Как настроить порт-нокинг на Микротике RB951G-2HnD  
для защиты от nmap-a и сканирования портов ?

1. Заходим на Winbox по маку или IP адресу.
2. Заходим в IP – Firewall – Filter Rules.
3. Создаём 5 правил.

**Первое**:

Chain: input

Src. Address List: **ПУСТО !**

Protocol: 17 (udp)

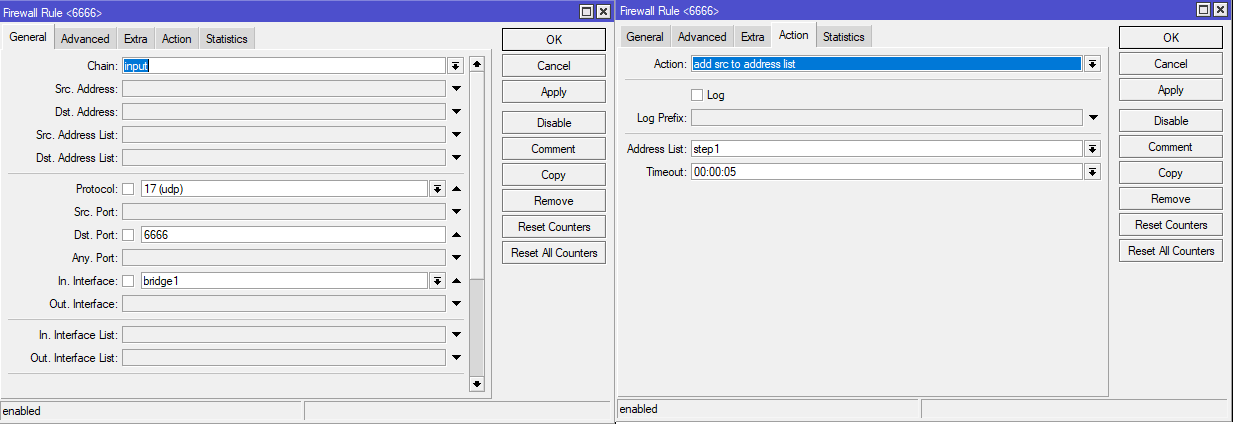
Dst. Port: **6666**

In. Interface: bridge1 (либо тот на котором у нас «входяшка»)

Action – Action: add src to address list

Address List: **step1**

Timeout: 00:00:05 (задержка 5 сек.)



**Второе:**

Chain: input

Src. Address List: step1

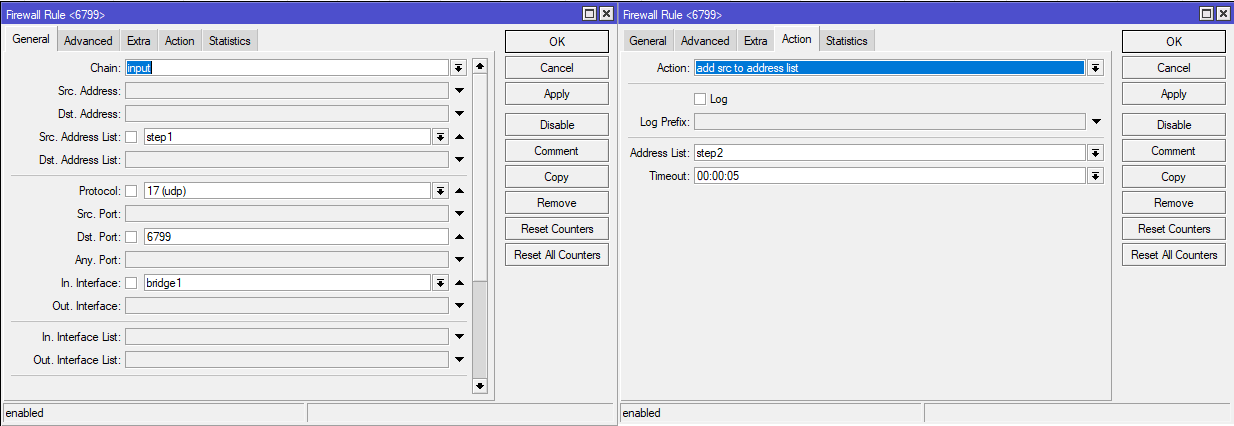
Protocol: 17 (udp)

Dst. Port: **6799**

In. Interface: bridge1 (наша «входяшка»)

Action – Action: add src to address list  
Address List: **step2**

Timeout: 00:00:05 (задержка 5 сек.)



**Третье:**

Chain: input

Src. Address List: step2

Protocol: 17 (udp)

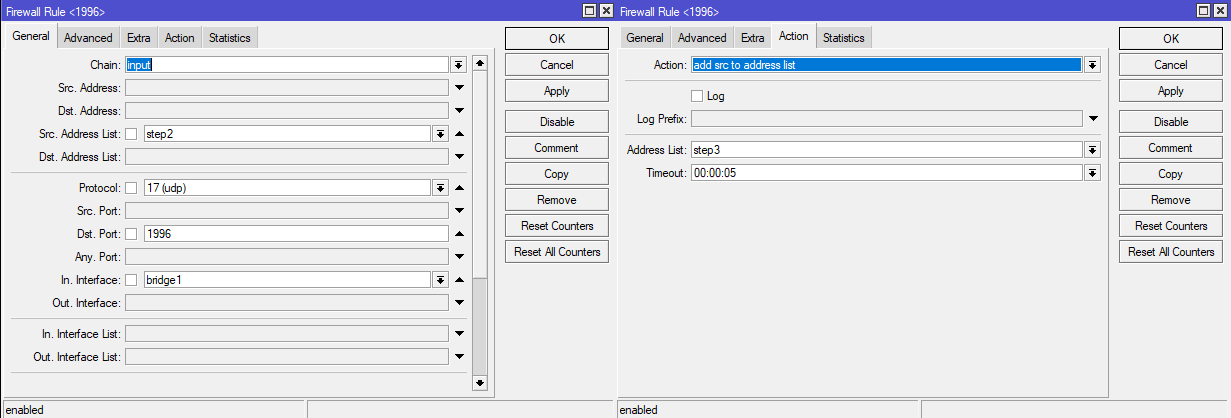
Dst. Port: **1996**

In. Interface: bridge1 (наша «входяшка»)

Action – Action – add src to address list

Address List: **step3**

Timeout: 00:00:05 (задержка 5 сек.)



**Четвёртое:**

Chain: input  
Src. Address List: step3

Protocol: 17 (udp)

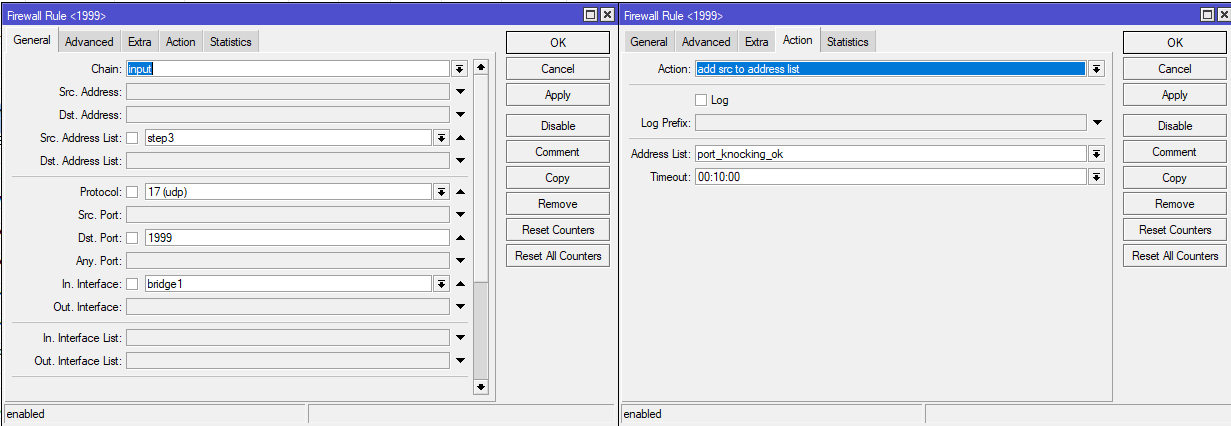
Dst. Port: **1999**

In. Interface: bridge1 (наша «входяшка»)

Action – Action – add src to address list

Address List: **port\_knocking\_ok**

Timeout: 00:10:00 (задержка на открытие портов 10 мин.)



*Первыми четырьмя правилами мы описали порт-нокинг. Сейчас нам нужно его разрешить, т.е. сделать Accept.*

**Пятое:**

Chain: input

Src. Address List: port\_knocking\_ok

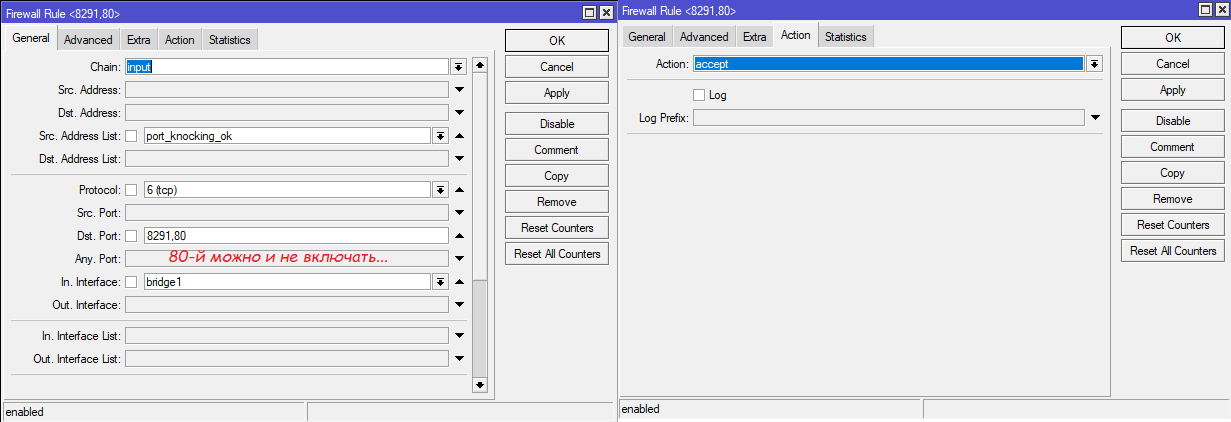
Protocol: 6 (tcp)

Dst. Port: 8291, 80 (здесь мы разрешаем Winbox и web-морду Микрота)

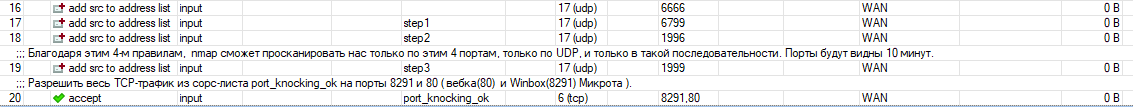
*Вебка, по идее, всегда выключена, так что 80-й порт можно и не включать.*

In. Interface: bridge1 (всё та же, наша «входяшка»)

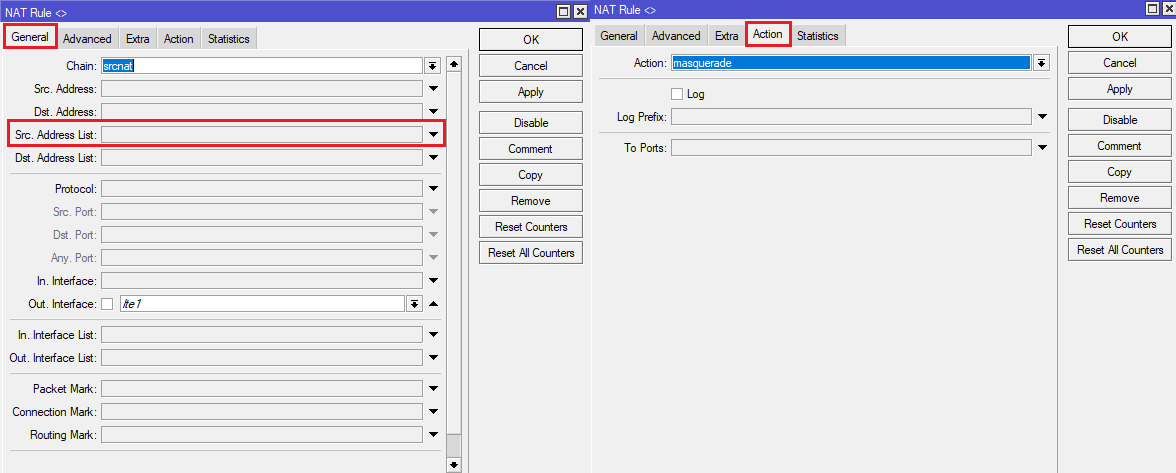
Action – Action – accept



Скриншот общим планом для наглядности:

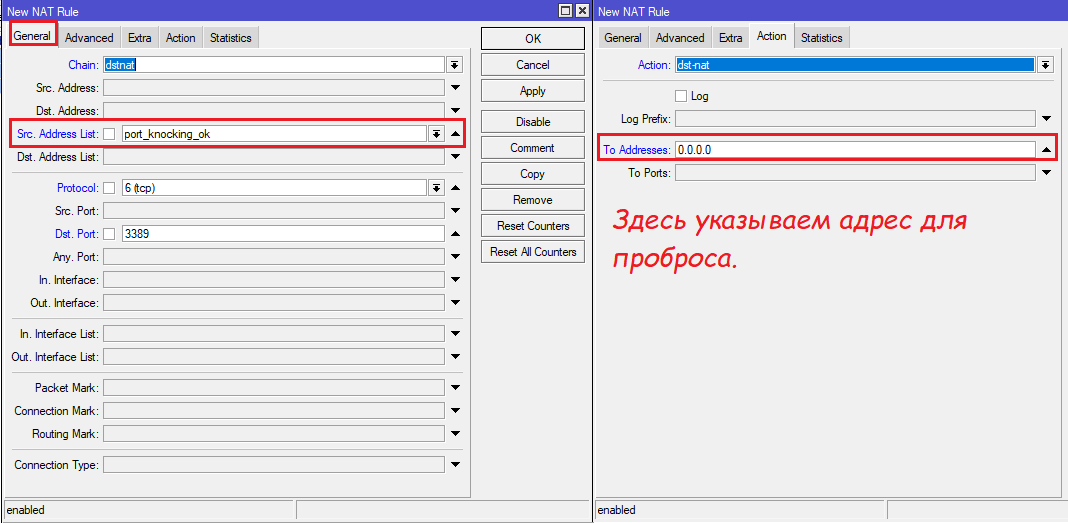


1. Теперь зайдём в NAT. Если у нас обычный «Маскарад», то в Src .Address List должно быть **ПУСТО**, иначе не будет работать интернет.



Если у нас сделан проброс портов, например, на порт 3389, то в Src. Address List нужно указать наш port\_knocking\_ok.

Вот так:



Таким образом, порт-нокинг с помощью nmap можно будет осуществить только

путём простукивания портов 6666, 6799, 1996 и 1999, только по UDP и только в таком порядке.

1. Если мы хотим автоматизировать работу nmap, можно написать небольшой скрипт на BASH.

#!/bin/bash

# Здесь прописываем адрес Микрота, который хотим просканировать nmap-ом

vtarget=здесь прописываем адрес Микрота, который хотим просканировать nmap-ом

vports=(6666 6799 1996 1999)

vproto=udp

function start\_udp() {

echo -ne 'null' > /dev/udp/$vtarget/${vports[0]}

sleep 2

echo -ne 'null' > /dev/udp/$vtarget/${vports[1]}

sleep 2

echo -ne 'null' > /dev/udp/$vtarget/${vports[2]}

sleep 2

echo -ne 'null' > /dev/udp/$vtarget/${vports[3]}

}

function start\_tcp() {

timeout 0.5 bash -c "echo -ne 'null' > /dev/tcp/$vtarget/${vports[0]}"

sleep 2

timeout 0.5 bash -c "echo -ne 'null' > /dev/tcp/$vtarget/${vports[1]}"

sleep 2

timeout 0.5 bash -c "echo -ne 'null' > /dev/tcp/$vtarget/${vports[2]}"

sleep 2

timeout 0.5 bash -c "echo -ne 'null' > /dev/tcp/$vtarget/${vports[3]}"

}

if [ "$vproto" == "udp" ]; then

echo "udp port knocking target $vtarget"

start\_udp

else

echo "tcp port knocking target $vtarget"

start\_tcp

fi

*Чтобы активировать данный скрипт на Линуксе, нам нужно будет установить nmap от имени суперпользователя:*

*sudo apt update*

*sudo apt install nmap (sudo yum install nmap)*

*Дальше, в самом скрипте, в самой первой строчке vtarget указать имя узла (Микротика), порты на котором нам нужно простучать.*

*Дальше сохранить данный скрипт под названием, например, knocking.sh*

*и дать ему права на исполнение: chmod +x knocking.sh*

*И запустить скрипт командой: ./knocking.sh*