Перевод раздела стандартной документации, который мы делали с одним моим знакомым ещё во времена Mikrotik 2.9.

Применимо к: V2.9
Главная информация
Общее
Файервол выполняет фильтрацию пакетов являясь таким образом инструментом обеспечивающим безопасность и управление потоками данных, проходящими через маршрутизатор. Вместе с трансляцией сетевых адресов NAT файервол служит инструментом предотвращения несанкционированного дотсупа к подключенной сети, что так же применимо к фильтрации исходящего трафика.
Примеры быстрой настройки
• Чтобы добавить правило, применяющее ко всем проходящим через роутер пакетам с портом назначения 135 правило DROP, нужно ввести следующую:
/ip firewall filter add chain=forward dst-port=135 protocol=tcp action=drop
• Чтобы запретить доступ к маршрутизатору через Telnet (протокол TCP, порт 23), нужно выполнить следующее:
/ip firewall filter add chain=input protocol=tcp dst-port=23 action=drop
• Чтобы разрешить не более пяти одновременных подключений для каждого из клиентов, нужно сделать следующее:
/ip firewall filter add chain=forward protocol=tcp tcp-flags=syn connection-limit=6,32 action=drop
Спецификации
Требуемый пакет: system
Требуемая лицензия: Level1 (P2P filters limited to 1) , Level3
Уровень подменю: /ip firewall filter
Стандарты и технологии: IP, RFC2113
Использование ресурсов: Возрастает с количеством правил
Документы по теме
• Software Package Management
• IP Addresses and ARP
• Routes, Equal Cost Multipath Routing, Policy Routing
• NAT
• Mangle
• Packet Flow
Фильтр файервола
Уровень подменю: /ip firewall filter
Описание
Брандмауэр обеспечивает защиту важной информации к которай можно получить доступ по сети.

Везде, где есть соприкасающиеся сети, всегда существует угроза проникновения в локальную сеть. Это может привести к краже и распространению важных данных, их изменению, порче или стироанию данных с жёстких дисков. Файервол используется как средство предотвращение и минимизации риска обычно предпринимающееся по отношению к другим сетям. Правильно сконфигурированный файервол играет ключевую роль в развёртывании рациональной и безопасной сетевой инфраструктуры.

Файервол Mikrotik RouterOS обладает мощными функциями и включает следующие возможности:

• Фильтрация пакетов;
• Фильтрация p2p протоколов
• Классификация трафика по:
o исходный MAC-адрес;
o IP-адрес (сеть или список) и тип адреса (бродкаст, локальный, мультикаст, юникаст);
o Порт или список портов;
o IP-протокол;
o Опции протокола (ICMP тип и другие коды, TCP флаги, IP опции и MSS)
o Интерфейс, откуда получен пакет или куда он назначается
o Внутренний поток или маркированное подключение
o Байт ToS (DSCP)
o Содержимое пакета
o Скорость получения пакетов и количество последовательностей
o Размер пакета
o Время получения пакета
o И многое другое!

Основные принципы фильтрации

Оперирование файерволом осуществляется посредством правил. Правило определяет выражение, которое говорит роутеру что делать с индивидуальным IP-пакетом. Каждое правило состоит из двух частей: первое описывает параметры, по которым должны классифицироваться приходящие пакеты, второе отвечает за действие над пакетом. Правила, для лучшего управления, организованы в цепочки.

Устройство фильтра по-умолчанию имеет три цепочки: input, forward и output, которые отвечают за приходяший, перемещаемый внутри роутера и исходящий трафик соответственно. Пользователь может добавить новые цепочки, если это будет нужно.

Под эти цепочки трафик по-умолчанию не попадает. Для этого используется метод action=jump с параметром jump-target в одной из предустановленных цепочек.

Цепочки фильтра

Как говорилось раньше, правила фильтрации в файерволе сгруппированы в цепочки. Это позволяет пакету попавшему под некий критерий в одной цепочке переходить к следующему правилу и следующим цепочкам. К примеру пакетам с определённого адреса и порта нужно применить много правил. Конечно, эти правила можно перечислить в цепочке forward, однако правильнее будет создать для них отдельную цепочку, перебросить туда попавшие под условие пакеты и выполнить над ними нужные нам действия: /ip firewall filter add src-address=1.1.1.2/32 jump-target="mychain". Это правило создаст новую цепочку mychain, в которую попадут все пакеты с адресом источника 1.1.1.2/32.

Три предустановленных цепочки, которые не могут быть удалены:

• Input-применимо к пакетам, приходящим на маршрутизатор, у которых адрес получателя такой же, как и у интерфейса, на который этот пакет поступил. Пакеты, проходящие через маршрутизатор не попадают под действие правил цепочки input.
• Forward – применимо к пакетам, проходящим через маршрутизатор;
• Output – применимо к пакетам созданным маршратизатором, которые покидают его через один из интерфейсов. Пакеты, проходящие через маршрутизатор не попадают под действие

цепочки output.
При попадании пакета в одну из цепочек, правила применяются от верхего к нижнему. Если пакет попадает под критерий одного из правил, над ним выполняется указанное в правиле действие и этот пакет не попадает больше под действие других правил из этой цепочки (исключение составляет только действие passthrough). Если пакет не попадает под действие ни одного из правил цепочки, к нему по умолчанию применяется действие Accept.
Описание параметров
action (accept | add-dst-to-address-list | add-src-to-address-list | drop | jump | log | passthrough | reject | return | tarpit; default: accept) - применяемое действие, если пакет совпал с правилом
accept - принять пакет. Не подразумевает каких-либо действий. Если пакет был принят, к нему больше не применяется никаких действий в цепочке.
add-dst-to-address-list - добавить адрес назначения пакета в address list , указанный в параметре address-list
add-src-to-address-list - добавить адрес источника пакета в address list , указанный в параметре address-list
drop - разрушить пакет (без посылки сообщения ICMP reject)
jump - перепрыгнуть в цепочку, указанную в параметре jump-target
log - каждое совпадение с этим действием добавит в системный лог сообщение
passthrough - игнорировать это правило и перейти к следующему
reject -отбросить этот пакет и постать сообщение ICMP reject
return - вернуть пакет в цепочку, из которой он был переброшен
tarpit - захватить и удерживать входящие TCP подключения (отвечать SYN/ACK на входящий TCP SYN пакет)
address-list (name) - указывает имя списка адресов, в которых хранятся IP-адреса из действий action=add-dst-to-address-list или action=add-src-to-address-list. Эти списки могут быть похже использованы в других правилах.
address-list-timeout (time; default: 00:00:00) - интервал времени, через который адреса будут удалены из списка, указанного в параметре address-list . Используется в сочетании с действиями add-dst-to-address-list или add-src-to-address-list .00:00:00 - означает оставить адреса в списке навсегда.
chain (forward | input | output | name) - указывает цепочку, в которую следует поместить правило. Разные типы трафика проходят через разные цепочки, поэтому будьте в курсе своего выбора, указывая то или иное значение этого параметра. Если указанное значение цепочки не совпадает ни с одним из уже существующих, система создаст новое правило с указанным именем.
comment (text) - комментарий описывает правило. В скриптах комментарии обычно служат для идентификации правил.
connection-bytes (integer-integer) - применять правило, если количество переданных байт через подключение превысило указанное значение. 0 - не ограничено, пример: connection-bytes=2000000-0 сработает в том случае, если количество данных, переданных через открытое подключение превысило 2MB;
connection-limit (integer,netmask) - ограничивает количество доступных подключений на адрес или блок адресов;
connection-mark (name) -пакеты, попавшие под действие правил в

mangle и названные в соответствии с параметром connection mark
connection-state (established | invalid | new | related) - интерпретация состояния подключения посредством анализа данных из connection tracking .
established - пакет, принадлежащийа уже установленному подключению. К примеру ответ от маршрутизатора.
invalid - пакет, который не может быть идентифицирован по какой-либо причине. К примеру это может быть переполнение памяти и ICMP ошибки. К таким пакетам нужно применять действие DROP
new - пакет, начинающий создание TCP подключения
related - запрошенный пакет, который не принадлежит уже установленным подключениям. К примеру ICMP ошибки, или пакет, начинающий передачу данных по протоколу FTP(/ip firewall service-port)
connection-type (ftp | gre | h323 | irc | mms | pptp | quake3 | tftp) - определение типа подключения, базирующееся на использовании данных из connection tracking. Конфигурирование производится в /ip firewall service-port
content (text) - содержимое текстового пакета
dst-address (IP address/netmask | IP address-IP address) - указывает диапазон адресов, у которых IP-адрес назначения совпадает с параметром. При неправильном введении пары address/netmask система сама подстроит эти параметры. К примеру:1.1.1.1/24 будет заменено на 1.1.1.0/24
dst-address-list (name) - совпадение адреса назначения пакета с определенными ранее значениями в address list
dst-address-type (unicast | local | broadcast | multicast) - совпадение типа адреса назначения пакета с заданным предустановленным значением:
unicast - IP-адреса, используемые ля передачи от одной точки к другой. В таком типе пакетов существует только один отправитель и один получатель
local - совпадеине с адресами, назначенными сетевым интерфейсам маршрутизатора
broadcast - IP-пакет, посылаемый сразу всем членам подсети
multicast - этот тип пакета используется для передачи данных от одного отправителя многим получателям в сети.
dst-limit (integer/time{0,1},integer,dst-address | dst-port | src-address{+},time{0,1}) - ограничивает скорость пакетов в секунду (packet per second (pps)) на IP-адрес или порт.
В результате работы правила каждый IP-адрес или порт назначения получает свой лимит.
Параметр имеет следующие опции:
Count - среднее количество пакетов в секунду (packets per second (pps))за время Time
Time - интервал времени, за который производится подсчёт среднего количества пакетов
Burst - количество пакетов в пике
Mode - классификатор для ограничения скорости пакетов
Expire - указывает интервал, через который записанные IP адреса /порты будут удалены
dst-port (integer: 0..65535-integer: 0..65535{*}) - интервал портов назначения
hotspot (multiple choice: from-client | auth | local-dst | http) - сравнивает пакеты полученные от клиентов с различными хот-спотами. все значения могут быть отклонены/инвертированы

from-client - true, если пакеты получены от Hot-Spot клиента
auth - true, если пакеты получены от авторизированного Hot-Spot клиента
local-dst - true, если пакет имеет локальный адрес назначения
hotspot - true, если TCP пакет от клиента и назначается на 80 порт прозрачного прокси сервера или клиент имеет адрес прокси сконфигурированный и аналогичный адресу:порту пакета
icmp-options (integer:integer) - совпадение полей ICMP Type:Code
in-interface (name) - интерфейс, с которого пакет поступил в маршратизатор
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) - совпадение параметров заголовка ipv4
any - совпадает по крайней мере один пакет с установленной ipv4 опцией
loose-source-routing - пакеты с опцией loose source routing. Эта опция используется для направления интернет дейтаграм основаных на информации поставляемой источником
no-record-route - пакеты с опцией no record route. Эта опция используется для направления интернет дейтаграм основаных на информации поставляемой источником
no-router-alert - совпадение пакетов с опцией no router alter
no-source-routing - совпадение пакетов с опцией no source routing
no-timestamp - совпадение пакетов с опцией with no timestamp
record-route - совпадение пакетов с опцией record route
router-alert - совпадение пакетов с опцией router alter
strict-source-routing - совпадение пакетов с опцией strict source routing
timestamp - совпадение пакетов со штампом времени
jump-target (forward | input | output | name) - имя целевой цепочки куда должен быть отправлен пакет при использовании action=jump.
limit (integer/time{0,1},integer) - ограничивает поток пакетов. Используется для уменьшения количества сообщений в логах
Count - максимальное среднее количество пакетов, указанное в пакетах в секунду (PPS Packet Per Second) за время в опции Time
Time - указывает интервал времени за который будет производиться подсчёт среднего количества пакетов
Burst - количество пакетов при пике
log-prefix (text) - все сообщения, записываемые в лог, будут иметь этот префикс. Используется вместе с опцией action=log
nth (integer,integer: 0..15,integer{0,1}) - совпадение каждого n-ного пакета, попавшего в правило. Всего доступно 16 счётчиков
Every - совпадение каждого Every+1th пакета. К примеру, если Every=1 тогда под действие правила попадёт каждый второй пакет
Counter - указывает какой счётчик будет использоваться. Счётчик увеличивается на 1 с каждым новым правилом где указанна опция nth
Packet -совпадает с номером данного пакета. Значение по очевидным причинам должно быть между нулем и Every. Если опиция используется для данного счетчика, тогда должно быть по

крайней мере Every+1 правило с этой опцией, охватывающее все значения между 0 и Every включительно out-interface (name) - интерфейс, через который пакеты будут покидать маршрутизатор
p2p (all-p2p | bit-torrent | blubster | direct-connect | edonkey | fasttrack | gnutella | soulseek | warez | winmx) - совпадение пакетов протоколов peer-to-peer (P2P)
packet-mark (text) - цепочка пакетов, промаркированная в разделе mangle файервола
packet-size (integer: 0..65535-integer: 0..65535{0,1}) - размер пакета в байтах
Min - указывает нижний предел диапазона размера пакета
Max - указывает верхний предел диапазона размера пакета

phys-in-interface (name) - физический интерфейс, указанный в качестве порта моста, по которому пакет поступил в маршрутизатор
phys-out-interface (name) - физический интерфейс, указанный в качестве порта моста, по которому пакет выйдет из маршрутизатора
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) - совпадение IP протокола. Указывается имя протокола или его номер. Вы должны указать эту опцию, чтобы получить доступ к специфическим параметрам для каждого протокола.
psd (integer,time,integer,integer) - попытка определения сканирования TCP и UDP портов. Необходимо назначить меньшее значение портам с высокими номерами для того, чтобы уменьшить количество ложных срабатываний. К примеру, при использовании пассивного режима FTP.
WeightThreshold - полный вес последних TCP/UDP пакетов с различными портами назначения, поступающими с одного хоста, которые распознанные как один из методов сканирования
DelayThreshold - задержка между пакетами с разными портами назначения, поступающие с одного хоста и распознанные как возможная последовательность сканирования
LowPortWeight - вес пакетов при сканировании привилегированных портов (<=1024)
HighPortWeight - вес пакетов на непривилегированные порты назначения
random (integer: 1..99) - совпадение пакетов с заданным уровнем случайности
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) - указывает причину по которой был отброшен пакет в action=reject
routing-mark (name) - совпадение пакетов, обозначенных в цепочке mangle параметром routing mark
src-address (IP address/netmask | IP address-IP address) - указывает диапазон адресов IP пакетов поступивших извне. Замечание: консоль конвертирует неправильно набранные IP значения address/netmask в правильный сетевой адрес. К примеру:1.1.1.1/24 будет конвертирован в 1.1.1.0/24
src-address-list (name) - совпадение адреса источника с списком IP-адресов в предустановленном пользователе address

list
src-address-type (unicast | local | broadcast | multicast) - совпадение типа IP-адреса:
unicast - IP адрес используется для передачи данных между двумя узлами, где только один отправитель и один получатель
local - совпадение адреса, назначенного одному из интерфейсов маршрутизатора
broadcast - IP пакет был отправлен из одной точки всем получателям и IP подсети
multicast - этот типа IP адресации ответственен за передачу между одной или несколькими точками одной или набору других точек
src-mac-address (MAC address) - MAC адрес источника
src-port (integer: 0..65535-integer: 0..65535{*}) - диапазон портов источника
tcp-flags (ack | cwr | ece | fin | psh | rst | syn | urg) - tcp флаги
ack - запрос данных
cwr - принимающее окно уменьшено
ece - ECN-флаг echo (explicit congestion notification)
fin - закрытие подключения
psh - функция push
rst - разорвать подключение
syn - новое подключение
urg - urgent data
tcp-mss (integer: 0..65535) - совпадение значения TCP MSS IP пакета
time (time-time,sat | fri | thu | wed | tue | mon | sun{+}) - позволяет создать фильтр, базирующийся на времени получения пакета или дате. Для локально созданных пакетов дате отправки
tos (max-reliability | max-throughput | min-cost | min-delay | normal) - совпадение с полем «тип сервиса» Type of Service (ToS) в IP загаловке
max-reliability - максимальная надёжность (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)
Заметки
Правила NAT применяются первыми, и это нужно помнить при создании правил файервола, так как оригинальные пакеты могли быть модифицированы в NAT.

Примеры применения
Защита вашего маршрутизатора RouterOS
Для защиты вашего маршрутизатора сменить пароль администратора недостаточно и нужно воспользоваться фильтрацией пакетов. Все пакеты с адресом назначения маршрутизатора попадают во входную цепочку файервола INPUT. Заметьте, что попавшие в цепочку INPUT пакеты не будут проходить через маршрутизатор.

```
/ 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"
```

Защита сети заказчика
Для защиты сети заказчика мы должны проверять весь трафик проходящий через маршрутизатор и блокировать 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"
```

Блокировать IP адреса, названные "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
```

Перебросить их в другую цепочку:

```
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
```

Создать цепочку tcp и запретить 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"
```

Запретить 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"
```

Разрешить только необходимые коды icmp в цепочке с именем icmp:

```
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"
```

Из той же оперы, но про AddressLists

Главная информация
Кратко
Adress lists позволяют создать списки IP адресов, которые используются при сравнении пакетов
Спецификации
Требуемые пакеты: Level1
Уровень подменю: /ip firewall address-list
Стандарты и технологии: IP
Потребление ресурсов: Not significant
Документы по теме
• Software Package Management
• NAT
• Filter
• Packet Flow
• Packet Flow
Address Lists
Описание
Списки адресов позволяют пользователю создать список сгруппированных вместе IP адресов. Фильтр файервола, mangle и NAT могут использовать списки адресов в отношении совпадения пакетов.
Списки адресов могут быть обновлены динамически через действия action =add-src-to-address-list или action=add-dst-to-address-list, возможности, найденные в разделе NAT и возможностях фильтра.

Описание свойств
list (name) - указывает имя списка адресов к корторому нужно добавить IP адрес
address (IP address/netmask | IP address-IP address) - указывает IP адрес или диапазон IP адресов для добавления в список. Замечание: консоль конвертирует неправильно набранные IP значения address/netmask в правильный сетевой адрес. К примеру:1.1.1.1/24 будет конвертирован в 1.1.1.0/24

Пример
Следующие правила создают список адресов людей, которые подключаются на 23 порт (telnet) маршрутизатора и блокируют весь дальнейший трафик от этих хостов. В дополнение список адресов будет иметь одну статическую запись address= 192.0.34.166/32 (www.example.com):

```
[admin@MikroTik] > /ip firewall address-list add
list=drop_traffic address=192.0.34.166/32
[admin@MikroTik] > /ip firewall address-list print
Flags: X - disabled, D - dynamic
# LIST ADDRESS
0 drop_traffic 192.0.34.166
[admin@MikroTik] > /ip firewall mangle add chain=prerouting
protocol=tcp dst-port=23 \
\... action=add-src-to-address-list address-list=drop_traffic
[admin@MikroTik] > /ip firewall filter add action=drop
chain=input src-address-list=drop_traffic
[admin@MikroTik] > /ip firewall address-list print
Flags: X - disabled, D - dynamic
# LIST ADDRESS
0 drop_traffic 192.0.34.166
1 D drop_traffic 1.1.1.1
2 D drop_traffic 10.5.11.8
[admin@MikroTik] >
```

Посмотрите на вывод последней команды print. Две новые динамические записи появились в списке адресов. Хосты с этими IP адресами предпринимали попытки создать подключение на 23 порт маршрутизатора и были блокированы файерволом.