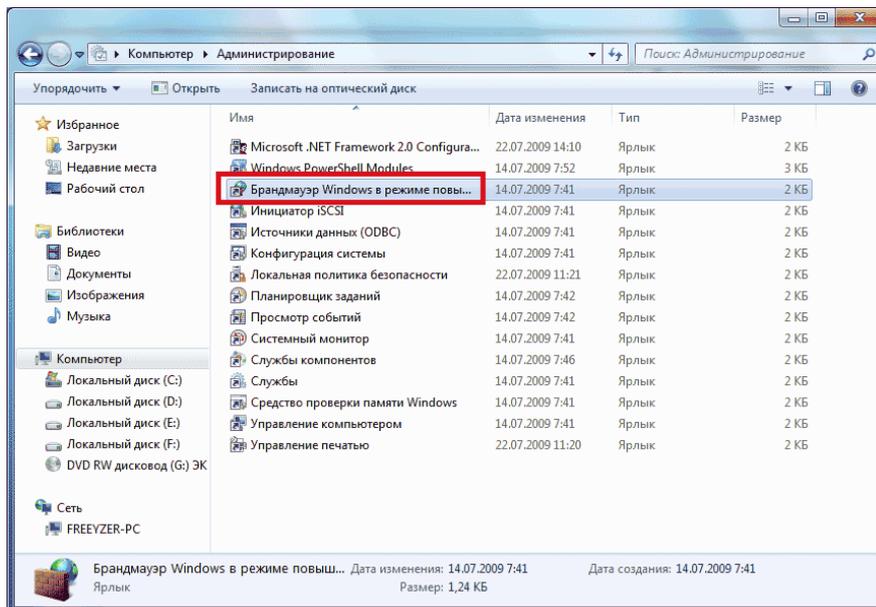


Рис. 21

В левой части открывшегося окна <Брандмауэр Windows в режиме повышенной безопасности> выбрать "Правила для входящих подключений" и затем в правой части окна выбрать действие "Создать правило" (см. Рис. 22).

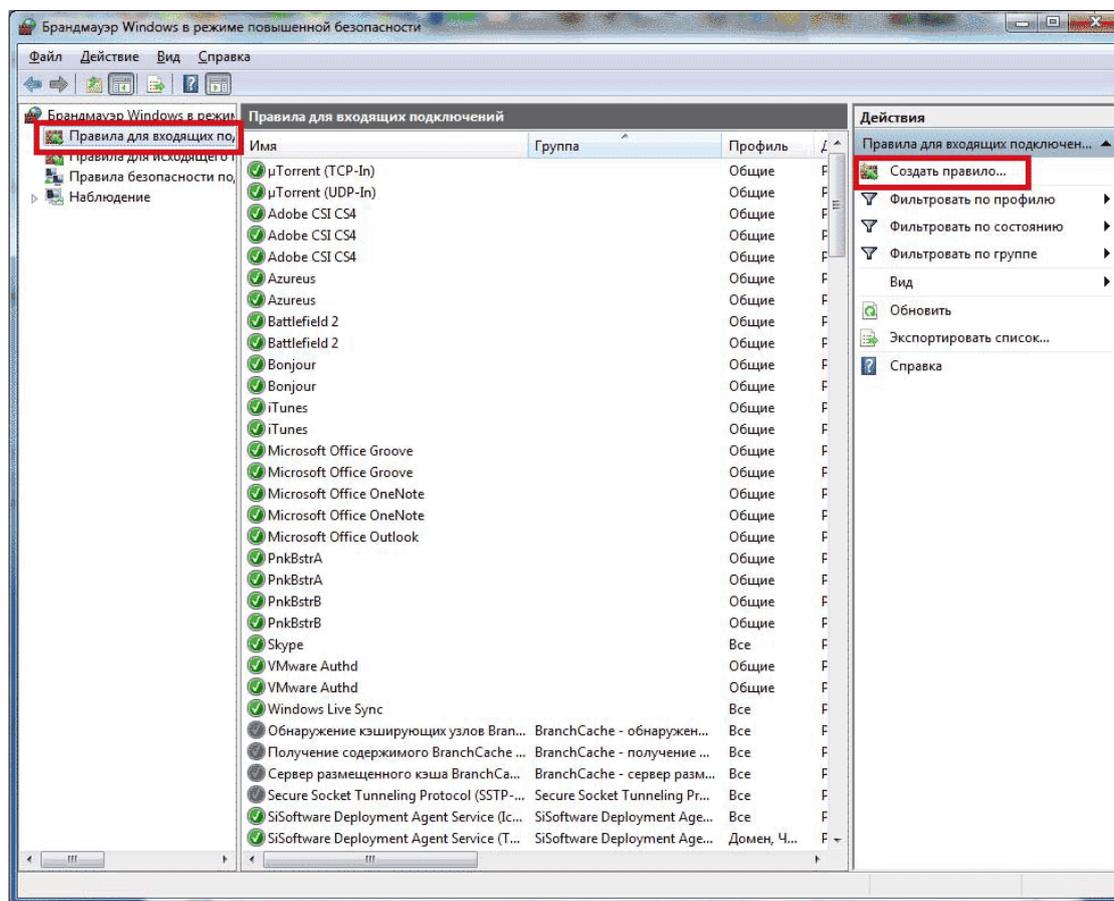


Рис. 22

Откроется окно <Мастера создания правил для нового входящего подключения> (см. Рис. 23). На первом шаге мастера "Тип правила" надо выбрать тип создаваемого правила, в нашем случае это настраиваемое правило, поэтому следует выбрать вариант Настраиваемые и щелкнуть по кнопке Далее.

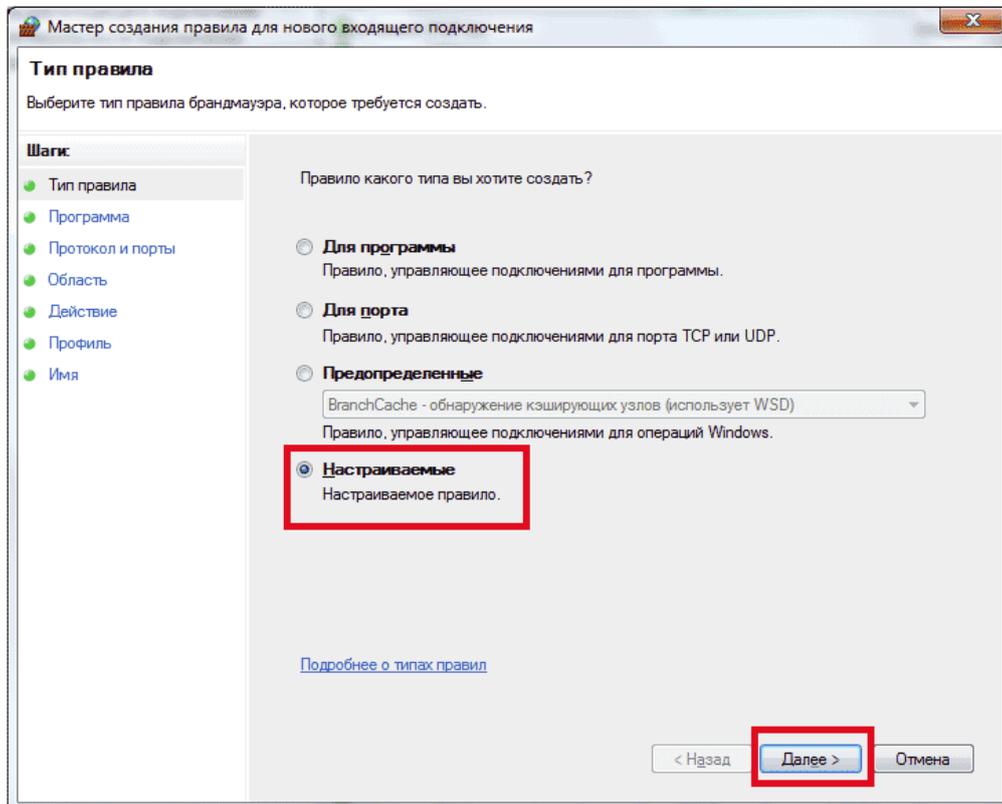


Рис. 23

На втором шаге мастера создания правил "Программа" следует выбрать имя исполняемого файла программы, для которой создается правило. В нашем случае следует выбрать вариант Все программы и щелкнуть по кнопке Далее (см. Рис. 24).

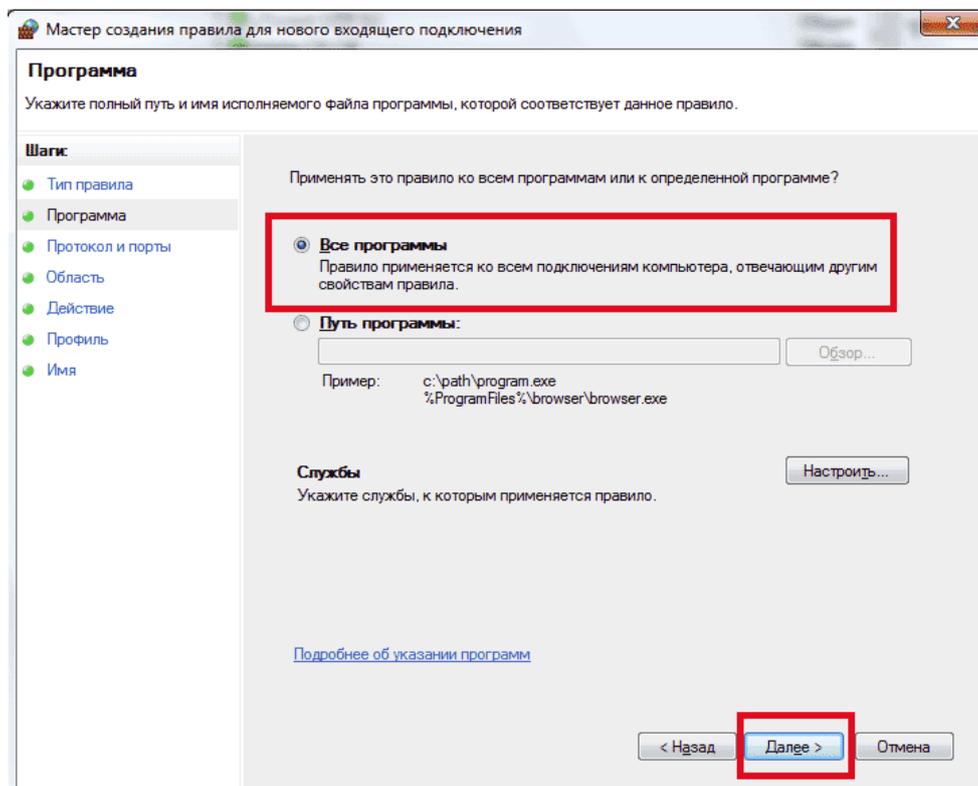


Рис. 24

На третьем шаге мастера создания правил "Протокол и порты" выбираются протоколы, к которым применяется создаваемое правило. Здесь надо в раскрывающемся списке Тип протокола выбрать протокол ICMPv4 и щелкнуть по кнопке Настроить (см. Рис. 25)

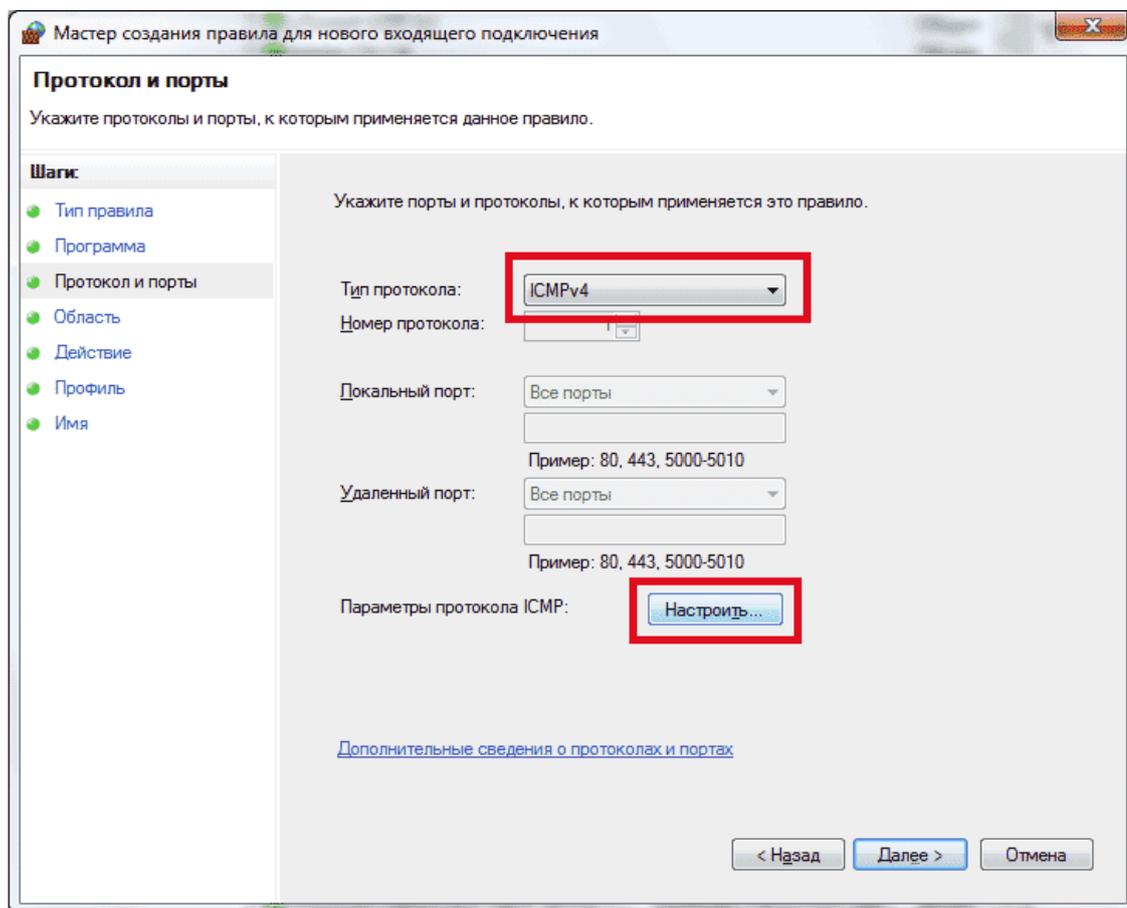


Рис. 25

В открывшемся окне <Настройка параметров ICMP> надо выбрать вариант Определенные типы ICMP, установить флаг Эхо-запрос и щелкнуть по кнопке ОК (см. Рис. 26).

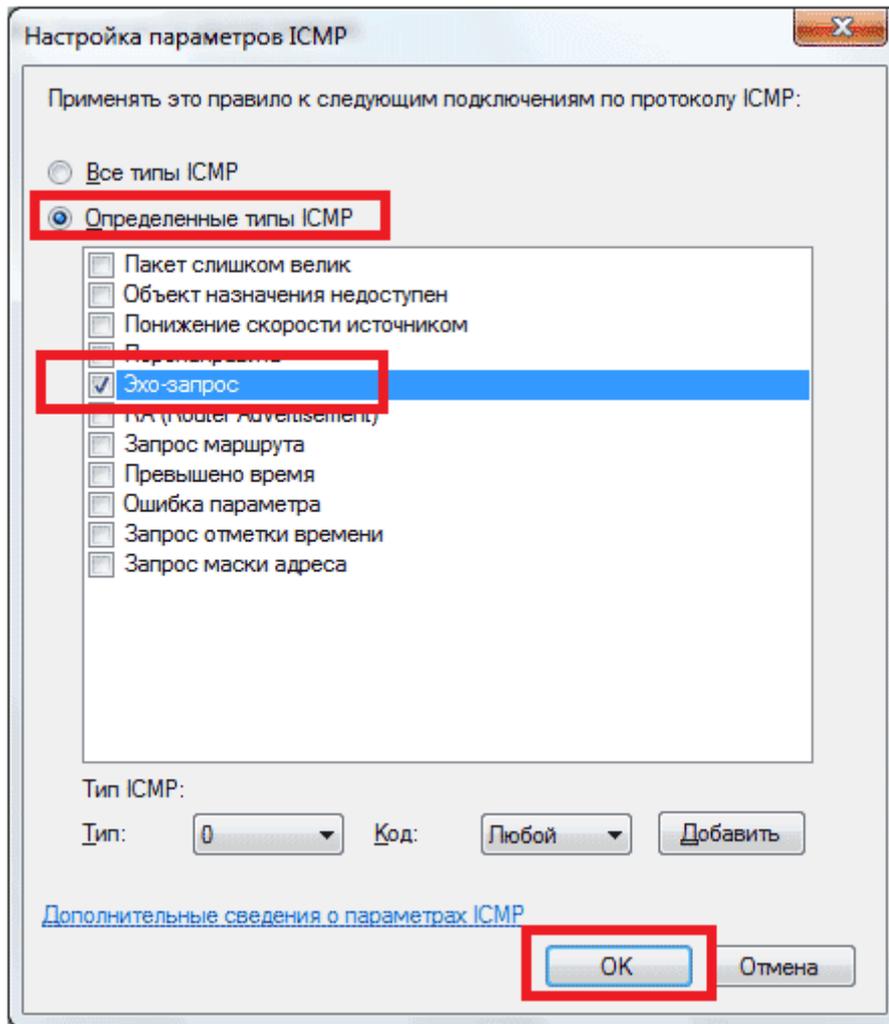


Рис. 26

Далее для перехода к следующему шагу мастера создания правила щелкнуть по кнопке Далее (см. Рис. 27)

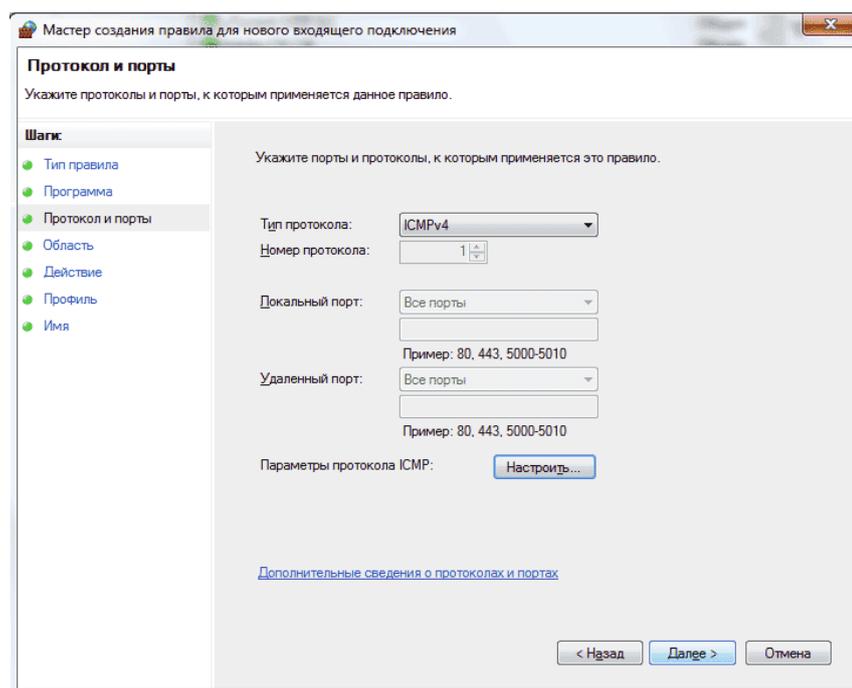


Рис. 27

На четвертом шаге "Область" указывают IP-адреса, к которым применяется создаваемое правило. Здесь надо выбрать варианты Любой IP-адрес и щелкнуть по кнопке Далее (см. Рис. 28).

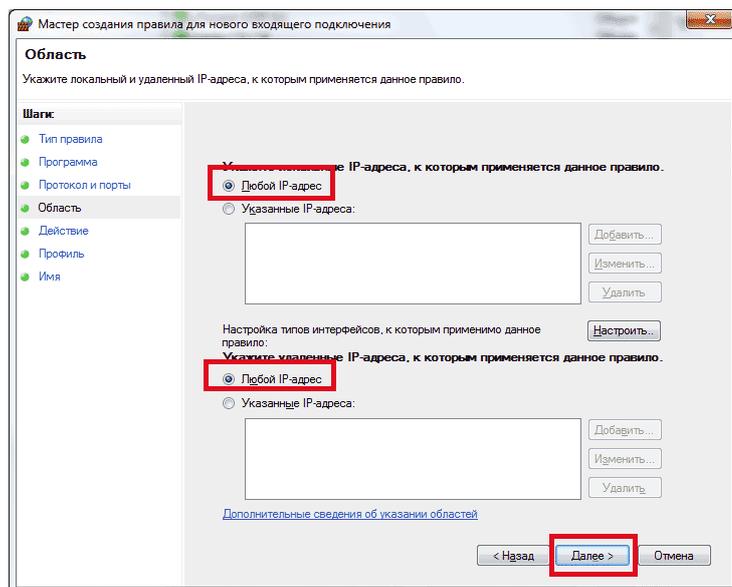


Рис. 28

На пятом шаге "Действие" указывают действие, выполняемое при соответствии подключения условиям, заданным в данном правиле. Здесь надо выбрать вариант Разрешить подключение и щелкнуть по кнопке Далее (см. Рис. 29).

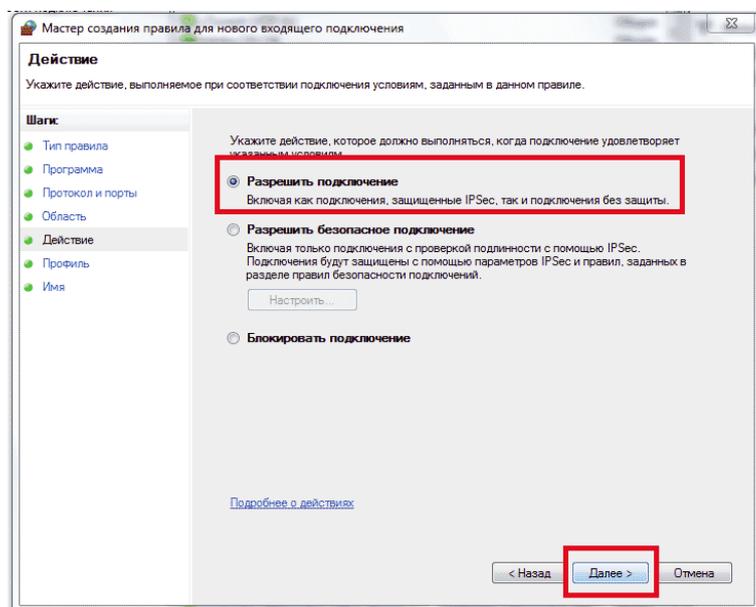


Рис. 29

На шестом шаге "Профиль" указываются профили, к которым применяется создаваемое правило. Здесь надо оставить установленные по умолчанию флаги Доменный, Частный и Публичный и щелкнуть по кнопке Далее (см. Рис. 30)

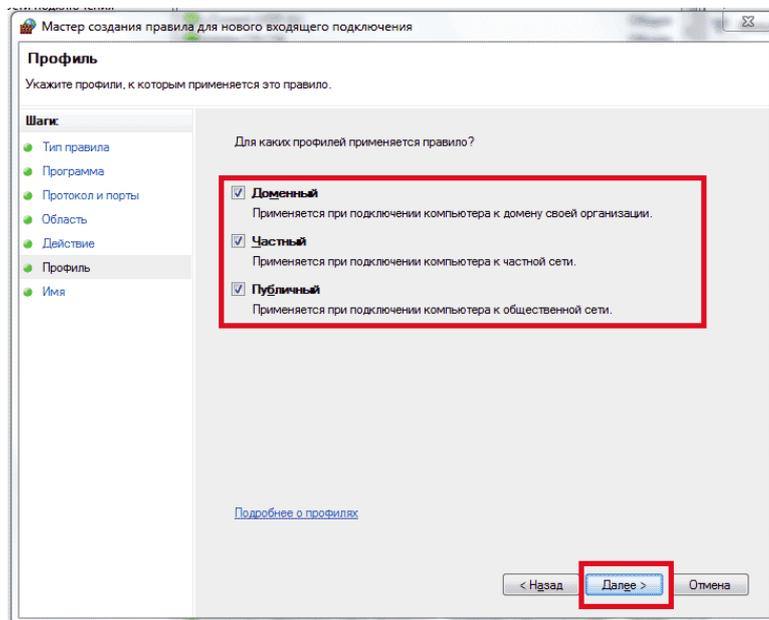


Рис. 30

На седьмом шаге "Имя" указывают имя создаваемого правила и щелчком по кнопке Готово завершают создание правила для эхо-запросов (см. Рис. 31).

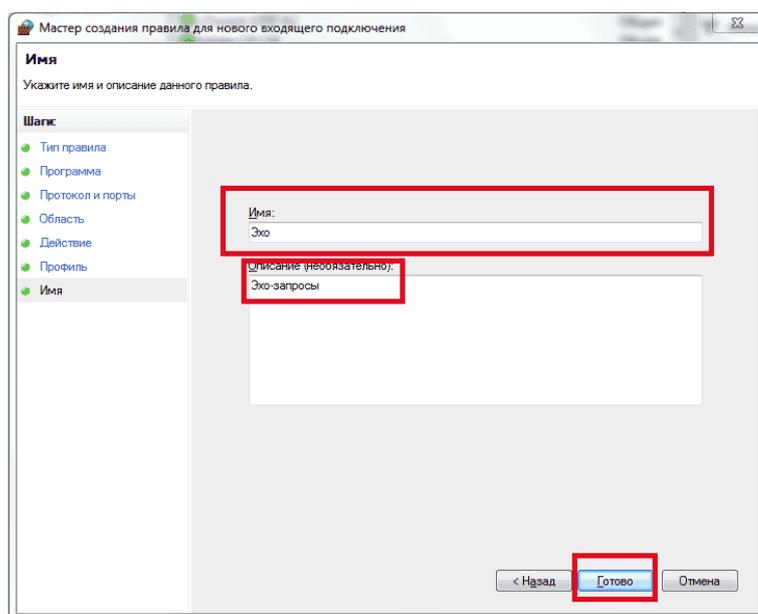


Рис. 31

На этом настройку сетевого экрана Windows 7 можно считать завершённой.

По материалам сайтов:

<http://www.secblog.info/bezopasnost/cto-takoe-firewall.html>

<http://www.botik.ru/abonents/faq/done/057-firewall-settings.html>