У меня дома давно стоит mikrotik в качестве роутера. Очень надежное решение. У меня не было внешнего IP адреса, поэтому настройкой firewall на mikrotik я не занимался. Мне просто было лень. Пришлось ее побороть.

> Если у вас есть желание научиться работать с роутерами микротик и стать специалистом в этой области, рекомендую пройти курсы по программе, основанной на информации из официального курса MikroTik Certified Network Associate. Все подробности читайте ниже.

> Данная статья устарела. Я опубликовал более современную и полную инструкцию по настройке фаервола в микротик. Рекомендую использовать ее для настройки межсетевого экрана.

Содержание:

Некоторое время назад приобрел статический внешний IP. Спустя несколько дней начались проблемы с интернетом. Он стал временами откровенно тупить. Mikrotik прямо из коробки предлагает все инструменты для решения подобных проблем. Зашел через winbox на него, открыл список интерфейсов, увидел траффик на внешнем. Зашел в его настройки, нажал Torch и стал смотреть, что там за траффик. Трафика там было полно, но без подробностей, только ip адреса. Ничего страшного. Идем в IP -> Firewall, открываем закладку Connections и смотрим, кто там и что от нас хочет. Скорее всего тупо боты сканят наш адрес в поисках уязвимостей. Больше всего запросов на 53-й порт.

Настройка Firewall в Mikrotik

Тут мне стало очевидно, что на Mikrotik надо настроить таки Firewall, чтобы закрыться от подобных соединений, которые приводят к тормозам в работе роутера. В интернете много информации по настройке fiewall в mikrotik, я не буду подробно описывать этот процесс. Прочитать подробно о настройке

можно тут или тут. Я просто приведу свой набор правил для обычного домашнего роутера. Это минимальный набор правил фаервола, ничего лишнего и в то же время полная защита от ненужных подключений.
Здесь ether2 — внешний интерфейс, 192.168.1.0/24 — моя локальна сеть, 45000 — порт торрента.

```
Разрешаем пинги
add chain=input action=accept protocol=icmp
add chain=forward action=accept protocol=icmp
```

```
Разрешаем установленные подключения
add chain=input action=accept connection-state=established
add chain=forward action=accept connection-state=established
```

```
Разрешаем связанные подключения
add chain=input action=accept connection-state=related
add chain=forward action=accept connection-state=related
```

```
Разрешаем все подключения из нашей локальной сети
add chain=input action=accept src-address=192.168.1.0/24 in-interface=!ether2
```

```
Разрешаем входящие подключения для торрента
add chain=forward action=accept protocol=tcp in-interface=ether2 dst-port=45000
```

```
Обрубаем инвалидные подключения
add chain=input action=drop connection-state=invalid
add chain=forward action=drop connection-state=invalid
```

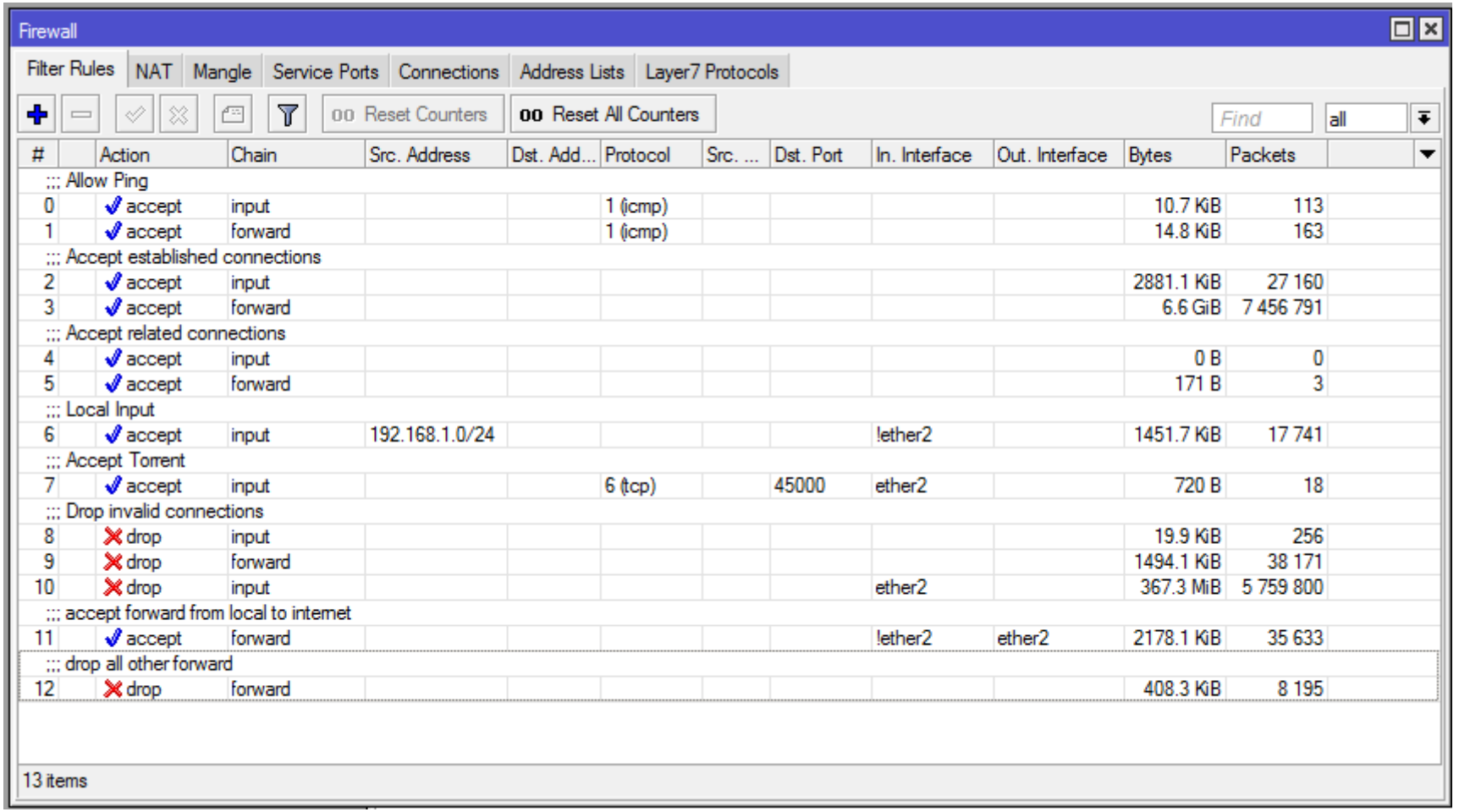
```
Обрубаем все остальные входящие подключения
add chain=input action=drop in-interface=ether2
```

```
Разрешаем доступ из локальной сети в интернет
add chain=forward action=accept in-interface=!ether2 out-interface=ether2
```

```
Обрубаем все остальные подключения
```

```
add chain=forward action=drop
```

Вот скриншот моих правил firewall. В принципе, по нему можно воссоздать все правила у себя на mikrotik:



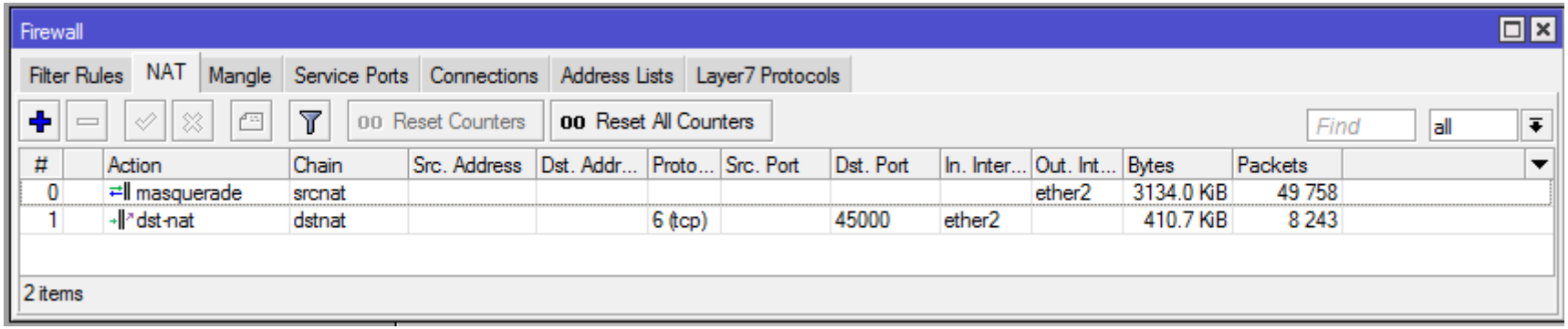
#	Action	Chain	Src. Address	Dst. Add...	Protocol	Src. ...	Dst. Port	In. Interface	Out. Interface	Bytes	Packets
;;; Allow Ping											
0	accept	input			1 (icmp)					10.7 KiB	113
1	accept	forward			1 (icmp)					14.8 KiB	163
;;; Accept established connections											
2	accept	input								2881.1 KiB	27 160
3	accept	forward								6.6 GiB	7 456 791
;;; Accept related connections											
4	accept	input								0 B	0
5	accept	forward								171 B	3
;;; Local Input											
6	accept	input	192.168.1.0/24					!ether2		1451.7 KiB	17 741
;;; Accept Torrent											
7	accept	input			6 (tcp)		45000	ether2		720 B	18
;;; Drop invalid connections											
8	drop	input								19.9 KiB	256
9	drop	forward								1494.1 KiB	38 171
10	drop	input						ether2		367.3 MiB	5 759 800
;;; accept forward from local to internet											
11	accept	forward						!ether2	ether2	2178.1 KiB	35 633
;;; drop all other forward											
12	drop	forward								408.3 KiB	8 195

13 items

Настройка NAT в Mikrotik

Стоит до полноты картины добавить еще пару правил в закладке NAT. Первое непосредственно натит интернет из локалки, второе пробрасывает порт 45000 с внешнего интерфейса на торрент качалку с адресом 192.168.1.50

```
add chain=srcnat action=masquerade out-interface=ether2
add chain=dstnat action=dst-nat to-addresses=192.168.1.50 to-ports=45000 protocol=tcp in-interface=ether2 dst-port=45000
```



На этом все. Интернет лагать перестал. Стоит отметить, что я запретил все входящие подключения, кроме торрента. То есть удаленно моим mikrotik я управлять не смогу, все подключения закрыты firewall. Мне это просто не нужно. Если у вас есть такая потребность, то не забудьте разрешить входящие подключения в firewall для winbox.

И еще важное замечание. Я не рекомендую настраивать fierwall в mikrotik, да и не только в микротик удаленно. Я во время настройки ошибся и отключил себе доступ к устройству. Пришлось его ресетить и настраивать заново. Благо это не долго, не заняло много времени. Но имейте это ввиду. Лучше перед настройкой сделать backup, если вдруг ресетить придется :)

Онлайн курсы по Mikrotik

Если у вас есть желание научиться работать с роутерами микротик и стать специалистом в этой области, рекомендую пройти курсы по программе, основанной на информации из официального курса MikroTik Certified Network Associate. Помимо официальной программы, в курсах будут лабораторные работы, в которых вы на практике сможете проверить и закрепить полученные знания. Все подробности на сайте Курсы по ИТ. Стоимость обучения весьма демократична, хорошая возможность получить новые знания в актуальной на сегодняшний день предметной области.

Помогла статья? Есть возможность отблагодарить автора

Рекомендую полезные материалы по схожей тематике:

- Пример настройки роутера микротик с нуля для чайников.
- Как настроить блокировку сайтов штатными средствами роутера Mikrotik.
- Настраиваем wifi роуминг с помощью технологии capsman.
- Записываем логи Mikrotik на удаленный rsyslog сервер.
- Переключение канала интернет при использовании 2-х провайдеров в Микротик.