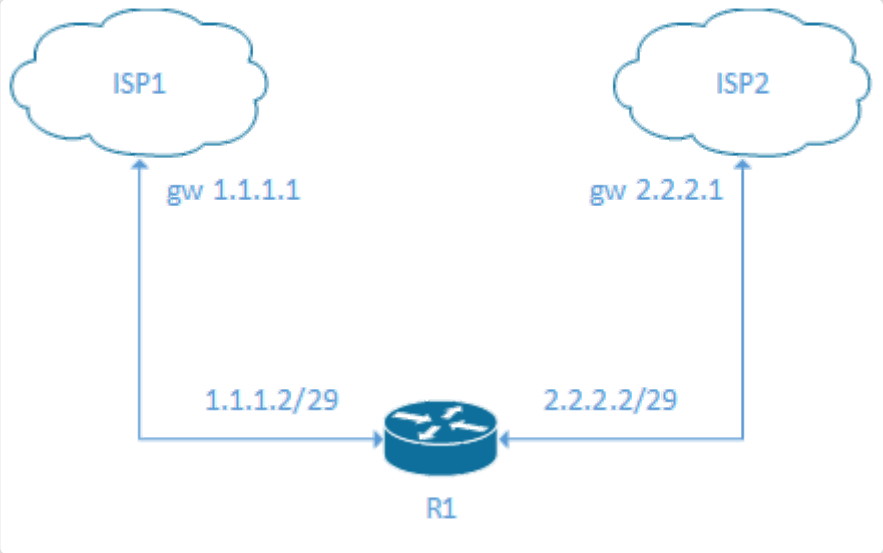
(https://vk.com/mikrotikrus)

MikroTik - Настройка нескольких провайдеров.

Очень часто ко мне обращаются с просьбой помочь в настройке двух и более провайдеров на одном устройстве.

Это статья посвящена только, настройке MikroTik на работу с двумя провайдерами.

Начнём конечно же с вводных данных, а именно нарисуем нашу схему сети.



Настроим IP адреса на интерфейсах

```
/ip address
add address=1.1.1.2/29 interface=ether1
add address=2.2.2.2/29 interface=ether2
```

Настроим NAT на интерфейсах провайдера

```
/ip firewall nat
add action=masquerade chain=srcnat out-interface=ether1
add action=masquerade chain=srcnat out-interface=ether2
```

Нам необходимо на маршрутизаторе обозначить соединения, которые пришли на каждый интерфейс отдельного провайдера.

Для трафика, который генерирует сам MikroTik по этим соединениям необходимо отправить в таблицу маршрутизации, которая будет отправлять трафик с того же интерфейса.

Создадим правила mangle для первого провайдера

```
/ip firewall mangle
add action=mark-connection chain=input in-interface=ether1 new-connection-mark=Input/ISP1
add action=mark-routing chain=output connection-mark=Input/ISP1 new-routing-mark=ISP1 passthr
ough=no
```

Создадим правила mangle для второго провайдера

```
/ip firewall mangle
add action=mark-connection chain=input in-interface=ether2 new-connection-mark=Input/ISP2
add action=mark-routing chain=output connection-mark=Input/ISP2 new-routing-mark=ISP2 passthr
ough=no
```

MikroTik с именованными таблицами маршрутизации работает по следующему принципу (Если маршрут в именованной таблице не найден, то ищем в таблице main), данное поведение не работает только с VRF, но это далеко за пределами данной статьи.

Нам необходимо гарантировать, что трафик уйдёт только с нужного интерфейса, ну а если не сможет (неактивный интерфейс), то от бросится самим маршрутизатором.

Создадим правила Route для первого провайдера

```
/ip route rule
add action=lookup-only-in-table routing-mark=ISP1 table=ISP1
```

Создадим правила Route для второго провайдера

```
/ip route rule
add action=lookup-only-in-table routing-mark=ISP2 table=ISP2
```

Осталось дело за малым. Настроить таблицу маршрутизации для двух провайдеров.

Создадим маршруты для наших провайдеров

```
/ip route
add distance=1 gateway=1.1.1.1 routing-mark=ISP1
add distance=1 gateway=2.2.2.1 routing-mark=ISP2
```

На этом этапе хотелось бы закончить, но вот незадача, у нас нету маршрута, под который бы попадал трафик самого MikroTik. (например, если маршрутизатор запросит DNS или обновления)

Ну и добавим изюминки будем следить за состоянием каналов с помощью рекурсивных маршрутов.

Добавим два адреса через которых мы будем строить рекурсивные запросы.

Я для этих целей использую Google DNS

```
/ip route
add distance=1 dst-address=8.8.4.4/32 gateway=2.2.2.1
add distance=1 dst-address=8.8.8.8/32 gateway=1.1.1.1
```

Ну и собственно сами рекурсивные маршруты, обратите внимание на target-scope

```
/ip route
add check-gateway=ping distance=10 gateway=8.8.8.8 target-scope=30
add check-gateway=ping distance=20 gateway=8.8.4.4 target-scope=30
```

Если вы всё правильно сделали, то в маршрутах вы должны увидеть что-то вроде

```
8.8.8.8 recursive via 1.1.1.1
```

Ну и собственно сами рекурсивные маршруты, обратите внимание на target-scope

Добавленно 29.12.2016

И так вроде всё хорошо и всё работает, но возникает ситуация, когда необходимо настроить разные IP туннели, например, GRE или IPIP с разных провайдеров, для этого нам необходимо указывать src адрес необходимого нам провайдера, но как мы все помним стандартный алгоритм выбора маршрута базируется на выборе адреса назначения (dst).

Нам необходимо сделать несколько действий.

Для начало добавить список bogon адресов, они нам необходимы для того чтобы исключить трафик в локальную сеть.

```
/ip firewall address-list
add list="BOGONS" address=0.0.0.0/8
add list="BOGONS" address=10.0.0.0/8
add list="BOGONS" address=100.64.0.0/10
add list="BOGONS" address=127.0.0.0/8
add list="BOGONS" address=169.254.0.0/16
add list="BOGONS" address=172.16.0.0/12
add list="BOGONS" address=192.0.0.0/24
add list="BOGONS" address=192.0.2.0/24
add list="BOGONS" address=192.168.0.0/16
add list="BOGONS" address=198.18.0.0/15
add list="BOGONS" address=198.51.100.0/24
add list="BOGONS" address=203.0.113.0/24
add list="BOGONS" address=224.0.0.0/3
```

И для каждого провайдера необходимо сделать по одному правилу. Для моей конфигурации они будут выглядеть так.

```
/ip firewall mangle
add action=mark-routing chain=output dst-address-list=!BOGONS new-routing-mark=ISP1 src-addre
ss=1.1.1.2
add action=mark-routing chain=output dst-address-list=!BOGONS new-routing-mark=ISP2 src-addre
ss=2.2.2.2
```

Добавленно 22.01.2017

Ну что же остался только один вопрос, как теперь настроить так чтобы **NAT** (проброс портов) работал корректно, иначе грош цена всей этой болтовне.

Проблема заключается в том, что, пробрасывая порт, трафик уже от хоста, на который пробрасывали порт, будет уходить в маршрут по умолчанию **0.0.0.0/0** в таблице **main**.

Нас конечно такой расклад не устраивает и будет настраивать **RouterOS** так чтобы он гарантированно направлял трафик обратно в тот же провайдер, с которого и прилетел.

Для начала нам понадобится промаркировать соединение, которое попадает под NAT.

```
/ip firewall mangle
add action=mark-connection chain=prerouting in-interface=ether1 new-connection-mark=Forward/I
SP1
add action=mark-routing chain=prerouting connection-mark=Forward/ISP1 in-interface=!ether1 ne
w-routing-mark=ISP1 passthrough=no
```

И для второго провайдера.

```
/ip firewall mangle
add action=mark-connection chain=prerouting in-interface=ether2 new-connection-mark=Forward/I
SP2
add action=mark-routing chain=prerouting connection-mark=Forward/ISP2 in-interface=!ether2 ne
w-routing-mark=ISP2 passthrough=no
```

Разберём, что мы тут делаем, собственно.

Так как цепочку input мы уже использовали на этом интерфейсе, то остаётся только **prerouting** именно в эту цепочку попадёт весь трафик, который будет попадать под правила **NAT**, данный коннект мы просто будем маркировать с именем **Forward/ISP1**.

Вторым правилом, мы выбираем весь трафик который идёт по маркированному соединению и не приходит с того же интерфейса что и провайдер, это необходимо для того чтобы правило не применилось уже к новому трафику. И такой трафик отправляем в именованную таблицу маршрутизации нужного нам провайдера.

Ну что же теперь вы можете спокойно настроить двух и более провайдеров, а также настроить **NAT** и пробросить порты до ваших локальных сервисов.

Иван Верес
Огромное спасибо!!!!! Настроил 2 провайдера и NAT через них.
15 ноя 2018 Комментировать

Роман Григорьев
может кто подскажет... суть проблемы такая, есть микротик, к нему подключены 2 компьютера, микр
компьютер выходил в интернет через свой l2tp
3 сен 2018 Комментировать

Павел Долженков
Годно. Спасибо.
13 мая 2018 Комментировать

Алексей Щур
Здравствуйте, подскажите, как реализовать, есть ipsec туннель, при недоступности основного канала
доступности основного обратно?
3 апр 2018 Комментировать

Николай Дятлов
Спасибо за инструкцию, много раз уже использовал.
Но ... тут назрел вопрос, а если мне нужно, что бы допустим на определенный пул адресов исходящий
Тут я понимаю, что можно указать банально роутами.
А если есть доменные имена, которые я могу вбить в адрес лист?
Возьмем для примера cloud.mikrotik.com, на одном из провайдеров у меня белый адрес, как сделать т
2 дек 2017 Комментировать

Александр Эри
/ip route rule
add action=lookup-only-in-table routing-mark=ISP1 table=ISP1

Интересный момент. В табле ISP1 у Вас нет конектед маршрутов, как ответный трафик попадет клиен
22 окт 2017 Комментировать

Александр Селищев
Тоже хочется пояснения, вы пишите (...у нас нету маршрута, под который бы попадал трафик самого N
Так он всё таки есть в примере или нет, я что то не нахожу!?
3 окт 2017 Комментировать

Василий Безфамильный
Немного не понял, а при падении одного из ISP, трафик пойдёт по второму маршруту, и после восстан
заданным правилам?
26 апр 2017 Комментировать

Максим Лобков
Спасибо, Кирилл. Последнее добавление особо полезное оказалось.
5 апр 2017 Комментировать

Александр Герасимов
А как же быть с DHCP & PPPOE ?
17 янв 2017 Комментировать

Контакты

vasilevkirill.com
г. Санкт-Петербург

T: (Phone)+7 (905) 207-3578
Мы работаем ежедневно с 10:00 до 18:00
Васильев Кирилл
me@vasilevkirill.com (mailto:me@vasilevkirill.com)

- Вконтакте (https://vk.com/vasilevkirill)
- Telegram (https://telegram.me/vasilevkirill)
- Хабра (https://habrahabr.ru/users/vasilevkirill/)
- Google Plus (https://plus.google.com/109858078981317921081)
- Города (/city)