

Лабораторная работа №16

Тема: «Включение и настройка системного брандмауэра»

Цели работы: Изучение понятия системного брандмауэра. Получение практических навыков по включению и настройке системного брандмауэра. Закрепление теоретического материала.

Теоретическая часть

Основные свойства

Брандмауэр Windows - встроенный в Microsoft Windows межсетевой экран. Одним из отличий от предшественника (Internet Connection Firewall) является контроль доступа программ в сеть. Брандмауэр Windows является частью Центра обеспечения безопасности Windows.

Первоначально Windows XP включала Internet Connection Firewall, который (по умолчанию) был выключен из-за проблем совместимости. Настройки Internet Connection Firewall находились в конфигурации сети, поэтому многие пользователи не находили их. В результате в середине 2003 года компьютерный червь Blaster атаковал большое число компьютеров под управлением Windows, используя уязвимость в службе Удалённый вызов процедур. Через несколько месяцев червь Sasser провёл аналогичную атаку. В 2004 году продолжалось распространение этих червей, в результате чего непропатченные машины заражались в течение нескольких минут. Microsoft решила значительно улучшить интерфейс и функциональность Internet Connection Firewall и переименовать его в «Брандмауэр Windows».

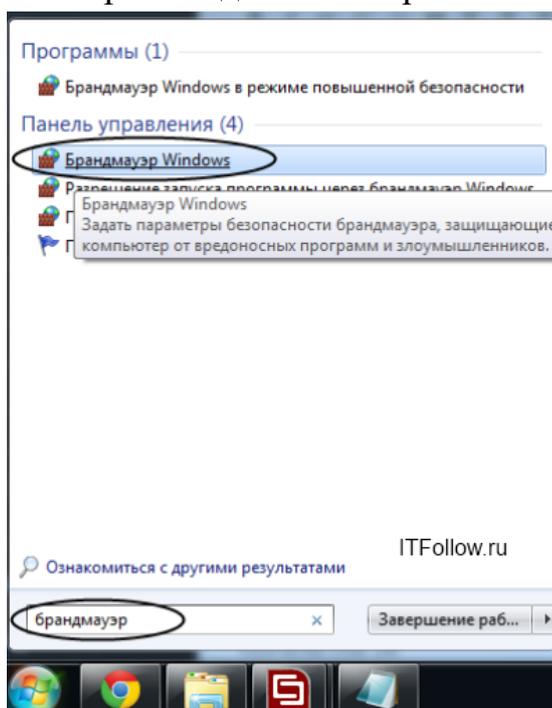
В брандмауэр Windows встроен журнал безопасности, который позволяет фиксировать IP-адреса и другие данные, относящиеся к соединениям в домашних и офисной сетях или в Интернете. Можно записывать как успешные подключения, так и пропущенные пакеты. Это позволяет отслеживать, когда компьютер в сети подключается, например, к web-сайту. Данная возможность по умолчанию отключена (её может включить системный администратор).

Изначально Брандмауэр Windows вышел в составе Windows XP Service Pack 2. Брандмауэр по умолчанию фильтрует все типы сетевых подключений: беспроводное, проводное, FireWire и VPN. Это позволяет решить проблему уязвимости, связанную с тем, что правило фильтрации начинает действовать лишь по истечении нескольких секунд после установления соединения. Брандмауэр Windows XP действует только для входящих подключений и не фильтрует исходящие соединения. Windows Server 2003 Service Pack 1, выпущенный в марте 2005 года, включал в себя уже несколько улучшенную версию брандмауэра данной операционной системы. Windows Vista привносит в Брандмауэр Windows новые возможности:

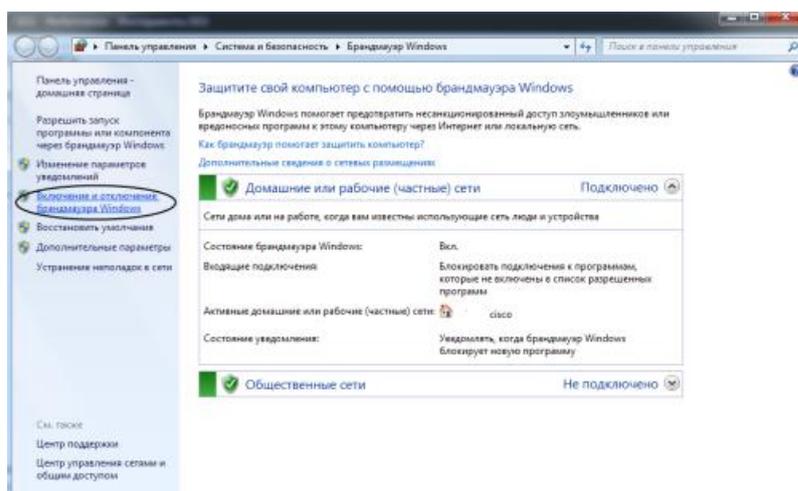
1. Применяя расширенный пакетный фильтр, появляется возможность использовать правила к определенным диапазонам портов и IP-адресов;
2. Новая оснастка консоли Брандмауэр Windows в режиме повышенной безопасности позволяет поддерживать удаленное администрирование и сделать доступными дополнительные возможности. Доступ к ней можно получить следующим образом: Пуск – Панель управления – Администрирование - Брандмауэр Windows в режиме повышенной безопасности. Либо наберите команду «wf.msc»;
3. Фильтрация исходящего трафика позволяет бороться с различными шпионскими программными обеспечениями и вирусами;
4. Фильтр соединений IPv6.

Включение, настройка и отключение системного брандмауэра

Проще всего найти брандмауэр в Windows 7 — это воспользоваться поиском через меню пуск. Для этого кликните по кнопке «Пуск» в левом нижнем углу экрана и в строку поиска вбейте Брандмауэр и кликните на появившемся значке «Брандмауэр Windows» который выделен на скриншоте ниже:

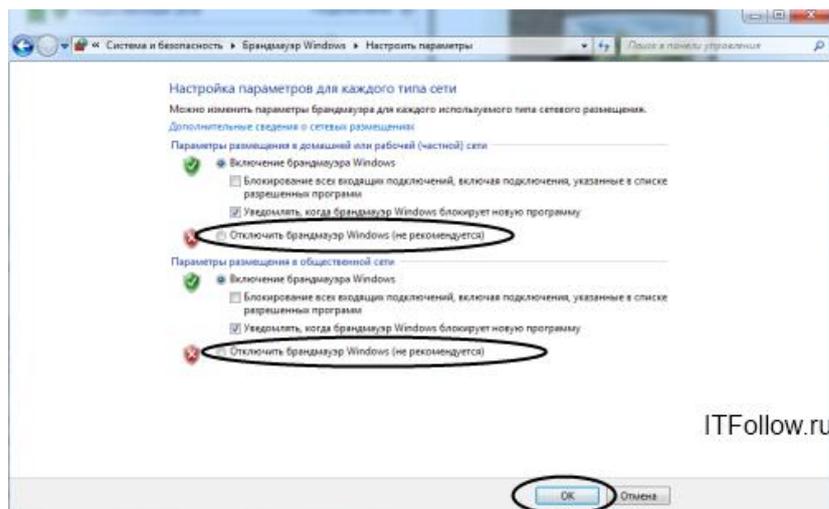


После того как откроется страница брандмауэра, выберите в левом меню пункт «Включение и отключение брандмауэра Windows 7»



Отключение брандмауэра Windows 7

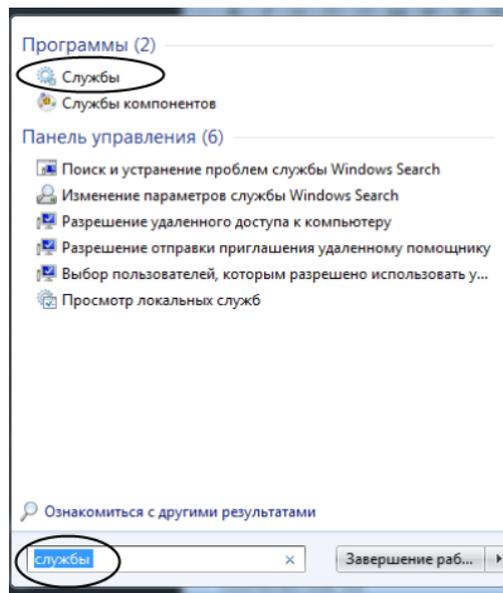
Кликнув по вкладке включение и отключение брандмауэра Windows, вы попадете на страницу, на которой можно как включить, так и отключить брандмауэр Windows 7, просто выбрав пункт меню **«Отключить Брандмауэр (не рекомендуется)»**, причем можно выбрать отключение как только для своей домашней сети, так и для всех остальных.



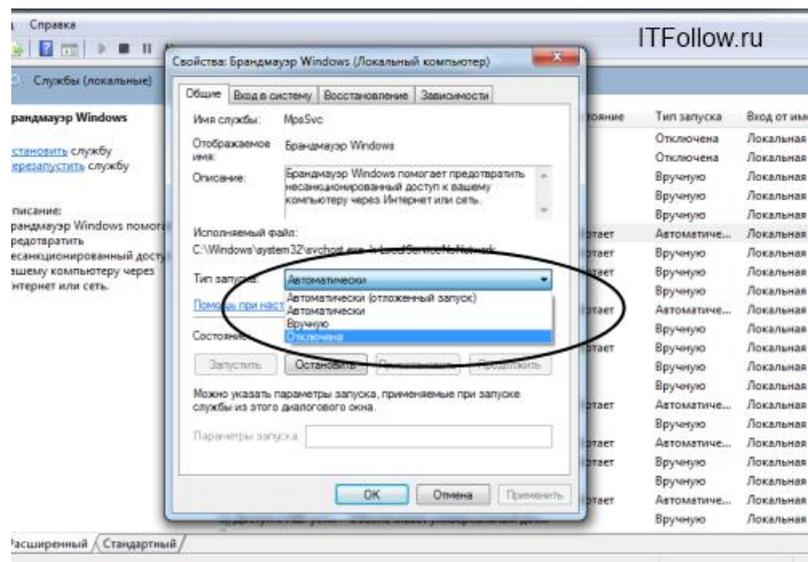
Как вы понимаете, включить брандмауэр Windows 7 (если он выключен) можно точно так же, только лишь необходимо отметить пункт меню **«Включение брандмауэра Windows»**. В этом же окошке можно снять галочки различных уведомлений когда брандмауэр блокирует новые программы.

Отключение службы Брандмауэр Windows

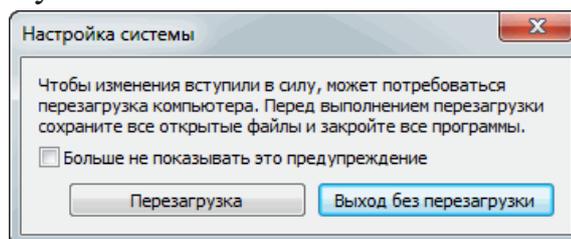
Для оптимизации операционной системы, так же рекомендуется отключить службу Брандмауэра Windows 7. Проще всего опять использовать поиск в меню **«Пуск»**. В строку поиска вбейте **«Службы»** и кликните по ним, для того что бы их открыть.



Для того что бы быстро найти службу Брандмауэр Windows, кликните на любой службе один раз и нажмите на клавиатуре букву Б, вы сразу же найдете нужную нам службу и уже на ней кликните двойным щелчком, для того что бы ее открыть.



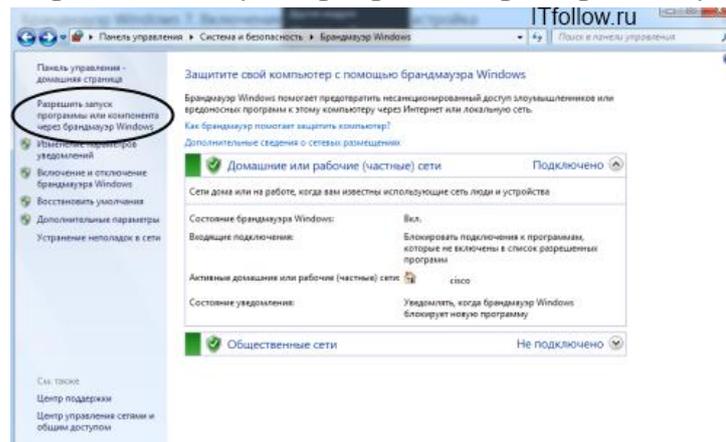
В строке Состояние — нажмите **Остановить**. Откройте выпадающее меню Тип запуска и выберите **Отключена** и нажмите **ОК**. Появится диалоговое окно с предложением перезагрузить компьютер прямо сейчас или вы можете выйти без перезагрузки, выполнив ее чуть позже.



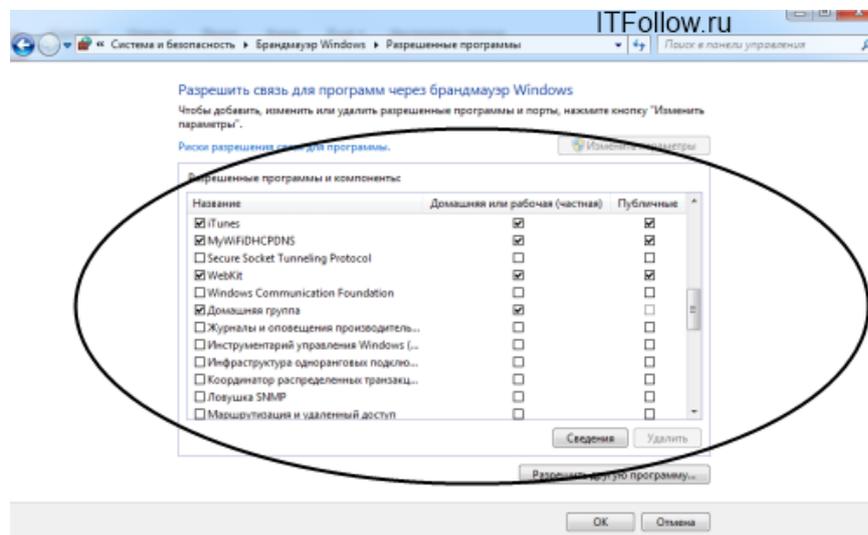
Для того что бы включить брандмауэр Windows 7, выполните те же действия в обратном порядке: Настройка брандмауэра Windows 7→Исключения брандмауэра Windows 7.

Когда брандмауэр блокирует приложения или например брандмауэр порой блокирует доступ к интернет сети для некоторых игр, существует достаточно простой способ снять это ограничение и дать полный доступ на выход в интернет для этого приложения, в этой сети, к которой вы подключены.

Для этого на странице межсетевого экрана (брандмауэра) выберите в левом меню пункт меню: *Разрешить запуск программ через брандмауэр Windows*.



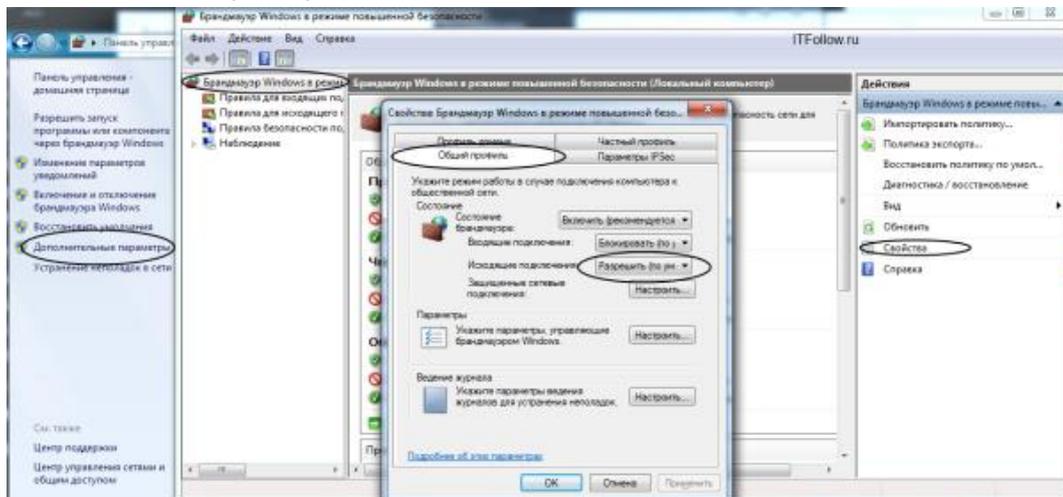
Далее найдите в списке свою программу и дайте ей доступ в нужной сети или сразу во всех, где нет галочек, таким образом можно добавлять **ИСКЛЮЧЕНИЯ брандмауэра Windows 7**.



Настройка брандмауэра Windows 7

Блокировка исходящего трафика. Для повышения безопасности компьютера, что иногда бывает особенно необходимо, можно воспользоваться способом полной блокировки исходящего трафика, т.е. такого трафика, который передается от вашего компьютера к удаленному серверу, разрешить лишь для некоторых необходимых приложений и их соответствующих служб.

Для настройки брандмауэра Windows , необходимо перейти на вкладку **Дополнительные параметры** в окне Брандмауэра. Выберите *Брандмауэр Windows в режиме повышенной безопасности* в левом меню, после чего в правой колонке, кликните по пункту «Свойства»



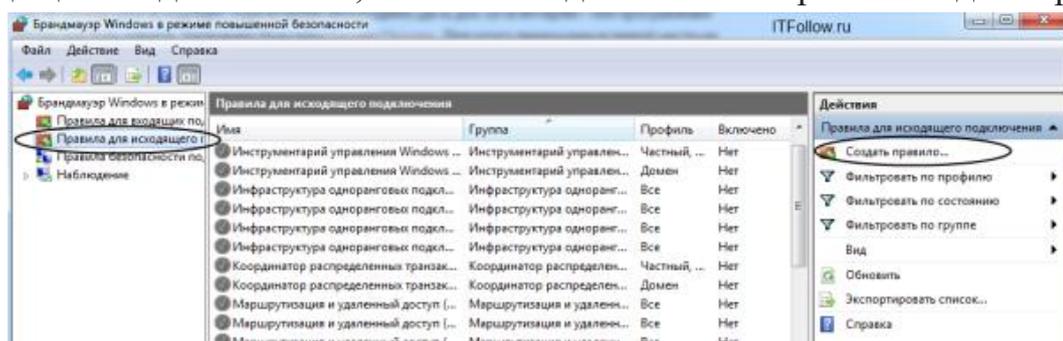
Откроется меню **Свойства Брандмауэра**, в котором можно заблокировать весь исходящий трафик, на вкладке *Исходящие подключения*.

В выпадающем меню выберите «*Блокировать*» и нажмите Ок.

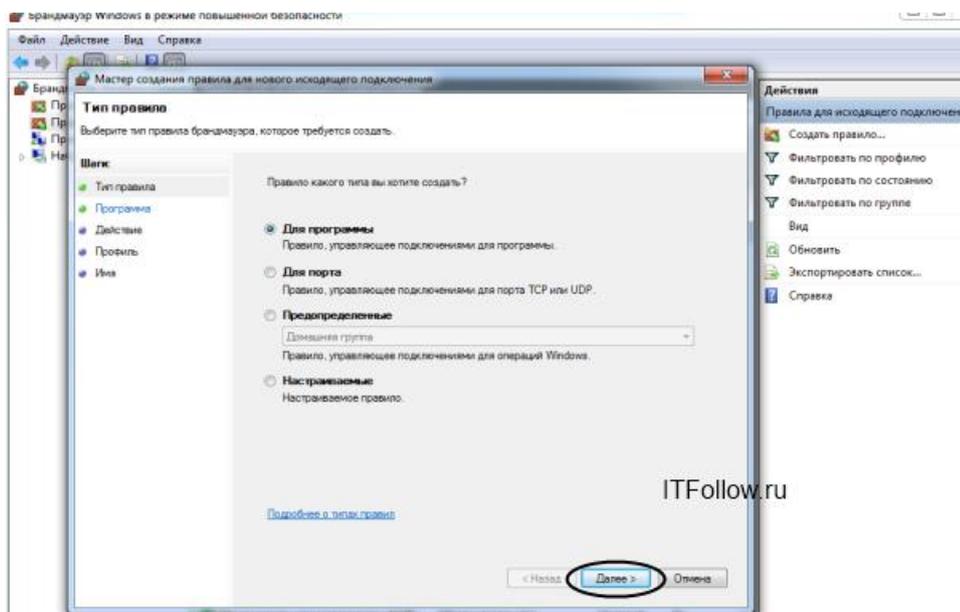
Разрешение для программ после блокировки

После того как были заблокированы все исходящие подключения к интернет, можно создать правило, которое позволит подключаться к интернету некоторым программам. Давайте для примера создадим правило разрешающее браузеру Google Chrome подключаться к сети интернет.

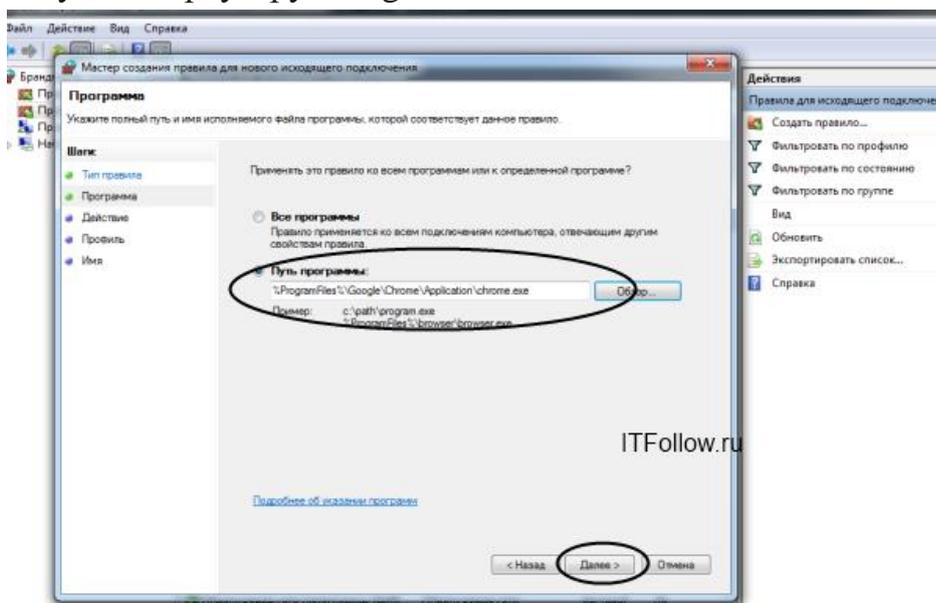
Для того что бы создать правило исходящего подключения, выберите «Правила для исходящего подключения», а в колонке действия выберите «Создать правило»:



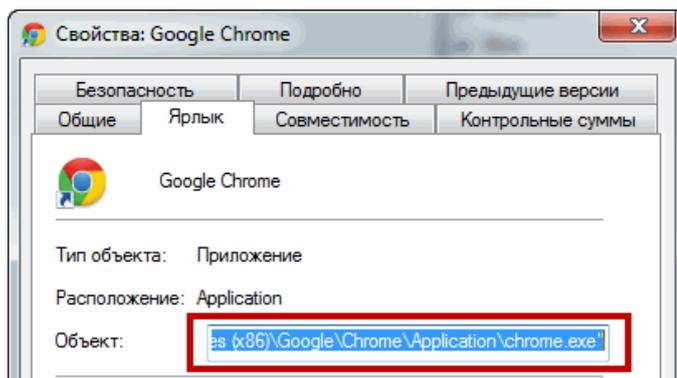
Появится мастер добавления нового правила, в котором необходимо нажать Далее→



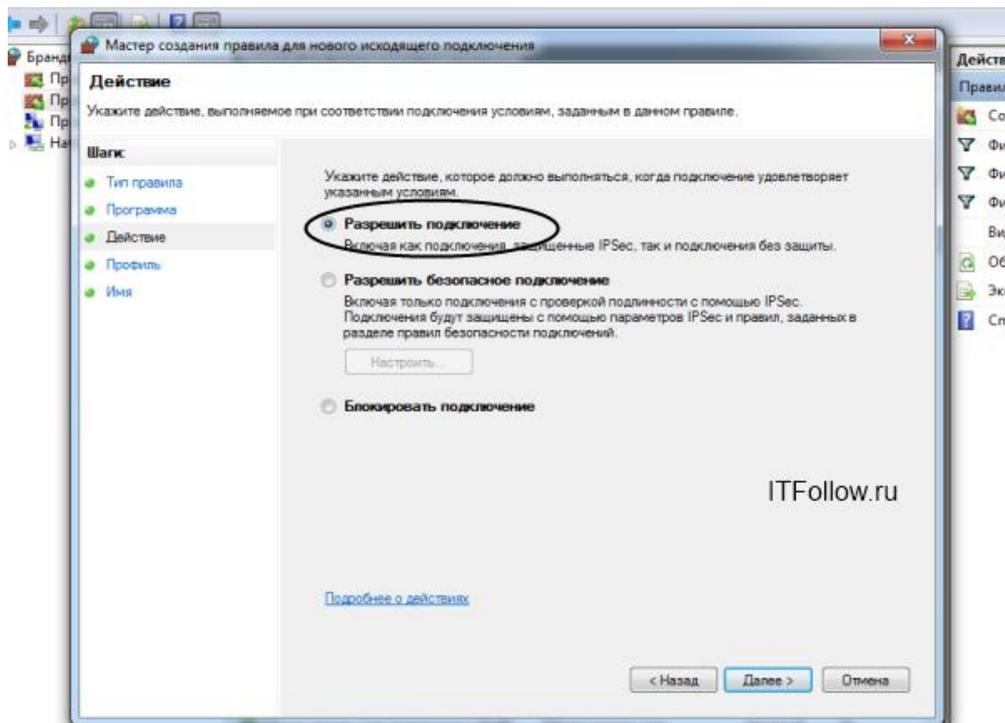
На следующей странице, используя кнопку Обзор добавляете путь к приложению, в нашем случае к браузеру Google Chrome.



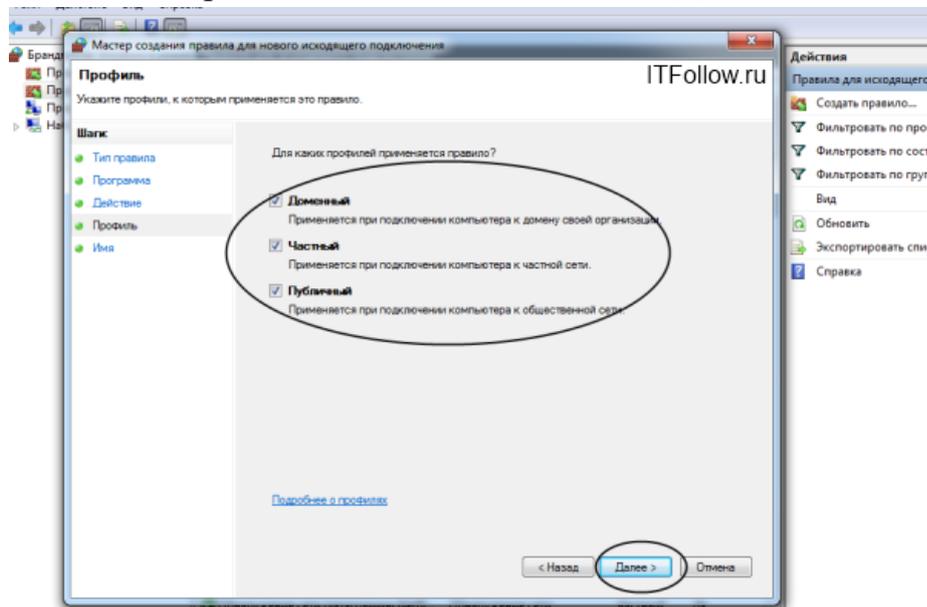
Для поиска пути расположения нужного exe файла, вы можете воспользоваться поиском или посмотреть в свойствах ярлыка, там всегда указан путь к приложению.



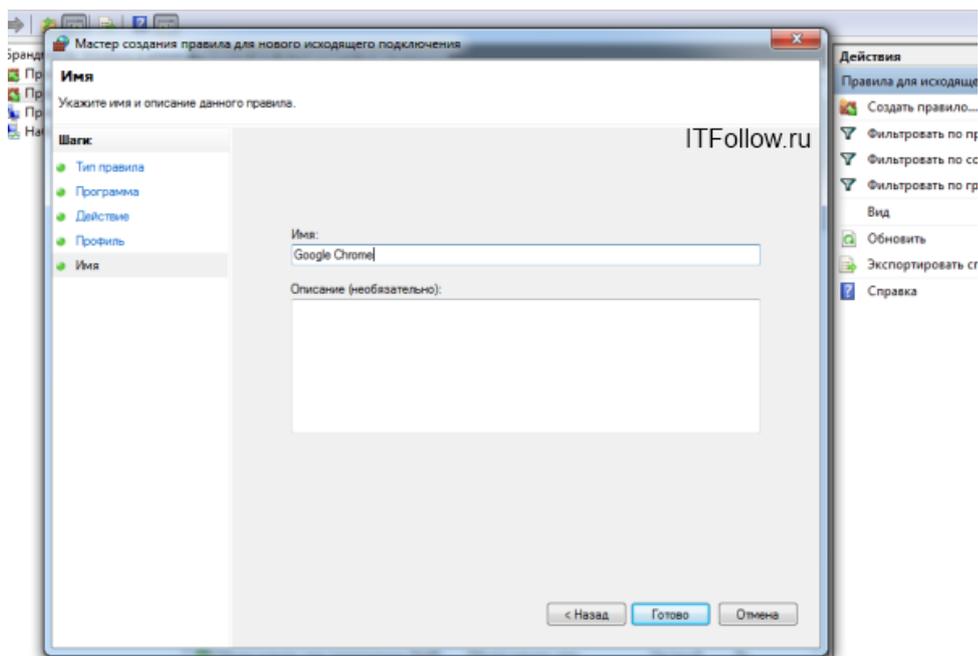
Нажимаете далее → на следующем шаге отмечаете **Разрешить подключение** и опять далее →



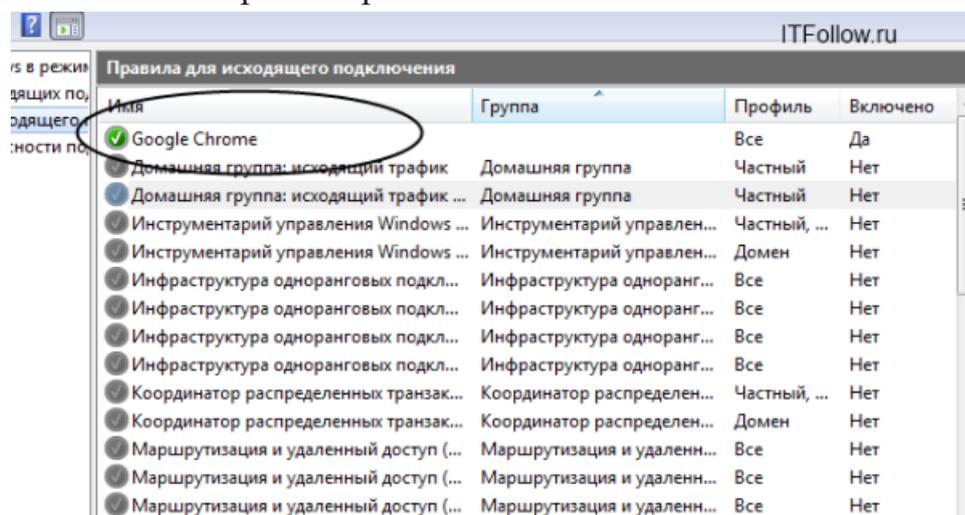
Отмечаете как на скриншоте ниже и нажимаете «Далее»:



На следующем шаге необходимо ввести имя для правила и если необходимо, то и его описание



Новое правило для брандмауэра успешно создано и работает, о чем свидетельствует зеленая галочка напротив правила.



Точно таким же образом можно добавить правило в брандмауэр для любого нужного порта, для этого в начале необходимо выбрать «Создать правило для порта».

Проверка Брандмауэра

По завершению проведения всех работ по настройке брандмауэра, рекомендуем проверить его работоспособность, воспользуйтесь для этого простым сервисом для тестирования фаерволов на сайте 2IP- <http://2ip.ru/firewalltest/>

Задание

Ознакомится с методическими рекомендациями по установке, настройке и отключению системного брандмауэра. Выполнить практической части с соответствии с методическими рекомендациями.

Контрольные вопросы

1. Дайте определение брандмауэра.
2. В чем заключается основная функция брандмауэра в понятии ОС?
3. В чем связана необходимость блокирования исходящего трафика?

Содержание отчета

4. Наименование и цель лабораторной работы
5. Скриншоты выполнения лабораторной работы.
6. Выводы по лабораторной работе.
7. Ответы на контрольные вопросы.