Небольшая заметка на тему использования известной технологии для защиты уязвимого сервиса при сохранении удаленного доступа к нему. Речь пойдет о настройке Port knocking в Mikrotik для защиты подключения к Winbox с сохранением доступа откуда угодно. Покажу работу технологии на простом и более сложном примере.

> Если у вас есть желание научиться работать с роутерами микротик и стать специалистом в этой области, рекомендую по программе, основанной на информации из официального курса **MikroTik Certified Network Associate**. Курс стоящий, все подробности читайте по ссылке.

Содержание

Что такое port knocking

Port knocking — защитный режим обслуживания сети, действие которого основано на следующем принципе. Сетевой порт является закрытым до тех пор, пока не будут выполнены определенные условия. В данном случае условием является определенная последовательность пакетов данных, направленная на целевое устройство, которое защищается с помощью port knocking.

В моем примере мы будет защищать порт 8291, который используется в mikrotik для подключения управляющей программы winbox. Для того, чтобы с ее помощью можно было подключиться к устройству, нужно будет отправить определенную последовательность пакетов по протоколу icmp.

Простая настройка port knocking из одного правила

Для того, чтобы не погружаться в теорию работы и настройки firewall в mikrotik, я буду считать, что вы настраивали его по моей статье на эту тему. Так как мое текущее повествование на достаточно узкую тему, сфокусируюсь только на ней.

Допустим, вы ограничили доступ к порту 8291, который использует winbox для подключения, фиксированным списком ip адресов. Название списка **winbox_remote**. Сейчас я покажу, как сделать так, чтобы в этот список временно попал тот ip адрес, который вам нужен, и который отсутствует в этом списке. Причем доступа к микротику у вас не будет. Тут нам как раз поможет технология **port knocking**.

Создаем следующее правило в фаерволе микротика.

```
add action=add-src-to-address-list address-list=winbox_remote address-list-timeout=30m chain=input comment="icmp port
knocking" in-interface=ether2-wan packet-size=144 protocol=icmp
```

Рассказываю, что мы тут настроили. При пинге с какого-то ip адреса размером пакета 116 байт, на микротик придет пакет размером 144 байта (28 байт заголовок) и адрес отправителя будет добавлен в список winbox_remote на 30 минут. Для проверки работы достаточно выполнить пинг с любого компьютера, примерно вот так:

```
ping 1.2.3.4 -l 116 -n 1
```

После этого адрес отправителя отправится в указанный список роутера. Там будет создана динамическая запись.

Чтобы правило сработало, оно должно быть правильно расположено в списке правил. Правило с port knocking обязательно должно быть выше правила,

разрешающего все icmp пакеты. Если этого не сделать, то первое разрешающее правило обработает все входящие icmp пакеты и до созданного нами в этой статье правила они просто не дойдут.

Более сложная проверка из трех правил

Теперь рассмотрим вариант немного посложнее. В список разрешенных ip адресов можно будет попасть, отправив не менее трех пакетов нужно длины. Для этого создаем 3 правила в firewall.

```
add action=add-src-to-address-list address-list=winbox_remote address-list-timeout=30m chain=input comment="icmp port
knocking" in-interface=ether2-wan log=yes packet-size=144 protocol=icmp src-address-list=stage2
add action=add-src-to-address-list address-list=stage2 address-list-timeout=1m chain=input in-interface=ether2-wan log=yes
packet-size=144 protocol=icmp src-address-list=stage1
add action=add-src-to-address-list address-list=stage1 address-list-timeout=1m chain=input in-interface=ether2-wan log=yes
packet-size=144 protocol=icmp
```

Обращаю внимание на порядок правил. Он должен быть именно такой. Первый пакет попадает на третье правило и адрес отправителя записывается в список stage1. Следующий пакет будет иметь адрес отправителя из stage1 (src-address-list=stage1), поэтому его заносим в список stage2. Третий пакет будет иметь адрес отправителя из stage2, поэтому добавляем его в winbox_remote.

Тут есть один важный нюанс. Чаще всего у вас первым правилом в списке firewall на mikrotik будет разрешение на уже установленные соединения. Примерно такое:

```
add action=accept chain=input comment="accept establish & related" connection-state=established,related
```

Оно будет захватывать второй и последующие пакеты icmp, поэтому они не попадут на 3 наших правила выше. Чтобы этого избежать, нужно правила с port knocking в mikrotik ставить либо выше этого правила, либо в этом правиле сделать исключение для протокола icmp, примерно так:

```
add action=accept chain=input comment="accept establish & related" connection-state=established,related protocol=!icmp
```

После этого все должно работать нормально. На время отладки рекомендую включить логирование целевых правил. Так будет проще разобраться в

проблемах, если будут возникать.

Таким способом можно наполнять разные списки и использовать их для доступа к различным сервисам. Как говорится, просто и сердито. Настроить не сложно, обойти такую защиту в очень хлопотно, особенно если время жизни записей в списке оставить 1 минуту. Для подключения к сервису этого вполне хватит, а дальше соединение получит статус established и будет оставаться активным, пока не закроется.