Руководство по Firewall

Быстрая установка

- Для предотвращения прохождения всех TCP пакетов идущих сквозь маршрутизатор на порт 135 используйте следующую команду:

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

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

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

Спецификация

Требуемые пакеты: **system**

Уровень лицензии: Level1(Фильтрация P2P ограничено 1), Level3
Уровень подменю: **/ip firewall**

Стандарты и технологии: IP

Аппаратные требования: Увеличиваются по мере увеличения колличества правил фильтрации

Сопровождающие документы

- Package Management
- IP Addresses and ARP
- Routes, Equal Cost Multipath Routing, Policy Routing
- Network Address Translation

- Packet Marking(Mangle)

Описание

Межсетевые экраны позволяют отделять локальную сеть от внешнего мира делая ее менее уязвимой. Всякий раз когда сети
объединяются есть вероятность что кто нибудь из вне вторгнется в вашу ЛВС. Такие взломы привести к потере данных и прочим проблемам.
Брандмауэры как средство предотвращения или уменьшения рисков вторжения в вашу ЛВС. В Mikrotik RouterOS также реализованы
такие особенности файервола как маскарадинг, который позволяет скрывать инфраструктуру вашей ЛВС.

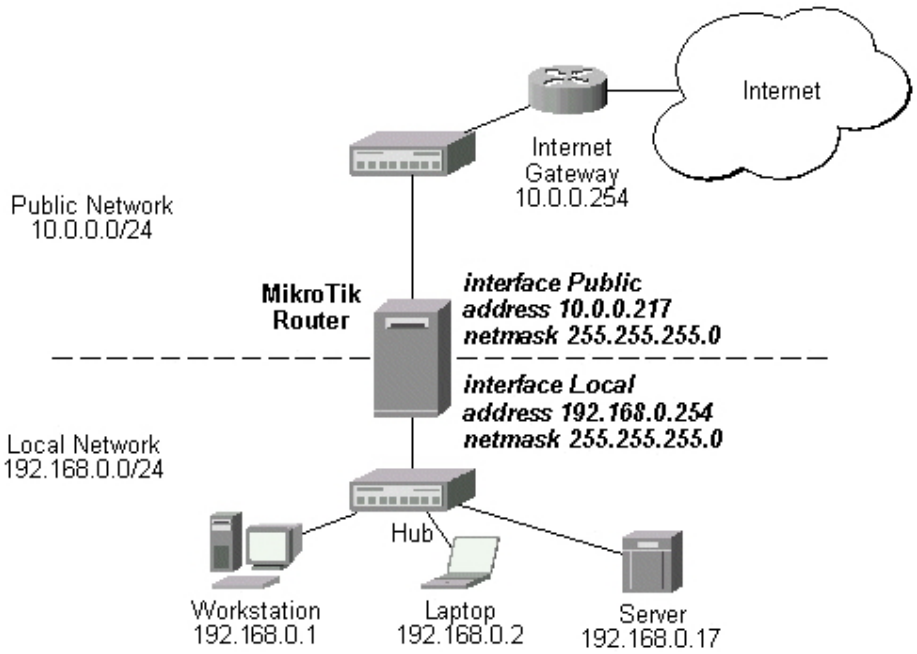
Прохождение пакета

Описание

MikroTik RouterOS упрощает создание и развертывание сложных политик безопасности. Фактически вы можете легко создавать
простой фильтр для трансляции адресов даже не задумываясь о том как пакет обрабатывается маршрутизатром.
Но если вы хотите развернуть более сложную политику безопасности необходимо знать некоторые детали процесса. Прохождение
пакета через маршрутизатор показано на следующей с хеме:

Как вы можете видеть пакет может поступить на обработку двумя путями. Первый пакет прибыл с сетевого интерфейса, второй
пакет был порожден самим маршрутизатором. Аналогично пакет может покинуть обработку т.е или уйти через сетевой интерфейс наружу
или если пакет предназначен локальным приложениям он будет отдан им.

Когда пакет прибывает на сетевой интерфейс правила файервола отрабатываются в следующем порядке.



- Сначала отрабатываются правила NAT. Файервольные правила цепочки input и решение о маршрутизации отрабатываются
  после прохождения правил NAT.

- Если пакет должен быть отправлен через маршрутизатор(forward), то следующим за NAT отрабатываются правила forward.

- Когда пакет покидает интерфейс первыми отрабатываются правила цепочки output, затем NAT и очереди.

Дополнительные стрелки от IPSec показывают обработку зашифрованных пакетов (сначала пакет проходит шифрацию/дешифрацию, а затем обрабатывается как обычный пакет).

Правила файервола

Уровень подменю: **/ip firewall rule**

Описание

Правило это определенное выражение, которое говорит маршрутизатору что делать с конкретным пакетом. Правило

состоит из двух логических частей: установки соответствия и установки действия. Для каждого пакета вам необходимо определить правило соответствия и действие.

Управление файервольными правилами может быть выполнено путем выбора желаемой цепочки. Если вы используете консоль WinBox, выберите желаемую цепочку и для открытия окна со списком правил выберите выпадающий список правил(справа вверху).

Peer-to-Peer Traffic Filtering

MikroTik RouterOS обеспечивает возможность фильтрации трафика для многих пиринговых программ использующих протокол P2P.

ICMP TYPE:CODE values

Для защиты вашего маршрутизатора и стоящей за ним частной сети, вам необходимо сконфигурировать файервол для сброса или отклонения большую часть ICMP трафика. однако некотрые ICMP пакеты необходимы для поддержки бесперебойной работы и диагностики неисправностей.

Ниже представлен список значений ICMP TYPE:CODE в нормальных пакетах. Эти типы ICMP трафика лучше разрешить.

Ping

- **8:0 - echo request(эхо запрос)**
- **0:0 - echo reply(эхо ответ)**

Trace

- **11:0 - TTL exceeded(превышени интервал)**
- **3:3 - Port unreachable(порт не доступен)**

Path MTU descovery

- **3:4 - Fragmentation-DF-Set(набор флагов фрагментации)**

Общее предложение по фильтрации ICMP трафика.

- **Разрешить исходящий ping ICMP Echo-Request и входящие сообщение Echo-reply**

- **Разрешить traceroute TTL-Exceeded и Port-Unrechable входящие сообщения**

- **Разрешить path MTU-ICMP Fragmentation-DF-Set входящие сообщения**

- **Все остальное блокировать**

Тип обслуживания

Интернет-пути изменяются по качеству обслуживания, которое они обеспечивают. Они могут изменятся по стоимости, надежности, задержке и пропускной способности. Эта ситуация предполагает некоторые взаимодействия то есть путь с самой маленькой задержкой может находится в самой медленной полосе. Поэтому самый "оптимальный" путь для пакета следующего через Интернет может зависеть от требуемого приложения и потребностей пользователя.

Поскольку сеть сама по себе не наделена знаниями об оптимизации пути выбранного приложением или пользователем, протокол IP обеспечивает возможность взаимодействия с протоколами верхнего уро вня, которые передают подсказки интернет-уровню как должны происходить обмены пакетами для данного соединения. Это средство называют Type of Service (типом сервиса).

Фундаментальное правило, если хост использует ToS его обслуживание должно быть по крайней мере столь же хорошим как если бы он не использовал его.

Тип обслуживания это стандартное поле TCP пакета использующее многие сетевые приложения и аппаратные средства для определения наилучшего пути прохождения пакета через маршрутизатор.

MikroTik RouterOS в полной мере использует ToS байт. Полученные биты в этом байте не принимаются во внимание (так как они были просмотрены много раз, такой подход обеспечивает большую гибкость). Это означает что можно обработать с

марками DiffServ(Differentiated Service s Codepoint, DSCP определена в RFC2474) и ECN codepoints (Explicit Congestion Notification определенный в RFC3168), которые используют поля в заголовке IP пакета. Отметьте, это не означает, что RouterOS поддерживает DiffServ или ECN, просто есть возможност ь доступа и изменения марков использующих этот протокол.

В RFC1349 определены следующие стандартные значения:

- **normal - нормальное обслуживание(ToS=0)**
- **low-cost - минимальная стоимость(ToS=2)**
- **max-reliability - максимальная надежность(ToS=4)**
- **max-troughput - максимальная пропускная способность(ToS=8)**
- **low-delay - минимальная задержка(ToS=16)**

Описание свойств

action(accept | drop | jump | passthrough | reject | return; по умолчанию accept) - предпринимаемое действие если пакет соответствует одному из п равил:

- **accept - принять пакет. Не имеет действия, то есть при прохождении пакета не предпринимается ни какого другого действия, кроме mangle.**
- **drop - сброс пакета без посылки ICMP reject сообщения**
- **jump - переход к цепочке определенной в значении параметра перехода.**

- **passthrough - проигнорировать это правило за исключением mangle и перейти к следующему. Это тоже самое, что и заблокировать правило, но при этом оставить возможность вносить изменения в заголовки.**

- **reject - отклонить пакет и послать ICMP сообщение.**

- **return - вернуться в предыдущую цепочку, в то место где был произведен jump.**

comment(текст; по умолчанию: "") - описательный комментарий правила.

connection(текст; по умолчанию"") - маркировка соединения. Только соединения (включая related) маркированы в MANGLE для соответствия

connection-limit(целое; по умолчанию"") - соответствие номеру конкурирующего соединения для каждого специфического IP адреса.

connection-state(any | established | invalid | new | related; по умолча нию any) - состояние соединения

content(text; по умолчанию: "") - содержание текстового пакета для соответствия правилу

disabled(yes | no; по умолчанию no) - определяет заблокировано правило или нет

dst-address(IP адрес маска:порт; по умолчанию 0. 0.0.0/0:0-65535) - адрес назначения

dst-netmask(IP адрес) - маска назначения в десятичном формате x.x.x.x

dst-port(целое: 0..65535) - порт назначения или диапазон портов

flow(текст) - поток марков в соответствии. Только пакеты промаркированные в MANGLE будут соответствовать

icmp-options(целое; по умолчанию any:any) - соответствие полям ICMP Type:Code

in-interface(имя; по умолчанию: all) - интерфейс на который заходят пакеты идущие через маршрутизатор

- **all - можно включить локальный интерфейс петля для пакетов, порожденных маршрутизатором**

jump-target(имя) - имя целевой цепочки, если действие=jump используется

limit-burst(целое; по умолчанию: 0) - разрешенное превышение относительно limit-count/limit-time, измеряется в bits/s

limit-count(целое; по умолчанию: 0) - сколько раз используется правило в течении периода limit-time

limit-time(целое; по умолчанию: 0) - временной интервал измеряемый в секундах, используется в паре с limit-count

- **0 - всегда**

log(yes | no; по умолчанию: no) - использовать действие лог или нет

out-interface(имя; по умолчанию:name) - интерфейс с которрого выходят пакеты уходящие с маршрутизатора

- **all может подключать интерфейс петля**

p2p(ane | all-p2p | bit-torrent | direct-connect | fasttrack | soulseek| blubster | edonkey | gnutella | warez; по умолчанию any) - соответсвие Peer-to-Peer(P2P) соединениям:

- **all-p2p - соответствует любому известному P2P трафику**

- **any - соответствие другим пакетам (то есть не проверять это свойство)**

protocol(ah | egp | ggp | icmp | ipencap| ospf | rspf | udp | xtp | all | encap | gre | idpr-cmtp | ipip |
pup | st | vmtp | ddp | esp | hmp | igmp | iso-tp4 | rdp | tcp | xns-idp; по умолчанию all) -

установка протокола

- **all не может быть использована, если вы хотите использовать специфичные порты**

src-address(ip адрес маска:порт; по умолчанию: 0.0.0.0/0:0 -65535) - адрес источника

src-mac-address(MAC адрес; по умолчанию 00:00:00:00:00:00) - MAC адрес хоста с которого получен пакет

src-netmask(IP адрес) - маска источника в десятичном представлении

src-port(целое: 0..65535) - номер порта источника в диапазоне(0..65535)

- **0 - все порты 1-65535**

tcp-port(any | syn-only | non-syn-only; по умолчанию: any) - TCP варианты

tos(<целое>| dont-change | low-cost | low-delay | max-reliability | max-throughput | normal | anyinteger;
по умолчанию any) - определение соответствия значению Type of Service(ToS) в поле заголовка IP пакета

- **any - соответствует любому пакету (т.е. не проверяет это свойство)**

Примечание

Имейте в виду, protocol должен быть указан явно, если вы хотите выбираете port

Пример

Для случая, когда вы хотите отклонить пакеты с dst-port=8080

```
/ip firewall rule input add dst-port=8080 protocol=tcp action=reject
[admin@MikroTik] ip firewall rule input> print
Flags: X - disabled, I - invalid
 0 src-address=0.0.0.0/0:0-65535 in-interface=all
 dst-address=0.0.0.0/0:8080 out-interface=all protocol=tcp
 icmp-options=any:any tcp-options=any connection-state=any flow=""
 sconnection="" content="" src-mac-address=00:00:00:00:00:00 limit-count=0
 limit-burst=0 limit-time=0s action=reject log=no
```

Для разрешения не более 4 конкурирующих коннектов от каждого IP адреса, вы можете использовать это правило

```
/ip firewall rule forward add protocol=tcp tcp-options=syn-only connection-limit=5
action=drop
```

Цепочки файервола

Уровень подменю: /ip firewall

Описание

Файерволные правила фильтрации группируются вместе в цепочках. Это позволяет разрешить пакеты объединив их общим критерием внутри одного правила и затем передать в другую цепочку объединив их другим критерием. Предполагается, что например пакеты собираются для конкретных IP адресов и портов. Соответственно если используются только IP адреса то указывать протокол и порт не обязательно. С другой стороны если указывать протокол и порт то использовать IP адрес

необязательно.

Существуют три преопределенных цепочки, которые не могут быть удалены:

- **Цепочка input используется для обработки пакетов входящих на маршрутизатор и предназначенных ему. Пакеты проходящие через маршрутизатор в цепочку input не попадают.**

- **Цепочка forward используется для обработки пакетов идущих через маршрутизатор.**

- **Цепочка output используется для обработки пакетов исходящих от маршрутизатора. Пакеты идущие через маршрутизатор в цепочку output не попадают.**

При обработке цепочки правила отбора расположены сверху вниз. Если пакет соответствует критерию правила то для этого пакета выполняется действие (указанное в правиле) и движение пакета по цепочке прекращается. Если пакет не соответствует ни одному правилу то к нему применяется политика по умолчанию.

Доступные политики по умолчанию:

- **accept - принять пакет**

- **drop - сбросить пакет(без отправки ICMP сообщения об отклонении)**

- **none - не применимо**

Обычно пакет должен соответствовать нескольким критериям. Общие правила фильтрации могут группироваться в отдельной цепочке. Чтобы прогнать пакет по правилам дополнительных цепочек, действие jump должно использовать адрес правил в пределах другой цепочки.

Политика пользователя добавленная в цепочку none, не может быть изменена. Цепочки не могут быть удалены, если они содержат правила(не пустые).

Примечание

В виду того что правила NAT обрабатываются первыми, важно не забыт ь об этом при построении межсетевого экрана, так как пакет уже может быть изменен NATом.

Пакеты следующие через маршрутизатор не обрабатываются правилами input или output.

Будьте осторожны при изменении политики по умолчанию дл цепочек input или output! Вы можете потерять коннект с маршрутизатором.

Пример

```
[admin@MikroTik] ip firewall> print
 # NAME POLICY
 0 input accept
 1 forward accept
 2 output accept

[admin@MikroTik] ip firewall> add name=router
[admin@MikroTik] ip firewall> print
 # NAME POLICY
 0 input accept
 1 forward accept
 2 output accept
 3 router none
```

Приложения межсетевого экрана

Описание

В этой секции будут рассмотрены некоторые сетевые приложения и примеры их использования.

Базовые принципы построения файервола.

Предположим что у нас есть маршрутизатор соединяющий клиентскую сеть с Интернетом. Базовые принципы построения файервола могут быть сгруппированы следующим образом.

- **Защита маршрутизатора от несанкционированного доступа**

  При подключении к маршрутизатору производить проверку IP адреса. Разрешить доступ к маршрутизатору только с определенных хостов на определенные порты. Это может быть достигнуто путем настройки правил цепочки input на соответствие пакетов с адресом назначения маршрутизатора на всех интерфейсах.

- **Защита пользовательских хостов.**

  Подключения к адресам в клиентской сети должны проверяться. Должен быть разрешен доступ только к определенным хостам и службам. Это может быть достигнуто путем настройки цепочки forward на проверку соответствия пакетов идущих через маршрутизатор в клиентскую сеть.

- **Используйте SRC-NAT(masquerading) для 'Маскировки' частной сети одним внешним адресом**

  Все подключения с приватных адресов замаскарадены, и выходят наружу с адресом маршрутизатора. Это можно сделать путем включения действия masquerade.

- **Настройте политику использования Интернета клиентской сетью.**

  Подключения из клиентской сети должны проверяться.

  Это можно сделать путем настройки правил цепочки forward, и/или включением маскарада только для тех подключений которые разрешены.

  Фильтрация оказывает влияние на быстродействие маршрутизатора. Чтобы

снизить потери правила, отслеживающие состояние соединения должны находится сверху. То есть пакеты с опцией non-syn-only.

Ниже приводятся примеры настройки файер вола.

Пример настройки файерволных фильтров.

1. **Защитить MikroTik маршрутизатор от несанкционированного доступа на всех интерфейсах.**
   Разрешить доступ только из 'доверенной' сети 10.5.8.0/24.

2. **Защитить пользовательские хосты в пределах сети 192.168.0.0/24 от несанкционированного доступа извне.**

3. **Дать доступ из Интернета к http и smtp ресурсам на 192.168.0.17**

4. **Разрешить только ICMP ping со всех пользовательских хостов и прохождения пакетов с прокси сервера 192.168.0.17**

Адреса и маршруты показаны ниже:

```
[admin@MikroTik] ip address> print
Flags: X - disabled, I - invalid, D - dynamic
  # ADDRESS NETWORK BROADCAST INTERFACE
  0 10.0.0.217/24 10.0.0.0 10.0.0.255 Public
  1 192.168.0.254/24 192.168.0.0 192.168.0.255 Local

[admin@MikroTik] ip route> print
Flags: X - disabled, I - invalid, D - dynamic, J - rejected,
C - connect, S - static, R - rip, O - ospf, B - bgp
```

```
# DST-ADDRESS G GATEWAY DISTANCE INTERFACE
0 S 0.0.0.0/0 r 10.0.0.254 1 Public
1 DC 192.168.0.0/24 r 0.0.0.0 0 Local
2 DC 10.0.0.0/24 r 0.0.0.0 0 Public
```

Защитим маршрутизатор от неавторизированного доступа, нам надо профильтровать все пакеты с адресом назначения наш маршрутизатор, и принять только те которые разрешены. Так как все пакеты обрабатываются в цепочке input, мы можем добавить в эту цепочку следующее.

```
/ip firewall rule input
add connection-state=invalid action=drop
 comment="Drop invalid connection packets"
add connection-state=established
 comment="Allow established connections"
add connection-state=related
 comment="Allow related connections"
add protocol=udp comment="Allow UDP connections"
add protocol=icmp comment="Allow ICMP messages"
add src-address=10.5.8.0/24
 comment="Allow access from 'trusted' network 10.5.8.0/24"
add action=drop log=yes
 comment="Reject and log everything else"
```

Таким образом, в цепочке input будут приняты все разрешенные соединения и сброшены, все остальные.

Защита клиентской сети

Для защиты клиентской сети нам необходимо проверить на соответствие все пакеты идущие через маршрутизатор с адресом назначения 192.168.0.0/24. Это можно сделать путем добавления правил в цепочку forward. Проверив на соответствие пакеты в цепочке forward перейдем в другую цепочку под названием forward. И так создадимновые цепочки и правил а.

```
/ip firewall add name=customer
/ip firewall rule customer
add connection-state=invalid action=drop
  comment="Drop invalid connection packets"
add connection-state=established
  comment="Allow established connections"
add connection-state=related
  comment="Allow related connections"
add protocol=udp
  comment="Allow UDP connections"
add protocol=icmp
  comment="Allow ICMP messages"
add protocol=tcp dst-address=192.168.0.17/32:80
  comment="Allow http connections to the server at 19 2.168.0.17"
add protocol=tcp dst-address=192.168.0.17/32:25
  comment="Allow SMTP connections to the server at 192.168.0.17"
add action=drop log=yes comment="Drop and log everything else"
```

Теперь все что осталось сделать это поместить эти правила в це почку forward.

```
/ip firewall rule forward
add out-interface=Local action=jump
  jump-target=customer
```

Назначение Интернет политики

Для назначение Интернет политики доступа клиентских хостов только ч ерез прокси сервер 192.168.0.17 мы должны добавить правило в цепочку forward.

```
/ip firewall rule forward
add connection-state=invalid action=drop
  comment="Drop invalid connection packets"
add connection-state=established
  comment="Allow established connections"
add connection-state=related
  comment="Allow related connections"
add protocol=icmp out-interface=Public
  comment="Allow ICMP ping packets"
add src-address=192.168.0.17/32 out-interface=Public
  comment="Allow outgoing connections from the server at 192.168.0.17"
add action=drop out-interface=Public log=yes
  comment="Drop and log everything else"
```

Пример source NAT(Masquerading)

Если вы хотите скрыть клиентскую сеть 192.168.0.0/24 одним адресом маршрутизатора 10.0.0.217, вам необходимо произвести трансляцию исходящих адресов. Маскарадинг будет подменять исходящий адрес и порт всех пакетов идущих из сети 192.168.0.0/24 на адрес маршрутизатора 10.0.0.217 когда пакет будет проходить через него.

```
/ip firewall src-nat action=masquerade out-interface=Public
```

Если вы хотите дать доступ к ресурсам внутри сети вам необходимо использовать destination NAT.

Пример destination NAT

Предположим, что вам необходимо сконфигурировать маршрутизатор так чтобы снаружи были видны ресурсы из клиентской сети.

Сервер к которому надо дать доступ имеет адрес 192.168.0.4 и на нем запущен web сервер слушающий запросы на 80 порту.
Мы хотим сделать его доступным из интернета с адресом 10.0.0.217:80 который будет транслироваться в локальный адрес 192.168.0.4:80. Для этого требуется одно правило транслирующее адрес назначения и порт:

```
/ip firewall dst-nat add action=nat protocol=tcp
 dst-address=10.0.0.217/32:80 to-dst-address=192.168.0.4
```