Настраиваем защиту от атак BruteForce на роутерах Mikrotik

Записки IT специалиста

Технический блог специалистов ООО"Интерфейс"

- Главная
- Настраиваем защиту от атак BruteForce на роутерах Mikrotik

Атаки "грубой силой" (BruteForce) - весьма распространенный тип атак в сети интернет, который сводится к попытке подбора пароля методом его перебора. Кроме этого, атакующие используют библиотеки словарных слов и списки скомпрометированных паролей, поэтому, даже если у вас используются сложные пароли, не стоит беспечно относиться к подобным угрозам. Конечно, полностью защититься от перебора паролей нельзя, но можно серьезно затруднить этот процесс блокируя атакующих и тем самым уменьшая скорость перебора. В данной статье мы рассмотрим, как защитить от данной атаки Winbox и WebFig роутеров Mikrotik.

Мы не будем разбирать вопрос, по какой именно причине интерфейсы Winbox и WebFig смотрят во внешний мир, потому что это тема отдельной статьи, в данном случае мы будем рассматривать исключительно меры защиты от перебора паролей. При этом подразумевается, что данные интерфейсы используются и легальными пользователями, которые должны иметь право на ошибку.

Защита Winbox от BruteForce

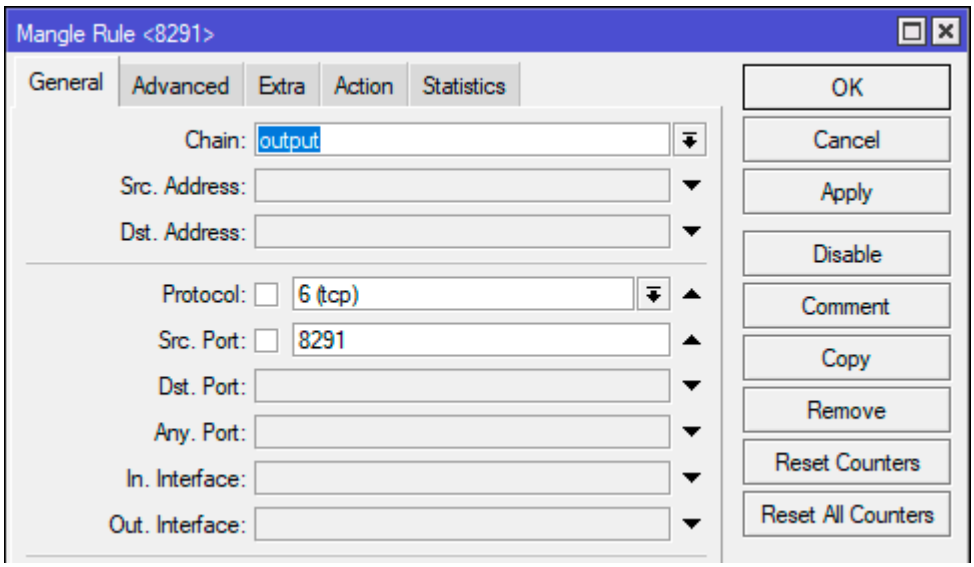
Winbox - это самый популярный метод управлениями устройствами Mikrotik и поэтому он достаточно популярен у взломщиков, поэтому наша задача определить попытки неверного ввода паролей и после нескольких попыток заблокировать атакующего. На наш взгляд легальному пользователю достаточно дать три попытки в течении одной минуты, это вполне укладывается в логику работы легального

пользователя, который после безуспешной попытки будет проверять раскладку, сверяться с записями, а не будет тупо долбиться. Если же попытки войти происходят чаще, то перед нами скорее всего атакующий.

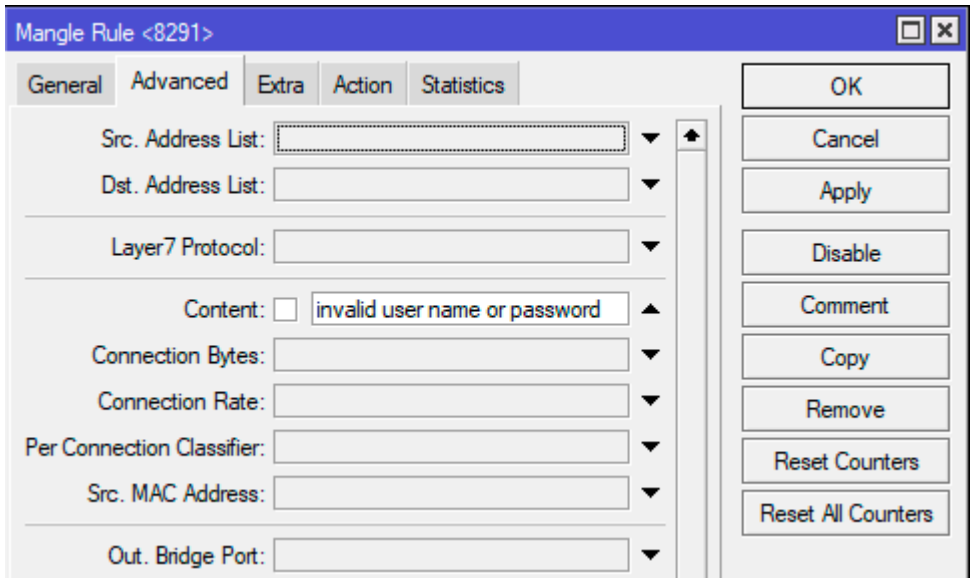
Как определить неверный ввод пароля? Достаточно просто, в ответном пакете роутер сообщит открытым текстом:

```
invalid user name or password
```

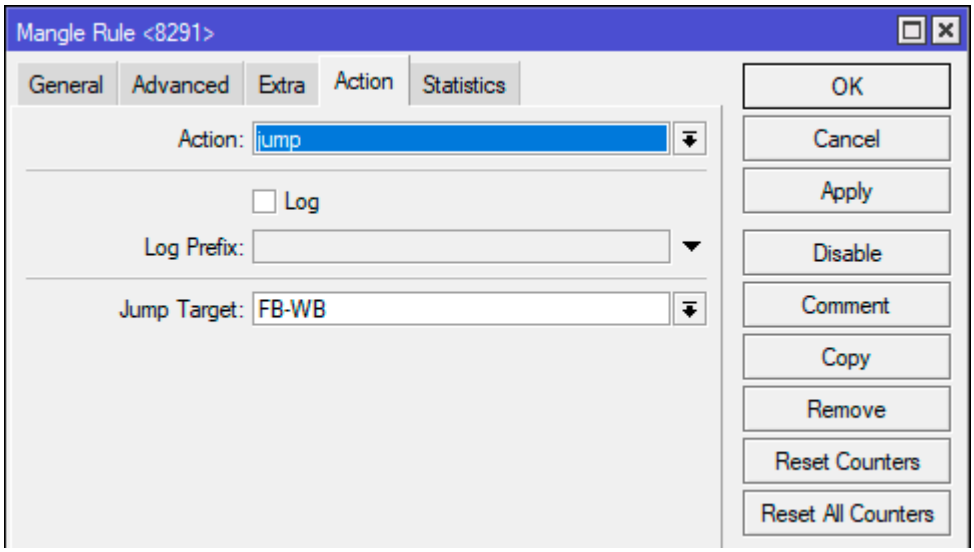
А получатель такого пакета будет являться предметом нашего повышенного интереса. Но прежде всего отследим само событие, для этого откроем **IP - Firewall - Mangle** и создадим правило: **Chain - output, Protocol - tcp, Src.Port - 8291**.



Затем на закладке **Advanced** добавим критерий: **Content - invalid user name or password**.



А на закладке **Action** укажем действие **jump** и в поле **Jump Target** укажем имя пользовательской цепочки, в нашем случае **FB-WB** (*Fail2Ban Winbox*).



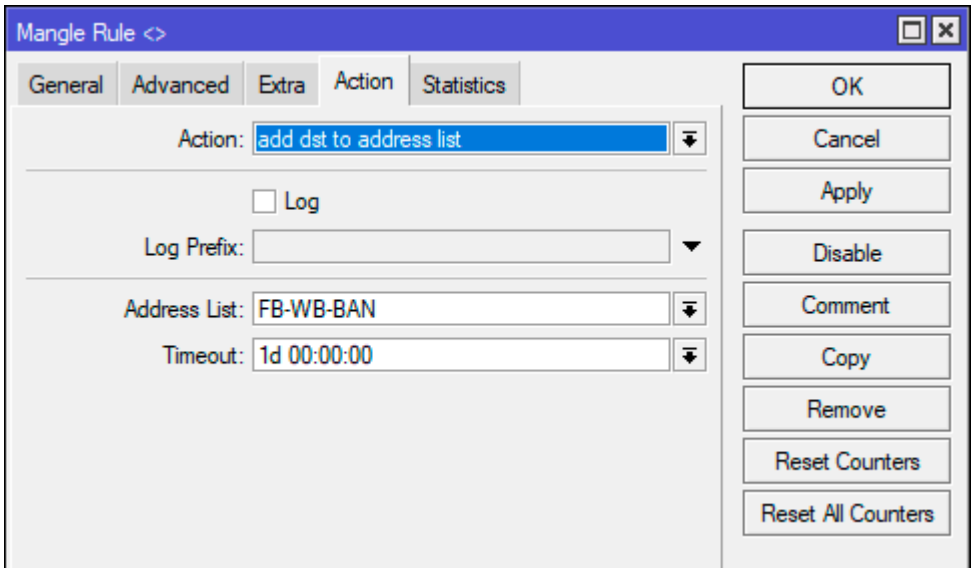
Это же правило в терминале:

```
/ip firewall mangle
add action=jump chain=output content="invalid user name or password" jump-
target=FB-WB protocol=tcp src-port=8291
```

Теперь немного поясним что мы сделали. Прежде всего мы выделили ответные пакеты роутера с сообщением об ошибке учетных данных и направили их в собственную цепочку брандмауэра. Это позволит далее работать с ними, персонально не проверяя каждый раз соответствие критерию наличия текста ошибки. Также это исключает прохождение по правилам цепочки других пакетов, что положительно сказывается на производительности.

А теперь начнем создавать правила для нашей цепочки и будем делать это от конца к началу. Для этого мы будем использовать несколько списков адресов и на основании повторения адреса в списках принимать решение о блокировке. Легальный пользователь будет иметь три попытки в течении минуты.

Там же, в **IP - Firewall - Mangle**, создадим правило: **Chain - FB-WB**. На закладке **Advanced** указываем **Dst. Address List - FB-WB-3**, а в **Action - add dst to address list, Address List - FB-WB-BAN, Timeout - 1d 00:00:00**.



В терминале:

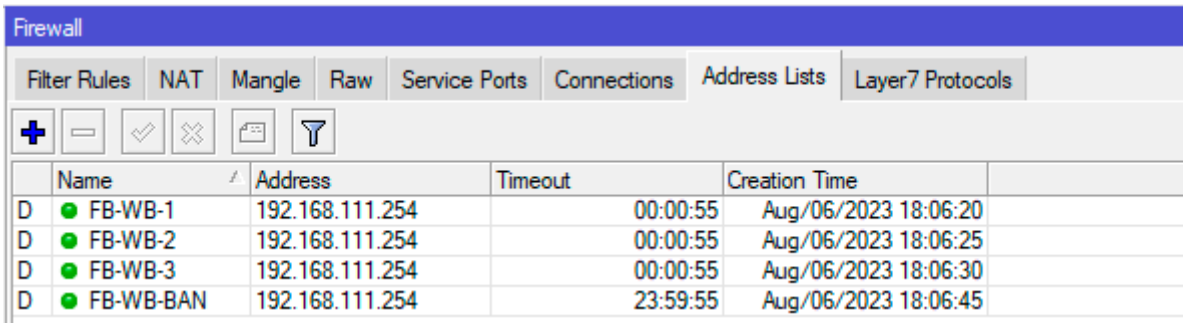
```
/ip firewall mangle
add action=add-dst-to-address-list address-list=FB-WB-BAN address-list-timeout=1d
chain=FB-WB dst-address-list=FB-WB-3
```

Данным правилом мы проанализировали **адрес назначения** ответного пакета роутера и если он есть в списке **FB-WB-3**, т.е. успел три раза вести неверный пароль, то отправляем его в список **FB-WB-BAN** сроком на одни сутки.

После чего подобным образом создадим правила на заполнение остальных списков. Так если адрес есть в списке **FB-WB-2**, то добавляем его в список **FB-WB-3** на одну минуту, если адрес есть в **FB-WB-1**, то добавляем его на минуту в **FB-WB-2**, а если его нет ни в одном списке, то добавим в **FB-WB-1** тоже на одну минуту:

```
/ip firewall mangle
add action=add-dst-to-address-list address-list=FB-WB-3 address-list-timeout=1m
chain=FB-WB dst-address-list=FB-WB-2
add action=add-dst-to-address-list address-list=FB-WB-2 address-list-timeout=1m
chain=FB-WB dst-address-list=FB-WB-1
add action=add-dst-to-address-list address-list=FB-WB-1 address-list-timeout=1m
chain=FB-WB
```

Для проверки правильности работы несколько раз пытаемся указать неверные учетные данные и наблюдаем как адрес атакующего последовательно заполняет списки от **FB-WB-1** до **FB-WB-BAN**.



Теперь дело за малым - заблокировать атакующих. Для этого переходим в **IP - Firewall - Raw** и создаем правило: **Chain - Prerouting**. Затем на закладке **Advanced** добавляем **Src. Address List - FB-WB-BAN** и на закладке **Action** указываем действие **drop**.

```
/ip firewall raw
add action=drop chain=prerouting src-address-list=FB-WB-BAN
```

Таким образом любой, кто более трех раз за минуту введет неверные учетные данные будет заблокирован на одни сутки. Временные лимиты указаны для примера, можете менять их на собственное усмотрение.

Защита WebFig от BruteForce

Защита веб-интерфейса WebFig от буртфорса осуществляется точно таким же образом, что и Windox, поэтому мы не будем приводить примеры для графического интерфейса, а ограничимся только командами в терминале.

Анализировать мы также будем ответы роутера с порта веб-сервера (80 TCP), в случае неверных учетных данных RouterOS 6 отвечает сообщением:

```
403 Forbidden
```

A RouterOS 7:

```
Error 403
```

А далее все как в предыдущем варианте. Прежде всего отправим все пакеты с нужным ответом в отдельную пользовательскую цепочку FB-WEB:

```
/ip firewall mangle
add action=jump chain=output content="403 Forbidden" jump-target=FB-WEB
protocol=tcp src-port=80
```

А затем начнем заполнять списки адресов, точно также, от конца к началу. Для каждого адреса проверяется наличие в списке и если оно подтверждается он попадает в вышестоящий список. Три списка FB-WEB-1 - FB-WEB-3 заполняются на одну минуту и дают возможность легальному пользователю совершить три ошибки. Четвертый список FB-WEB-BAN предназначен для блокировки и срок нахождения в нем адресов - одни сутки.

```
/ip firewall mangle
add action=add-dst-to-address-list address-list=FB-WEB-BAN address-list-timeout=1d
chain=FB-WEB dst-address-list=FB-WEB-3
add action=add-dst-to-address-list address-list=FB-WEB-3 address-list-timeout=1m
chain=FB-WEB dst-address-list=FB-WEB-2
add action=add-dst-to-address-list address-list=FB-WEB-2 address-list-timeout=1m
chain=FB-WEB dst-address-list=FB-WEB-1
add action=add-dst-to-address-list address-list=FB-WEB-1 address-list-timeout=1m
chain=FB-WEB
```

После чего блокируем атакующих в таблице Raw:

```
/ip firewall raw
add action=drop chain=prerouting src-address-list=FB-WEB-BAN
```

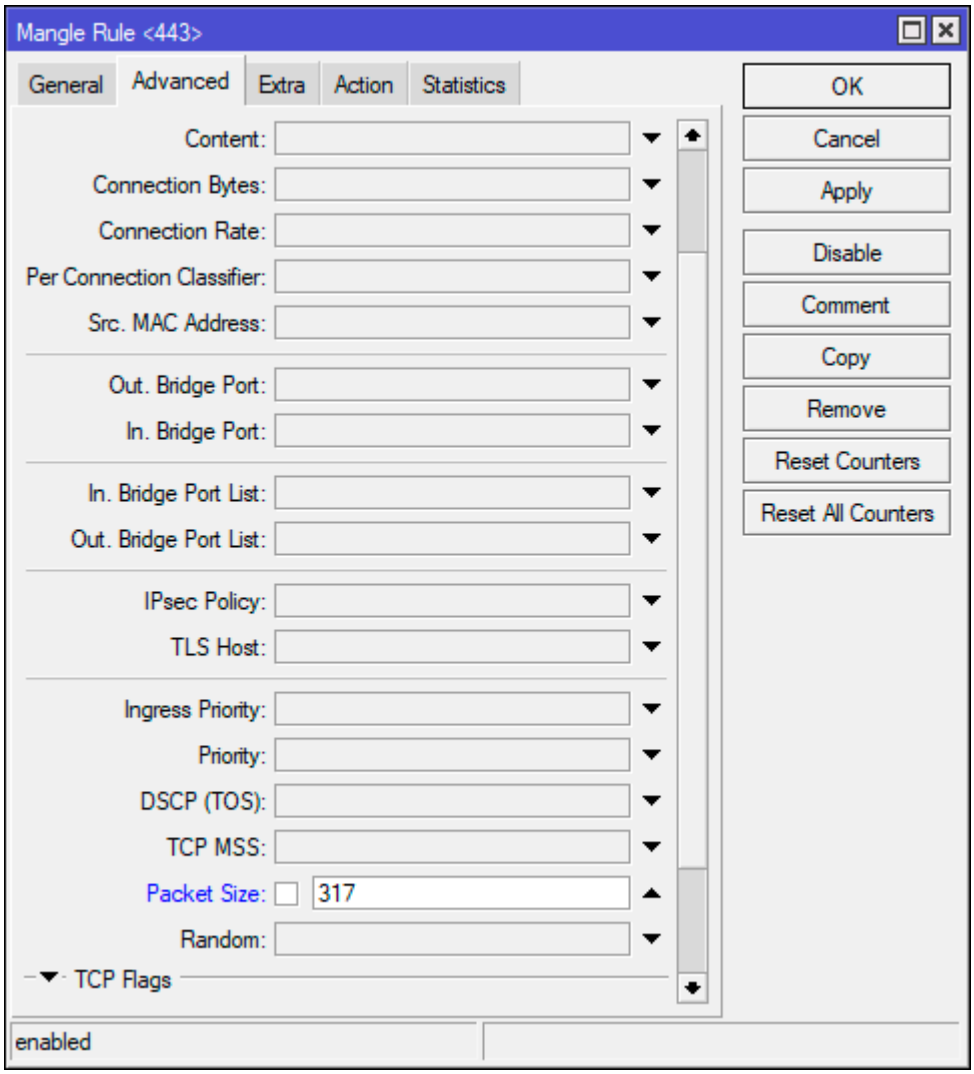
Время нахождения в списках и количество попыток вы можете регулировать на свое усмотрение.

Защита WebFig SSL от BruteForce

А вот здесь у нас задача посложнее, при включении SSL защиты мы не можем анализировать содержимое ответного пакета и нам нужно найти какой-либо иной критерий, который бы указывал на попытку подбора паролей. В ходе наших исследований, эмпирическим путем было установлено, что в качестве критерия можно использовать размер ответного пакета, который составляет **317 байт** для **RouterOS 6** и **378 байт** для **RouterOS 7**.

Важно! Данные цифры **не являются официальными**, а получены **экспериментальны**м путем и в будущем могут иметь иные значения!

В остальном принцип защиты остается тем же, прежде всего направим соответствующие критерию пакеты в отдельную пользовательскую цепочку, только используем порт источника **443** и критерий на вкладке **Advanced** вместо Content должен быть **Packet Size**:



В терминале:

```
/ip firewall mangle
add action=jump chain=output jump-target=FB-SSL packet-size=317 protocol=tcp src-
port=443
```

Далее точно также заполняем четыре таблицы:

```
/ip firewall mangle
add action=add-dst-to-address-list address-list=FB-SSL-BAN address-list-timeout=1d
chain=FB-SSL dst-address-list=FB-SSL-3
add action=add-dst-to-address-list address-list=FB-SSL-3 address-list-timeout=1m
chain=FB-SSL dst-address-list=FB-SSL-2
add action=add-dst-to-address-list address-list=FB-SSL-2 address-list-timeout=1m
chain=FB-SSL dst-address-list=FB-SSL-1
add action=add-dst-to-address-list address-list=FB-SSL-1 address-list-timeout=1m
chain=FB-SSL
```

А затем всех тех, кто добрался до последней таблицы блокируем в таблице Raw:

```
/ip firewall raw
add action=drop chain=prerouting src-address-list=FB-SSL-BAN
```

Как видим, защитить роутер Mikrotik от перебора паролей довольно несложно, но для этого нужно иметь определенный набор знаний и навыков, позволяющих выделить из потока трафика нужные сообщения или воспользоваться нашей статьей.

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.