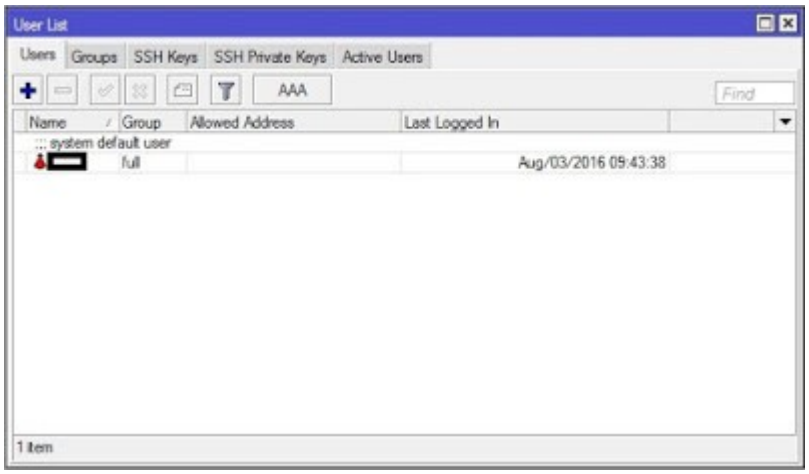
MikroTik / RouterOS
Настройки Bunker(a)

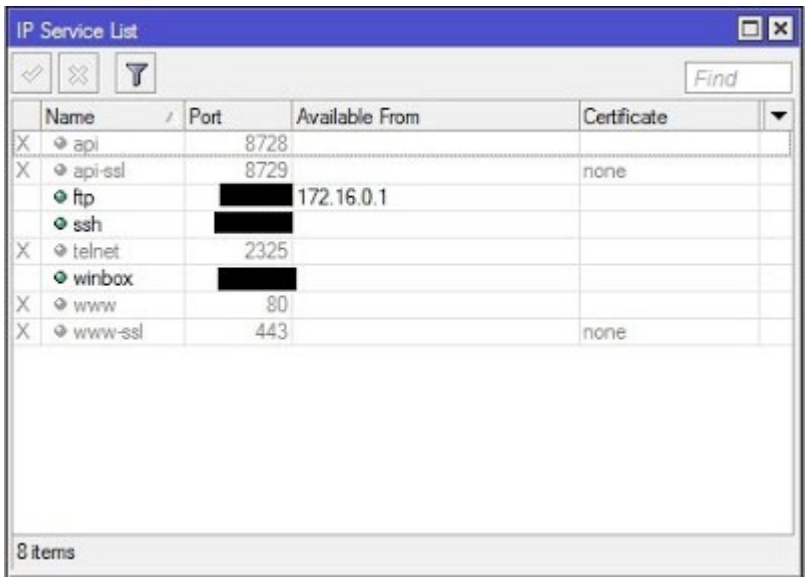
В статье используются разные интерфейсы пользователя (скрипты), измените на свой, например interface=ether1-velton > ether1

После первоначальной настройки роутера Mikrotik его нужно защитить от сканирования и атак из WAN-интерфейса. Это нужно делать обязательно, во избежания неприятностей. Защиту внутри локальной сети тоже нужно производить, но она не так критична, хотя и важна. Сами методы разделю по пунктам.

1) Отключаем учетную запись admin. Создаем новую учетную запись, Имя должно быть не общепринятое, что-бы комбинация логин-пароль служила доп. защитой. Не используйте имена user, guest, admin и другие стандартные. Не используйте пароли 12345, qwerty и тому подобные, а также совпадающие с логином. Пароль должен быть не меньше 8 символов, содержать буквы верхнего и нижнего регистров, цифры и, в идеале, символы.

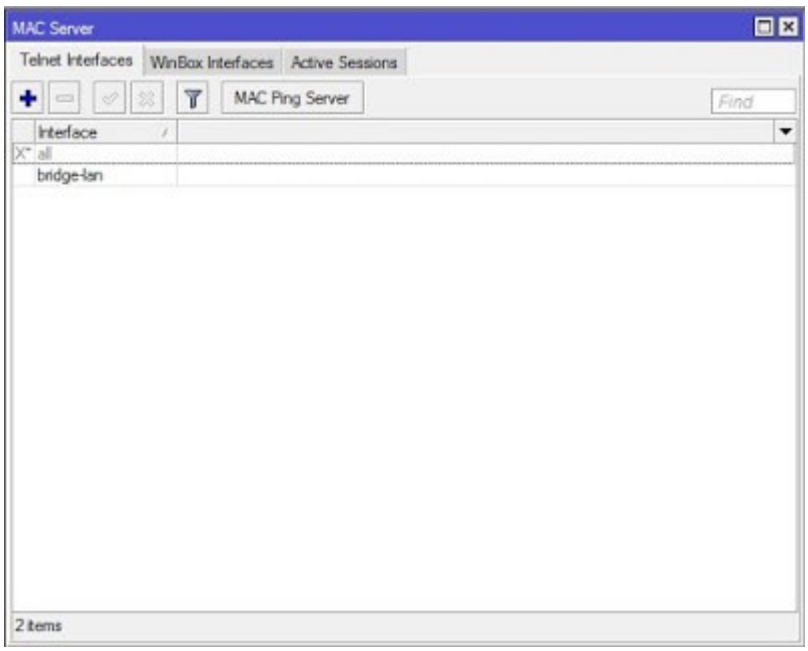


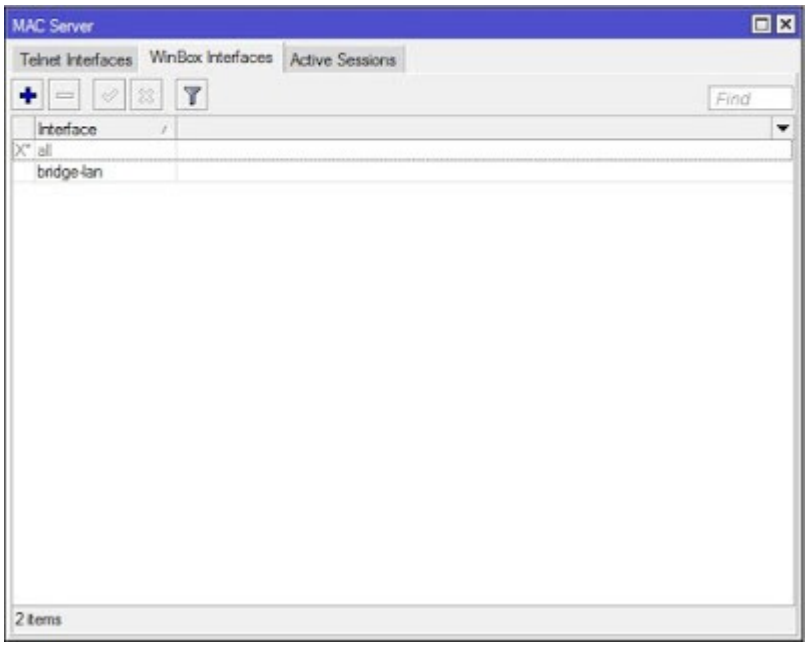
2) Отключаем ненужные сервисы, все нужные переводим на не стандартные порты! Список не зарезервированных портов можно найти в Википедии: Список портов TCP и UDP. Доступ из-вне отставляем только реально нужным сервисам. Если есть возможность, сервисы ограничиваем по подсетям.



3) Отключаем "поиск соседей". MNDP (Neighbor Discovery Protocol) - протокол, с его помощью роутеры MikroTik получают информацию друг о друге и могут выполнить автоматическую настройку некоторых функций. Однако протокол MNDP передает информацию о версии операционной системы и функции, которые включены в роутере. Отключаем в ip/neighbors поиск на WAN-интерфейсе.

4) Отключаем подключение к роутеру по MAC-адресу из-вне в Tools/MAC Server. На вкладках Telnet Interfaces и WinBox Interfaces добавляем интерфейс LAN, удаляем если есть любые другие интерфейсы и отключаем интерфейс "*all".





_Теперь идет настройка непосредственно firewall, правила имеют очередность, поэтому команды выполнять в последовательности. Перед началом работ сделайте бекап. И помните - удаленная настройка фаервола -к выезду!

5) Организовываем ловушку от перебора портов. Грубый метод. В пункте 8 будет представлено более утонченное решение. Но в нашем деле все методы хороши. Теория такова, если злоумышленник будет перебирать открытые порты вашего маршрутизатора, при попадании на определенный порт, этот IP попадет в блек-лист. Порт нужно выбирать осторожно, что бы он нигде в вашей конфигурации не использовался, и был свободен. После того как определились с портом, добавим 2 правила.

```
/ip firewall filter
add action=add-src-to-address-list address-list=perebor_portov_drop address-list-
timeout=30m chain=input comment=Perebor_portov_add_list dst-port=22 in-
interface=ether1-velton log=yes log-prefix=Attack protocol=tcp
add action=drop chain=input comment=Perebor_portov_list_drop in-interface=ether1-
velton src-address-list=perebor_portov_drop
```

Первым правилом при обращении на порт 22 IP добавляем в дроп-лист "perebor_portov_drop". Вторым правилом - баним его. В последнем скриншоте этих правила нет, но они идут в начале списка в /ip firewall filter.

* На "MUM Москва 2016" докладчик рассказывал, что ловит злоумышленников в эту ловушку на популярные порты. Например SSH (22/TCP) или RDP (3389/TCP). Можно еще добавить SIP-порт (5060). Вероятность скана именно этих портов - велика. Если вы их не используете для доступа из-все (что разумно) - смело можно воспользоваться этим методом.

6) Ограничиваем количество ICMP-запросов (делаем защиту от флуд-пинг). Вводим дополнительное правило Drop для отслеживания ICMP Drop. Последнее правило не обязательно - нужно лишь для визуального представления администратору сколько пакетов словилось. Необязательное - потому-как в конце у нас все не разрешенные запросы с WAN - блокируются.

```
/ip firewall filter
add chain=input comment=Allow_limited_pings in-interface=ether1-velton limit=\
    50/5s,2:packet protocol=icmp
add action=drop chain=input comment=Pings_Drop in-interface=ether1-velton \
    protocol=icmp
```

7) Ставим лимит входящих соединений. Если с одного IP адреса подключений больше лимита, то этот IP попадает в "черный список" и в дальнейшем блокируется. Например

```
/ip firewall filter add chain=input protocol=tcp connection-limit=LIMIT,32 \
action=add-src-to-address-list address-list=blocked-addr address-list-timeout=1d
```

Где LIMIT - максимальное количество соединений в определенного IP. Предел должен быть от 100 и выше, так как многие услуги, используют несколько соединений (HTTP, Torrent, и другие P2P-программы). После того как пакеты добавлены в address-list можно выставить их drop или опцию tarpit. Она позволяет вместо того чтобы просто удалять пакеты атакующего - захватить и удерживать соединения и с достаточно мощным маршрутизатором это может замедлить скорость атаки.

```
/ip firewall filter add chain=input protocol=tcp src-address-list=blocked-addr \
connection-limit=3,32 action=tarpit
```

Но нам такие сложности не к чему, просто добавим правило с лимитом 200 соединений с одного IP и блоком на сутки:

```
/ip firewall filter
add action=add-dst-to-address-list address-list=connection-limit \
    address-list-timeout=1d chain=input comment=Connection_limit \
    connection-limit=200,32 in-interface=ether1-velton protocol=tcp
add action=drop chain=input comment=Adr_list_connection-limit_drop \
    in-interface=ether1-velton src-address-list=connection-limit
```

8) Включаем защиту от сканеров портов на WAN-интерфейсе:

```
/ip firewall filter
add action=drop chain=input comment=Port_scanner_drop src-address-list=\
    "port scanners"
add action=add-src-to-address-list address-list="port scanners" \
    address-list-timeout=2w chain=input in-interface=ether1-velton protocol=\
    tcp psd=21,3s,3,1
add action=add-src-to-address-list address-list="port scanners" \
    address-list-timeout=2w chain=input in-interface=ether1-velton protocol=\
    tcp tcp-flags=fin,!syn,!rst,!psh,!ack,!urg
add action=add-src-to-address-list address-list="port scanners" \
    address-list-timeout=2w chain=input in-interface=ether1-velton protocol=\
    tcp tcp-flags=fin,syn
add action=add-src-to-address-list address-list="port scanners" \
    address-list-timeout=2w chain=input in-interface=ether1-velton protocol=\
    tcp tcp-flags=syn,rst
add action=add-src-to-address-list address-list="port scanners" \
    address-list-timeout=2w chain=input in-interface=ether1-velton protocol=\
    tcp tcp-flags=fin,psh,urg,!syn,!rst,!ack
add action=add-src-to-address-list address-list="port scanners" \
    address-list-timeout=2w chain=input in-interface=ether1-velton protocol=\
    tcp tcp-flags=fin,syn,rst,psh,ack,urg
add action=add-src-to-address-list address-list="port scanners" \
    address-list-timeout=2w chain=input in-interface=ether1-velton protocol=\
    tcp tcp-flags=!fin,!syn,!rst,!psh,!ack,!urg
```

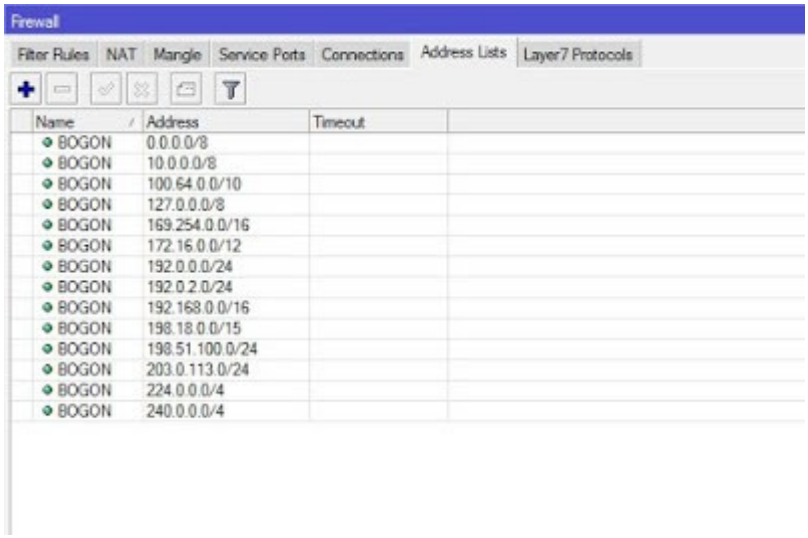
9) Защищаем от перебора паролей подключения по нестандартному порту к WinBox и SSH из вне. Комментарии читать снизу-вверх.

```
/ip firewall filter
# все IP в black_list - отклоняем
add action=drop chain=input comment=Drop_winbox_black_list dst-port=5323,5324 \
    in-interface=ether1-velton protocol=tcp src-address-list=black_list
# если новые подключения с адрес-листа Winbox_Ssh_stage3 продолжаются -
заносим в новый адрес-лист black_list на 5 минут.
add action=add-src-to-address-list address-list=black_list \
    address-list-timeout=5m chain=input comment=Winbox_add_black_list \
    connection-state=new dst-port=5323,5324 in-interface=ether1-velton \
    protocol=tcp src-address-list=Winbox_Ssh_stage3
# если новые подключения с адрес-листа Winbox_Ssh_stage2 продолжаются -
заносим в новый адрес-лист Winbox_Ssh_stage3
```

```
add action=add-src-to-address-list address-list=Winbox_Ssh_stage3 \
    address-list-timeout=1m chain=input comment=Winbox_Ssh_stage3 \
    connection-state=new dst-port=5323,5324 in-interface=ether1-velton \
    protocol=tcp src-address-list=Winbox_Ssh_stage2
# если новые(значит была неудачная попытка, например - неправильный пароль, и соединение разорвалось) подключения с адрес-листа Winbox_Ssh_stage1 продолжаются - заносим в новый адрес-лист Winbox_Ssh_stage2
add action=add-src-to-address-list address-list=Winbox_Ssh_stage2 \
    address-list-timeout=1m chain=input comment=Winbox_Ssh_stage2 \
    connection-state=new dst-port=5323,5324 in-interface=ether1-velton \
    protocol=tcp src-address-list=Winbox_Ssh_stage1
# заносим все айпи, которые создали новые подключения на наши порты в адрес-лист на 1 минуту
add action=add-src-to-address-list address-list=Winbox_Ssh_stage1 \
    address-list-timeout=1m chain=input comment=Winbox_Ssh_stage1 \
    connection-state=new dst-port=5323,5324 in-interface=ether1-velton \
    protocol=tcp
# разрешаем подключение к Winbox и Ssh по портам 5323 и 5324
add chain=input comment=Accept_Winbox_Ssh dst-port=5323,5324 in-interface=\
    ether1-velton protocol=tcp
```

10) Блокируем bogon-сети. Это зарезервированные диапазоны IP адресов которые еще не были закреплены ни за одним провайдером в мире. Это свободные/пустые диапазоны. Частные сети прячутся от интернета средствами компании или провайдером. Поэтому если к вам вдруг прилетает пакет с сорсом из этих списков, ничего хорошего он принести не может. Bogon IP часто используют злые хакеры для своих вредоносных атак. Актуальный список сетей можно посмотреть тут: http://www.team-cymru.org/Services/Bogons/bogon-bn-nonagg.txt.

```
/ip firewall address-list
add address=0.0.0.0/8 disabled=no list=BOGON
add address=10.0.0.0/8 disabled=no list=BOGON
add address=100.64.0.0/10 disabled=no list=BOGON
add address=127.0.0.0/8 disabled=no list=BOGON
add address=169.254.0.0/16 disabled=no list=BOGON
add address=172.16.0.0/12 disabled=no list=BOGON
add address=192.0.0.0/24 disabled=no list=BOGON
add address=192.0.2.0/24 disabled=no list=BOGON
add address=192.168.0.0/16 disabled=no list=BOGON
add address=198.18.0.0/15 disabled=no list=BOGON
add address=198.51.100.0/24 disabled=no list=BOGON
add address=203.0.113.0/24 disabled=no list=BOGON
add address=224.0.0.0/4 disabled=no list=BOGON
add address=240.0.0.0/4 disabled=no list=BOGON
```



Само запрещающее правило:

```
/ip firewall filter
add action=drop chain=input comment=Bogon_Wan_Drop in-interface=ether1-velton \
   src-address-list=BOGON
```

11) Разрешаем все уже установленные подключения (connection state=established). Established - Существующее соединение. Пакет относится у уже установленному соединению, обрабатываемому в данный момент маршрутизатором.

```
add chain=input comment=Established_Wan_Accept connection-state=established
```

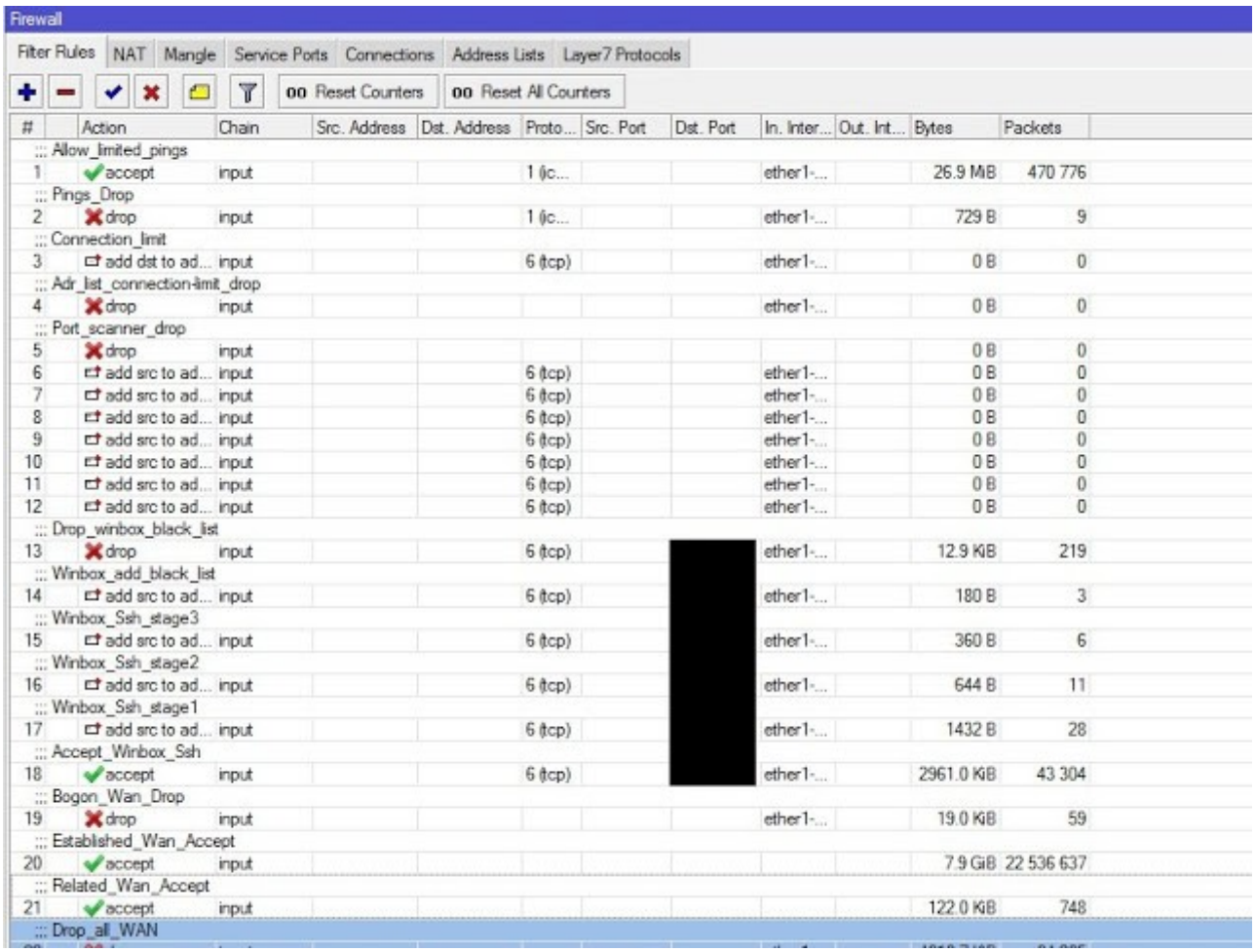
12) Разрешаем все зависимые подключения (connection state=related). Related – Связанное соединение. Пакет, который связан с существующим соединением, но не является его частью. Например, пакет, который начинает соединение передачи данных в FTP-сессии (он будет связан с управляющим соединением FTP), или пакет ICMP, содержащий ошибку, отправляемый в ответ на другое соединение.

```
add chain=input comment=Related_Wan_Accept connection-state=related
```

13) Блокируем все входящие соединения с WAN.

```
add action=drop chain=input comment=Drop_all_WAN in-interface=ether1-velton
```

Визуально последовательность правил выглядит так:



Это минимальная настройка безопасности. Если вы хотите разрешить подключение VPN к роутеру, то как минимум нужно открыть порт. Например, для соединений по порту 1723 (PPTP):

```
/ip firewall filter
add chain=input dst-port=1723 protocol=tcp
```

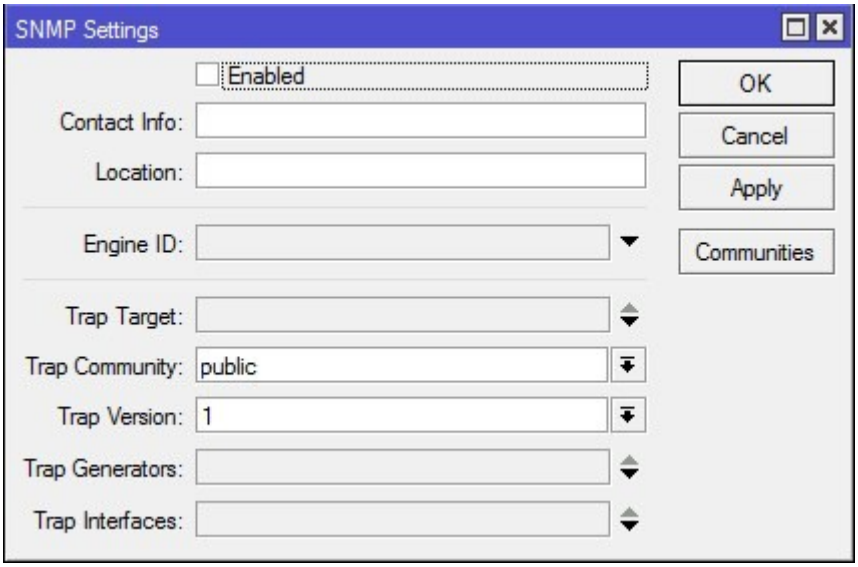
Так же рекомендую использовать скрипт Оповещение администратора о входе в Mikrotik. Метод защиты сервисов, на которые проброшенные порты с Mikrotik описан в статье тут.

В дополнение к основной статье Защита WAN-интерфейса в Mikrotik хочется отметить несколько важных моментов в безопасности вашего маршрутизатора. Описанные тут пункты не имеют критически важное значение в защите роутера Mikrotik, но, в комплексе, помогают защитить маршрутизатор еще лучше. Я специально буду продолжать пункты, описанные в предыдущем материале, что бы подчеркнуть - эта статья является продолжением и дополнением первой и отдельно рассматриваться не может.

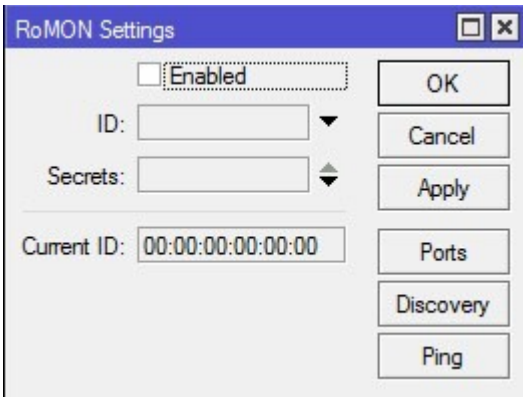
Не смотря на запрещающее правило в пункте 13 ("add action=drop chain=input comment=Drop_all_WAN in-interface=ether1-velton") в конце первой статьи, рекомендую проверить активность сервисов. Если какой-то сервис не используется - в целях безопасности его отключить.

14) Проверяем сервис SNMP в IP/SNMP. По-умолчанию он выключен. Если мы его не

используем - проследите что-бы не стояла галочка Enabled. Если используем - позаботитесь о его защите.



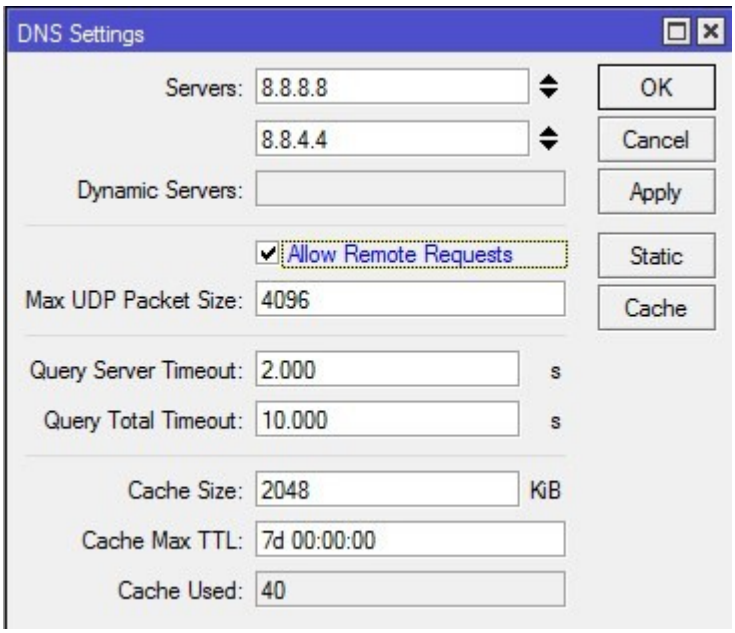
15) Аналогично с сервисом RoMon (Tools/RoMon) - нечего светить лишнее в сети. По-умолчанию он тоже отключен.



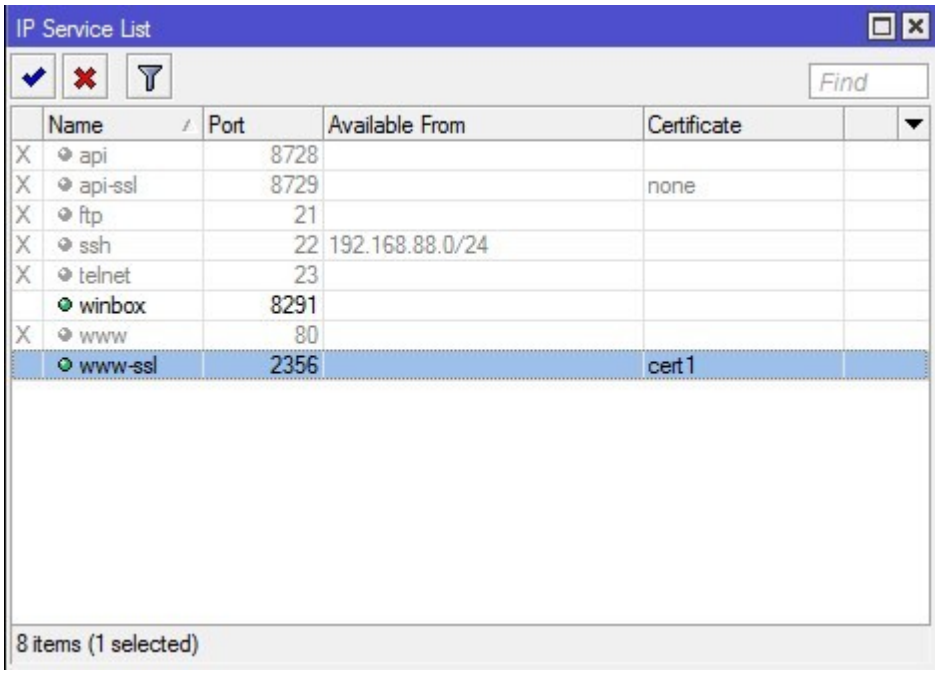
16) Если вы используете NTP-сервер, проследите что-бы порт 123/UDP снаружи был закрыт. Если вы используете общее запрещающее правило как в пункте 13 - доп. правило для этого порта писать не нужно.

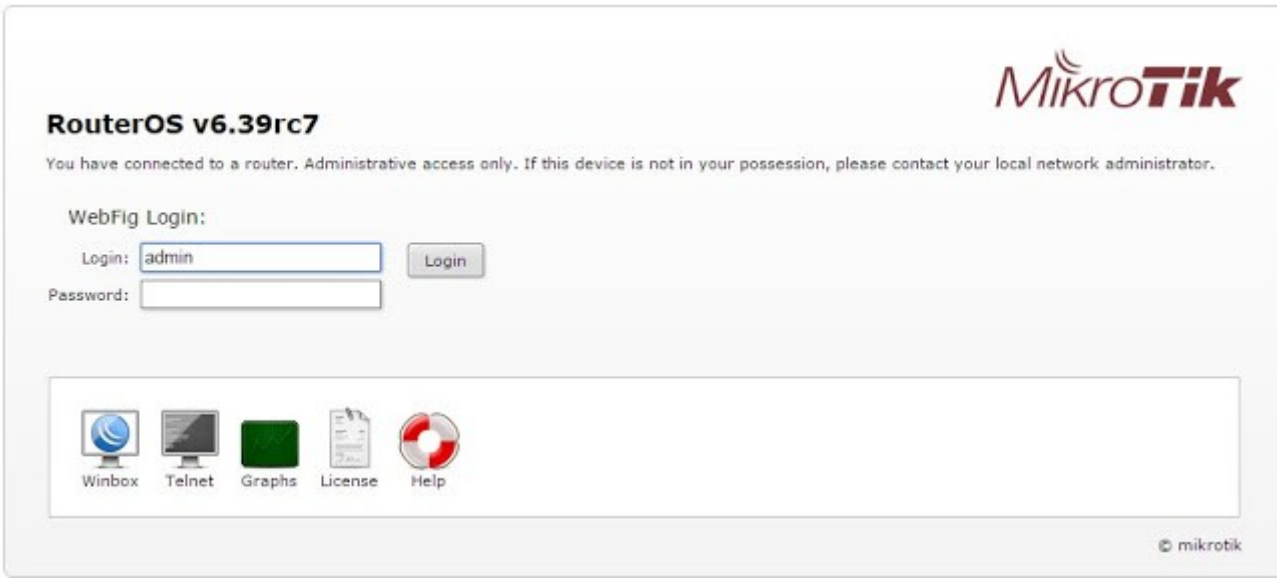
17) Если вы не используете общее запрещающее правило, то при включении галочки Allow Remote Requests в DNS Settings ваш роутер будет отвечать на все ДНС-запросы со всех интерфейсов. Именно поэтому очень часто многие админы сталкиваются с днс-флудом на внешнем интерфейсе. Обязательно используем запрещающее правило для закрытия этой уязвимости:

```
/ip firewall filter
add chain=input action=drop protocol=udp in-interface=ether1 dst-port=53
```

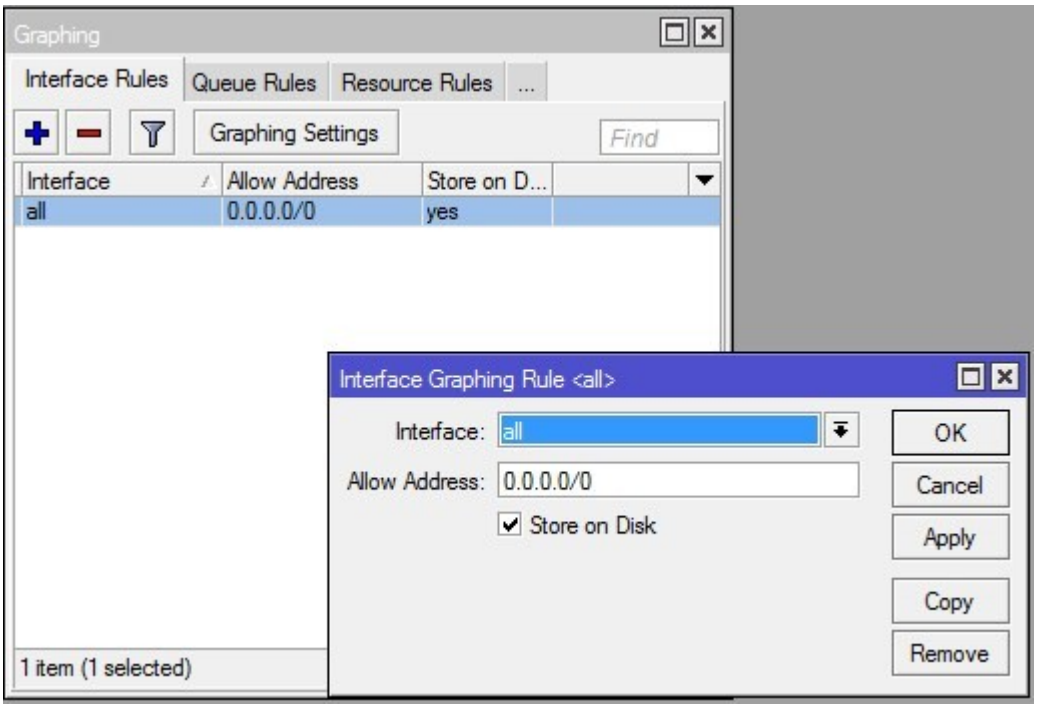


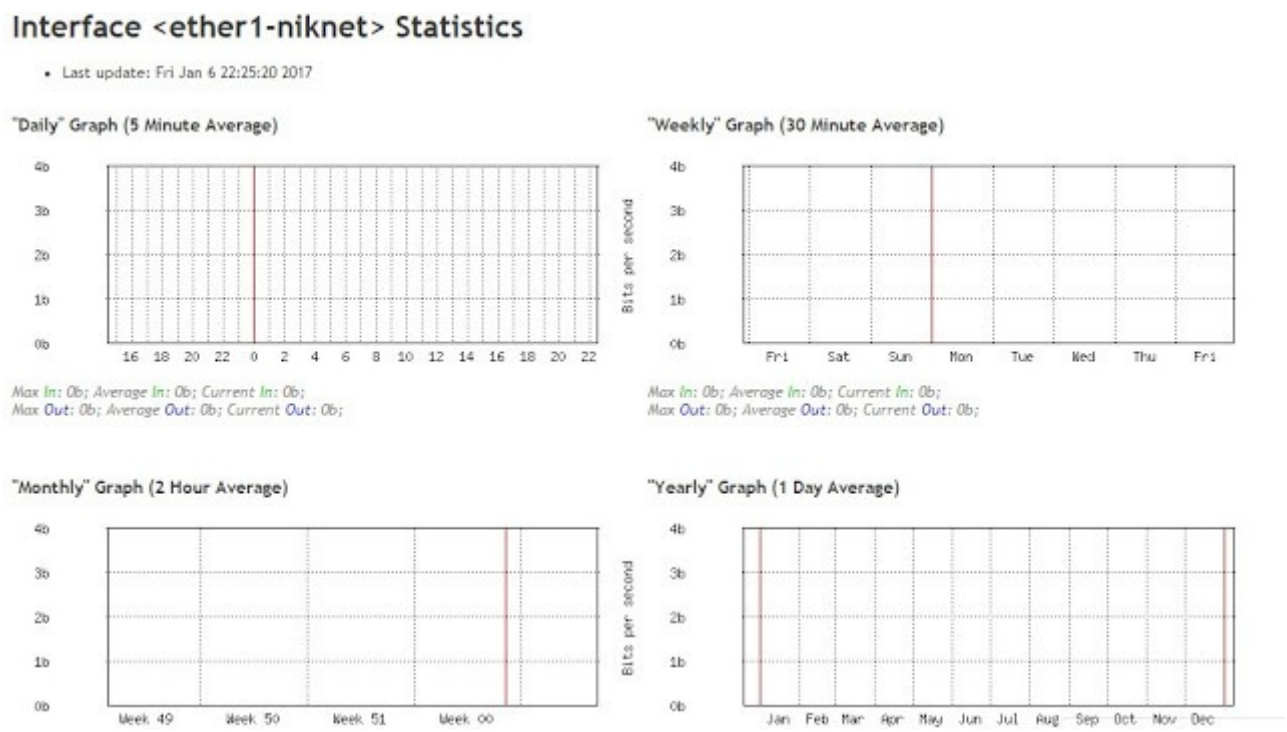
18) Если вы используете доступ на веб-интерфейс из-вне, вы ОБЯЗАТЕЛЬНО должны ограничить по подсетям или отключить сервис http - как не безопасный протокол. Вместо него нужно использовать https с самоподписанным SSL-сертификатом и нестандартным портом. Как это реализовать описано в статье [Подключение к веб-интерфейсу Mikrotik используя ssl протокол](#).





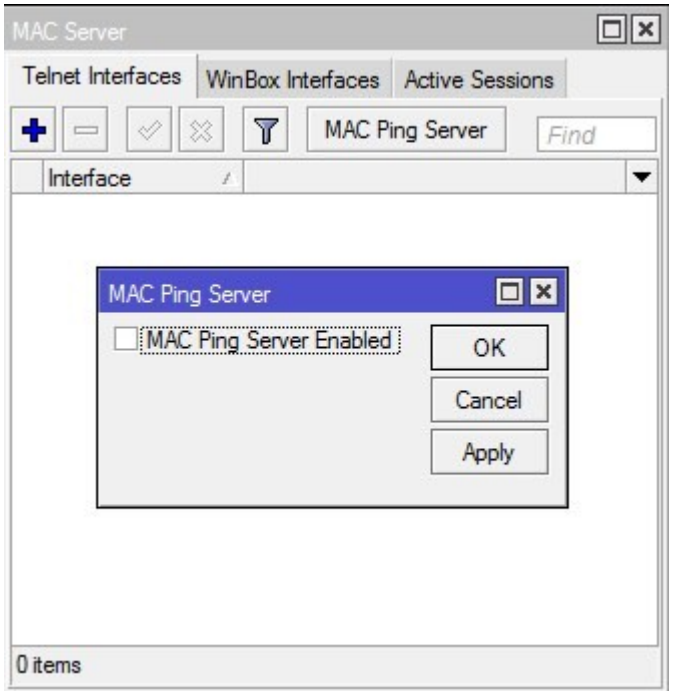
Нужно помнить - если вы добавите графики и не ограничите их отображение по подсетям, то любой человек сможет увидеть движение трафика по интерфейсам.

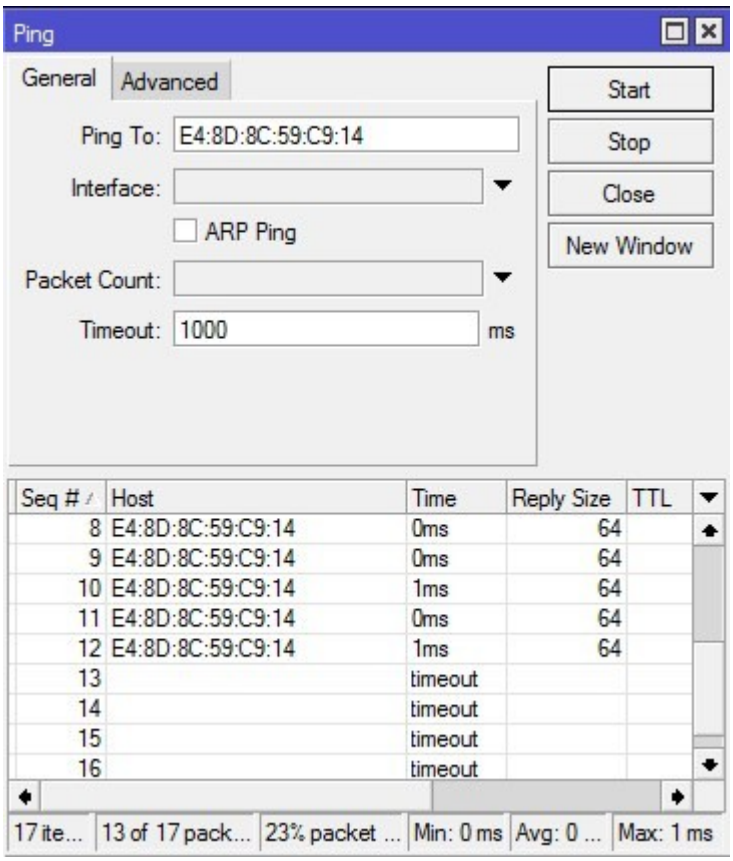




19) В Tools/MAC Server отключаем Mac Ping Server. Это отключит отклик устройства при пинге через MAC-ping.

/tool mac-server ping set enabled=no





20) MAC-адрес содержит информацию о производителе устройства. В первых шести символах MAC-адреса имеется информация о вендоре (производителе) устройства. Определив производителя злоумышленник может подобрать метод взлома. Например, 00:00:0C - Cisco Systems, Inc. Поэтому рекомендуется изменить MAC-адрес нашего роутера на внешнем интерфейсе.

/interface ethernet set ether1 mac-address=XX:XX:XX:XX:XX:XX

Следует помнить, что изменяя MAC вы можете спровоцировать конфликт, поэтому будьте осторожны. Я использую MAC устройств, которые врятли появятся у меня в сети, например 9C:93:4E - Xerox Corporation. Посмотреть информацию по физическим адресам разных вендоров можно тут:

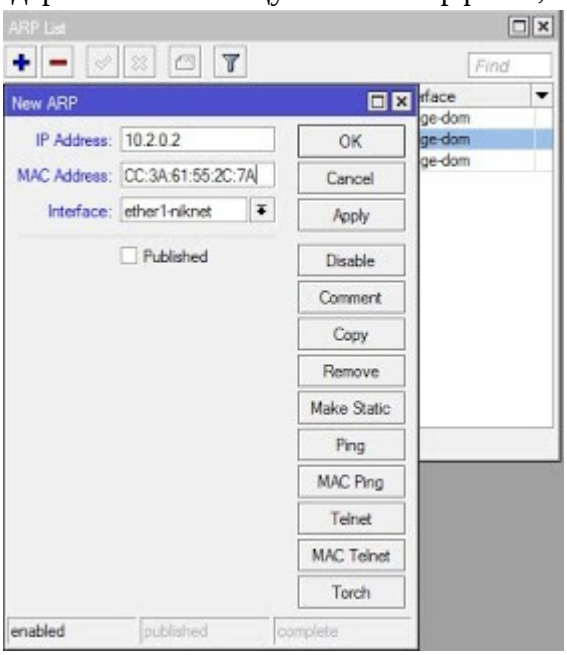
http://www.coffer.com/mac_find/

Изменив MAC-мы запутаем взломщика, а значит это плюс к безопасности. В сети есть материал, где человек придумал скрипт, который периодически меняет MAC на WAN-интерфейсе. Эта схема будет работать, если у вашего провайдера нет привязки на физический адрес.

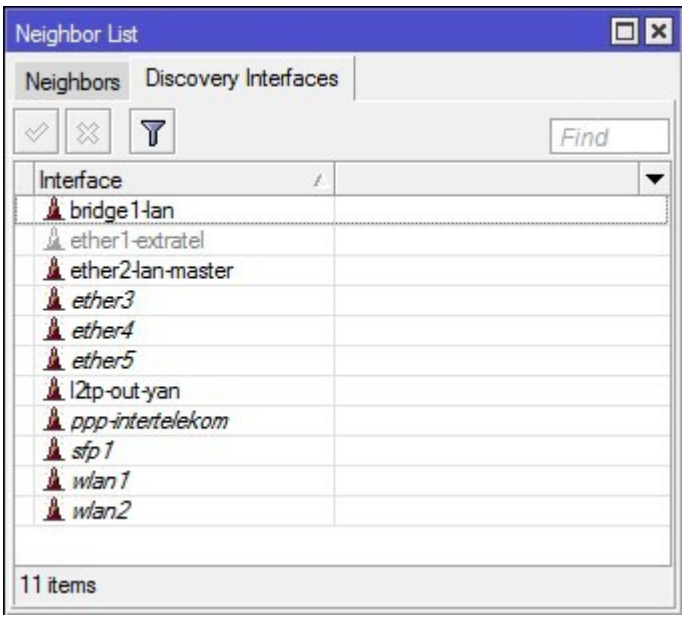
21) Что-бы защитится от "подмены аплинка", а именно, защитить свой маршрутизатор от злоумышленника, который вмешается в сеть L2 между вами и провайдером и захочет "хакнуть" ваше устройство можно на WAN-порту поставить опцию опцию ARP "reply only" и занести MAC-адрес провайдерского конечного устройства в таблицу ARP интерфейса. Тем самым злоумышленнику будет не достаточно просто ввести IP, ему нужно будет еще подобрать MAC для связи с вашим роутером. Это делается командой

/interface ethernet set ether1 arp=reply-only

Стоит учитывать - при такой схеме, если провайдер поменяет оборудование - вам придется внести новый MAC провайдера в ARP-таблицу WAN-интерфейса, иначе связи не будет.



22) Периодически делайте ревизию Discovery-интерфейсов (смотри пункт 3 первой статьи). Дело в том, что созданные новые интерфейсы (pptp, l2tp и любые другие) автоматически попадают в Neighbor Discovery - и остаются там активные, пока вы их не отключите. А это - информация всем на интерфейсе о модели устройства, о версии OS, о MAC и IP адресах,об UpTime, наличии IPv6 и прочее.



23) Если говорить о Neighbor, то при отключении Discovery-интерфейсов невозможно посмотреть информацию об других устройствах на этом интерфейсе. А очень бы хотелось свою информацию скрыть, а информацию об соседних устройствах иметь. Для этого не достаточно добавить запрещающее правило udp с портом 5678 на ван-интерфейс

/ip firewall filter add chain=output action=drop protocol=udp dstport=5678 out-interface=ether1

Neighbor использует не только UDP, но и L2 протокол CDP/VDP, а это значит заблочить его Firewall невозможно.

Нужно либо полностью отключать службу Neighbors на интерфейсе командой

/ip neighbor discovery set ether1 discover=no

либо фильтровать исходящий L2 трафик на предмет MNDP-пакетов с помощью bridge filters.

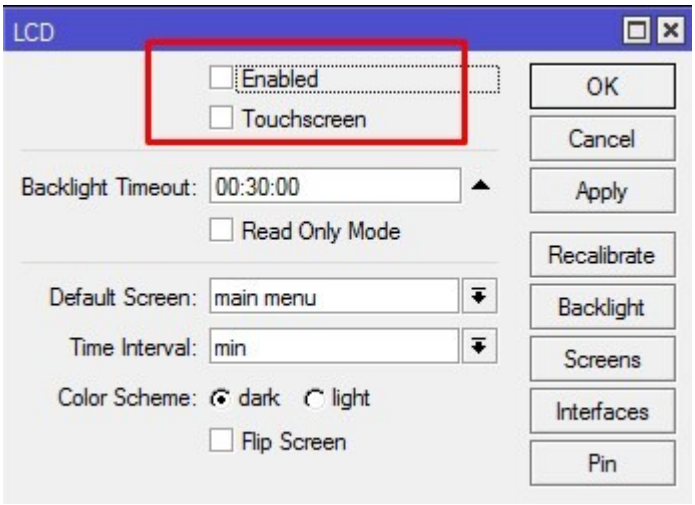
Например, вот так:

> **/interface bridge filter add action=drop chain=output disabled=no dst-mac-address=01:00:0C:CC:CC:CC/FF:FF:FF:FF:FF:FF out-interface=ether1**

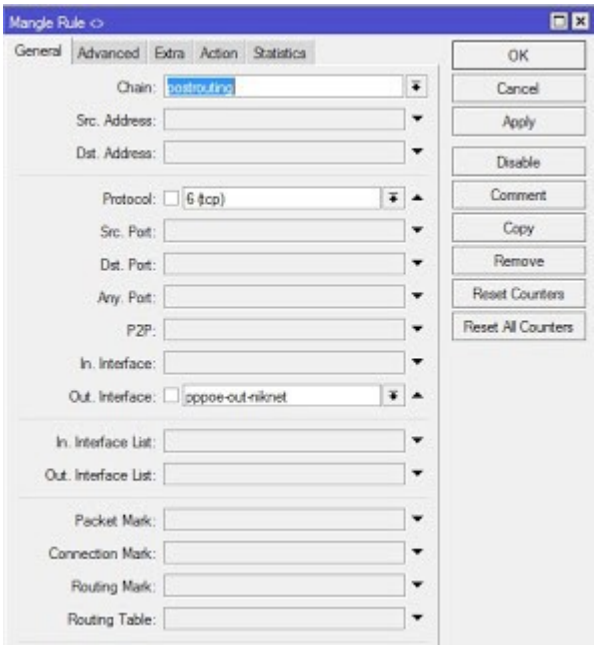
Так же в 6.38 наконец-то добавлена поддержка открытого протокола LLDP. Поэтому если не хотим отключать Discovery на WAN - рассылку мультикаст на MAC, согласно картинке, тоже запрещаем.

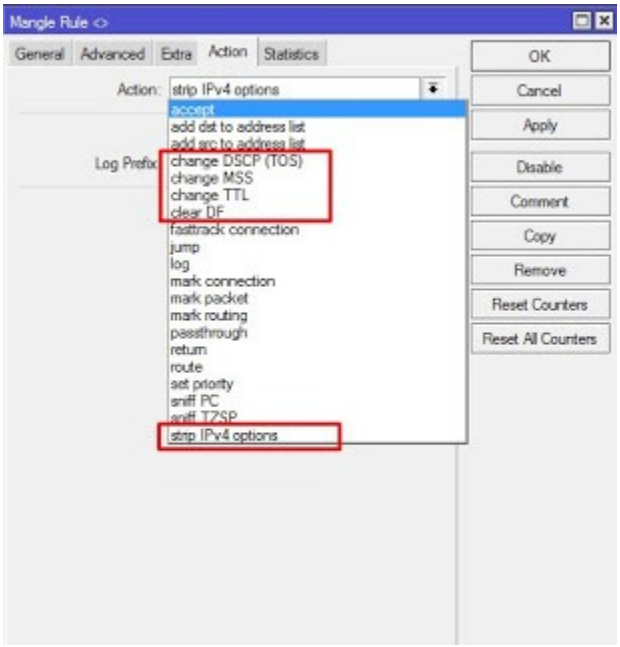
24) Не используйте службу FTP, встроенную в Mikrotik без ограничений по подсетям! При Telnet-подключении все наблюдают такое приглашение: "220 MikroTik-951 FTP server (MikroTik 6.38) ready". А это значит мы можем показать злоумышленнику производителя, модель устройства и его версию RouterOS. Кроме того, при взломе ftp-аккаунта злоумышленник сможет скопировать бекап и вытянуть пароль, выполнить файл типа rsc.auto, загрузить свои пакеты типа "system" и прочее.

25) Если роутер стоит в помещении, где могут находится посторонние люди и в нем есть LCD-дисплей с сенсорным вводом (например как в RB2011), то желательно его отключить - дабы не смущать своим видом людей, мало-ли кто-то захочет потыкать туда пальчиком.



26) Последний пункт является информационным. В Mikrotik есть возможность спрятать информацию о системе которая передается в пакетах TCP - заголовках пакета, опциях, информации об ОС ваших компьютеров и т.д. Это можно сделать и для транзитного трафика проходящего от вашего компьютера через Mikrotik в Интернет. Тем самым мы можем запутать злоумышленника. Для этого в Firewall есть несколько инструментов.





- change-dscp - изменение значение поля DSCP (точка кода дифференцированных услуг), другим параметром new-dscp;
- change-mss - изменение максимального размера сегмента пакета на значение, определенное параметром new-mss;
- change-ttl - изменение значения "время жизни пакета" на значение, определенное параметром new-ttl;
- clear-df - очищение флага "не фрагментировать";
- strip-ipv4-options - очищение IPv4-опций из IP пакета.

Настройка довольно тонкая и зависит от конкретного случая - материал отдельной статьи.