Как настроить хитрую цепочку для фильтрации ICMP пакетов в Микротик ?

*С помощью такой цепочки мы защитим себя от атаки Ping Flood*

*и разрешим только обычный Ping и Трассировку.*

1. Заходим IP – Firewall – Filter rules.
2. Создаём **1 правило**.

chain: input

protocol: 1 (icmp)

In. Interface List: WAN (т.е. из внешки)

Advanced – Packet Size: 0-128 (говорим, чтобы размер пакетов был не больше 128 байт)

Extra – Limit – Rate: 5 / sec, Burst: 5, Mode: packet

*Rate: 5 – количество пакетов в секунду, Burst: 5 – максимальное количество пакетов в секунду, Mode: packet – что считать – пакеты, или биты, в нашем случае – пакеты.*

Action – Action – jump

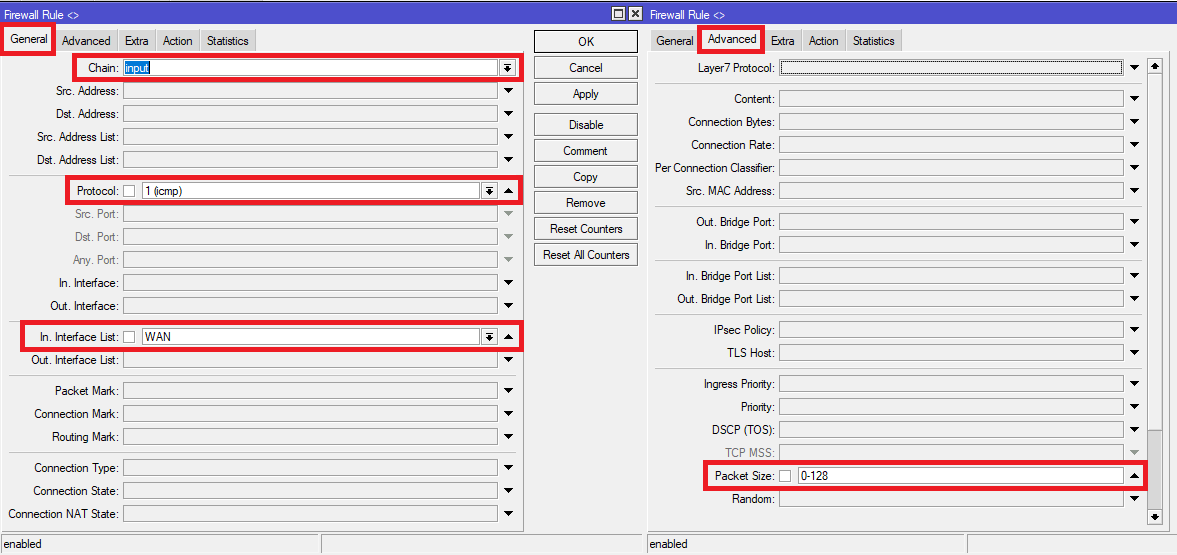
Jump Target – ICMP

*Создаём кастомную цепочку и уже в этой кастомной цепочке проверяем пакеты на валидность.*

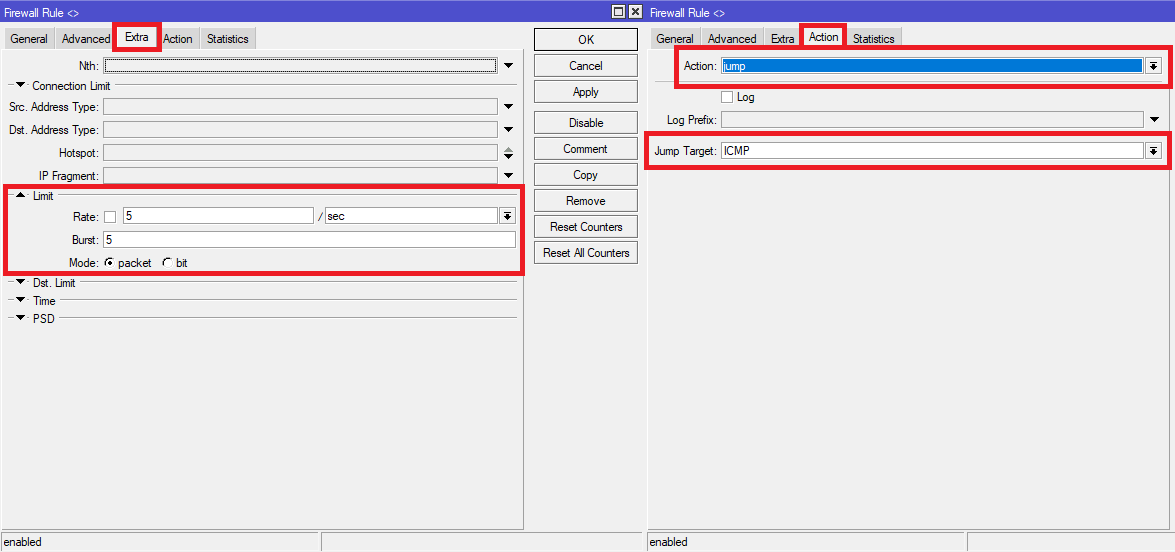
*Названия ICMP в Jump Target, понятное дело, не будет, его пишем руками.*

Скриншоты для наглядности.

Это во вкладках General и Advanced.



Это во вкладках Extra и Action.



1. Теперь создаём саму цепочку.

**1 звено.**

chain: input

Protocol: 1 (icmp)

Advanced – ICMP Options – echo reply: **0** / ICMP Code: **0**

Action – Action – Accept

Comment: Разрешить обычный Ping (echo reply: 0 / ICMP Code: 0)

**2 звено.**

chain: input

Protocol: 1 (icmp)

Advanced – ICMP Options – echo reply: **0** / ICMP Code: **8**

Action – Action – Accept

Comment: Разрешить обычный Ping (echo reply: 0 / ICMP Code: 8)

**3 звено.**

chain: input

Protocol: 1 (icmp)

Advanced – ICMP Options – time exceeded: **11** / ICMP Code: **0**

Action – Action: Accept

Comment: Разрешить Трассер (time exceeded: 11 / ICMP Code: 0)

**4 звено.**

chain: input

Protocol: 1 (icmp)

Advanced – ICMP Options – destination unreachable: **3** / ICMP Code: **3**

Action – Action: Accept

Comment: Разрешить Трассер (destination unreachable: 3 / ICMP Code: 3)

**5 звено.**

chain: input

Protocol: 1 (icmp)

Advanced – ICMP Options – destination unreachable: **3** / ICMP Code: **4**

Action – Action – Accept

Comment: Разрешить автоматическое определение самого большого размера пакета MTU (destination unreachable: 3 / ICMP Code: 4)

Скриншот крупным планом.

