

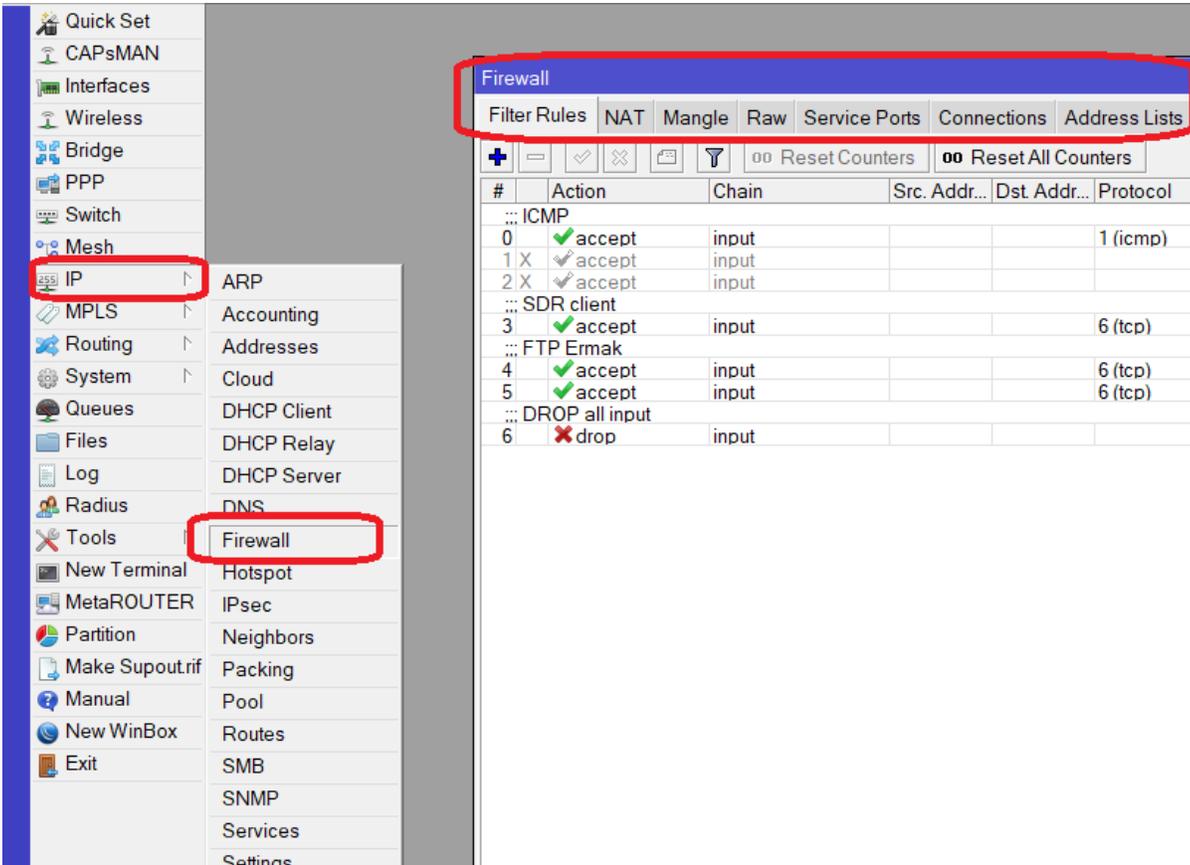
# Настройка роутеров MikroTik для удаленного доступа к трансиверу

Часто необходимо подключиться к трансиверу, находящемуся в локальной сети за NAT. Для этого необходимо:

- Получить у провайдера "белый" IP адрес. Обычно, за эту услугу надо ежемесячно вносить небольшую плату
- Подключить трансивер в домашней сети по статическому IP адресу.

Предположим, вы подключили трансивер по статическому IP адресу **192.168.0.130** и веб доступ настроили по порту **8072**

- Заходим на роутер через WinBox. Открываем меню IP-Firewall



- На вкладке NAT создать правило для проброса порта на ваш трансивер. Нажимаем плюсик и вводим значения полей, как показано на скриншотах. В данном примере **ether1** - ваша внутренняя сеть

NAT Rule <8072>



General   **Advanced**   Extra   Action   ...

Chain:  ▼

Src. Address:

Dst. Address:

Protocol:   ▲▼

Src. Port:

Dst. Port:   ▲▼

Any. Port:

In. Interface:   ▲▼

Out. Interface:

In. Interface List:

Out. Interface List:

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

Connection Type:

OK

Cancel

Apply

Disable

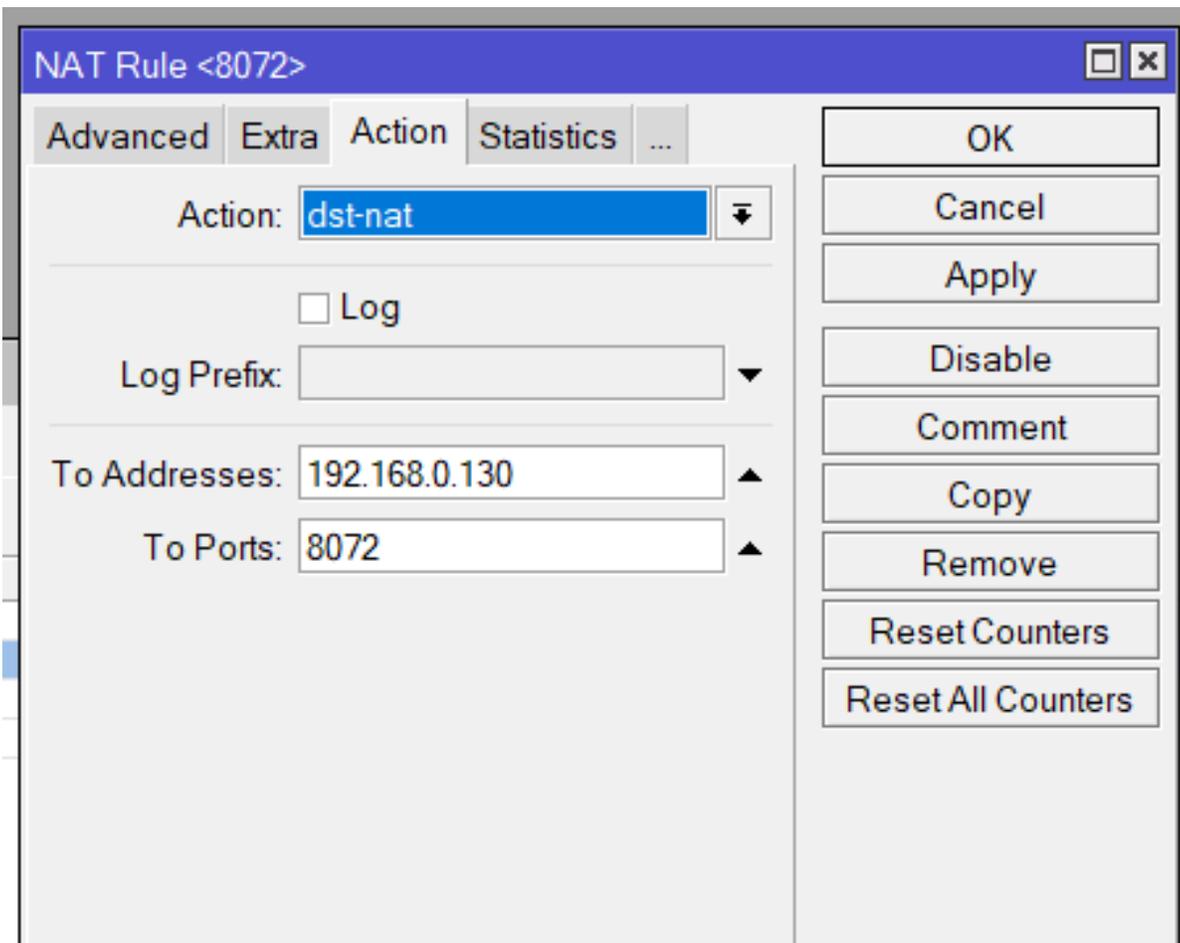
Comment

Copy

Remove

Reset Counters

Reset All Counters



- Нажимаем кнопку **Apply** и **OK**
- В результате - создано правило NAT

#	Action	Chain	Src. Addr...	Dst. Addr...	Prot...	Src. Port	Dst. Port	In. Inte...	Out. In...	Bytes	Packets
0	all	dstnat			6 (tcp)		8072	ether1	ether1	128.3 M...	731.000
1	dstnat	dstnat			6 (tcp)		8072	ether1	ether1	1184 B	23
2	dstnat	dstnat			6 (tcp)	2113-2140		ether1	ether1	2052 B	66
3	dstnat	dstnat			6 (tcp)	2112		ether1	ether1	496 B	10

- Создаем правило Firewall для разрешения доступа извне к вашему порту (8072 в нашем примере). Переходим во вкладку **Firewall**
- Нажимаем плюсики и вводим значения полей, как показано на скриншотах.

3025.2... 33 895  
0 B 0

Firewall Rule <8072>

General | Advanced | Extra | Action | Statistics

Chain:

Src. Address:

Dst. Address:

Protocol:  6 (tcp)

Src. Port:

Dst. Port:  8072

Any. Port:

P2P:

In. Interface:

Out. Interface:

In. Interface List:

Out. Interface List:

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

Connection Type:

Connection State:

Connection NAT State:

OK  
Cancel  
Apply  
Disable  
Comment  
Copy  
Remove  
Reset Counters  
Reset All Counters

Firewall Rule <8072>

General | Advanced | Extra | Action | Statistics

Action:

Log

Log Prefix:

OK  
Cancel  
Apply  
Disable  
Comment  
Copy  
Remove  
Reset Counters  
Reset All Counters

- Нажимаем кнопку **Apply** и **OK**
- В результате - создано правило firewall. Обязательно убедитесь, что созданное правило расположено выше правила **drop all**, которое запрещает подключение по всем внешним портам

1	✓	accept	input				
2	X	✓	accept	input			
... SDP client							
3	✓	accept	input		6 (tcp)		8072
... FTP Ernak							
4	✓	accept	input		6 (tcp)		2113-2140
5	✓	accept	input		6 (tcp)		2112
... DROP all input							
6	✗	drop	input				