Настраиваем Honeypot для внутренней сети на роутерах Mikrotik

Записки IT специалиста

Технический блог специалистов ООО"Интерфейс"

- Главная
- Настраиваем Honeypot для внутренней сети на роутерах Mikrotik

Не так давно мы рассматривали, как настроить классический Honeypot (приманку) на роутерах Mikrotik. Такой подход позволяет выявить и впоследствии заблокировать адреса, с которых проявляют нездоровый интерес к вашей сети, однако в современных условиях эффективность данного метода низкая. В тоже время имеет смысл создать подобную приманку и внутри локальной сети, благодаря этому мы сможем своевременно выявить вредоносную активность внутри периметра, а также различные подозрительные действия пользователей, которые могут и не являться вредоносными, но выходить за рамки их должностных обязанностей.

Про то, как настроить Honeypot для внешней сети вы можете прочитать в нашей статье:

Настраиваем Honeypot на роутерах Mikrotik

При этом никто не мешает настроить сразу две приманки, как для внешних, так и для внутренних пользователей, главное - быть внимательными и не допустить пересечения списков, особенно тех, на основании которых вы осуществляете блокировку.

Что касается внутренних пользователей, то мы будем применять два метода. Первый из них направлен на выявление вредоносной активности и чрезмерно любопытных пользователей и представляет тот же Honeypot, но только внутри сети. Здесь мы исходим из того, что любой вредонос прежде всего начнет сетевое сканирование доступных узлов, либо попытки подключиться на известный набор

портов. Тоже самое касается и излишне активных пользователей, если рядовой сотрудник интересуется портом Winbox - то это уже повод присмотреться к нему внимательнее.

Второй метод, по сути, приманкой (Honeypot) не является, но близок к ней по своей сути. В нем мы будем анализировать транзитный трафик на интересующий нас набор портов и выявлять пользователей, которые пытаются установить соединения с внешними RDP, SMTP и иными серверами, особенно не принадлежащим организации. Это тоже определенный звоночек, возможно даже более интересный службе безопасности, нежели админам, но хороший админ также должен знать, кто чем живет и дышит в его сети.

В отличии от внешнего Honeypot, где наша окончательная задача заблокировать все запросы от подозрительных узлов, внутренний Honeypot никого блокировать не должен, в данном случае мы просто собираем списки и регулярно отправляем их "куда надо" для последующего ознакомления и реагирования.

Следующий вопрос - где именно мы будем ловить наши пакеты. Обычно он с завидной регулярностью вызывает дальнейшие расспросы. Это можно сделать как в таблице **mangle**, так и в таблице **filter**. Так как нам нужно разделять локальный и транзитный трафик, то мы будем использовать цепочки **INPUT** и **FORWARD**.

Более правильным является использовать для этой цели таблицу **mangle**, но не будет большой ошибкой, если вы используете для этого **filter**. Просто **mangle** изначально именно для этого и предназначена и обрабатывается **раньше,** чем **filter**, т.е. вы можете не волноваться, что нужный пакет попадет под какое-либо терминальное правило и к вам не дойдет. Если же вы выбрали для расположения правил таблицу **filter**, то размешайте правила в самом начале таблицы.

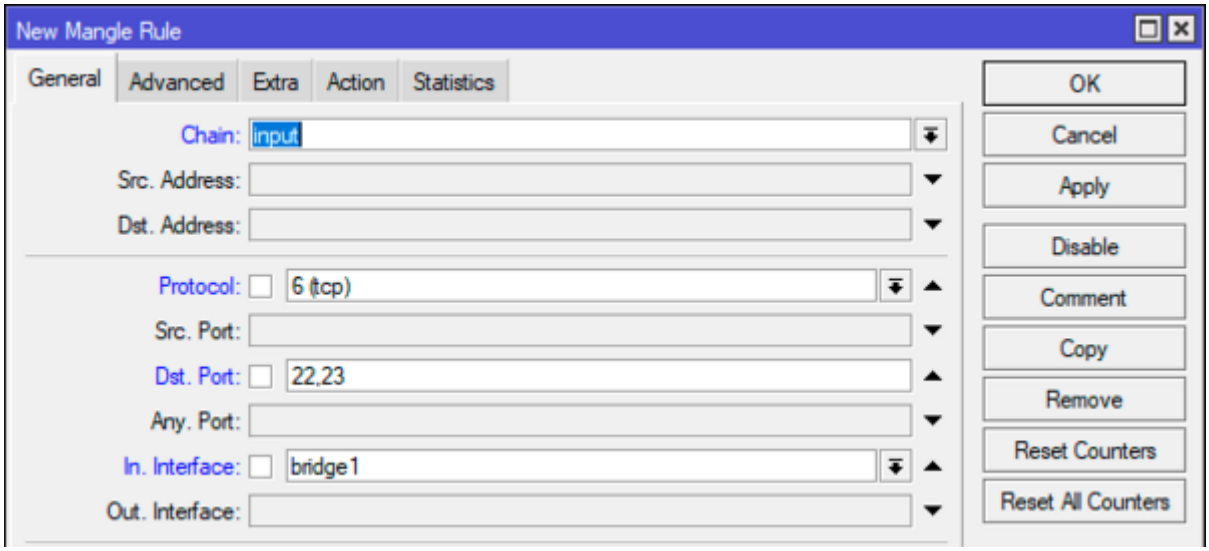
Еще раз повторим, что принципиальной разницы между размещением правил в **mangle** или **filter** нет, руководствуйтесь тем, как вам удобнее и как будет проще читать конфигурацию брандмауэра вашим коллегам.

Начнем с создания внутреннего Honeypot, используем те же порты. что и для внешнего, которые представляют наибольший интерес для злоумышленников:

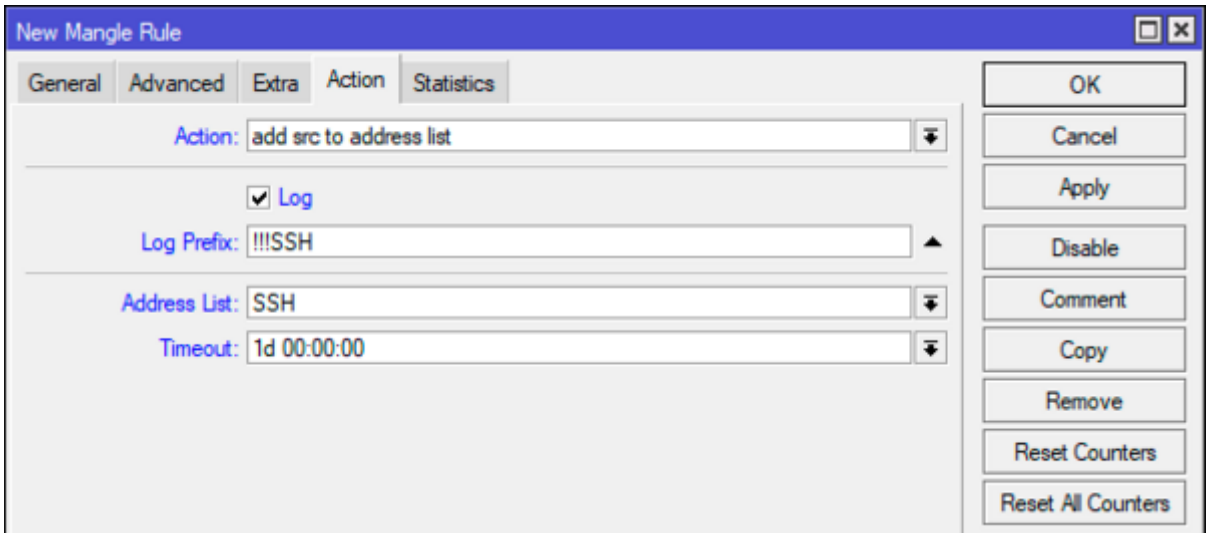
- **TCP:** 22- SSH, 23 - Telnet, 25 - SMTP, 135-139,445 - Netbios, 3389 - RDP, 5060 - SIP, 8291 - Winbox
- **UDP:** 123 - NTP, 135-139,445 - Netbios, 3389 - RDP, 5060 - SIP.

Кроме стандартных портов также есть смысл указывать некоторые нестандартные, которые часто используются в реальной жизни, например, 3390 - RDP, или 2222 или 2223 - SSH. При этом не стоит указывать все порты в одном правиле, потому что в таком случае вы без анализа логов не сможете понять куда именно пытался подключиться попавший в списки узел. Имеет смысл сделать отдельные правила для SSH, RDP, Netbios и т.д. и формировать отдельные списки.

Начнем, перейдем в **IP - Firewall - Mangle** и создадим правило, в нем мы будем контролировать обращения на порты 22 и 23 - SSH и Telnet: **Chain - input, Protocol - tcp, Dst. Port - 22,23, In. Interface** - внутренний интерфейс, в нашем случае **bridge1**.



На закладке **Action** добавим действие - **add src to address list** и указываем список для адресов, например, **SSH**. В поле **Timeout** указываем срок пребывания адреса в листе, в нашем случае сутки. Такое время выбрано исходя из того, чтобы не засорять листы, которые мы будем отправлять на почту администратору раз в сутки. Также для последующего анализа включим запись события в лог, для чего присвоим ему собственный префикс **!!!SSH**.



В терминале это можно быстро сделать командой:

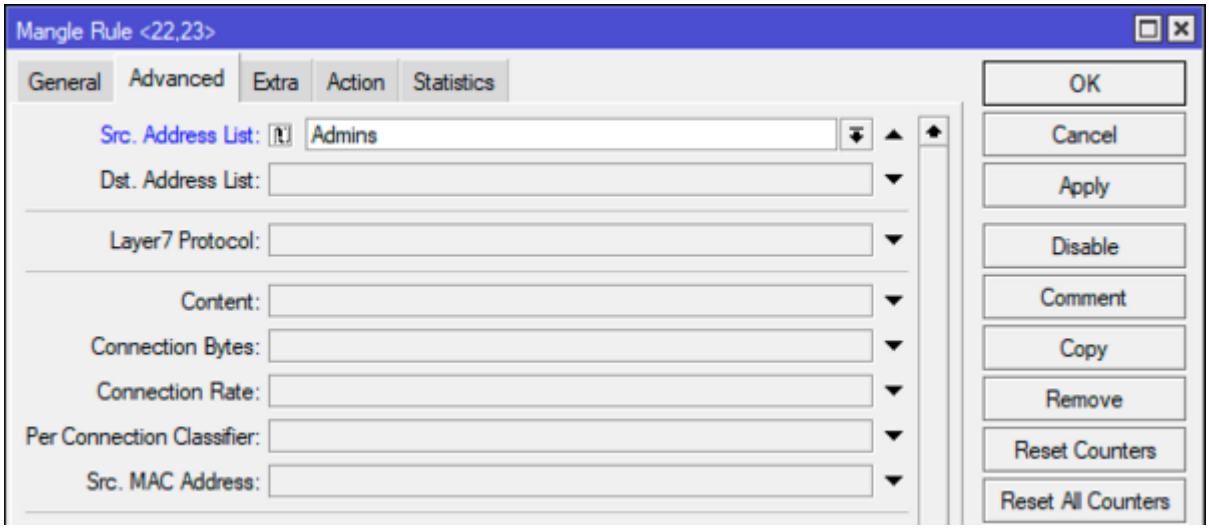
```
/ip firewall mangle
add action=add-src-to-address-list address-list=SSH address-list-timeout=1d \
    chain=input dst-port=22,23 in-interface=bridge1 log=yes log-prefix=!!!SSH \
    protocol=tcp
```

Здесь возникает еще один тонкий момент: как быть, если указанным сервисом легально пользуются некоторые сотрудники, тем же SSH могут пользоваться администраторы. Все просто - добавим их в исключение, для этого перейдем в **IP -**

Firewall - Address Lists и создадим новый список, например, **Admins**, куда внесем все адреса администраторов.

```
/ip firewall address-list
add address=192.168.111.125 list=Admins
```

После чего в правиле на закладке **Advanced** добавим дополнительный критерий: **Src. Address List - ! Admins**, что исключит его срабатывание на адреса источников из этого списка.

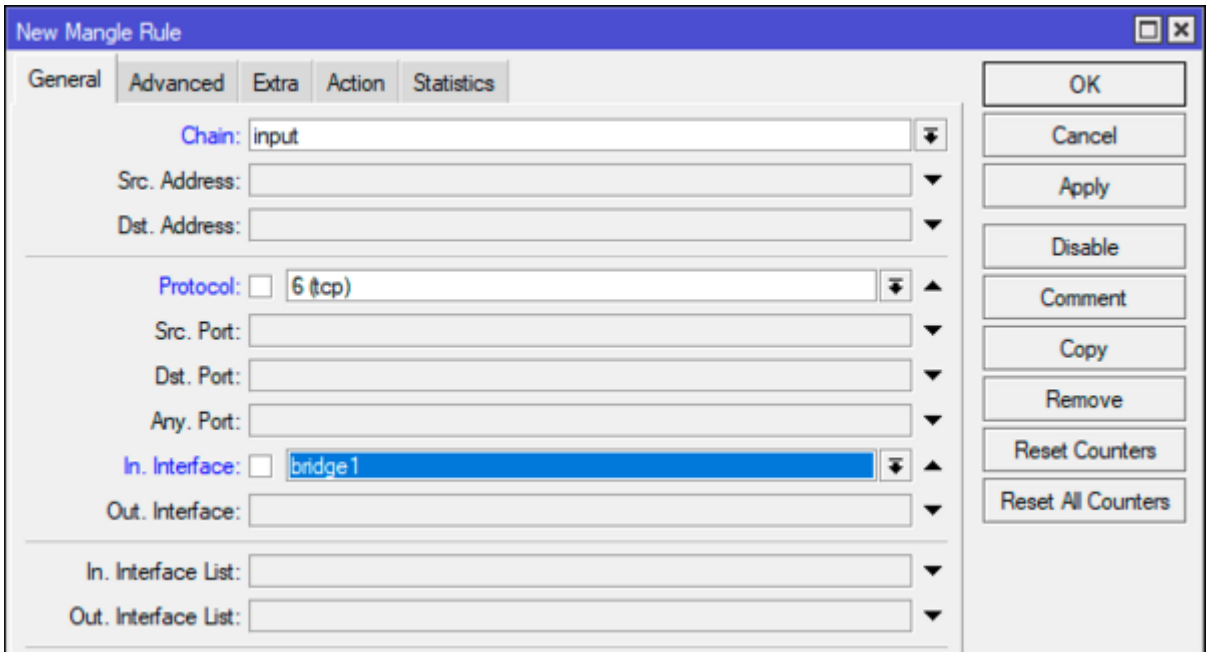


В терминале:

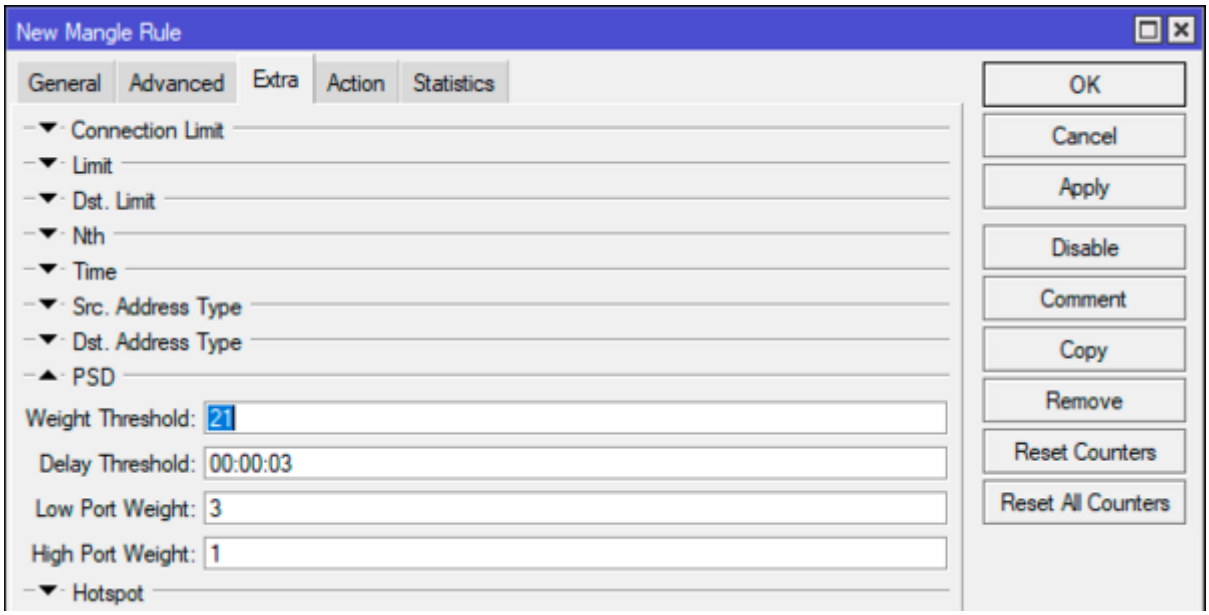
```
/ip firewall mangle
add action=add-src-to-address-list address-list=SSH address-list-timeout=1d \
 chain=input dst-port=22,23 in-interface=bridge1 log=yes log-prefix=!!!SSH \
 protocol=tcp src-address-list=!Admins
```

Аналогичным образом создаем правила для других наборов портов и начинаем собирать списки адресов, которые проявляют нездоровую активность во внутренней сети.

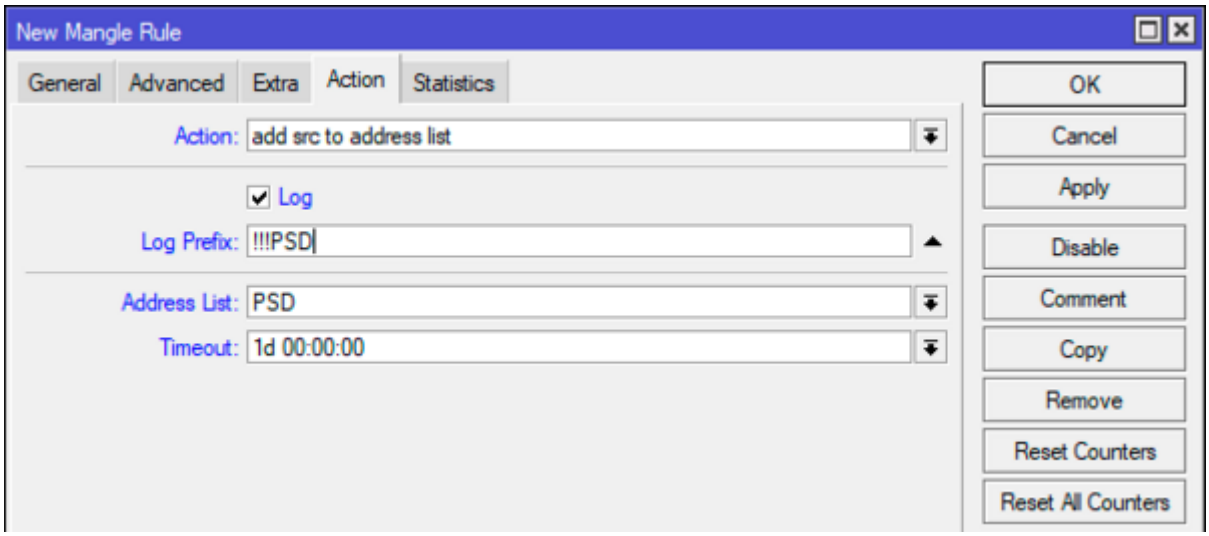
Отдельно стоит упомянуть про сканирование портов, RouterOS имеет собственные инструменты для выявления сканирования, для этого создадим правило: **Chain - input, Protocol - tcp, In. Interface - bridge1**.



На закладке **Extra** развернем блок **PSD**, для начала можно оставить настройки по умолчанию, смысл их довольно прост: за 3 секунды сканирующий должен набрать 21 очко, за каждый "низкий" порт (0-1023) присваивается 3 очка, за каждый "высокий" (1024-65535) - одно очко.



Действия на закладке **Action** аналогичные предыдущему правилу: добавляем адрес источник в отдельный список адресов и делаем запись в логе с уникальным префиксом:

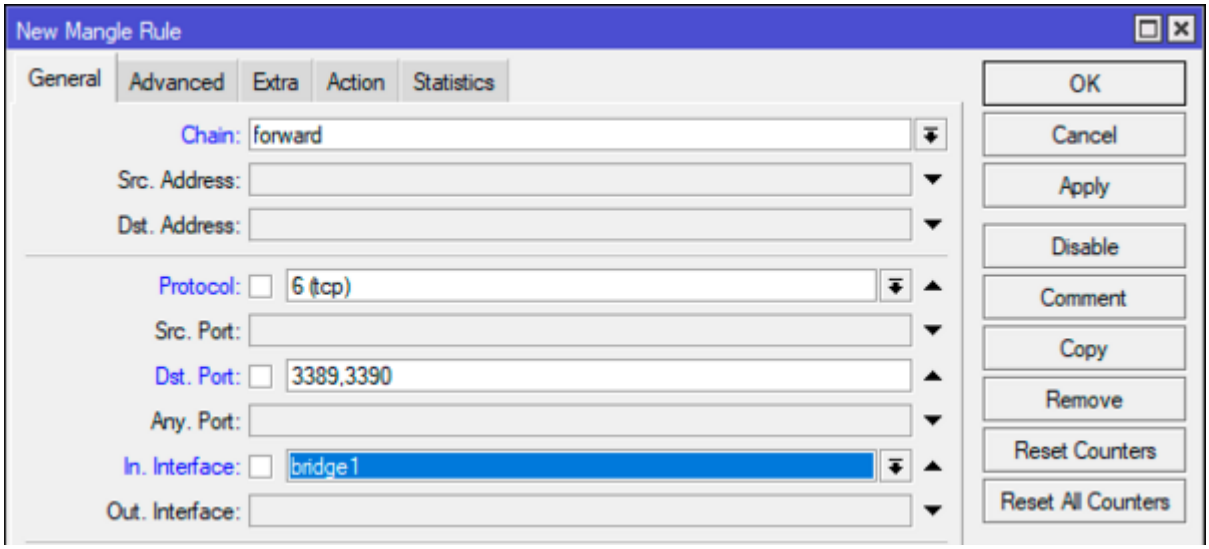


Эти же действия в терминале:

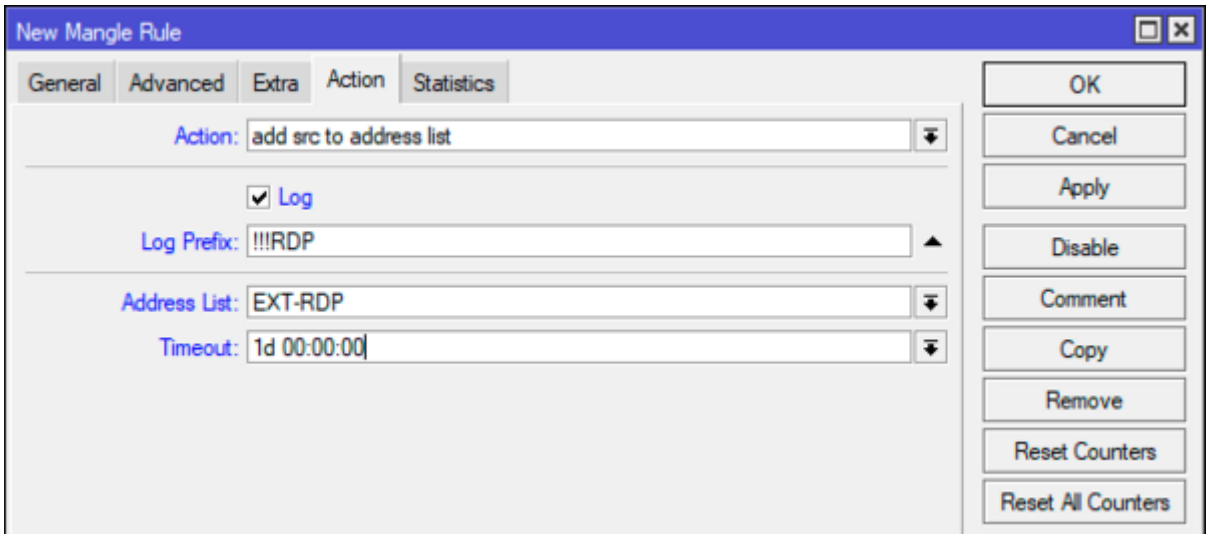
```
/ip firewall mangle
add action=add-src-to-address-list address-list=PSD address-list-timeout=1d \
 chain=input in-interface=bridge1 log=yes log-prefix=!!!PSD protocol=tcp \
 psd=21,3s,3,1
```

Теперь перейдем к транзитному трафику. Здесь мы будем выявлять не столько вредоносную активность, сколько различные подозрительные действия пользователей. Скажем, ситуация, когда бухгалтер регулярно подключается к чужому RDP - это уже повод присмотреться к ее работе повнимательнее.

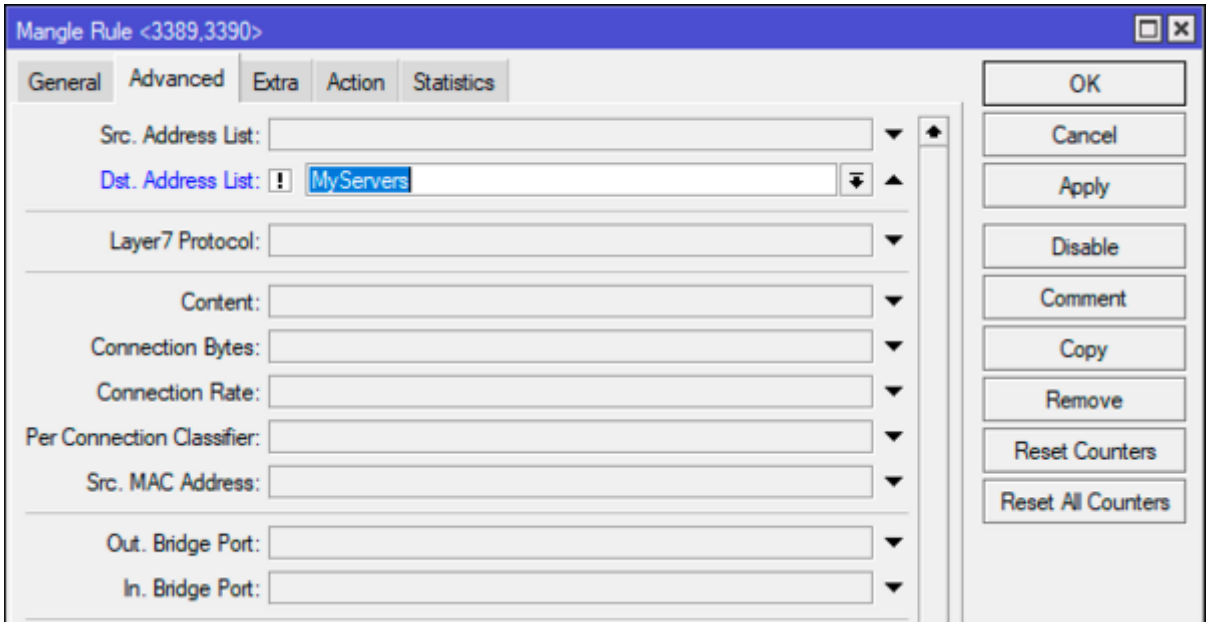
Вот с RDP мы и начнем. Снова возвращаемся в **IP - Firewall - Mangle** и создаем правило: **Chain - forward, Protocol - tcp, Dst. Port - 3389,3390, In. Interface - bridge1**.



На закладке **Action** также добавляем адрес-источник в список адресов на сутки и пишем событие в лог с собственным префиксом.



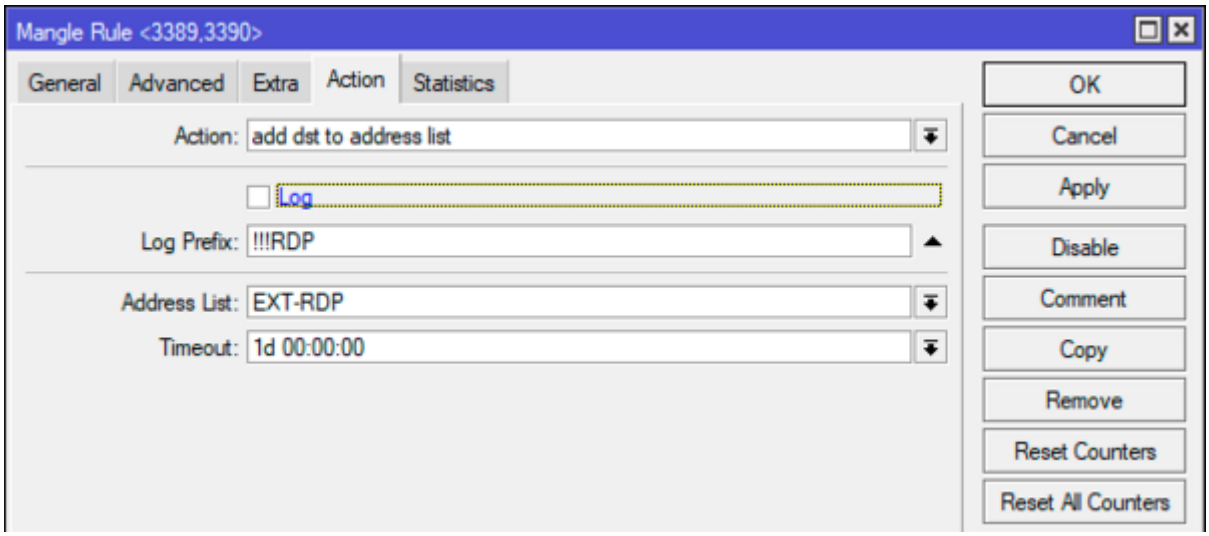
Если у вас есть собственные внешние сервера, то создайте еще один список адресов, скажем - **MyServers**, в который внесите их IP-адреса и укажите его как исключение на закладке **Advanced** для адресов назначения: **Dst. Address List - ! MyServers**.



В терминале:

```
/ip firewall mangle
add action=add-src-to-address-list address-list=EXT-RDP address-list-timeout=1d \
    chain=forward dst-address-list=!MyServers dst-port=3389,3390 \
    in-interface=bridge1 log=yes log-prefix=!!!RDP protocol=tcp
```

В случае с внешними ресурсами нас интересует не только кто, но и куда. Поэтому имеет смысл добавлять в тот-же список и адреса назначения, т.е. куда пытались подключиться наши пользователи. Для этого делаем копию правила и на закладке **Action** меняем действие **add src to address list** на **add dst to address list** и выключаем логирование, чтобы не делать дублирующую запись в логе.



В терминале:

```
/ip firewall mangle
add action=add-dst-to-address-list address-list=EXT-RDP address-list-timeout=\
 1d chain=forward dst-port=3389,3390 in-interface=bridge1 protocol=tcp
```

Итак, правила созданы, наполняются адресами и теперь нам нужно настроить их отправку нужным сотрудникам, для этого напишем небольшой скрипт. Перейдем в **System - Scripts** и создадим новый скрипт с именем **SendListsToMail** в который добавим следующие строки:

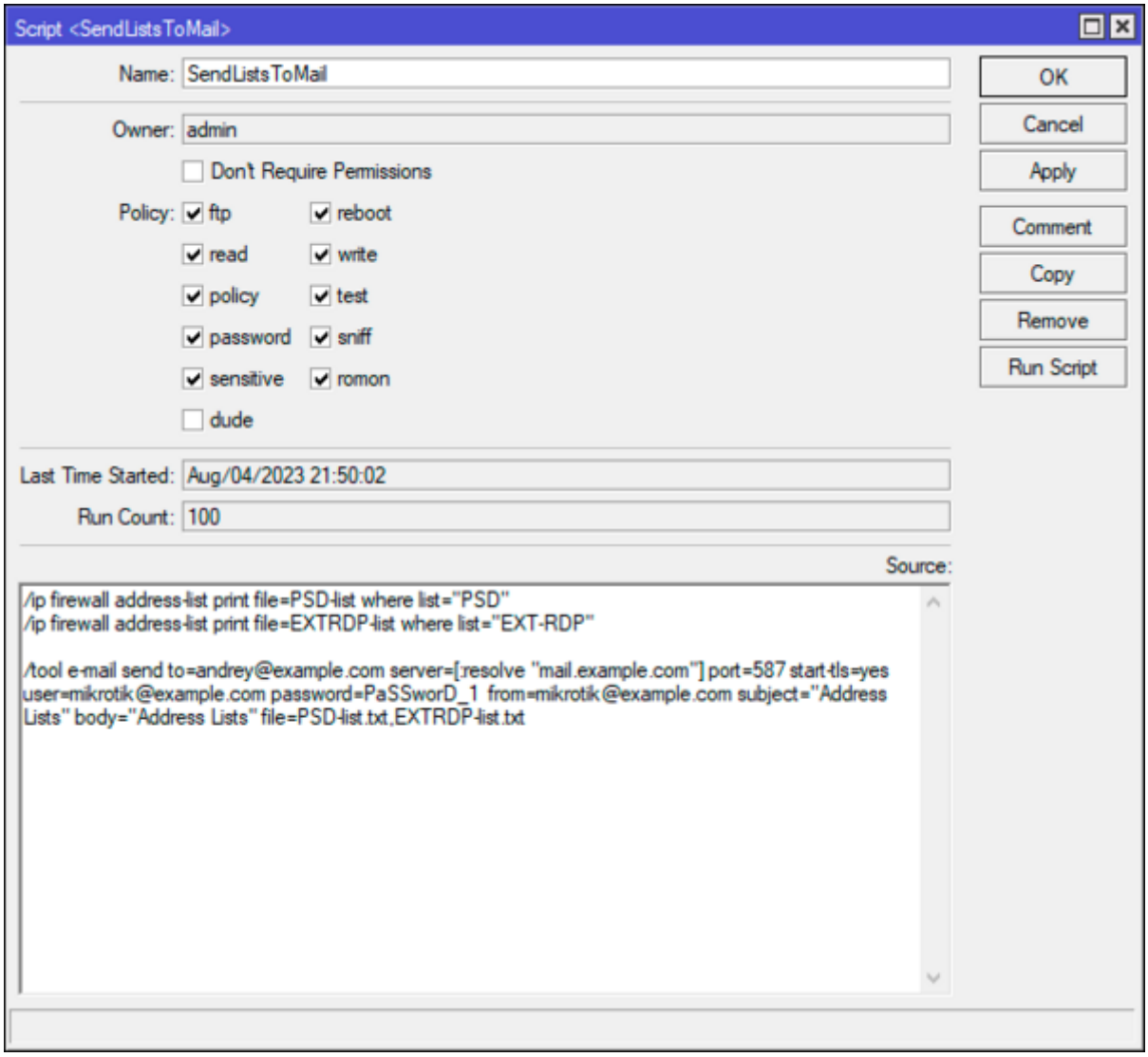
```
/ip firewall address-list print file=PSD-list where list="PSD"
/ip firewall address-list print file=EXTRDP-list where list="EXT-RDP"


/tool e-mail send to=andrey@example.com server=[:resolve "mail.example.com"]
port=587 \
    start-tls=yes user=mikrotik@example.com password=PaSSworD_1
from=mikrotik@example.com \
    subject="Address Lists" body="Address Lists" file=PSD-list.txt,EXTRDP-list.txt
```

Первые две команды выгружают листы в текстовые файлы, в команде указываем только имя файла, расширение добавится автоматически, последняя отправляет их как вложения на почту. Разберем ее подробнее:

- **send to** - адрес получателя
- **server** - адрес сервера, если используем FQDN, то используем синтаксис [:resolve "mail.example.com"]
- **port** - порт для отправки почты
- **start-tls** - включаем использование START-TLS
- **user** - логин пользователя на почтовом сервере
- **password** - пароль пользователя на почтовом сервере
- **from** - почтовый адрес отправителя
- **subject** - тема письма
- **body** - тело письма

- **file** - файлы вложения, несколько файлов разделяем запятой без пробелов.

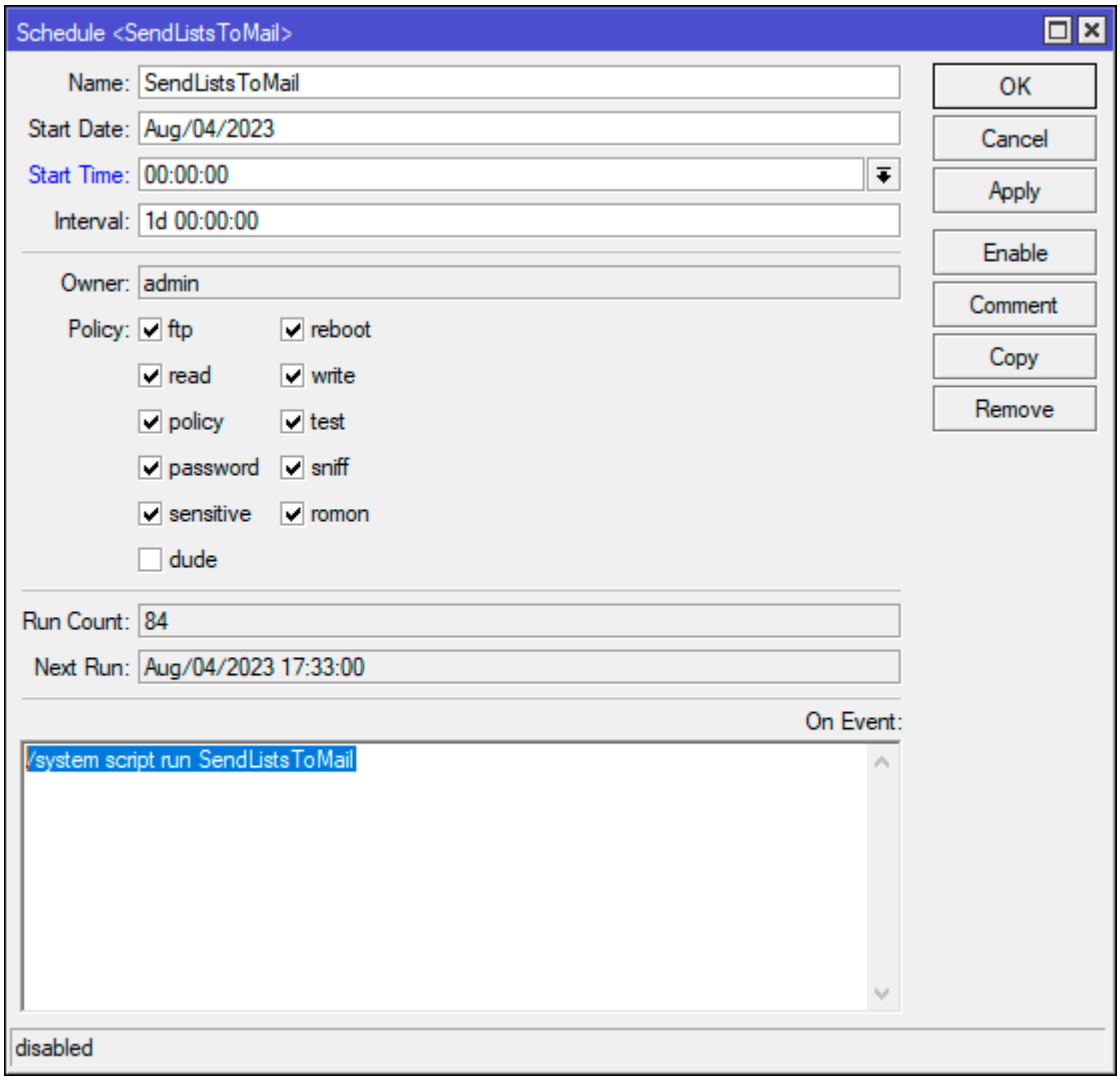
Сохраняем скрипт нажав **Apply** и проверяем кнопкой **Run Script**:



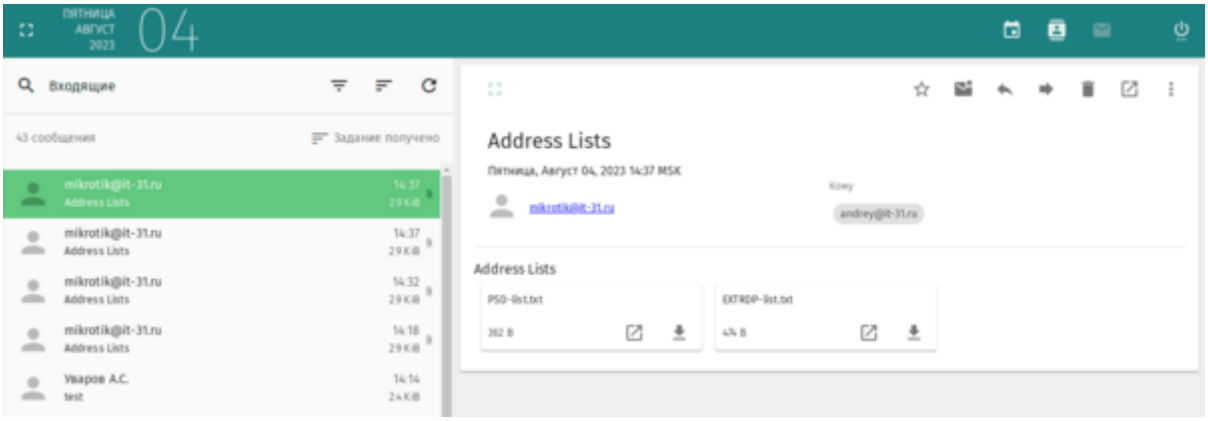
Если все сделано правильно, то вы получите на указанную почту файлы со списками. Теперь нужно добавить данный скрипт в планировщик. Переходим в **System - Scheduler** и добавим новое задание, в нем нас интересует два параметра: **Start Time** - время срабатывания и **Interval** - периодичность выполнения. На время отладки можно задать срабатывание на ближайшие несколько минут, чтобы проверить задание, а потом установить нужное время, интервал указываем равный суткам.

В поле **On Event** пишем команду запуска нашего скрипта:

```
/system script run SendListsToMail
```



Дожидаемся времени исполнения и проверяем почту, списки должны прийти строго по расписанию:



Конечно, данная статья не охватывает всех возможностей данного решения, мы только лишь дали необходимую базу, а дальше каждый из вас может сам гибко настроить его под свои потребности. Надеемся, что данный материал окажется вам полезен.

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.
