**Лекция на тему:” Файервол: задачи, сравнительный анализ, настройка.”**

**Что такое Firewall?**

Компьютерная сеть изначально является системой, незащищенной и уязвимой для внешних атак. Чтобы предотвратить несанкционированный доступ к устройству, подключенному к глобальной или частной сети, необходимо использовать специальные программные средства, называемые Firewall, сетевой фильтр, брандмауэр (все названия являются синонимами).

**Понятие Firewall**

Firewall переводится с английского как «огненная стена». Суть этой «стены» - защита компьютера, локальной сети или отдельных узлов от внешних атак, вредоносного программного обеспечения, фильтрация входящих и исходящих пакетов данных, обеспечение дополнительной безопасности при работе в сети.

**Типы Firewall**

Сетевые фильтры подразделяются на разные типы, в зависимости от своих характеристик и выполняемых функций. Это могут быть:

* Коммутаторы;
* Фильтры сетевого уровня с анализом IP-адреса отправителя и получателя;
* Шлюзы для контроля состояния канала сеансового уровня;
* Шлюз прикладного уровня (прокси-сервер);
* Брандмауэр с динамической фильтрацией входящих и исходящих пакетов.

Firewall можно устанавливать как на персональный компьютер (устройство) поверх операционной системы для защиты непосредственно этой машины, так и на сеть - для выполнения функции шлюза данной сети. Исходя из этого, брандмауэр может именоваться host-based или network.

Сетевой Firewall, основанный на стандартном ПК, называется PC-based. Если функционал Firewall разработан на аппаратном уровне отдельной системы, то это ASIC-accelerated Firewall.

Установка и настройка сетевого фильтра должна производиться квалифицированным специалистом по сетевой безопасности, так как некомпетентное вмешательство в функционал брандмауэра может нанести существенный вред защищаемой сети (могут быть запрещены или ограничены в действиях некоторые необходимые службы).

**Функции Firewall**

К основным функциям Firewall, обеспечивающим защиту компьютера или сети от внешних угроз, относят:

* Ограничение и контроль доступа к незащищенным службам узла сети;
* Формирование регламента порядка доступа к службам;
* Регистрирование и учет попыток доступа к устройству извне и от объектов внутренней сети;
* Препятствование получению информации об устройстве или сети;
* Трансляция ложных данных о защищаемой сети.

Использование Firewall, несомненно, приносит существенную пользу, но в то же время ощутимо увеличивает время отклика сети и снижает ее пропускную способность, так как на фильтрацию всех пакетов требуется определенное время.

Необходимо сказать, что сетевой фильтр не защитит компьютер от загружаемого непосредственно пользователем вредоносного программного контента (вирусов), а также от утечки персональных данных. Для этих целей рекомендуется использовать антивирусы и соблюдать условия конфиденциальности в сети.

**Фаервол**, (firewall — огненная стена) ещё его называют брандмауэр или сетевой экран, это программа для защиты ваших компьютеров от сетевых атак и от потери конфиденциальных данных. Основной задачей сетевого экрана является защита компьютера от несанкционированного доступа. Кроме того, фаерволы часто называют фильтрами, так как их основная задача — не пропускать (фильтровать) пакеты, не подходящие под критерии, определённые в правилах.

Обычно сетевые экраны запускаются как служба, при загрузке операционной системы и контролирует сетевую активность вашего компьютера. Фаервол блокирует неугодные вам исходящие соединения и является преградой для внешних сетевых атак на компьютер пользователя.

Большинство таких программ легко настраиваются и имеют автоматический режим для неопытных пользователей. Зачастую в хороших фаерволах есть режим автоматического обучения, программа следит за входящими и исходящими соединениями и добавляет их в список доверенных или в блокированных.

На сегодняшний день существует множество различных программных продуктов для обеспечения сетевой защиты. Условно я поделил их на группы.

В первую группу мы включаем наиболее надежные решения. По оценкам специалистов эти фаерволы лучше всего справляются со своей работой и поэтому рекомендованы к установке.  
  
http://win61.ru/cnws/data/upimages/firewall/Private.gif Privatefirewall  
http://win61.ru/cnws/data/upimages/firewall/PC-cillin.gif Trend Micro PC-cillin Internet Security  
http://win61.ru/cnws/data/upimages/firewall/Comodo.gif Comodo Internet Security  
http://win61.ru/cnws/data/upimages/firewall/Jetico.gif Jetico Personal Firewall  
http://win61.ru/cnws/data/upimages/firewall/ZoneAlarm.gif ZoneAlarm Free  
http://win61.ru/cnws/data/upimages/firewall/Outpost.gif Outpost Firewall PRO  
http://win61.ru/cnws/data/upimages/firewall/Kaspersky.gif Kaspersky Internet Security

Вторая группа включает в себя фаерволы, зарекомендовавшие себя как довольно добротные продукты, пропустив всего несколько сетевых атак, которые в обычной ситуации у домашнего пользователя крайне маловероятны. Исходя из этого, данные решения можно рекомендовать к использованию.  
  
http://win61.ru/cnws/data/upimages/firewall/F-Secure.gif F-Secure Internet Security  
http://win61.ru/cnws/data/upimages/firewall/McAfee.gif McAfee Internet Security Suite  
http://win61.ru/cnws/data/upimages/firewall/Lavasoft.gif Lavasoft Personal Firewall  
http://win61.ru/cnws/data/upimages/firewall/BlackICE.gif BlackICE PC Protection  
http://win61.ru/cnws/data/upimages/firewall/Kerio.gif Sunbelt Kerio Personal Firewall  
http://win61.ru/cnws/data/upimages/firewall/LookNStop.gif Look ’n’ Stop  
http://win61.ru/cnws/data/upimages/firewall/Norton.gif Norton Internet Security 2010

Следующая группа фаерволов плохо справилась со своей работой и получила оценку неудовлетворительно. Если один из них ваш выбор, то будьте очень внимательны, возможно, они не полностью справятся с поставленной задачей.  
  
http://win61.ru/cnws/data/upimages/firewall/SafetyNet.gif Safety.Net  
http://win61.ru/cnws/data/upimages/firewall/Avira.gif Avira Premium Security Suite  
http://win61.ru/cnws/data/upimages/firewall/Sygate.gif Sygate Personal Firewall

А вот группа фаерволов, которые я не рекомендую к использованию, все они практически полностью провалили тесты.  
  
http://win61.ru/cnws/data/upimages/firewall/CA.gif CA Personal Firewall  
http://win61.ru/cnws/data/upimages/firewall/Filseclab.gif Filseclab Personal Firewall  
http://win61.ru/cnws/data/upimages/firewall/Ashampoo.gif Ashampoo FireWall Pro  
http://win61.ru/cnws/data/upimages/firewall/AVG.gif AVG Anti-Virus plus Firewall  
http://win61.ru/cnws/data/upimages/firewall/Panda.gif Panda Antivirus + Firewall  
http://win61.ru/cnws/data/upimages/firewall/BitDefender.gif BitDefender Internet Security

Важно обратить внимание на то, что большая часть фаерволов, представленных в обзоре, являет собой системные комплексные решения, которые включают в себя и фаервол и антивирус, поэтому стоит заметить, что если фаервол в этой системе провалил тест, это не значит, что как антивирус он будет бесполезен. Вполне возможно, что его антивирусная часть вполне достойно сражается с вирусами.  
Ниже представлены ссылки на программы из первой группы которые получили оценку отлично.

**Как настроить фаервол?**

Фаервол представляет собой определенный сетевой фильтр, задача которого – защищать ПК от несанкционированного доступа и не пропускать различные данные, не соответствующие определенным критериям. Параметры работы фаервола устанавливаются автоматически, но при этом каждый пользователь может внести определенные изменения.

Настройки фаервола у всех операционных системы схожи и не имеют существенных отличий. Важно заметить, что если пользователь для защиты своего компьютера использует антивирус Касперского, то управления параметров и внесения изменений, придется осуществлять при помощи специальных приложений. Поэтому нужно или временно остановить работу программы, или удалите ее. Важно знать, где находятся настройки фаервола. Все настройки брандмауэра расположены в разделе «Безопасность».

В общем, существует не так много параметров, которые можно подкорректировать:

1. Поскольку фаервол блокирует все попытки внешнего подключения за исключением определенных служб и программ, пользователь может внести свои исключения.
2. Еще можно провести изменения в списке подключений, во время использования которых активируется защитный экран. Обычно по умолчанию доступной является только локальная сеть, но список можно расширить.
3. Чтобы было удобно пользоваться брандмауэром, можно создать персональный журнал работы. Он позволит контролировать деятельность фильтра и быстро выявлять ошибки.

Переходим непосредственно к настройке фаервола Windows 7 (мы уже говорили, что схему можно использовать и для другой операционной системы). Предлагаем перевести работу исходящих подключений в режим белой фильтрации и настроить список разрешений. Необходимо открыть оснастку Windows Firewall with Advanced Security.

Настройка фаервола Windows 8, 7 и XP осуществляется по такой схеме:

1. Первое что рекомендуется сделать – запретить исходящие подключения для публичных и частных сетей. Для этого вызовите окно свойств брандмауэра и во вкладках, находящихся возле частного и публичного профиля, переведите опцию во входящих подключениях в состояние «Блокировать».
2. Теперь нужно создать правила для приложений. Чтобы было легче понять, как это сделать, предлагаем рассмотреть пример. Пользователь хочет разрешить браузеру осуществлять исходящее подключение. Чтобы реализовать задуманное необходимо перейти во вкладку «Исходящие подключения» и добавить там новое правило. В итоге на экране появится мастер создания, где нужно указать, что правило предназначено для приложений. Переходим на следующий шаг и прописываем путь к приложению, в нашем примере, это ИЕ. Нажмите «Далее» и теперь задача заключается в том, чтобы позволить или отказать в подключении. Мы останавливаемся на первом варианте.
3. Выберите сетевое расположение, а затем, введите имя правила и его описание.

Если вы что-то сделали не так, не нужно переживать, поскольку настройки фаервола [Windows](http://kak-bog.ru/kak-ustanovit-windows-xp-s-fleshki) 7, 8 и ХР, можно вернуть к начальным параметрам. Для этого в фильтре есть специальная кнопка. Напоследок хотелось бы предупредить, что если вы планируете отключить брандмауэр, то не стоит этого делать, в том случае, если компьютер останется полностью без антивирусной защиты.