

MikroTik.Me

MikroTik.Me

- Васильев Кирилл
- Санкт-Петербург
- Курсы MikroTik
- Поддержка
- Разработка ПО
- Продажа



MikroTik.Me

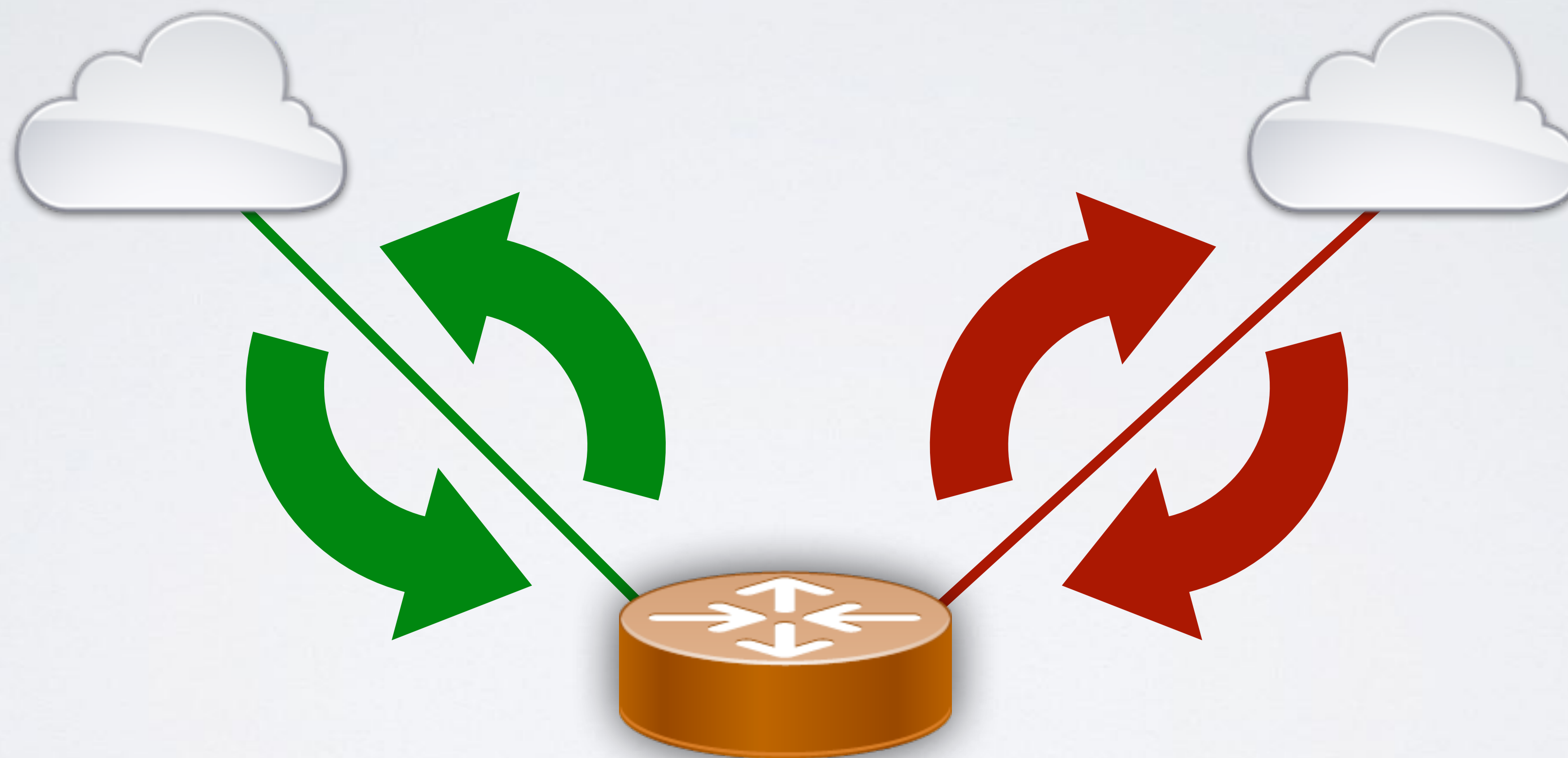


Настройка RouterOS для одновременной работы с несколькими провайдерами

Multiwan

- Обеспечить доступ к маршрутизатору
- Организовать правильный выход с маршрутизатора
- Одновременный доступ к ресурсам «за» NAT
- Распределение нагрузки по каналам

Доступ к маршрутизатору



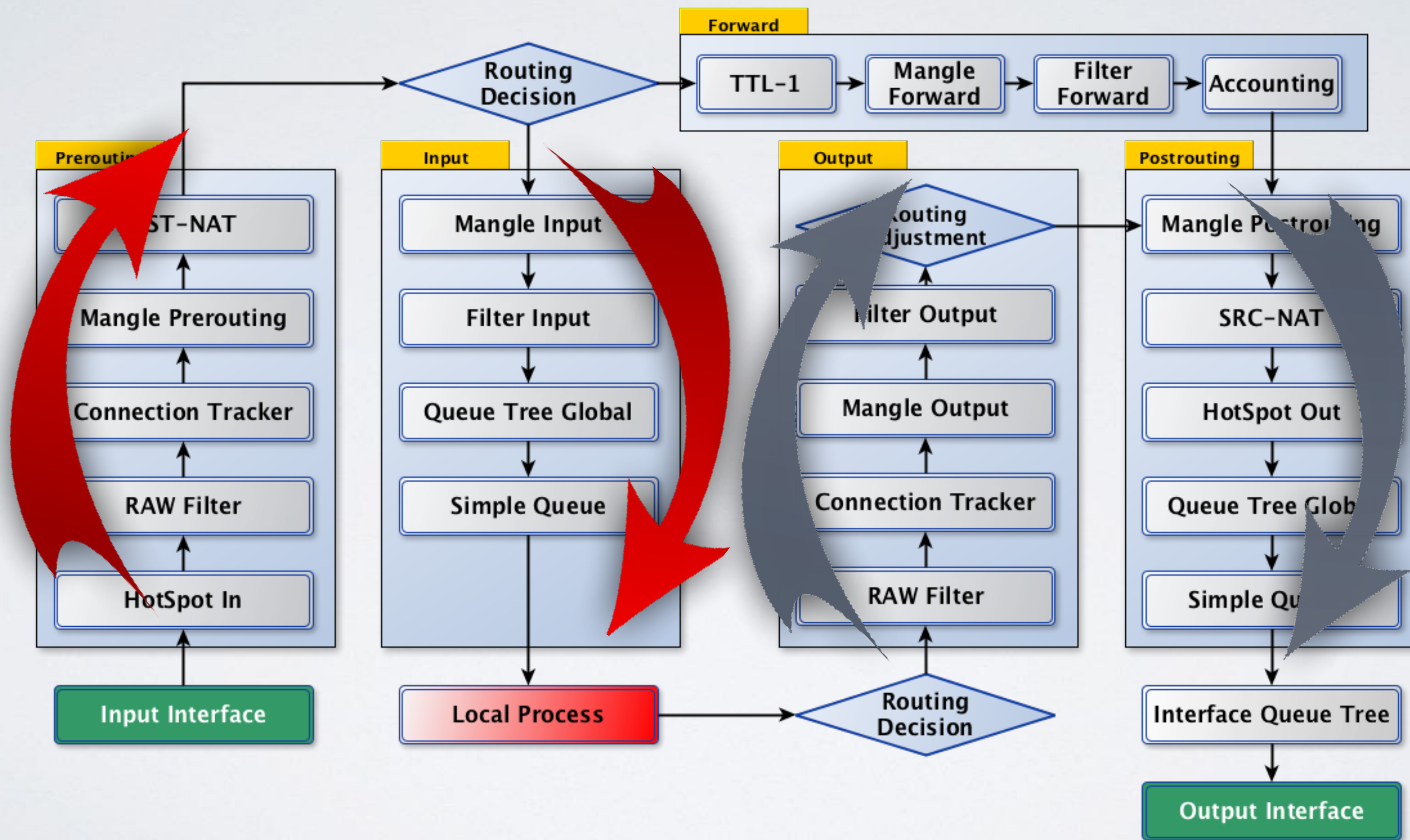
Доступ к маршрутизатору

- Управление маршрутизатором
 - WinBox, ssh, snmp, icmp etc...
- Нормальная работа VPN
 - Point-to-Point и IP Туннели, а также IPSec
- А также другие сервисы CPU

Доступ к маршрутизатору

- Необходимо обеспечить выход с того же самого интерфейса, с которого пришёл трафик

Выход с маршрутизатора



Доступ к маршрутизатору

- Цепочка **Prerouting**
- Маркируйте соединение на входе в маршрутизатор
- Учитывайте в маркировке **каждый шлюз**
- Учитывайте в маркировке интерфейс провайдера
- Только для пакетов **connection-state=new**
- Для удобства именуруйте соединения с учётом IP адреса шлюза
- **«Prerouting/GW/I.I.I.I»**

Доступ к маршрутизатору

- На выходе **из** маршрутизатора, все пакеты в именованном соединении отправляем в отдельную таблицу маршрутизации
- Трафик должен вернуться в тот же интерфейс маршрутизатора, с которого пришёл
- Данный трафик должен уйти с тем же **source** адресом, на который **destination** адрес он пришёл

Доступ к маршрутизатору

ISP 1

```
/ip firewall mangle
```

```
add chain=prerouting dst-address=1.1.1.0/29 in-interface=ether1 \  
connection-state=new action=mark-connection \  
new-connection-mark=Prerouting/GW/1.1.1.1 passthrough=no
```

```
add chain=output connection-mark=Prerouting/GW/1.1.1.1 \  
action=mark-routing new-routing-mark=Next-Hop/1.1.1.1 \  
passthrough=no
```

Доступ к маршрутизатору

- Создайте таблицу маршрутизации, где уникальность маршрута определяется не IP адресом, а адресом nexthop
- Данная таблица должна **«смотреть только в себя»**
- Проверка доступности шлюза **check-gateway** не имеет смысла

Доступ к маршрутизатору

ISP 1

/ip route

add gateway=1.1.1.1 routing-mark=Next-Hop/1.1.1.1

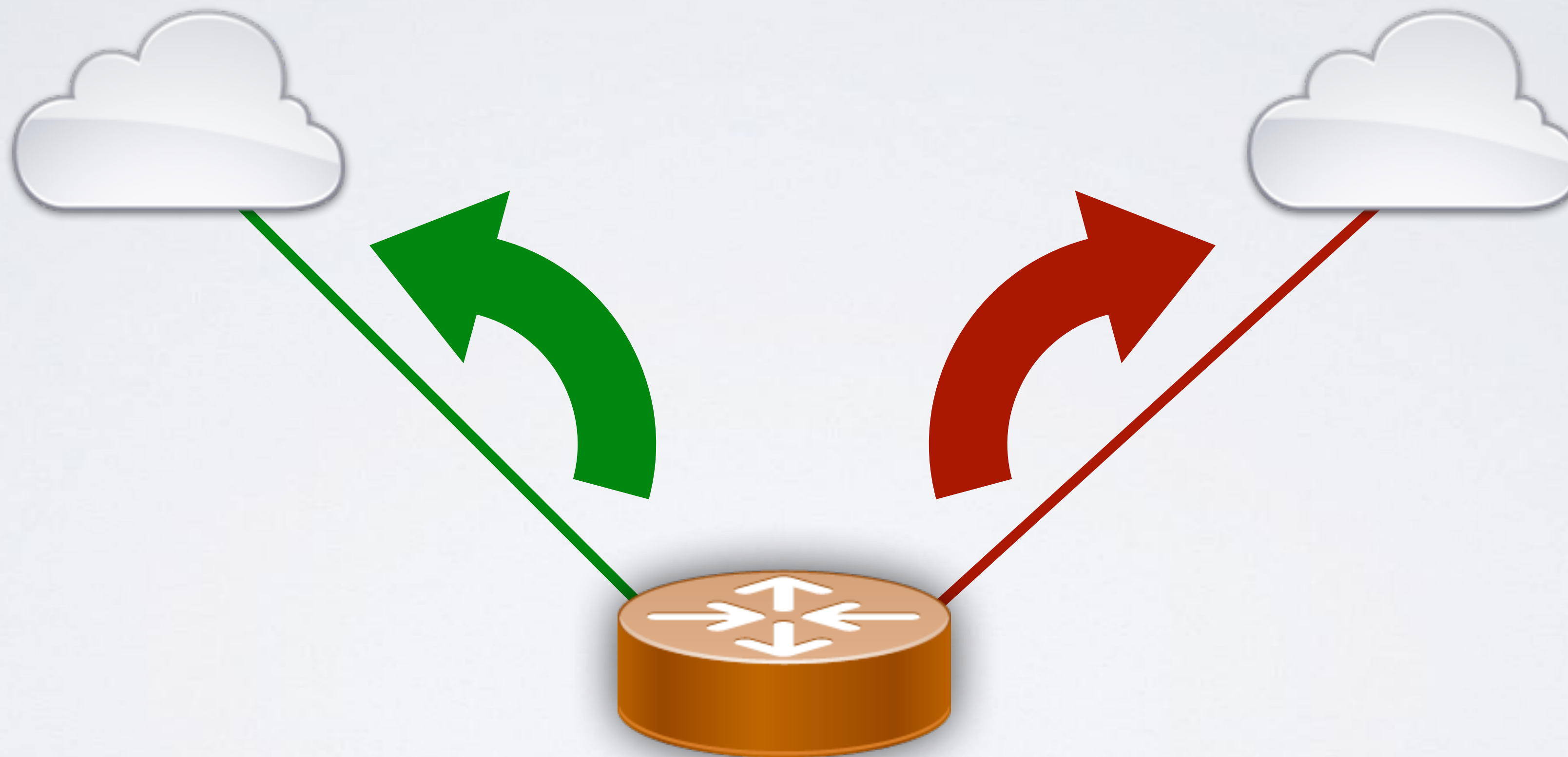
/ip route rule

**add action=lookup-only-in-table routing-mark=Next-Hop/1.1.1.1 \
table=Next-Hop/1.1.1.1**

Доступ к маршрутизатору

- Нет необходимости **NAT**ить данный трафик

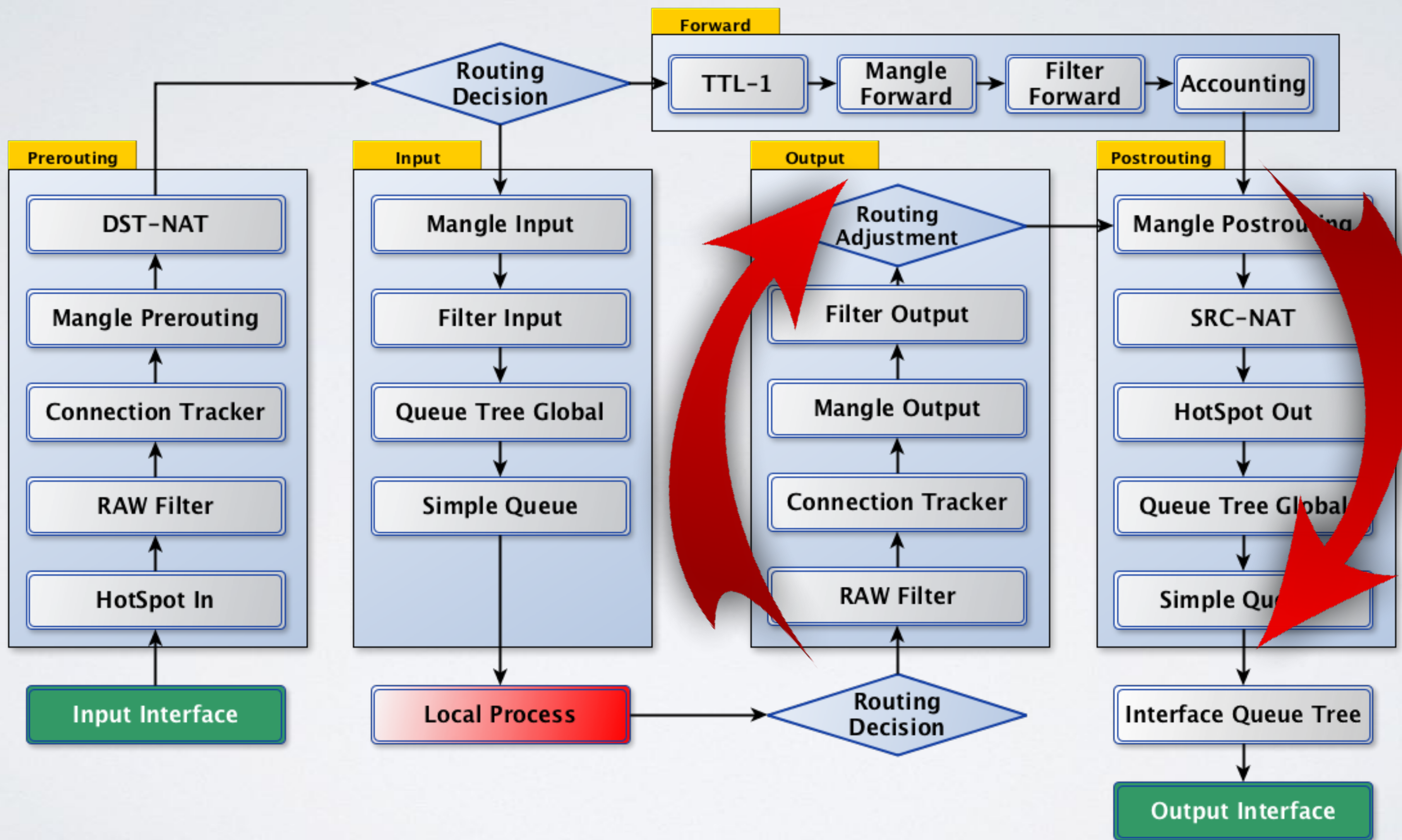
Выход с маршрутизатора



Выход с маршрутизатора

- Подключение к внешним сервисам с маршрутизатора
- VPN, IP Туннели и IPSec
- Функционал RouterOS, где можно указать source или local адрес

Выход с маршрутизатора



Выход с маршрутизатора

- Цепочка **Output**
- Нет возможности определить исходящий интерфейс, для определения внутрисетевого трафика
- Используйте префиксы BOGON для **исключения** внутрисетевого трафика
- Учитывайте **каждую** подсеть
- Используйте существующую именную таблицу маршрутизации

Bogon / RFC5735

0.0.0.0/8	192.0.0.0/24	198.51.100.0/24
10.0.0.0/8	192.0.2.0/24	203.0.113.0/24
127.0.0.0/8	192.88.99.0/24	224.0.0.0/4
169.254.0.0/16	192.168.0.0/16	240.0.0.0/4
172.16.0.0/12	198.18.0.0/15	255.255.255.255/32

Выход с маршрутизатора

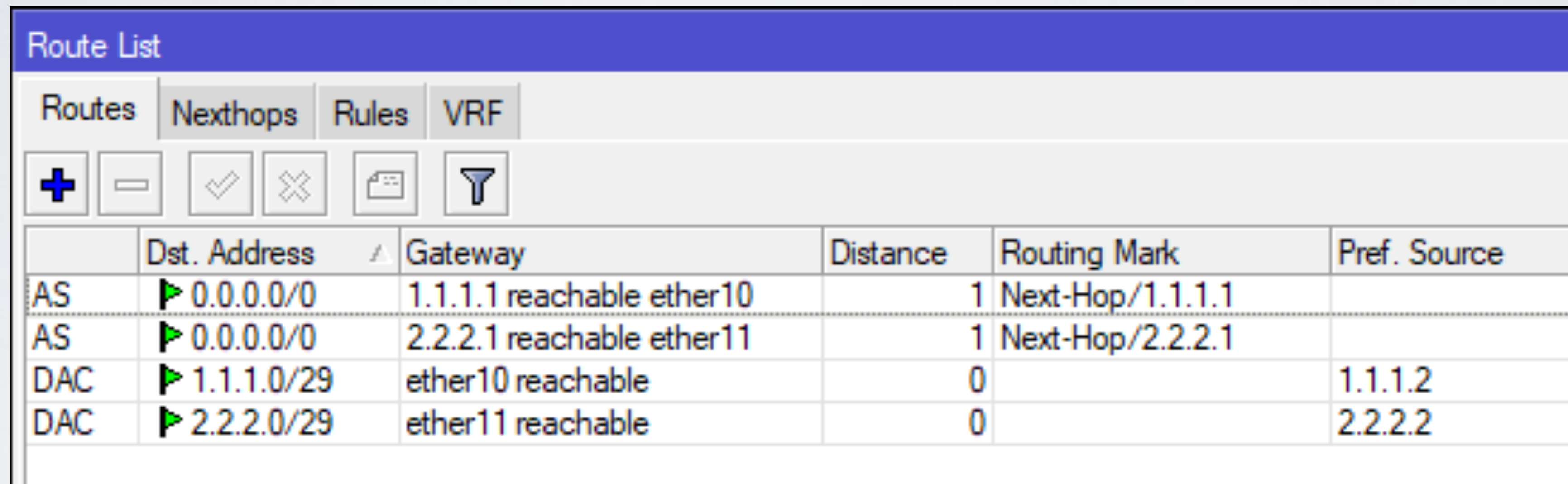
```
/ip firewall mangle
```

```
add chain=output src-address=1.1.1.0/29 dst-address-list=!BOGON \  
    action=mark-routing new-routing-mark=Next-Hop/1.1.1.1 \  
    passthrough=no
```

Выход с маршрутизатора

- Нет необходимости **NAT**ить данный трафик

Выход с маршрутизатора

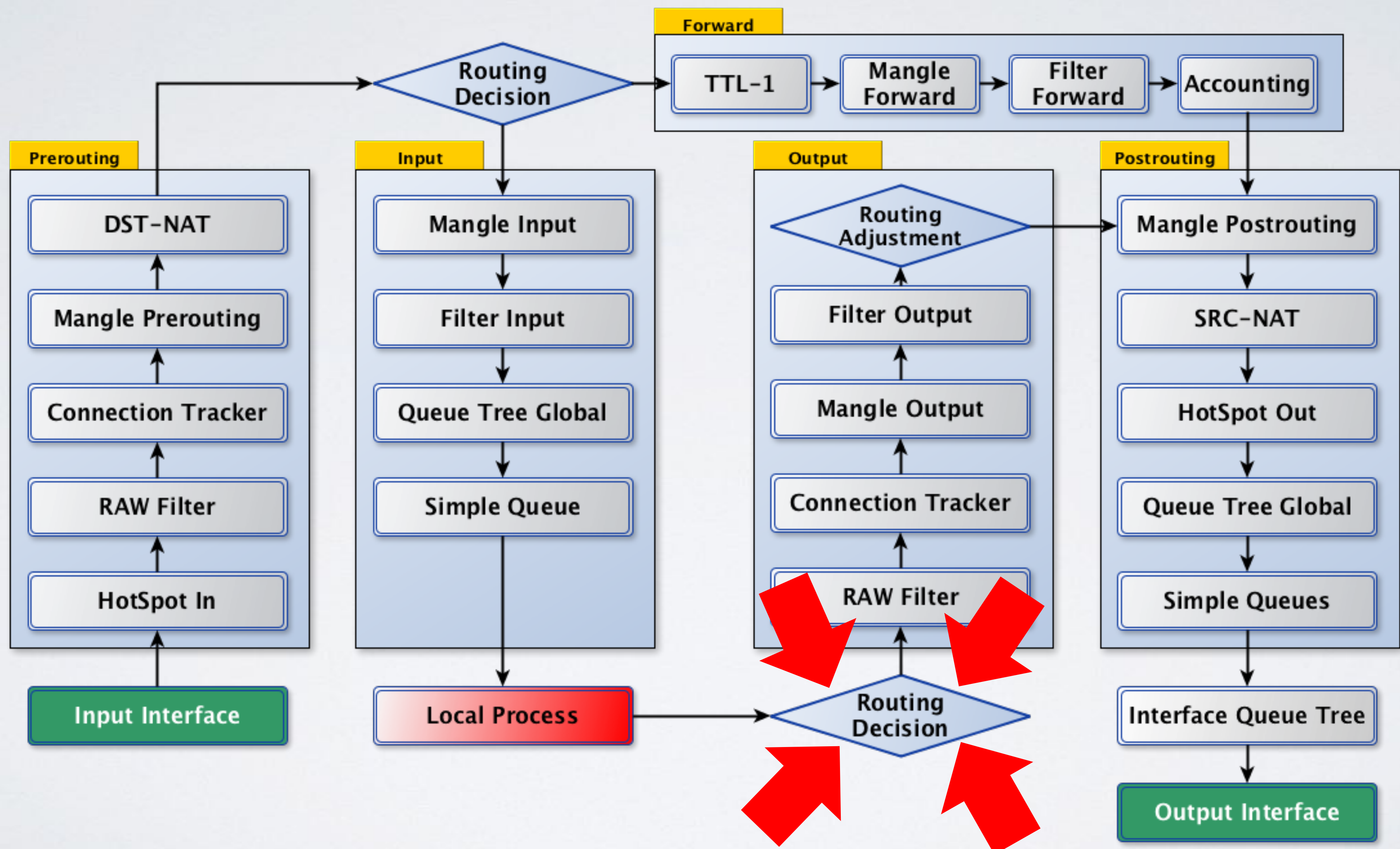


The screenshot shows the 'Route List' window in MikroTik WinBox. It features a blue header bar with the title 'Route List'. Below the header are four tabs: 'Routes' (selected), 'Nexthops', 'Rules', and 'VRF'. A toolbar contains icons for adding (+), removing (-), checking (✓), unchecking (✗), refreshing (refresh icon), and filtering (funnel icon). The main area is a table with the following columns: 'AS', 'Dst. Address', 'Gateway', 'Distance', 'Routing Mark', and 'Pref. Source'. The table contains four rows of data.

	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
AS	▶ 0.0.0.0/0	1.1.1.1 reachable ether10	1	Next-Hop/1.1.1.1	
AS	▶ 0.0.0.0/0	2.2.2.1 reachable ether11	1	Next-Hop/2.2.2.1	
DAC	▶ 1.1.1.0/29	ether10 reachable	0		1.1.1.2
DAC	▶ 2.2.2.0/29	ether11 reachable	0		2.2.2.2

Достаточно ли данных настроек для управления маршрутизатором?

Выход с маршрутизатора



Выход с маршрутизатора

- Необходим unicast **активный** маршрут в таблице **MAIN**
- Используйте пустой **Bridge**, как **loopback** интерфейс
- Создайте **default route** через **loopback** интерфейс
- Укажите максимальную рабочую distance для маршрута
- Используйте **pref-src** для определения src IP адреса остального трафика

Выход с маршрутизатора

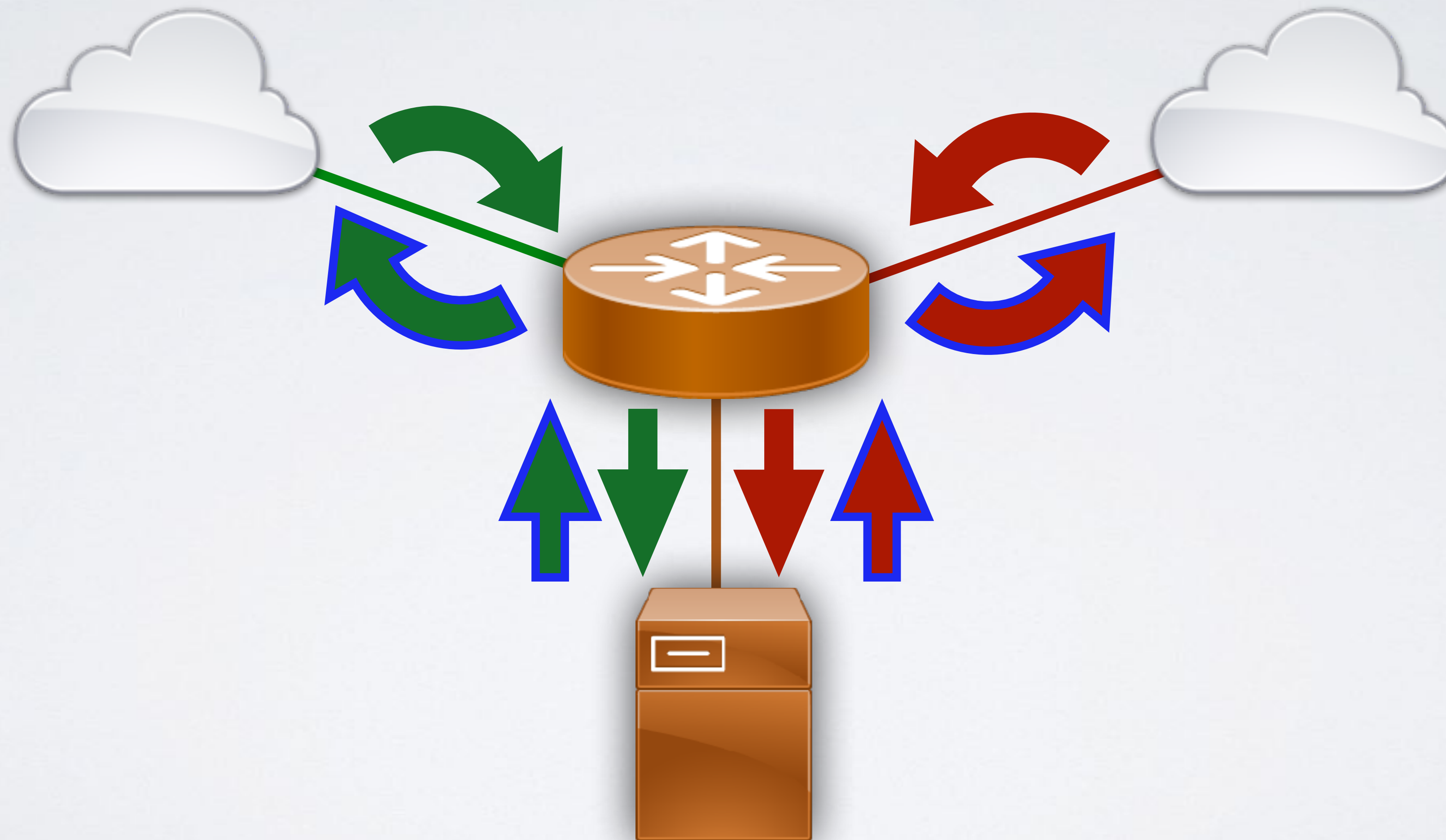
```
/interface bridge
```

```
add name=Br-Loopback
```

```
/ip route
```

```
add gateway=Br-Loopback distance=254 pref-src=1.1.1.2
```

Доступ «за» NAT



Доступ «за» NAT

- Одновременный доступ к внутренним сервисам
- CDN, SMTP, WEB, etc...
- **DNS Round Robin**, как вариант распределения внешней нагрузки на каналы, современные браузеры замечательно работают с данной технологией и отрабатывают отказ

Доступ «за» NAT

Настройте dst NAT так, как обычно это делаете

Доступ «за» NAT

- Уже существует маркированное соединение
- Цепочка **Prerouting**
- **Исключите** интерфейс провайдера из фильтра
- Отправляется в именную таблицу маршрутизации

Доступ «за» NAT

```
/ip firewall nat
```

```
add chain=dstnat dst-address=1.1.1.2 protocol=tcp \  
    dst-port=80,25,443 in-interface=ether1 action=dst-nat \  
    to-addresses=192.168.1.2
```

```
/ip firewall mangle
```

```
chain=prerouting in-interface=!ether1 \  
connection-mark=Prerouting/GW/1.1.1.1 \  
action=mark-routing new-routing-mark=Next-Hop/1.1.1.1 \  
passthrough=no
```

Доступ «за» NAT

Нет необходимости **NAT**ить данный трафик

За вас это сделает **connection-tracker**

Доступ «за» NAT

Connection <5.19.245.3->1.1.1.1:80>

General Statistics

Src. Address: 5.19.245.3:65207

Dst. Address: 1.1.1.1:80

Reply Src. Address: 192.168.0.100:80

Reply Dst. Address: 5.19.245.3:65207

Protocol: 6 (tcp)

Connection Type:

Connection Mark:

Timeout: 23:59:53

TCP State: established

OK

Remove

expected seen reply assured confirmed dying fasttrack srcnat dstnat

Доступ «за» NAT

Connection <5.19.245.3->1.1.1.1:80>

General Statistics

Src. Address: 5.19.245.3:65207

Dst. Address: 1.1.1.1:80

Reply Src. Address: 192.168.0.100:80

Reply Dst. Address: 5.19.245.3:65207

Protocol: 6 (tcp)

Connection Type:

Connection Mark:

Timeout: 23:59:53

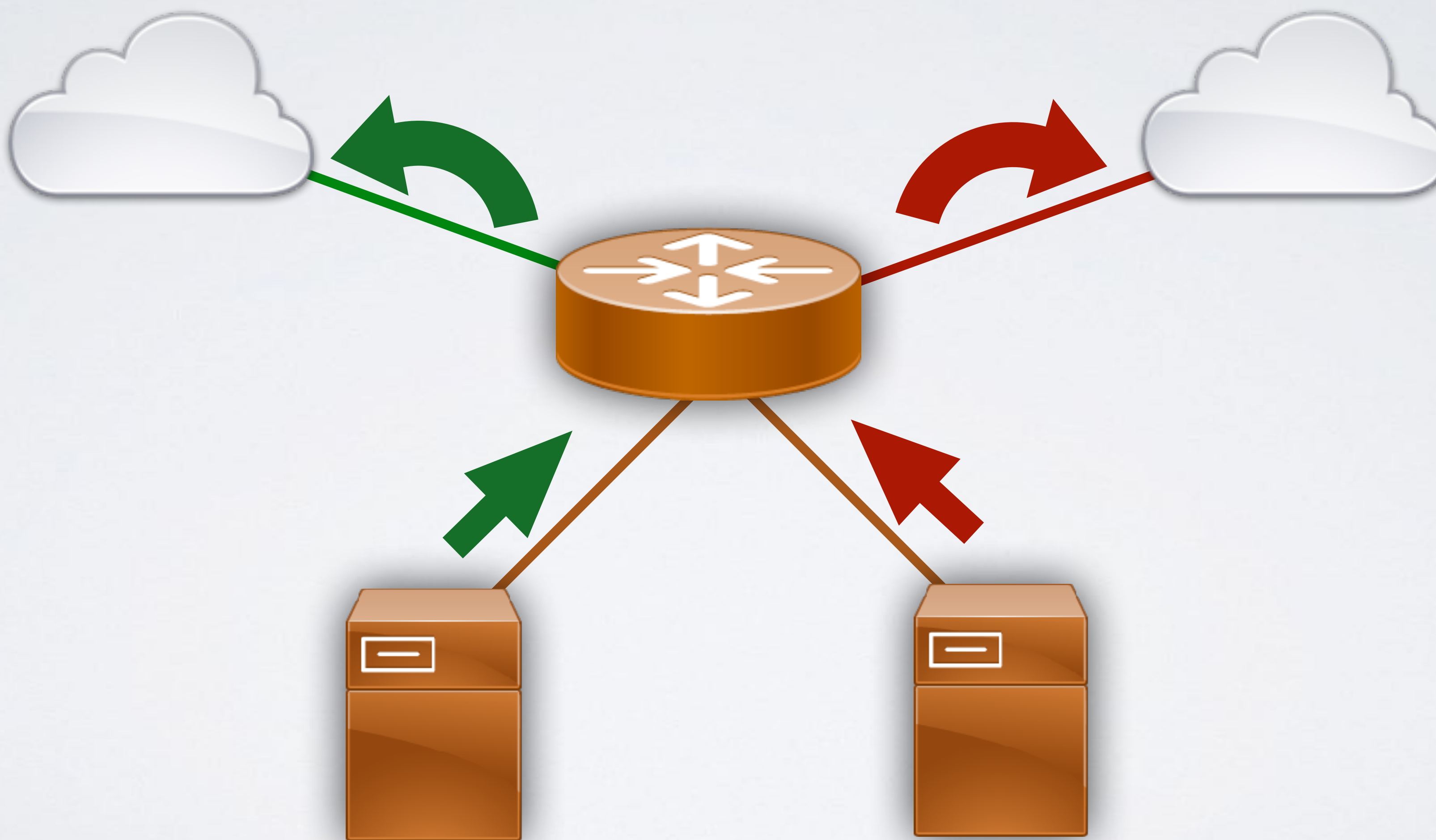
TCP State: established

OK

Remove

expected seen reply assured confirmed dying fasttrack srcnat dstnat

Предопределить IP Адрес



Предопределить IP Адрес

- Выход хоста из под определённого IP адреса
- Позволяет организовать работу сложных протоколов или IP зависимых сервисов
- Asterisk, банкинг, IPsec с внутренних хостов
etc...

Предопределить IP Адрес

- Цепочка **Prerouting**
- Используйте **address-list** для определения списка хостов
- Адрес листы именуйте информативно «**via\1.1.1.2**»
- Количество внутрисетевых интерфейсов, может быть больше чем один
- Используйте **Bogon** адрес лист для исключения внутрисетевого трафика

Предопределить IP

ISP 1

Адрес

```
/ip firewall mangle
```

```
add chain=prerouting src-address-list=via/1.1.1.2 \  
    dst-address-list=!BOGONS action=mark-routing \  
    new-routing-mark=Next-Hop/1.1.1.1 passthrough=no
```

```
/ip firewall nat
```

```
add chain=srcnat routing-mark=Next-Hop/1.1.1.1 \  
    src-address-list=via/1.1.1.2 action=src-nat \  
    to-addresses=1.1.1.2
```

Предопределить IP Адрес

Необходимо настроить src NAT для данного
типа трафика

Load Balance

- Распределить нагрузку по каналам
- Обеспечить выход с необходимого IP адреса

Load Balance

- Per-connection-classifier
- Nth
- Random
- ECMP

Load Balance / ECMP

- Equal-cost multi-path
- Round Robin
- Позволяет распределить нагрузку между next-hop
- Очень простой в настройке
- **10 минут хранит в кэше выбор шлюза**
- Используйте главную таблицу маршрутизации

Load Balance / ECMP

/ip route

add gateway=1.1.1.1,2.2.2.1 pref-src=1.1.1.2

ИЛИ

add gateway=1.1.1.1,2.2.2.1,2.2.2.1 pref-src=1.1.1.2

**нельзя просто так взять и настроить
ЕСМР**

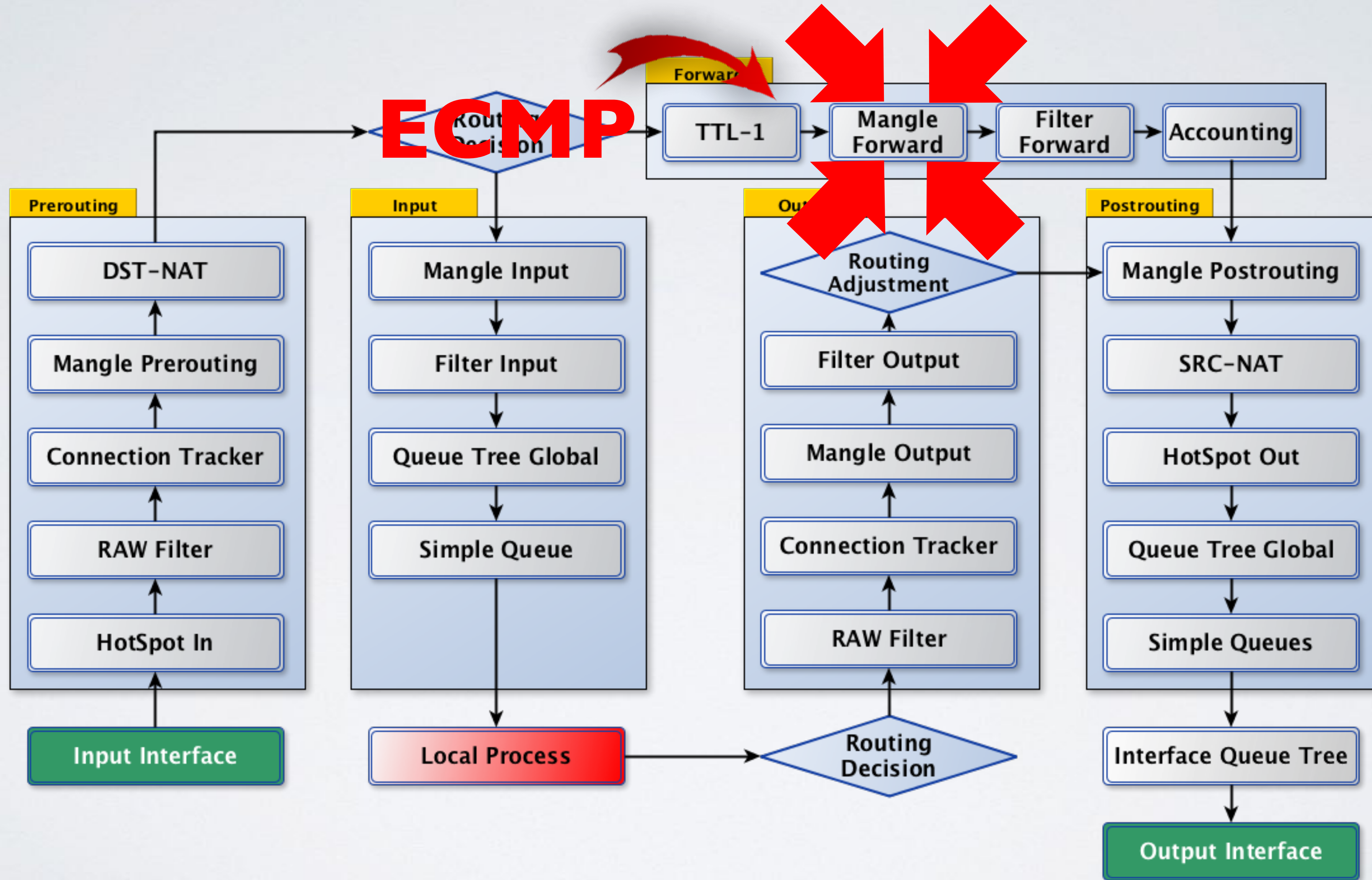


Через NAT

Load Balance / ECMP

Необходимо убрать ограничение 10 минут

Load Balance / ECMP



Load Balance / ECMP

- Цепочка **forward**
- Только для **connection-state=new**
- Учитывайте таблицу маршрутизации
- Учитывайте исходящий интерфейс

Load Balance / ECMP

- Цепочка **Prerouting**
- Только для маркированных соединений
- Используйте ранее созданную таблицу маршрутизации

Load Balance / ECMP

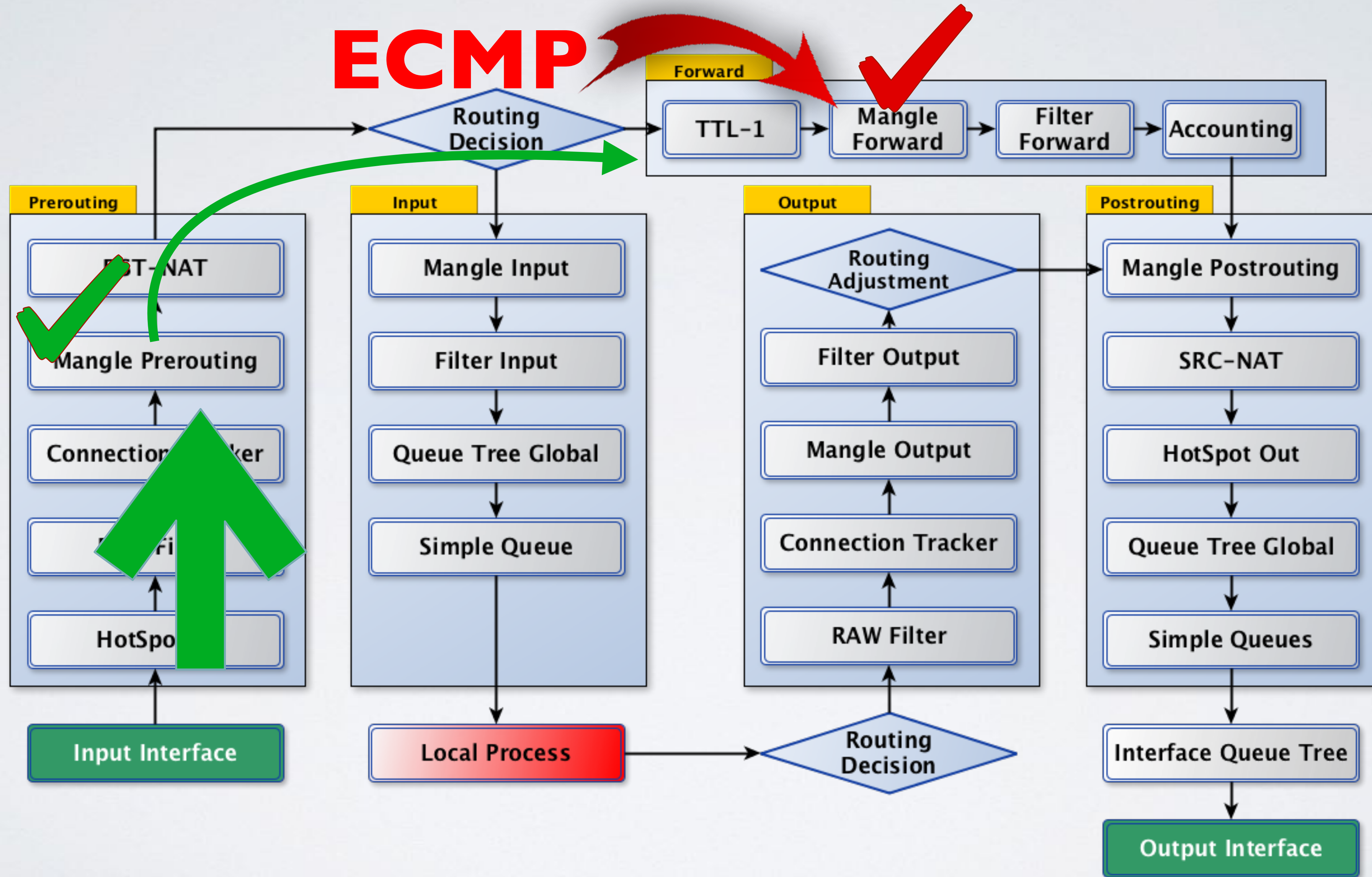
ISP 1

```
/ip firewall mangle
```

```
add chain=forward connection-state=new \  
    out-interface=ether1 routing-table=main \  
    action=mark-connection \  
    new-connection-mark=ECMP/1.1.1.2 passthrough=no
```

```
add chain=prerouting in-interface=!ether1 \  
    connection-mark=ECMP/1.1.1.2 action=mark-routing \  
    new-routing-mark=Next-Hop/1.1.1.1 passthrough=no
```

Load Balance / ECMP



Load Balance / ECMP

Необходимо настроить src NAT для данного типа трафика

Load Balance / ECMP

ISP 1

```
/ip firewall nat
```

```
add action=src-nat chain=srcnat connection-mark=ECMP/1.1.1.2 \  
to-addresses=1.1.1.2
```

Load Balance

Random

Load Balance / Random

- Правила в firewall терминирующие
- Рассчитайте правильно процентное соотношение
- Учитывайте в расчёте уже отфильтрованные проценты
- Только для **connection-state=new**

Load Balance / Random

ISP 1

```
/ip firewall mangle
```

```
add chain=prerouting connection-state=new random=30 \  
src-address-list=BOGONS dst-address-list=!BOGONS \  
connection-mark=no-mark action=mark-connection \  
new-connection-mark=RND/1.1.1.2 passthrough=YES
```

```
add chain=prerouting in-interface=!ether1 \  
connection-mark=RND/1.1.1.2 action=mark-routing \  
new-routing-mark=Next-Hop/1.1.1.1 passthrough=no
```


Load Balance / Random

ISP 2

```
/ip firewall mangle
```

```
add chain=prerouting connection-state=new \  
    src-address-list=BOGONS dst-address-list=!BOGONS \  
    connection-mark=no-mark action=mark-connection \  
    new-connection-mark=RND/2.2.2.2 passthrough=YES
```

```
add chain=prerouting in-interface=!ether2 \  
    connection-mark=RND/2.2.2.2 action=mark-routing \  
    new-routing-mark=Next-Hop/2.2.2.1 passthrough=no
```

Load Balance / Random

Необходимо настроить src NAT для данного типа трафика

Load Balance / Random

```
/ip firewall nat
```

```
add action=src-nat chain=srcnat connection-mark=RND/1.1.1.2 \  
to-addresses=1.1.1.2
```

```
add action=src-nat chain=srcnat connection-mark=RND/2.2.2.2 \  
to-addresses=2.2.2.2
```

Load Balance / Random

Пример расчёта

20Mbps / 10Mbps / 5Mbps

100% = 35Mbps

57% / 28% / 15%

Load Balance / Random

- Первое правило **random=15** (5Mbps)

$$20 + 10 \text{Mbps} = 100\%$$

- Второе правило **random=33** (10Mbps)
- Третье правило, без random (20Mbps)

Вопросы?

- MikroTik.Me
- VasilevKirill.com
- <https://t.me/mikrotikme>
- <https://vk.com/mikrotikrus>