Mikrotik: защищаем SSH от брутфорса

Отсюда: http://wiki.leonchik.ru/doku.php?id=mikrotik:protect-ssh

Идея проста: имеется 4 таблицы. 3 промежуточных и одна в которой хранятся заблокированные адреса. Все таблицы динамические. Адрес по мере подключения добавляется в каждую таблицу по очереди. У нас 3 промежуточных таблицы, адреса в которых хранятся по одной минуте. Таким образом получается, что если в течение одной минуты с одного и того же адреса будут произведены более 3-х попыток подключения, адрес попадает в самую главную таблицу, 4-ю. Адреса там в моем случае хранятся 30 минут. Если кому не хватает - можно больше :)

Примечание: можно защищать не только ssh, но и долбежку на любой другой порт

```
ip firewall filter add action=drop chain=input dst-port=22 protocol=tcp src-
address-list=ssh_blacklist
ip firewall filter add action=add-src-to-address-list address-
list=ssh_blacklist address-list-timeout=30m chain=input \
    connection-state=new dst-port=22 protocol=tcp src-address-
list=ssh_stage3
ip firewall filter add action=add-src-to-address-list address-
list=ssh_stage3 address-list-timeout=1m chain=input \
    connection-state=new dst-port=22 protocol=tcp src-address-
list=ssh_stage2
ip firewall filter add action=add-src-to-address-list address-
list=ssh_stage2 address-list-timeout=1m chain=input \
    connection-state=new dst-port=22 protocol=tcp src-address-
list=ssh_stage1
ip firewall filter add action=add-src-to-address-list address-
list=ssh_stage1 address-list-timeout=1m chain=input \
    connection-state=new dst-port=22 protocol=tcp
ip firewall filter add chain=input connection-state=new dst-port=22
protocol=tcp
```

И еще вот отсюда: http://wiki.mikrotik.com/wiki/Bruteforce_login_prevention

Данная настройка разрешает всего 10 неверных попыток подключения к FTP в минуту, после чего блокирует атакующего на 3 часа:

```
ip firewall filter add chain=input protocol=tcp dst-port=21 src-address-
list=ftp_blacklist action=drop \ comment="drop ftp brute forcers"
ip firewall filter add chain=output action=accept protocol=tcp content="530
Login incorrect" dst-limit=1/1m,9,dst-address/1m
ip firewall filter add chain=output action=add-dst-to-address-list
protocol=tcp content="530 Login incorrect" \
address-list=ftp_blacklist address-list-timeout=3h
```

При брутфорсе SSH атакующий попадает в бан на 10 дней:

```
ip firewall filter add chain=input protocol=tcp dst-port=22 src-address-
list=ssh_blacklist action=drop \
comment="drop ssh brute forcers" disabled=no
ip firewall filter add chain=input protocol=tcp dst-port=22 connection-
state=new \
src-address-list=ssh_stage3 action=add-src-to-address-list address-
list=ssh_blacklist \
address-list-timeout=10d comment="" disabled=no
ip firewall filter add chain=input protocol=tcp dst-port=22 connection-
state=new \
src-address-list=ssh_stage2 action=add-src-to-address-list address-
list=ssh_stage3 \
address-list-timeout=1m comment="" disabled=no
ip firewall filter add chain=input protocol=tcp dst-port=22 connection-
state=new src-address-list=ssh_stage1 \
action=add-src-to-address-list address-list=ssh_stage2 address-list-
timeout=1m comment="" disabled=no
ip firewall filter add chain=input protocol=tcp dst-port=22 connection-
state=new action=add-src-to-address-list \
address-list=ssh_stage1 address-list-timeout=1m comment="" disabled=no
```

If you want to block downstream access as well, you need to block the with the forward chain:

```
add chain=forward protocol=tcp dst-port=22 src-address-list=ssh_blacklist
action=drop \
comment="drop ssh brute downstream" disabled=no
```

Для просмотра блэклиста (заблокированных), даем следующие команды:

```
[admin@mikrotik] > /ip firewall address-list
[admin@mikrotik] /ip firewall address-list> print
```

mikrotik, ssh, bruteforce, secure, защита