Настраиваем Honeypot на роутерах Mikrotik

Записки IT специалиста

Технический блог специалистов ООО"Интерфейс"

- Главная
- Настраиваем Honeypot на роутерах Mikrotik

Современный интернет такое место, где вы сразу же становитесь предметом нездорового любопытства для самых широких масс. Вас будут постоянно сканировать, проверять на наличие уязвимостей, открытых портов, пытаться подбирать пароли и т.д. и т.п. В этом случае есть смысл действовать на опережение и использовать Honeypot для выявления потенциальных злоумышленников. В данной статье мы рассмотрим суть этого метода и расскажем к настроить его на роутерах Mikrotik.

Honeypot - в переводе "горшочек с медом", специальная приманка в виде открытого порта, который для реальной работы не используется, а любая попытка обращения на данный порт будет считаться проявлением нездорового интереса и занесением обратившегося в список злоумышленников. Действительно, если у вас нет почтового сервера, а кто-то пытается стучаться в "открытый" 25-й порт, то он явно не письмо от Деда Мороза принес, а ищет уязвимые или неправильно сконфигурированные почтовые сервера, поэтому самым правильным будет просто заблокировать такого товарища.

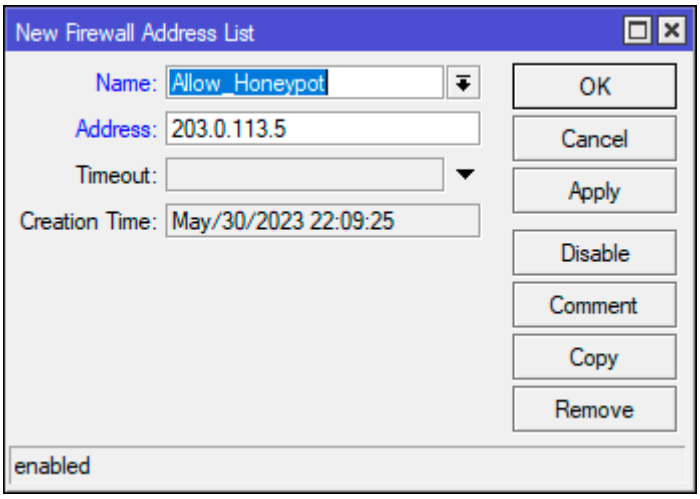
Но ведь у нас есть нормально закрытый брандмауэр, скажет внимательный читатель, который все равно его заблокирует. Да, это так. Но есть несколько моментов. Первый - нагрузка на роутер, особенно если у вас достаточно много правил. Второй - у вас действительно могут оказаться уязвимые или слабо защищенные сервисы и поэтому лучше, если потенциальный злоумышленник будет заблокирован сразу. без возможности дальше изучать вашу систему.

Правда, не все так просто, в собственный "горшочек" можно легко попасть самому. Поэтому настройку Honeypot нужно начать с составления белого списка, в который следует внести адреса всех внешних пользователей, админов, филиалов и внешних площадок, сторонних сервисов и т.д. и т.п. В общем всех, кто может с вполне легальными целями стучаться на ваш внешний интерфейс. Для пользователей без былых IP-адресов имеет смысл включать в список целые диапазоны подсетей провайдеров, да, это в чем-то снизит безопасность, но значительно повысит удобство использования такого решения.

Для создания такого списка перейдите в **IP - Firewall - Address Lists** и добавьте в список, скажем **Allow_Honeypot**, все необходимые адреса и сети.

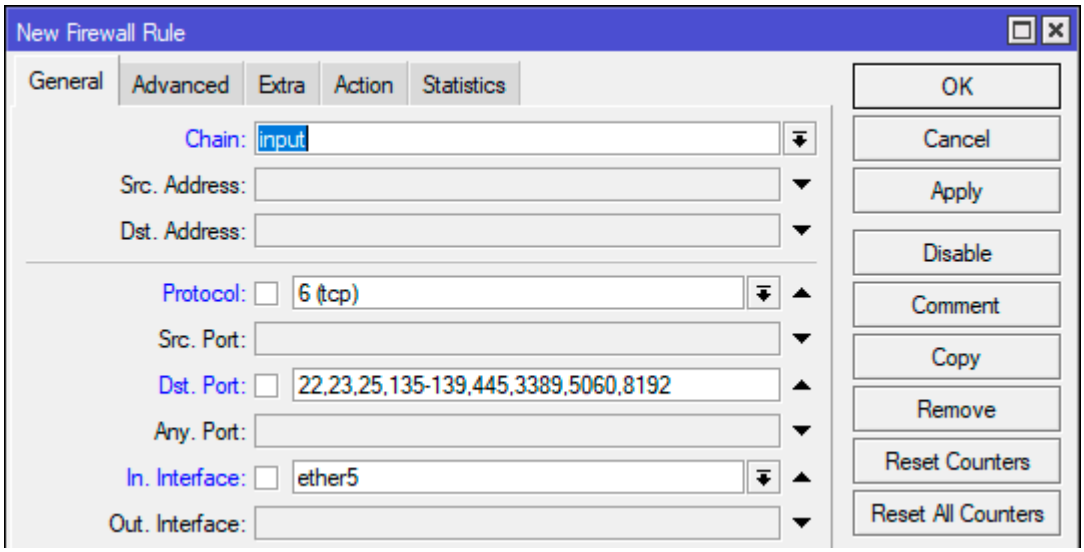
В терминале адрес можно добавить так:

```
/ip firewall address-list
add address=203.0.113.5
list=Allow_Honeypot
```

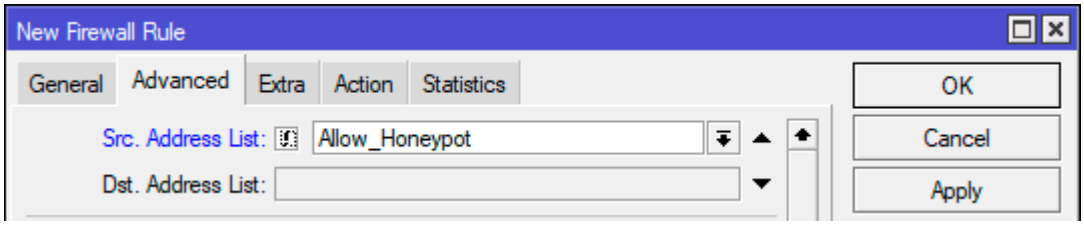


Теперь определим список портов для приманки, это могут быть для TCP: 22- SSH, 23 - Telnet, 25 - SMTP, 135-139,445 - Netbios, 3389 - RDP, 5060 - SIP, 8291 - Winbox и многие другие. Для UDP есть смысл контролировать: 123 - NTP, 135-139,445 - Netbios, 3389 - RDP, 5060 - SIP. Если у вас на этом порту работает какой-то легальный сервис, то можно перенести его на нестандартный порт, а стандарный оставить за приманку. От обнаружения сервиса это не спасет, но поможет отсеять совсем ту часть злоумышленников, которые постучаться на стандартный порт.

Переходим в **IP - Firewall - Filter Rules** и создаем правило для наших портов приманок: **Chain - input, Protocol - tcp, Dst. Port - 22,23,25,135-139,445,3389,5060,8291, In. Interface** - внешний интерфейс, в нашем случае **ether5**.

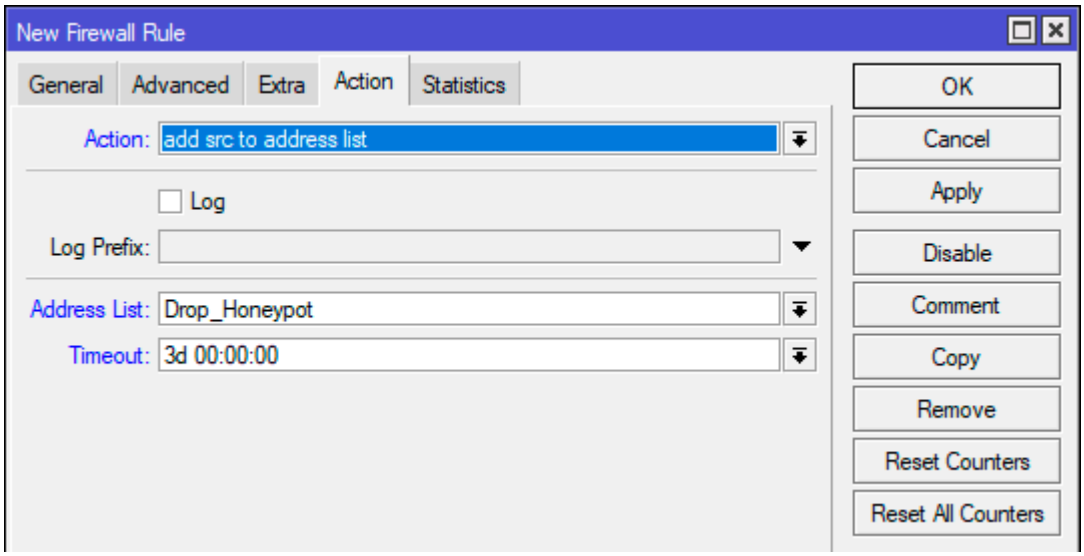


Затем на вкладке **Advanced** вносим в исключения наш белый список: **Src. Address List - ! Allow_Honeypot**.



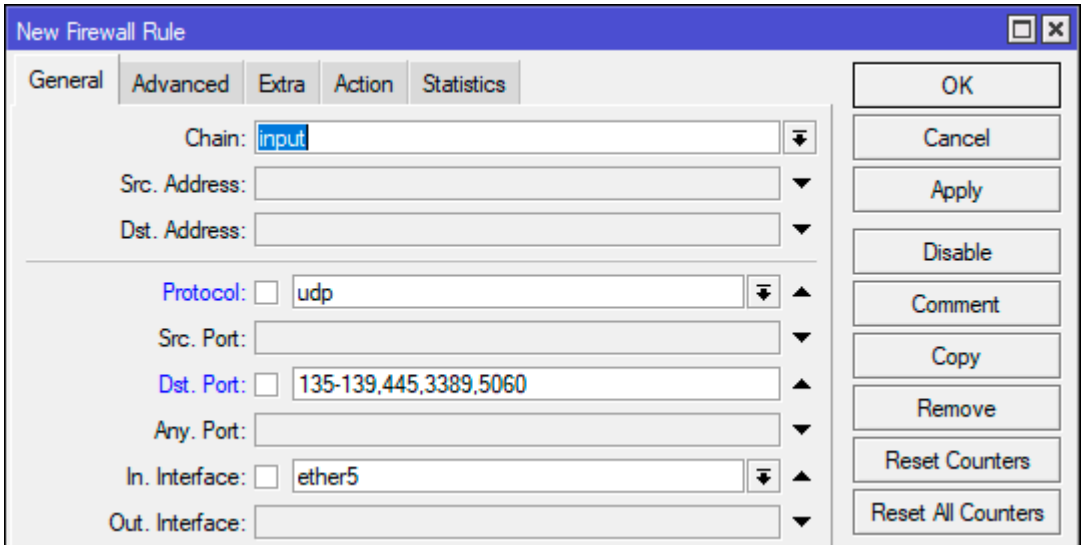
И наконец в **Action** ставим действие **add src to address list** и указываем список для адресов злоумышленников, например, **Drop_Honeypot**. В поле **Timeout** указываем срок пребывания адреса в листе, в нашем случае 3 суток. К выбору этого параметра нужно относиться осмотрительно, больший срок упрощает работу и снижает износ флеш-памяти, но увеличивает вероятность того, что туда по ошибке попадут какие-то легальные адреса и вам придется их оттуда доставать руками.

Поэтому, на первых порах, мы не рекомендуем ставить большой срок, сначала следует отладить систему, а уже потом сроки нахождения в списках можно увеличить.

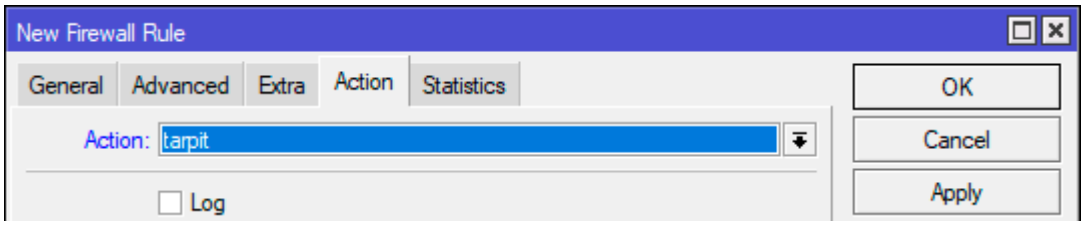


Данное правило помещаем в самое начало цепочки **input**, т.е. выше всех остальных правил.

Затем копируем его и исправляем протокол на UDP, также корректируем список отслеживаемых портов.



Кроме того, мы можем повысить правдоподобность нашего "горшочка" действительно открывая TCP-порты используя действие tarpit, только открываться они будут в никуда и соединения будут висеть до истечения таймаута, что также затруднит работу злоумышленникам и снизит нагрузку на устройство. Для этого еще раз скопируйте правило для TCP и на закладке **Action** установите действие **tarpit**.

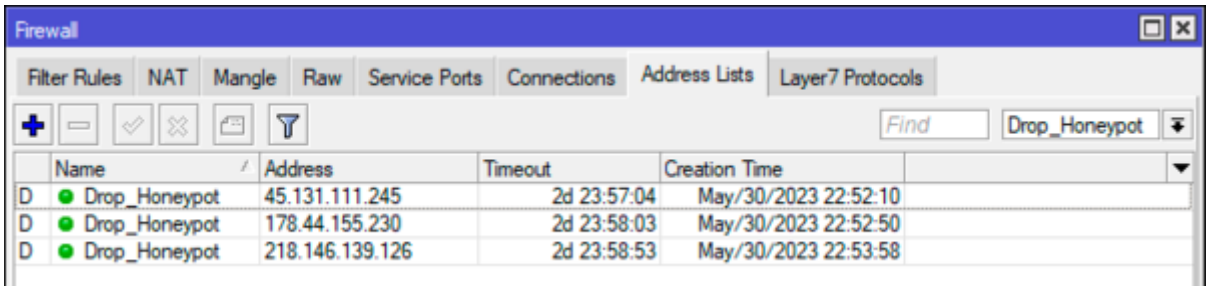


Оба этих правила также должны быть подняты в самый верх, правило с tarpit должно располагаться ниже правила с добавлением в список адресов.

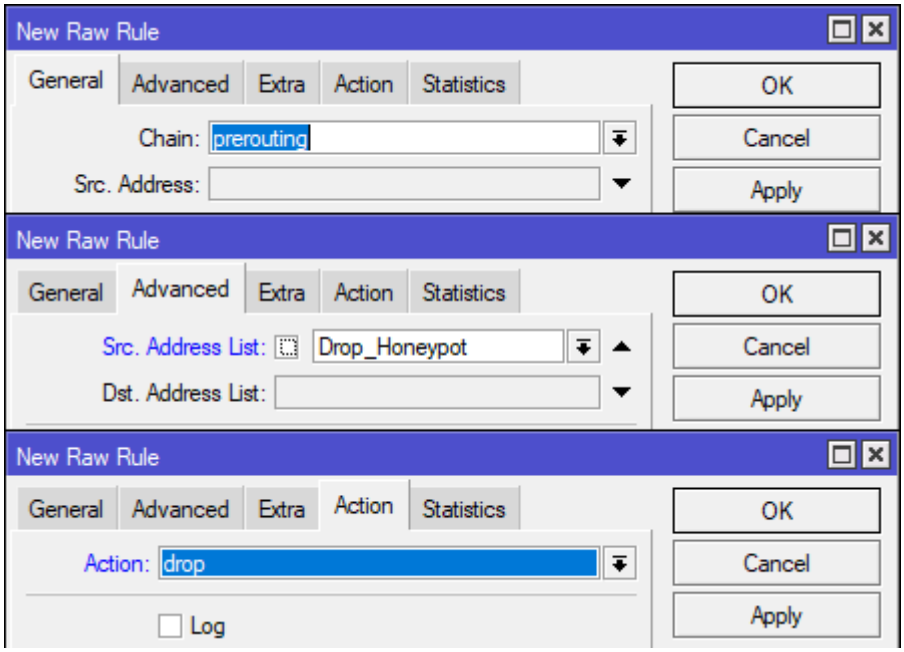
Быстро создать правила в терминале можно командами:

```
/ip firewall filter
add action=add-src-to-address-list address-list=Drop_Honeypot address-list-
timeout=3d chain=input dst-port=22,23,25,135-139,445,3389,5060,8291 \
 in-interface=ether5 protocol=tcp src-address-list=!Allow_Honeypot
add action=tarpit chain=input dst-port=22,23,25,135-139,445,3389,5060,8291 in-
interface=ether5 protocol=tcp src-address-list=!Allow_Honeypot
add action=add-src-to-address-list address-list=Drop_Honeypot address-list-
timeout=3d chain=input dst-port=135-139,445,3389,5060 in-interface=ether5 \
 protocol=udp src-address-list=!Allow_Honeypot
```

Некоторое время советуем просто понаблюдать за происходящим и убедиться, что в список не попадают легальные адреса, в противном случае условия правил нужно откорректировать, либо дополнить нужными адресами белый список.



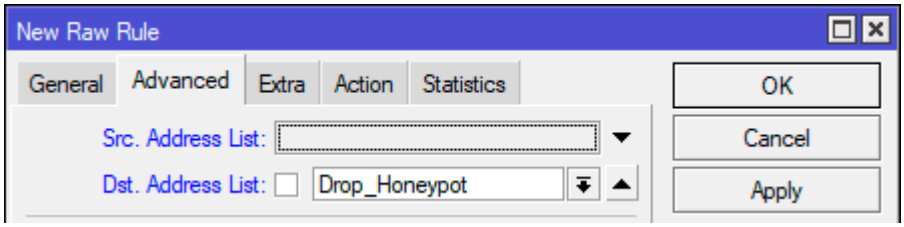
После этого можно переходить к решительным мерам, для этого мы будем использовать таблицу **raw**, что позволит максимально снизить нагрузку на устройство. Переходим в **IP - Firewall - Raw** и создаем новое правило: на закладке **General** ставим **Chain - prerouting**, на **Advanced - Src. Address List - Drop_Honeypot**, а в **Action** указываем действие **drop**.



В терминале:

```
/ip firewall raw
add action=drop chain=prerouting src-address-list=Drop_Honeypot
```

В целом этого достаточно, чтобы заблокировать потенциальным злоумышленникам доступ к нашей сети, но если вы хотите большего, то можете заблокировать потенциальные соединения из вашей сети к злоумышленникам, для этого скопируйте правило, только на **Advanced** вместо **Src. Address List - Drop_Honeypot** укажите **Dst. Address List - Drop_Honeypot**.



Теперь можем спать спокойно, роутер сам будет собирать список подозрительных личностей и блокировать их.

Онлайн-курс по MikroTik

Научиться настраивать MikroTik с нуля или систематизировать уже имеющиеся знания можно на углубленном курсе по администрированию MikroTik. Автор курса, сертифицированный тренер MikroTik Дмитрий Скоромнов, лично проверяет лабораторные работы и контролирует прогресс каждого своего студента. В три раза больше информации, чем в вендорской программе MTCNA, более 20 часов практики и доступ навсегда.
