Фильтр

Быстрый старт

Для добавления правила файервола которое будет сбрасывать все **TCP** пакеты с портом назначения **135** идущие через маршрутизатор используйте следующую команду:

```
/ip firewall filter add chain=forward dst-port=135 protocol=tcp action=drop
```

Для запрещения доступа к маршрутизатору через Telnet(протокол TCP, порт 23) выполните следующую команду:

```
/ip firewall filter add chain=input protocol=tcp dst-port=23 action=drop
```

Спецификация

Требуемые пакеты: **system**

Требуемый уровень лицензии: Level1(фильтрация P2P ограничена одним соединением)

Уровень подменю: **/ip firewall filter**

Стандарты и технологии: IP,
Аппаратное обеспечение: в зависимости от количества фильтрующих правил (чем бодрее тем лучше)

Фильтр Брандмауэра

Сетевые брандмауэры защищают данные находящиеся в сети от внешней угрозы. Всякий раз когда объединяются сети существует угроза вторжения извне в вашу ЛВС. Такое вторжение может привести к краже или даже потере ценных данных. Брандмауэры используются как средство предотвращения или уменьшения рисков вторжения извне. Должным образом формируемый брандмауэр и грает ключевую роль в эффективном развертывании безопасной инфраструктуры ЛВС. В MikroTik RouterOS реализован мощный брандмауэр со следующими особенностями:

- полная фильтрация пакетов
- фильтрация по протоколу peer-to-peer
- классификация трафика по:
  - исходящий MAC адрес
  - IP адреса(сети или списки) и типы адресов(broadcast, local, multicast, unicast)
  - порты или диапазон портов
  - IP протоколы
  - опции протоколов(ICMP типы и кодовые поля, флаги TCP, IP опции и MSS)
  - входящий исходящий трафик
  - внутренний поток и маркировка соединений
  - ToS(DSCP) байт
  - содержимое пакета
  - лимитирование, количества пакетов(по состоянию счетчика)

- размер пакета
- количество пакетов полученных за определенное время
- и многое другое

Основные принципы фильтрации

Файервольные операции выполняются средствам и файервольных правил. Правила имеют строгий синтаксис, который позволяет объяснить маршрутизатору что сделать с текущим IP пакетом. Каждое правило состоит из двух частей - это образец, который используется для сопоставления с траффиком и действие, которое определяет что необходимо сделать в случае если пакет соответствует образцу. Для более удобного управления правила организованы в цепочки.

Средство фильтр снабжено по умолчанию тремя цепочками: **input**, **forward** и **output** эти цепочки отвечают за входящий, транзитный и исходящий трафик соответственно. Новые пользовательские цепочки могут быть добавлены, как обязательные. Со старта эти цепочки не имеют образцов для сопоставления с трафиком, правила, содержащие **action=jump** и **jump-target** могут быть добавлены в одну или более цепочек по умолчанию.

Фильтрующие цепочки

Как упоминалось ранее, файервольные правила фильтрации группируются вместе в цепочки. Эта возможность позволяет сопоставить пакет образцу в одной цепочке и после этого передать его на обработку другой цепочке. Например, пакет должен быть сопоставлен с парой **IP address:port**.
Конечно это может быть достигнуто путем добавления большого количества правил с образцом **IP address:port** как критерий для цепочки **forward**, но лучшим способом будет добавить одно правило для сопоставления с текущим IP адресом, т.е: /ip firewall filter add src-address=1.1.1.2/32 jump-target=mychain и в случае совпадения передать управление IP пакетом некоторой другой цепочке, то есть **mychain** в данном примере. Затем правила смогут продолжить сопоставление с образцом по порту в **mychain** без проверки IP адреса.

Ниже описываются три цепочки которые не могут быть удалены:

1. **input** - используется для фильтрации входящего на маршрутизатор трафика через один из интерфейсов с адресом назначения IP одного из этих интерфейсов. Транзитный пакет (пакет идущий через маршрутизатор) не проходит через правила цепочки **input**
2. **forward** используется для фильтрации транзитных пакетов
3. **output** - используется для фильтрации пакетов порожденных маршрутизатором и исходящих с одного из интерфейсов. Транзитный трафик не попадает в правила цепочки **output**

При прохождении цепочки, правила описанные в ней рассматриваются сверху вниз. Если пакет соответствует критерию правила, то к нему применяется определенное ранее действие, и пакет прекращает свое движение по цепочке т.е к нему более не применяется ни одного правила из этой цепочки (исключение составляет действие **passthrough**). Если для пакета не найдено совпадений в цепочке то он принимается.

Описание свойств

action(accept | add-dst-to-address-list | add-src-to-address-list | drop | jump | log | passthrough | reject | return | tarpit; по умолчанию: **accept**) - действие
применяемое к пакету если найдено соответствие в правиле.

accept - принять пакет. Не предпринимать ни каких д ействий т.е пакет принят и никакие правила к нему больше не применяются

add-dst-to-address-list - добавить адрес назначения IP пакета в список адресов определенный в параметре **address-list**

add-src-to-address-list - добавить адрес источника IP пакета в спис ок адресов определенный в параметре **address-list**

drop - тихо сбросить пакет(без посылки ICMP сообщения об отклонении пакета)

jump - прыгнуть в цепочку определенную значением в параметре **jump-target**

log - каждое соответствие с этому действию будет добавлено в системный журнал

passthrough - игнорировать это правило и следовать к следующему

reject - отклонить пакет и послать ICMP сообщение об отклонении

return - вернуть контроль в то место цепочки откуда был совершен прыжок

tarpit - захват и удержание входящих TCP соединений(применимо с флагами SYN/ACK во входящем TCP SYN пакете)

address-list(name) - определенное имя списка адресов для сбора IP адресов из правил, в которых определено действие **action=add-dst-address-liyst** или **action=add-src-address-list**. Эти списки адресов могут быть в последствии использованы в правилах.

address-list-timeout(time; по умолчанию: **00:00:00**) - временной интервал после которого адрес будет удален из списка адресов определенного параметром **address-list**. Используется в совокупности с действием **add-dst-to-address-list** или **add-src-to-address-list**

00:00:00 - всегда удалять адрес из списка адресов

chain (forward | input | output | name) - определенная цепочка в которую вставляется правило. Так как различный траффик проходит через различные правила то будьте осторожны при выборе цепочки для определенного правила. Если введенное значение не будет соответствовать название уже существующей цепочки то новая цепочка будет создана.

comment(text) - комментарий к правилу. Комментарий который может быть использован для описания правил.

connections-bytes(integer-integer) - пакеты т.е количество байт прошедших через конкретное соединение.

бесконечность: **connection-bytes=2000000-0** правило имеет смысл, если более чем 2Mb может быть пропущено через соотв етствующее соединение

connection-limit(integer,netmask) - ограничение кол-ва соединений к адресу или блокировка адреса

connection-mark(name) - маркировка соответствующих пакетов средствами mangle марками соответсвующего соединения

connection-state(estabilished | осиinvalid | new | related) - трассировка соединений и анализ данных определенного пакета

estabilished - пакет принадлежащий уже установленному соединению, например пакет ответа

invalid - пакет который не может быть идентифицирован по некоторым пр ичинам. Например при нехватки памяти и ICMP ошибках которые не могут быть присвоены другим соединениям. Это главное сообщение о том что пакет должен быть сброшен.

new - первый пакет в соединении.

related - пакет, который связан с другим соединением, как на пример ICMP ошибки пакет который принадлежит FTP data соединению (последнее требует включения FTP трассировщика соединений в **/ip firewall service-port**)

connection-type(ftp | gre | h323 | irc | mms | pptp | quake3 | tftp) - соответствие пакетов из связанного соединения базирующихся на информации вспомогательного соединения. Соотношение вспомогательным элементам должно быть включено в **/ip firewall service-port content**(text) - текст пакета необходимый для соответствия правилу

dst-address(IP address/netmask | IP address-IP address) - определенный диапазон IP адресов назначения. Примечание консоль конвертирует ввод значения **address/netmask** в валидный сетевой адрес т.е: **1.1.1.1/24** будет конвертирован в **1.1.1.0/24**

dst-address-list(name) - соответствие пакета адресу назначения взятому из определенного пользователем списка адресов

dst-address-type (unicast | local | broadcast | multicast) - соответствие адресов назначения с одним из типов IP пакетов:

unicast - IP адрес использован для соединения точка-точка. В данном случае этот пакет только один посылает и один принимает пакет

local - соответствие адресам маршрутизатора

broadcast - пакет посланный от одной точки всем точкам IP подсети

multicast - этот тип IP адресации предназначен для передачи от одной или более точек к другим точкам

dst-limit - (integer/time{0,1},integer,dst-address | dst-port | src-address{+},time{0,1}) - ограничение количества пакетов в секунду лимитируется по IP адресу назначения или портам назначения. Как противоположность общему лимитирован ию каждый IP адрес / порт назначения имеет свой лимит. Опции показаны ниже (в порядке появления)

Count - максимальное среднее нормирование пакетов, измеряемый в пакетах в секунду (pps), если не сопровождается выбранной(опцией) **Time**

Time - определенный интервал времени, с помощью которого нормируется пакет

Burst - количество пакетов определяющих взрыв

Mode - классификация пакета для лимитирования

Expire - определенный интервал по истечении, которого записи IP адресов / портов будут удалены

dst-port (integer: 0..65535-integer: 0..65535{*}) - порт назначения или диапазон портов

hotspot (from-client | auth | local-dst | http) - соответствие пакетов полученных от клиентов HotSpot. Все значения могут быть инвертированы

from-client - правда, если пакет пришел от клиента HotSpot

auth - правда, если пакет пришел от аутентифицированного клиента

local-dst - правда, если пакет имеет локальный IP адрес назначения

hotspot - правда если это TCP пакет от клиента и также включен прозрачный прокси на 80 порту или на клиенте сконфигурирован адрес прокси и этот адрес равен адресу:порту IP пакета

icmp-options (integer:integer) - соответствие ICMP Type:Code полям

in-interface (name) - интерфейс на который заходит пакет следующий через маршрутизатор

ipv4-options (any | loose-source-routing | no-record-route | no-router-alert | no-source-routing | no-timestamp | none | record-route | router-alert | strict-source-routing | timestamp) - соответствие заголовка опциям ipv4

any - соответствие пакета с одной из опций ipv4

loose-source-routing - соответствие пакетов свободной исходной опции конфигурации. Эта опция используется для маршрутизации дейтаграмм , базируясь на адресе источника

no-record-route - соответствие пакетов с несуществующими записями маршрутизации. Эта опция используется для маршрутизации дейтаграмм , базируясь на адресе источника

no-router-alert - соответствие пакетов опции тревога(alert)

no-source-routing соответствие пакетов опции нет маршрута источника

no-timestamp - соответствие пакетов опции нет временной метки

record-route - соответствие пакета с записью опции маршрутизации

router-alert - соответствие пакетов опции тревога(alert)

strict-source-routing - строгое соответствие пакетов опции маршрутизации источника

timestamp - соответствие опции временной метки

jump-target (forward | input | output | name) - название цепочки в которую осуществляется переход, если используется опция **action=jump**

limit (integer/time{0,1},integer) – ограничение (лимитирования) соответствующего пакета. Уменьшает количество системных сообщений

Count - максимальная средняя скорость передачи пакета, измеряется в пакетах за секунду (pps), если не сопровождается выбранной опцией **Time**

Time - выбранный временной интервал, которым нормируется прохождение пакета

Burst - число пакетов для соответствия взрыву

log-prefix(text) - все сообщения записывающиеся в системный журнал и снабжающиеся префиксом определяются здесь. Используется в добавлении с **action=log**

nth (integer,integer: 0..15,integer{0,1}) - соответствие специфичному Nth пакету полученному из правила. Один из 16 доступных счетчиков может быть использован для подсчета пакетов.

Every - соответствует каждому **Every+1th** пакету. Например, если **Every=1** тогда правило соответствует каждому второму пакету

Counter - определяет какой счетчик использовать. Счетчик увеличивается каждый раз когда правило находит соответствие **nth**

Packet - соответствие отдельно взятому пакету выбранному по номеру. Взятое значение(номер) имеет смысл между **0** и **Every**. Если эта опция используется для конкретного счетчика , тогда должен быть по крайней мере **Every+1** правило с этой опцией, перекрывающее все значения между **0** и **Every** включительно

out-interface (name) - интерфейс через который пакет покидает маршрутизатор.

p2p (all-p2p | bit-torrent | blubster | direct-connect | edonkey | fasttrack | gnutella | soulseek | warez | winmx) - соответствие пакетов протоколам peer-to-peer(P2P)

packet-mark(text) - соответствие пакетов маркированных средством mangle соответствующим маркам.

packet-size (integer: 0..65535-integer: 0..65535{0,1}) - соответствие пакета определенному размеру или размеру в заданном диапазоне заданному в байтах.

Min - нижняя граница размера диапазона или отдельно взятого значения

Max - верхняя граница размера диапазона

phys-in-interface (name) - соответствие порту физического входящего(input) устройства добавленного в bridge устройство. Эта возможность может использоваться только если пакет прибывает на bridge.

phys-out-interface (name) -соответствие порту физического исходящего(output) устройства добавленного в bridge устройство. Эта возможность может использоваться, только если пакет покидает маршрутизатор с bridge.

protocol (ddp | egp | encap | ggp | gre | hmp | icmp | idrp-cmtp | igmp | ipencap | ipip | ipsec-ah | ipsec-esp | iso-tp4 | ospf | pup | rdp | rspf | st | tcp | udp | vmtp | xns-idp | xtp | integer) - соответствие определенному IP протоколу по имени или номеру. Вам необходимо использовать эту возможность, если вы хотите определять в правилах порты.

psd (integer,time,integer,integer) - попытка определить TCP и UDP сканеры. Рекомендуется назначать небольшой вес(пакета) портам старше 1024 для уменьшения количества отрицательных ответов, также как при пассивной передаче через F TP

WeightThreshold - полный вес последних TCP/UDP с отличными (старше 1024) портами назначения и, пришедшими от некоторого хоста будут рассматриваться как сканер портов

DelayThreshold - задержка пакетов с отличными (старше 1024) портами назначения и, пришедшими с некоторого хоста будут рассматриваться как подсканер портов

LowPortWeight - вес пакетов с привелегированными(<=1024) портами назначения

HighPortWeight - вес пакета с непривелигерованым портом назначения

random(integer 1..99) - соответствие пакетов взятым наугад

reject-with (icmp-admin-prohibited | icmp-echo-reply | icmp-host-prohibited | icmp-host-unreachable | icmp-net-prohibited | icmp-network-unreachable | icmp-port-unreachable | icmp-protocol-unreachable | tcp-reset | integer) изменение пакета ответа действием **reject**

routing-mark(name) - соответствие пакетов маркам сделанными средством mangle со определенной маркировкой маршрута

src-address (IP address/netmask | IP address-IP address) - определенный диапазон IP пакетов пришедших от. Примечание консоль конвертирует введеное занчение **address/netmask** в валидный сетевой адрес т.е: **1.1.1.1/24** будет конвертирован в **1.1.1.0/24**

src-address-list(name) - соответствие исходящего адреса пакета элементу списка адресов

src-address-type (unicast | local | broadcast | multicast) - соответствие типа пакета с исходящим адресом одному из критериев:

IP адреса используются для передачи от одной точки к другим точкам

local - адреса соответствуют адресам маршрутизатора

broadcast - пакет посылаемый от одной точки ко все м точкам подсети

multicast - этот тип адресации применяется для передачи от одной или более точек к другим точкам

src-mac-address (MAC address) - исходящий MAC адрес(MAC источника)

src-port (integer: 0..65535-integer: 0..65535{*}) - порт источника или диапазон портов.

tcp-flags (ack | cwr | ece | fin | psh | rst | syn | urg) - соответствие следующим tcp флагам:

ack - подтверждение получения данных

cwr - уменьшение окна скопления

ece - ECN-echo флаг(явное уведомление о скоплении)

fin - закрытие соединения

psh - функция вталкивания

rst - сброс соединения

syn - новое соединение

urg - срочные данные

tcp-mss(integer: 0..65535) - соответствие IP пакета значению TCP MSS

time(time-time,sat | fri | thu | wed | tue | mon | sun{+}) - применяется на создании фильтра базирующегося на времени и дате прибытия пакета или, для пакетов сгенерированных локально на времени и дате отбытия пакета

tos(max-reliability | max-throughput | min-cost | min-delay | normal) - определение соответствия со значением поля Тип Обслуживания(T oS) заголовка пакета

max-reliability - максимальная надежность(ToS=4)

max-throughput - максимальная пропускная способность(ToS=8)

min-cost - минимальная стоимость(ToS=2)

min-delay - минимальная задержка(ToS=16)

normal - нормальное обслуживание(ToS=0)

Примечание

Ввиду того что правила NAT применяются первыми, важно помнить об этом при написании правил файервола, учтите что оригинальный пакет мог быть уже изменен с помощью NAT

Применения фильтра

Защитите ваш RouterOS маршрутизатор

Для защиты вашего маршрутизатора недостаточно только смены пароля администратора, также необходимо организовать фильтрацию пакетов. Все пакеты предназначенные маршрутизатору следуют через цепочку input. Примечание: пакеты следующие через маршрутизатор не попадают в цепочку input.

```
/ ip firewall filter
add chain=input connection-state=invalid action=drop
 comment=Drop Invalid connections
add chain=input connection-state=established action=accept
 comment=Allow Established connections
add chain=input protocol=udp action=accept
 comment=Allow UDP
add chain=input protocol=icmp action=accept
 comment=Allow ICMP
add chain=input src-address=192.168.0.0/24 action=accept
 comment=Allow access to router from known network
add chain=input action=drop comment=Drop anything else
```

Защитите свою сеть

Для защиты сети вам необходимо проверять весь трафик, проходящий через маршрутизатор и блокировать нежелательный. Для icmp, udp и tcp трафика создадим цепочки, куда будем сбрасывать нежелательные пакеты

```
/ip firewall filter
add chain=forward protocol=tcp connection-state=invalid
  action=drop comment=drop invalid connections
add chain=forward connection-state=established action=accept
  comment=allow already established connections
add chain=forward connection-state=related action=accept
  comment=allow related connections
```

Блокируем IP адреса вызывающие bogons

```
add chain=forward src-address=0.0.0.0/8 action=drop
add chain=forward dst-address=0.0.0.0/8 action=drop
add chain=forward src-address=127.0.0.0/8 action=drop
add chain=forward dst-address=127.0.0.0/8 action=drop
add chain=forward src-address=224.0.0.0/3 action=drop
add chain=forward dst-address=224.0.0.0/3 action=drop
```

Создадим переход в новые цепочки

```
add chain=forward protocol=tcp action=jump jump-target=tcp
add chain=forward protocol=udp action=jump jump-target=udp
add chain=forward protocol=icmp action=jump jump-target=icmp
```

Создадим tcp правила в цепочке tcp и запретим некоторые tcp порты

```
add chain=tcp protocol=tcp dst-port=69 action=drop
  comment=deny TFTP
```

```
add chain=tcp protocol=tcp dst-port=111 action=drop
  comment=deny RPC portmapper
add chain=tcp protocol=tcp dst-port=135 action=drop
  comment=deny RPC portmapper
add chain=tcp protocol=tcp dst-port=137-139 action=drop
  comment=deny NBT
add chain=tcp protocol=tcp dst-port=445 action=drop
  comment=deny cifs
add chain=tcp protocol=tcp dst-port=2049 action=drop comment=deny NFS
add chain=tcp protocol=tcp dst-port=12345-12346 action=drop comment=deny
NetBus
add chain=tcp protocol=tcp dst-port=20034 action=drop comment=deny NetBus
add chain=tcp protocol=tcp dst-port=3133 action=drop comment=deny
BackOriffice
add chain=tcp protocol=tcp dst-port=67-68 action=drop comment=deny DHCP
```

Запретим udp порты в цепочке udp

```
add chain=udp protocol=udp dst-port=69 action=drop comment=deny TFTP
add chain=udp protocol=udp dst-port=111 action=drop comment=deny PRC
portmapper
add chain=udp protocol=udp dst-port=135 action=drop comment=deny PRC
portmapper
add chain=udp protocol=udp dst-port=137-139 action=drop comment=deny NBT
add chain=udp protocol=udp dst-port=2049 action=drop comment=deny NFS
add chain=udp protocol=udp dst-port=3133 action=drop comment=deny
BackOriffice
```

Разрешим необходимые icmp коды в icmp цепочке

```
add chain=icmp protocol=icmp icmp-options=0:0 action=accept
  comment=drop invalid connections
add chain=icmp protocol=icmp icmp-options=3:0 action=accept
  comment=allow established connections
add chain=icmp protocol=icmp icmp-options=3:1 action=accept
  comment=allow already established connections
add chain=icmp protocol=icmp icmp-options=4:0 action=accept
  comment=allow source quench
add chain=icmp protocol=icmp icmp-options=8:0 action=accept
  comment=allow echo request
add chain=icmp protocol=icmp icmp-options=11:0 action=accept
  comment=allow time exceed
add chain=icmp protocol=icmp icmp-options=12:0 action=accept
  comment=allow parameter bad
add chain=icmp action=drop comment=deny all other types
```