?????? Firewall

Фаервол в MikroTik реализует как stateful (с отслеживанием состояния) (с использованием connection tracking), так и stateless (без отслеживания состояния) фильтрацию пакетов, обеспечивая функции безопасности для управления потоком данных к маршрутизатору, от него и через него. Вместе с технологией Network Address Translation (NAT) фаервол служит инструментом для предотвращения несанкционированного доступа к напрямую подключённым сетям и самому маршрутизатору, а также фильтром для исходящего трафика.

Сетевые фаерволы защищают внутренние сети от внешних угроз. Когда объединяются разные сети, всегда существует риск, что кто-то извне проникнет в локальную сеть (LAN). Такие вторжения могут привести к краже и распространению приватных данных, изменению или уничтожению ценной информации, либо полному удалению данных с дисков. Фаервол используется для предотвращения или минимизации рисков безопасности, связанных с подключением к другим сетям. Правильно настроенный фаервол играет ключевую роль в создании эффективной и безопасной сетевой инфраструктуры.

MikroTik RouterOS обладает очень мощной реализацией фаервола с возможностями, включая:

- проверку пакетов без отслеживания состояния (stateless packet inspection);
- проверку пакетов с отслеживанием состояния (stateful packet inspection);
- обнаружение протоколов уровня 7 (Layer-7 protocol detection);
- фильтрацию пиринговых протоколов (peer-to-peer protocols filtering);
- классификацию трафика по:
    - MAC-адресу источника;
    - IP-адресам (сети или списки) и типам адресов (broadcast, local, multicast, unicast);
    - порту или диапазону портов;
    - IP-протоколам;
    - опциям протокола (ICMP type и code, TCP-флаги, IP options и MSS);
    - интерфейсу, через который пакет пришёл или ушёл;
    - внутренним отметкам потока и соединения (flow and connection marks);
    - DSCP байту;
    - содержимому пакета;
    - скорости поступления пакетов и номерам последовательности;
    - размеру пакета;
    - времени поступления пакета;
    - и многое другое!

Межсетевой экран разделен на три основных модуля:

- filter/raw — используется для отказа в трафике на основе настроенных политик. Фильтрация в RAW таблицах позволяет экономить ресурсы, если не требуется отслеживание соединений.
- mangle — используется для маркировки определенных соединений, пакетов, потоков, установления приоритетов и выполнения других задач.
- nat — используется для установки правил преобразования адресов, перенаправлений и проброса портов.

???????

Правила фильтрации межсетевого экрана сгруппированы в цепочки. Это позволяет сопоставить пакет с одним общим критерием в одной цепочке, а затем передать на обработку по другим критериям в другую цепочку.

Например, пакет должен быть сопоставлен с парой IP адрес:порт. Конечно, это можно достичь, добавив столько правил с совпадением по IP адресу и порту, сколько требуется, в цепочку forward, но лучшим способом может быть добавление одного правила, которое соответствует трафику от определенного IP адреса. Затем можно добавить правила, которые проводят сопоставление по отдельным портам, в цепочку mychain без указания IP адресов.

```
/ip firewall filter add chain=mychain protocol=tcp dst-port=22 action=accept
add chain=mychain protocol=tcp dst-port=23 action=accept
add chain=input src-address=1.1.1.2/32 jump-target="mychain"
```

При обработке цепочки правила берутся из цепочки в порядке их перечисления сверху вниз. Если пакет соответствует критериям правила, то выполняется указанное действие, и остальные правила в этой цепочке не обрабатываются (исключением является действие passthrough и некоторые операции Mangle).

Если пакет не соответствует ни одному правилу в цепочке, то он принимается.

Каждый модуль межсетевого экрана имеет свои предопределенные цепочки:

- **raw**:
  - prerouting
  - output
- **filter**:
  - input
  - forward
  - output
- **mangle**:
  - prerouting

    - input
    - forward
    - output
    - postrouting

- **nat**:
    - srcnat
    - dstnat

Более детальная обработка пакетов в RouterOS описана в диаграмме Packet Flow в RouterOS.

Revision #2
Created 11 November 2025 15:56:25 by Admin
Updated 11 November 2025 16:20:11 by Admin