Как включить простейшую защиту от сканирования портов на   
Микротике RB951G-2HnD ?

*Её лучше всего включать в дополнение к port-knocking,*

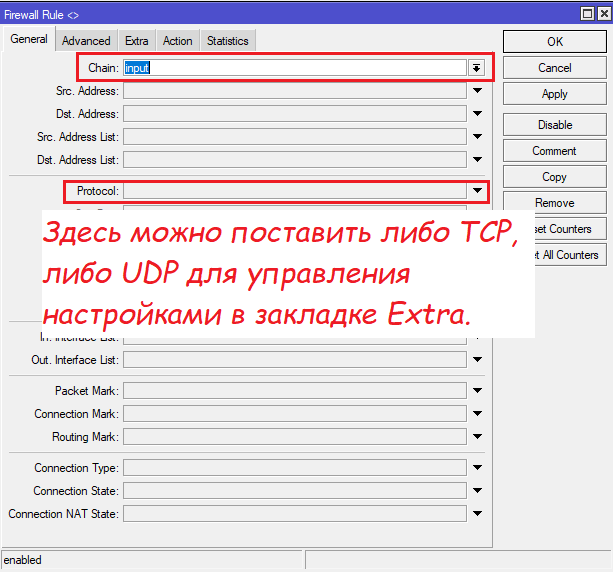
*дабы максимально защитить устройство от простукивания портов nmap-ом.*

1. Заходим на Микрот через Winbox по IP, или Мак-адресу.
2. IP – Firewall – Filter Rules.
3. Добавляем одно новое правило.

Сначала на вкладке **General.**

Chain: input

Protocol: *если хотим менять настройки, то здесь ставим либо TCP, либо UDP, но тогда придётся делать несколько правил.  
Если хотим оставить дефолтные настройки, тогда здесь ничего не пишем.  
В нашем случае, настройки будут дефолтные.*

**

Дальше, переходим на вкладку **Extra** – вкладка «PSD» и убеждаемся, что там выставлены дефолтные параметры.

Если в параметре Protocol у нас ничего не прописано, то эти параметры изменить будет нельзя.

Weight Threshold: 21

*Максимальная задержка между пакетами с разными портами назначения, пришедших с одного адреса.*

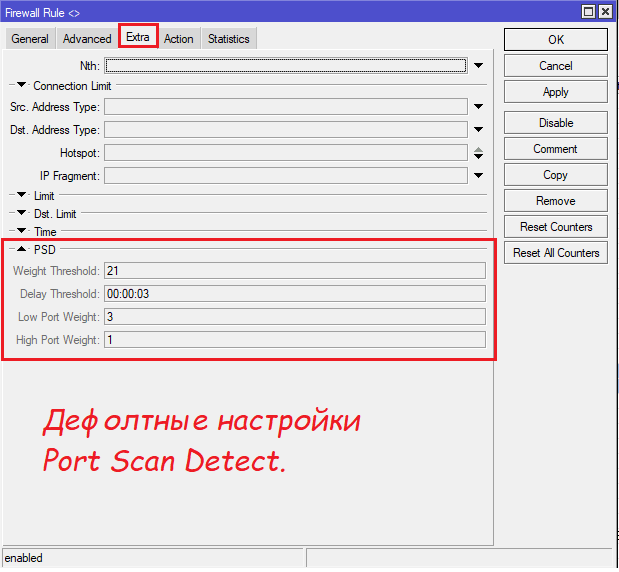
Delay Threshold: 00:00:03

*При каком значении баллов сработает. Это значит, что есть некая условная единица, условное количество баллов, которые должен набрать злоумышленник. В случае своего сканирования, злоумышленник должен в течение, например, 3 секунд просканировать 7 портов в диапазоне от 0 до 1023 или, например, 21 порт в диапазоне от 1024 до 65 535.  
Высокие порты оцениваются условно, как одна единица, низкие порты оцениваются гораздо выше – как три единицы.  
Port Scan Detect работает с TCP и UDP.*

Low Port Weight: 3

*Сколько при подсчёте стоит каждый порт в диапазоне от 0 до 1023 (низкие порты).*

High Port Weight: 1  
*Сколько при подсчёте стоит каждый порт в диапазоне от 1024 до 65 535 (высокие порты).*

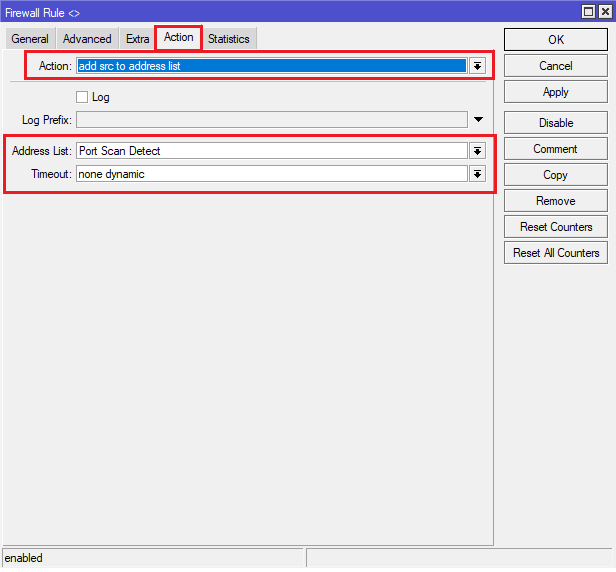
**

Теперь переходим на вкладку **Action.**

В Action ставим «add src to address list», т.е. добавить ip адрес источника в некий адрес лист.

Address List: здесь пишем Port Scan Detect (здесь лучше писать полностью, а не сокращённо).

Timeout можно оставить в динамическом режиме, т.е. none dynamic

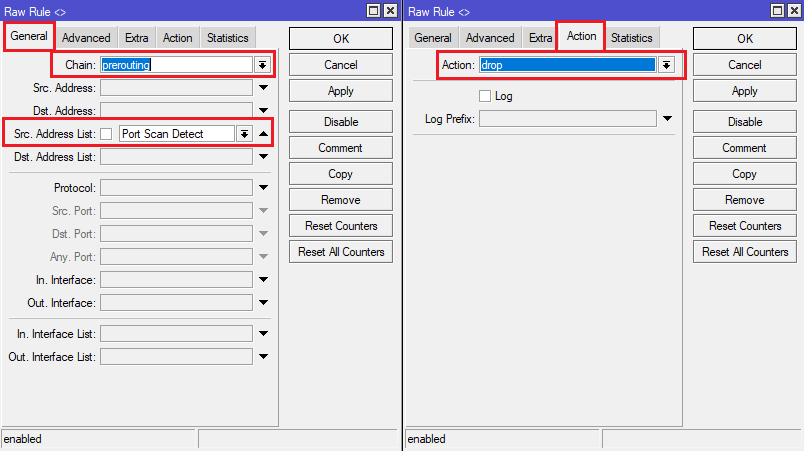


Здесь всё. Теперь переходим на вкладку **RAW.**

Chain: prerouting

Src. Address List: Port Scan Detect

Action – Action: Drop



*Что такое RAW – prerouting ? Если в двух словах, то это механизм, который позволяет обрабатывать пакеты до того, как они попадут в таблицу фильтрации файерволла. То есть, это ПРЕфильтрация.  
Если мы точно уверены, что нам НЕ нужен этот трафик, то его можно дропать ещё до того, как он попадёт в файерволл*

*и, тем самым, немного разгрузить железные ресурсы маршрутизатора.*