Как сделать простую защиту от DoS атаки на Микротике RB951G-2HnD ?

Данный способ не защитит нас от ботнета, зато спасёт от простых одиночных атак.

*DOS – одиночная атака, DDoS – множественная атака с помощью ботнета.*

1. Заходим на Микрот по маку или IP через Winbox.
2. Далее заходим Firewall – Filter Rules и создаём правила.

**Первое.**

Chain: input (входящие соединения на Микротик)

Protocol: 6 (tcp)

Dst. Port: 8219, 80 (порты 8219 и 80, Winbox и вебка Микротика)

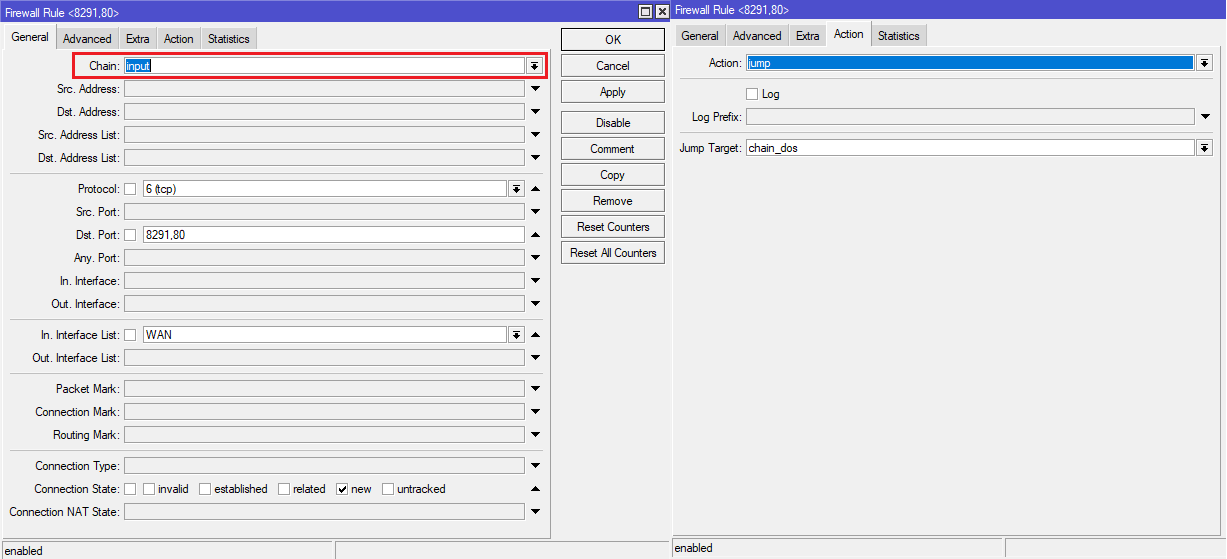
In. Interface List: WAN (список интерфейсов – внешний, т.е. интерфейс провайдера)

Connection State: [**V**] new (отслеживать только новые соединения)

Action – Action – jump (jump – это помещение в цепочку)

Jump Target: chain\_dos (в цепочку chain\_dos)

Комментарий: «Детектирование DoS атаки»



**Второе.**

*Во втором правиле всё тоже самое, только вместо input ставим forward.*

Chain: forward (это те соединения, которые проходят через наш роутер дальше в сеть)

Protocol: 6 (tcp)

Dst. Port: 8219, 80 (порты 8219 и 80, Winbox и вебка Микротика)

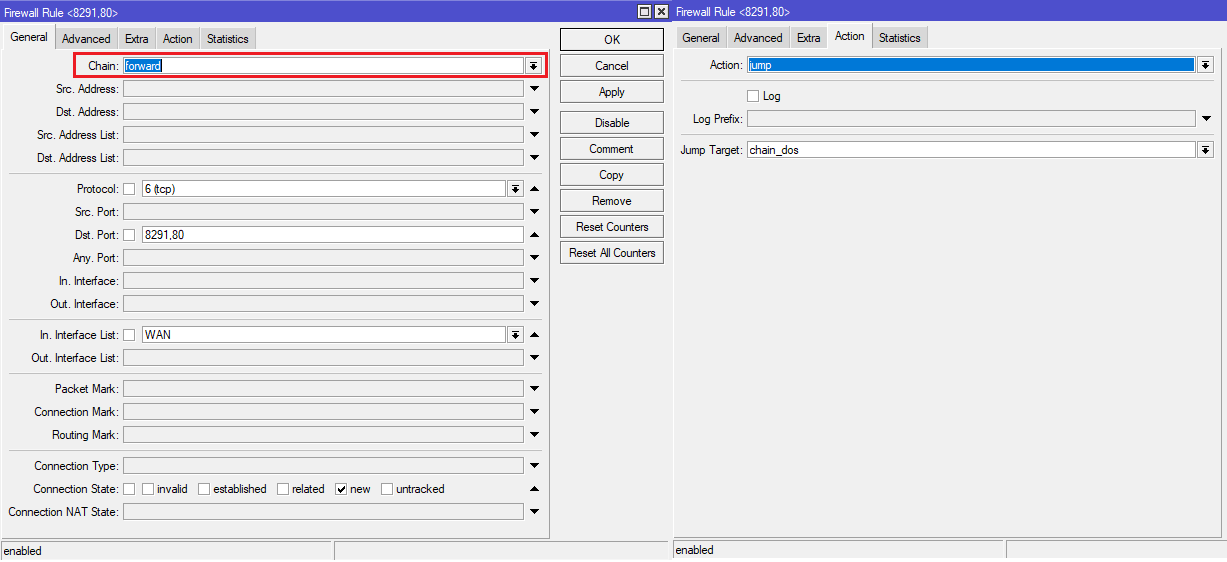
In. Interface List: WAN (список интерфейсов – внешний, т.е. интерфейс провайдера)

Connection State: [**V**] new (отслеживать только новые соединения)

Action – Action – jump (jump – это помещение в цепочку)

Jump Target: chain\_dos (в цепочку chain\_dos)

Комментарий: «Детектирование DoS атаки»



**Третье.**

Во вкладке General, в позиции Chain: выбираем chain\_dos. Всё, больше ничего не трогаем.

Теперь переходим на вкладку Extra и раскрываем позицию Dst. Limit.

В этом месте мы задаём лимиты, при которых данное правило сработает.

Rate 10 / sec. (это количество соединений в секунду)

Burst 25 («Всплеск соединений», или максимальное количество допустимых соединений в секунду)

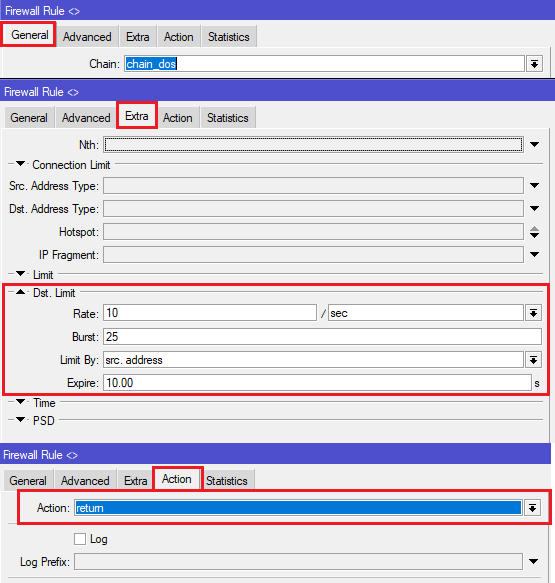
*Для чего нужен Burst? Он нужен для того чтобы нормальные, не атакующие юзеры не попали в бан.  
То есть, в течении 10 секунд, разрешается до 25 соединений в секунду.*

Limit by: src. address (адрес источника)

Expire: 10.00 (лимит времени в течении которого действует Burst)

Теперь переходим во вкладку Action – Action – Return.

*Что это значит? Если правило не попало под действие вышеописанных параметров, то оно возвращается в обычную цепочку маршрутизации. Если оно попало, значит переходим к следующему правилу…*

**

**Четвёртое.**

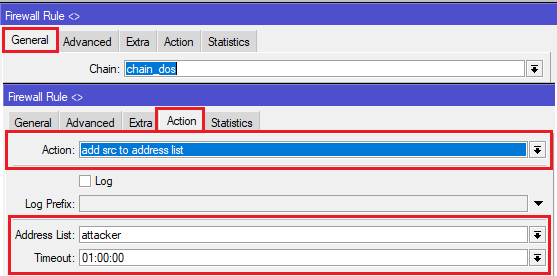
Chain: chain\_dos

Action – Action – add src to address list (добавить адрес источника в список)

Address List: attacker (название адрес-листа)

Timeout: 01:00:00

*Почему 1 час ? Не нужно ставить дни и часы. Атакующий может менять IP адреса и к предыдущим не возвращаться.  
Однако, если у нас очень слабый Микрот, то мы очень быстро забьём этим адрес-листом оперативную память.  
То есть, мы получим зависшую железку, а атакующий получит результат.  
Таким образом, 1 час – это оптимальное значение для того, чтобы адрес-лист успевал очищаться.*

**

**Пятое.**

Переходим на вкладку RAW.

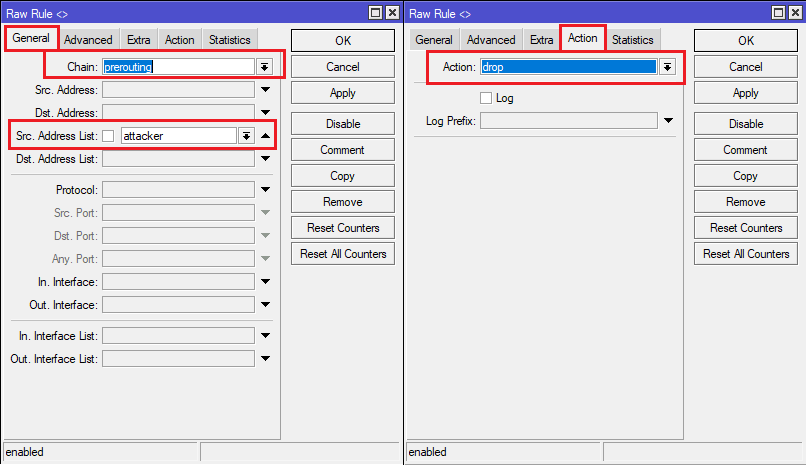
Chain: prerouting

Src. Address List: attacker

Dst. Address List: *сюда также можно внести список доверенных IP адресов, чтобы они не попали в блокировку.*

Action – Action: Drop

*Почему prerouting? Таким образом мы будем блокировать и отбрасывать пакеты до того как они пошли по цепочке  
маршрутизации, чтобы не нагружать наш процессор. Это просто небольшая экономия ресурсов.  
  
Почему Drop ? То есть, никак не реагируем на пакет и просто отбрасываем.*



**Пояснение.**

Адрес-лист attacker во вкладке Address Lists вручную создавать не нужно.  
При атаке, он создастся сам и будет иметь атрибут «D» то есть «Dynamic».

То есть, атакующий попадёт во временный адрес-лист «attacker» и будет отброшен.