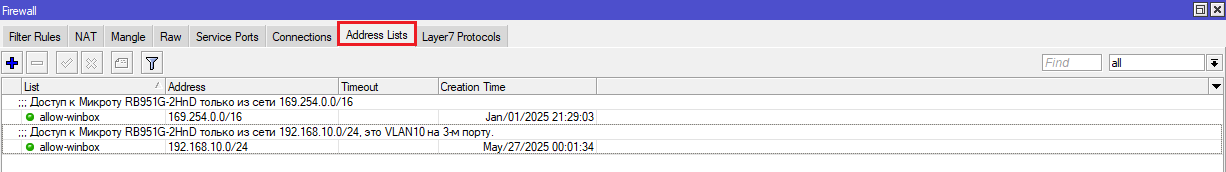
Как настроить защиту от брутфорса на Микротике RB951G-2HnD  
для Winbox и SSH по портам 8291 и 22 ?

1. Заходим в IP – Firewall – Address Lists.
2. Создаём Address Lists «allow-winbox».

Например, вот такой.



*Таким образом, доступ к Winbox-у у нас будет только из этих двух подсетей.*

1. Теперь заходим IP – Firewall – Filter rules.

**----- Для начала, создадим правила для Winbox (8291). -----**

**1 Правило.**

chain: input

Src. Address List [**!**] allow-winbox (т.е. все КРОМЕ allow-winbox)

Protocol: 6 (tcp)

Dst. Port: 8291

Connection State: [**v**] new

Action: add src to address list

Address List: winbox\_stage1 (его не будет, его пишем руками)

Timeout: 00:01:00 (1 минута)

Комментарий: Кидаем все подозрительные попытки брутфорса на Winbox в winbox\_stage1 на 1 минуту.

**2 Правило.**

Chain: input

Src. Address List: winbox\_stage1

Protocol: 6 (tcp)

Dst. Port: 8291

Connection State: [**v**] new

Action: add src to address list

Address List: winbox\_stage2 (его не будет, его пишем руками)

Timeout: 00:10:00 (10 минут)

Comment: Кидаем все подозрительные попытки брутфорса на Winbox в winbox\_stage2 на 10 минут.

**3 Правило.**

Chain: input

Src. Address List: winbox\_stage2

Protocol: 6 (tcp)

Dst. Port: 8291

Connection State: [**v**] new

Action: add src to address list

Address List: winbox\_stage3 (его не будет, его пишем руками)

Timeout: 00:30:00

Comment: Кидаем все подозрительные попытки брутфорса на Winbox в winbox\_stage3 на 30 минут.

**4 Правило.**

Chain: input

Src. Address List: winbox\_stage3

Protocol: 6 (tcp)

Dst. Port: 8291

Connection State: [**v**] new

Action: add src to address list

Address List: winbox\_blacklist (его не будет, его пишем руками)

Timeout: 10d 00:00:00

Comment: Кидаем все подозрительные попытки брутфорса на Winbox в winbox\_blacklist на 10 дней.

**5 Правило.**

Chain: input

Src. Address List: winbox\_blacklist

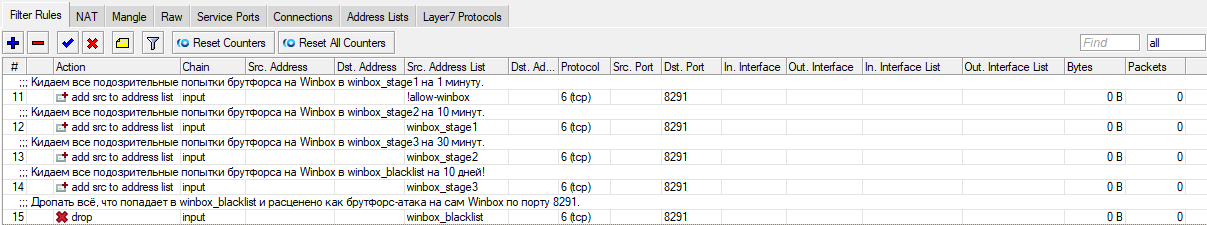
Protocol: 6 (tcp)

Dst. Port: 8291

Action: drop

Comment: Дропать всё, что попадает в winbox\_blacklist и расценено как брутфорс-атака на сам Winbox по порту 8291.

Скриншот для наглядности.



*Последнее правило (drop) идёт после правил с «add src to address list», так как сначала идёт оценка происходящего и небольшая блокировка на 1, 10 и 30 минут и, если атакующий не успокаивается, последним идёт бан на 10 дней.*

**----- Теперь, сообразим всё тоже самое, но для SSH (22). -----**

*Здесь всё по аналогии с Winbox (8291).*

**1 Правило.**

chain: input

Src. Address List: [**v**] allow-winbox (т.е. все КРОМЕ allow-winbox)

Protocol: 6 (tcp)

Dst. Port: 22

Connection State: [**v**]

Action: add src to address list

Address List: ssh\_stage1 (его не будет, его пишем руками)

Timeout: 00:01:00

Comment: Кидаем все подозрительные попытки брутфорса на SSH в ssh\_stage1 на 1 минуту.

**2 Правило.**

chain: input

Src. Address List: ssh\_stage1

Protocol: 6 (tcp)

Dst. Port: 22

Connection State: [**v**]

Action: add src to address list

Address List: ssh\_stage2 (его не будет, его пишем руками)

Timeout: 00:10:00

Comment: Кидаем все подозрительные попытки брутфорса на SSH в ssh\_stage2 на 10 минут.

**3 Правило.**

chain: input

Src. Address List: ssh\_stage2

Protocol: 6 (tcp)

Dst. Port: 22

Connection State: [**v**]

Action: add src to address list

Address List: ssh\_stage3 (его не будет, его пишем руками)

Timeout: 00:30:00

Comment: Кидаем все подозрительные попытки брутфорса на SSH в ssh\_stage3 на 30 минут.

**4 Правило.**

chain: input

Src. Address List: ssh\_stage3

Protocol: 6 (tcp)

Dst. Port: 22

Connection State: [**v**] new

Action: add src to address list

Address List: ssh\_blacklist

Timeout: 10d 00:00:00

Comment: Кидаем все подозрительные попытки брутфорса на SSH в ssh\_blacklist на 10 дней!

**5 Правило.**

chain: input

Src. Address List: ssh\_blacklist

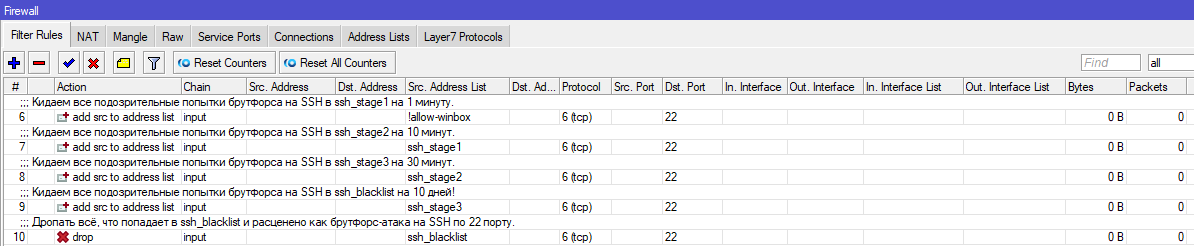
Protocol: 6 (tcp)

Dst. Port: 22

Action: drop

Comment: Дропать всё, что попадает в ssh\_blacklist и расценено как брутфорс-атака на SSH по 22 порту.

Всё по аналогии. Последнее правило с drop-ом в конце.



*Таким образом, если будет попытка брутфорс-атаки, злоумышленник сначала попадёт в бан на 1 минуту, затем на 10, затем на 30, а потом на 10 дней. Его IP адрес попадёт в динамически создаваемые адрес-листы. Вручную ничего заполнять не надо. Это сделано потому, что у атакующего, скорее всего, будут динамические IP и он, скорее всего, будет их время от времени менять, поэтому и адрес-листы у нас тоже динамические, чтобы подстроиться под атаку.*