IP Firewall

IP Firewall – механизм фильтрации проходящих через узел IP-сети пакетов в соответствии с различными критериями. Администратор сети может определить набор входных и выходных фильтров. Входные фильтры определяют, какие пакеты могут быть приняты узлом, выходные – какие пакеты могут быть пересланы узлом в результате маршрутизации. Каждый фильтр описывает класс пакетов и определяет, как эти пакеты должны быть обработаны (отклонить и зарегистрировать, принять, принять и зарегистрировать).

Пакеты могут быть отфильтрованы на основе следующих критериев:

- Протокол (IP, TCP, UDP, ICMP, ARP)
- Адрес источника и/или адрес назначения (и номера портов для TCP и UDP)
- Входной сетевой интерфейс
- Является ли пакет запросом TCP/IP-соединения (пакет пытается запустить TCP/IP-сессию)
- Является ли пакет заголовком, промежуточным или конечным IP-фрагментом
- Имеет ли пакет определенные IP-опции
- MAC-адрес станции-получателя или станции-отправителя

На рисунке показана обработка пакетов при помощи механизма фильтрации маршрутизатора:

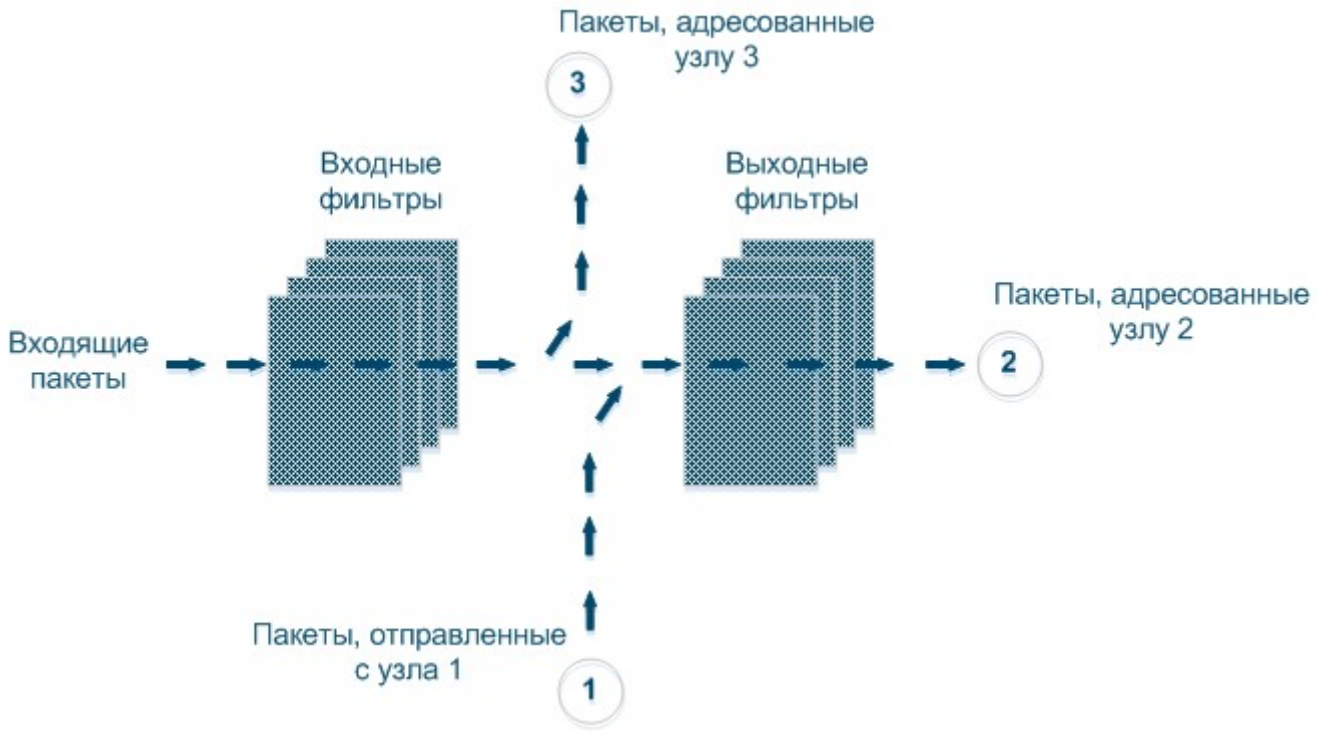

Рисунок - IP Firewall

Существует 2 класса (набора) фильтров – запрещающие (отбрасывают) и разрешающие (принимают).

Кроме того, фильтр может применяться ко всем входящим пакетам или только к пакетам, приходящим с определенного интерфейса. Каждый принимаемый пакет проверяется всеми фильтрами в порядке, определяемом последовательностью их установки.

Первый фильтр, которому соответствует принимаемый пакет, определяет, как этот пакет обрабатывается. Если фильтр принимающий, пакет принимается, если запрещающий – отбрасывается. Если пакет не соответствует ни одному фильтру или если фильтры не заданы, пакет принимается.

ПРЕДОСТЕРЕЖЕНИЕ

Пакеты отбрасываются без уведомления отправителя.

Правила фильтрации пакетов

Каждый пакет, приходящий на маршрутизатор, проходит через набор входных (блокирующих) фильтров. Пакеты, принимаемые набором входных фильтров, обрабатываются IP-уровнем ядра маршрутизатора. Если IP-уровень определяет, что пакет не относится к данному узлу и должен пройти дальше, пакет отправляется на выходные (маршрутизирующие) фильтры.

Информация о пакетах, отбрасываемых любым фильтром, отображается на терминале оператора, а сами пакеты отбрасываются без уведомления отправителя.

Пакеты, проходящие через набор фильтров, проверяются каждым фильтром от первого до последнего, или до тех пор, пока не дойдут до первого подходящего фильтра. Алгоритм следующий:

1. Если фильтры не заданы, пакет принимается
2. Если фильтры заданы, первый подходящий фильтр решит судьбу пакета. Если фильтр разрешающий, пакет принимается, если запрещающий – пакет отбрасывается.
3. Если ни один из фильтров не подходит пакету, пакет принимается.

Параметры IP Firewall

В разделе "IP Firewall" представлена информация о ранее созданных правилах IP Firewall и предусмотрена возможность их редактирования.

Чтобы создать новое правило, нажмите кнопку "**Добавить правило**".

Чтобы удалить правило, нажмите кнопку "**Удалить прав**."

Параметр правила IP firewall	**Описание**

Действие	• Установить действие для правила: разрешить/отказать/пропустить:
	  • "*Разрешить"* – пакет обрабатывается системой (игнорируя другие правила "IP firewall")
	  • "*Отказать"* – пакет отбрасывается
	  • "*Пропустить"* – пакет пропускается к следующему правилу в списке.

Канал	• Активен только если, выбрано действие "Разрешить" • Назначить логический канал, если он был создан в разделе "Контроль трафика" • Если не указать номер канала или указать номер логического канала, не заданного в разделе "Контроль трафика", это никак не отразится на конфигурации данного правила • О том, как создать логический канал, см. раздел "Контроль трафика"

Приоритет	• Назначить приоритет для пакетов, проходящих через данное правило фильтра:
	  • "*Up to"* – повышает приоритет пакета до указанной величины, если он имел более низкий приоритет
	  • "*Set"* – назначает пакету новый приоритет независимо от того, какой приоритет он имел до этого

Log	• Включить/отключить запись действий фильтра в системный журнал

Направление	• Установить направление действия правила фильтрации:
	  • “*Вход*” – правило используется для обработки входящего трафика
	  • “*Выход*” – правило используется для обработки исходящего трафика и для фильтрации пакетов после маршрутизации

Интерфейс	• Установить интерфейс для применения правила • Все доступные интерфейсы (физические и логические) отображаются в раскрывающемся списке • Если выбрана опция "*Все*", правило применяется ко всем доступным интерфейсам

Группа	• Установить номер группы коммутации для применения правила • Группа коммутации должна быть предварительно создана
Правило	• Указать PCAP-фильтр для IP firewall • Синтаксис PCAP-выражений см. Подробное описание синтаксиса правил фильтрации • Чтобы проверить синтаксис выражения в поле "Правило", нажмите кнопку "**Проверка**"

Таблица - IP Firewall

Правила обрабатываются по одному в той последовательности, в которой они расположены в списке (сверху вниз).

Чтобы изменить порядок правил в списке, используйте стрелки "**вверх**/**вниз**" в правой части области настройки правил.

> **ВНИМАНИЕ**
>
> Обратите внимание на информацию в разделе «Применение, проверка и предварительный просмотр конфигурации», поясняющую действие кнопок «**Применить**», «**Проверить**» и «**Предпросмотр**».