

Solution.
Production.
Warranty.

Официальный
дистрибьютор Mikrotik
В России

8 800 700 97 66
www.spw.ru info@spw.ru

РЕАЛИЗАЦИЯ MULTIWAN. ВОПРОСЫ, ПРОБЛЕМЫ И РЕШЕНИЯ

АВТОР ДОКЛАДА: ИЛЬЯ КНЯЗЕВ

Об авторе

- Илья Николаевич Князев
- г. Санкт-Петербург, Россия
- Технический директор компании spw.ru
- Сертифицированный тренер Mikrotik
- Сертификаты МТСНА, МТСТСЕ, МТСВЕ, МТСУМЕ, МТСРЕ, МТСИНЕ, МТСIPv6E

SPW



Solution.
Production.
Warranty.

Официальный
дистрибьютор Mikrotik
В России

8 800 700 97 66
www.spw.ru info@spw.ru

Зачем нужен MultiWAN

- Для резервирования подключения к Интернет через нескольких провайдеров
- Для распределения нагрузки между несколькими провайдерами
- Для доступа к маршрутизатору через несколько внешних каналов



Solution.
Production.
Warranty.

Официальный
дистрибьютор Mikrotik
В России

8 800 700 97 66
www.spw.ru info@spw.ru

В чем сложность настройки?

- Маршрутизация, маркировка пакетов в Mangle и NAT являются независимыми процессами RouterOS
- Без понимания их взаимосвязей невозможно добиться правильной настройки и корректной работы маршрутизатора
- Существует конечное количество основных ошибок, которые встречаются в различных вариантах



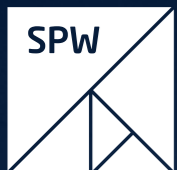
Solution.
Production.
Warranty.

Официальный
дистрибьютор Mikrotik
В России

8 800 700 97 66
www.spw.ru info@spw.ru

Основные этапы реализации

- Обеспечить чтобы маршрутизатор отвечал с того же интерфейса на который пришел пакет снаружи
- Обеспечить корректное распределение трафика между WAN-интерфейсами
- Обеспечить корректное построение туннелей при их наличии
- Не совершить типовых ошибок при настройке
- Решить нестандартные ситуации



Solution.
Production.
Warranty.

Официальный
дистрибьютор Mikrotik
В России

8 800 700 97 66
www.spw.ru info@spw.ru

Ответ маршрутизатора с правильного интерфейса

- Основная проблема связана с тем, что пакет приходит на один из интерфейсов маршрутизатора, а маршрутизатор может ответить с другого интерфейса, если имеется более выгодный маршрут
- Например если пакет придет снаружи на адрес 2.2.2.2 маршрутизатора, он ответит с адреса 1.1.1.2

```
[admin@MikroTik] > /ip route print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
#      DST-ADDRESS      PREF-SRC      GATEWAY      DISTANCE
0  S  0.0.0.0/0          1.1.1.1          1
1  S  0.0.0.0/0          2.2.2.1          2
2  ADC 1.1.1.0/30         1.1.1.2          ether1-WAN1      0
3  ADC 2.2.2.0/30         2.2.2.2          ether2-WAN2      0
4  ADC 192.168.1.0/24    192.168.1.163   ether3-LAN       0
```

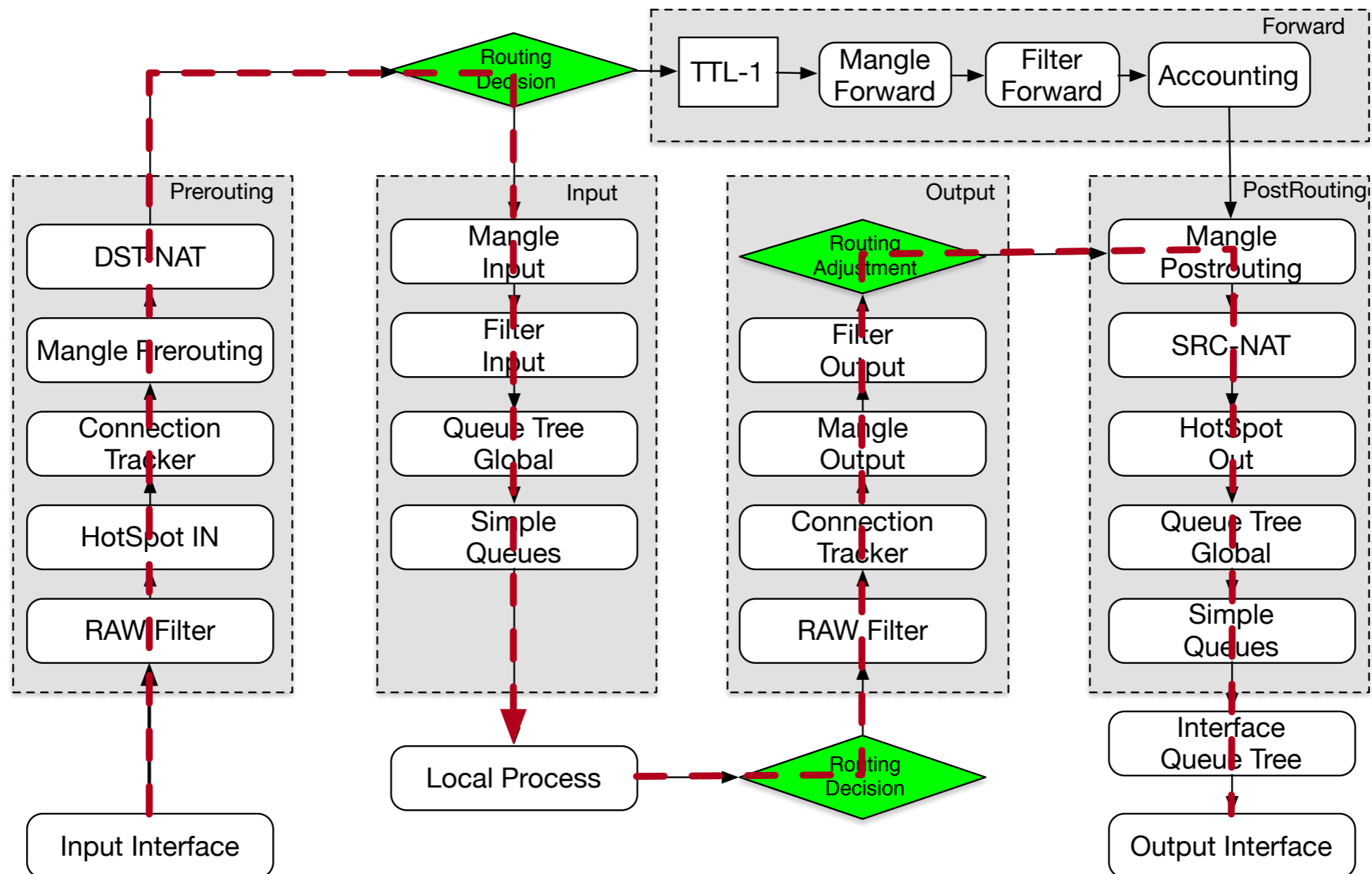


Solution.
Production.
Warranty.

Официальный
дистрибьютор Mikrotik
в России

8 800 700 97 66
www.spw.ru info@spw.ru

Ответ маршрутизатора с правильного интерфейса



Solution.
Production.
Warranty.

Официальный
дистрибьютор Mikrotik
в России

8 800 700 97 66
www.spw.ru info@spw.ru

Ответ маршрутизатора с правильного интерфейса

- Для изменения порядка выбора маршрута в RouterOS ВОЗМОЖНО
- Маркировать маршрут в Mangle (только цепочки Prerouting и Output)
- Воспользоваться командой `/ip route rule`
- Воспользоваться `action=route` в mangle prerouting



Solution.
Production.
Warranty.

Официальный
дистрибьютор Mikrotik
В России

8 800 700 97 66
www.spw.ru info@spw.ru

Важные нюансы

- При принятии решения об маршрутизации пакета с маркировкой маршрута и отсутствии или недоступности маршрута с маркировкой, пакет будет обработан в основной таблице маршрутизации (main)
- Управлять этим можно через /ip route rule (lookup-only-in-table)



Solution.
Production.
Warranty.

Официальный
дистрибьютор Mikrotik
В России

8 800 700 97 66
www.spw.ru info@spw.ru

Ответ маршрутизатора с правильного интерфейса

- Классический вариант решения задачи это маркировка **соединения** в mangle input
- Маркировка **маршрута** в Mangle Output
- Создание маркированных маршрутов в /ip route

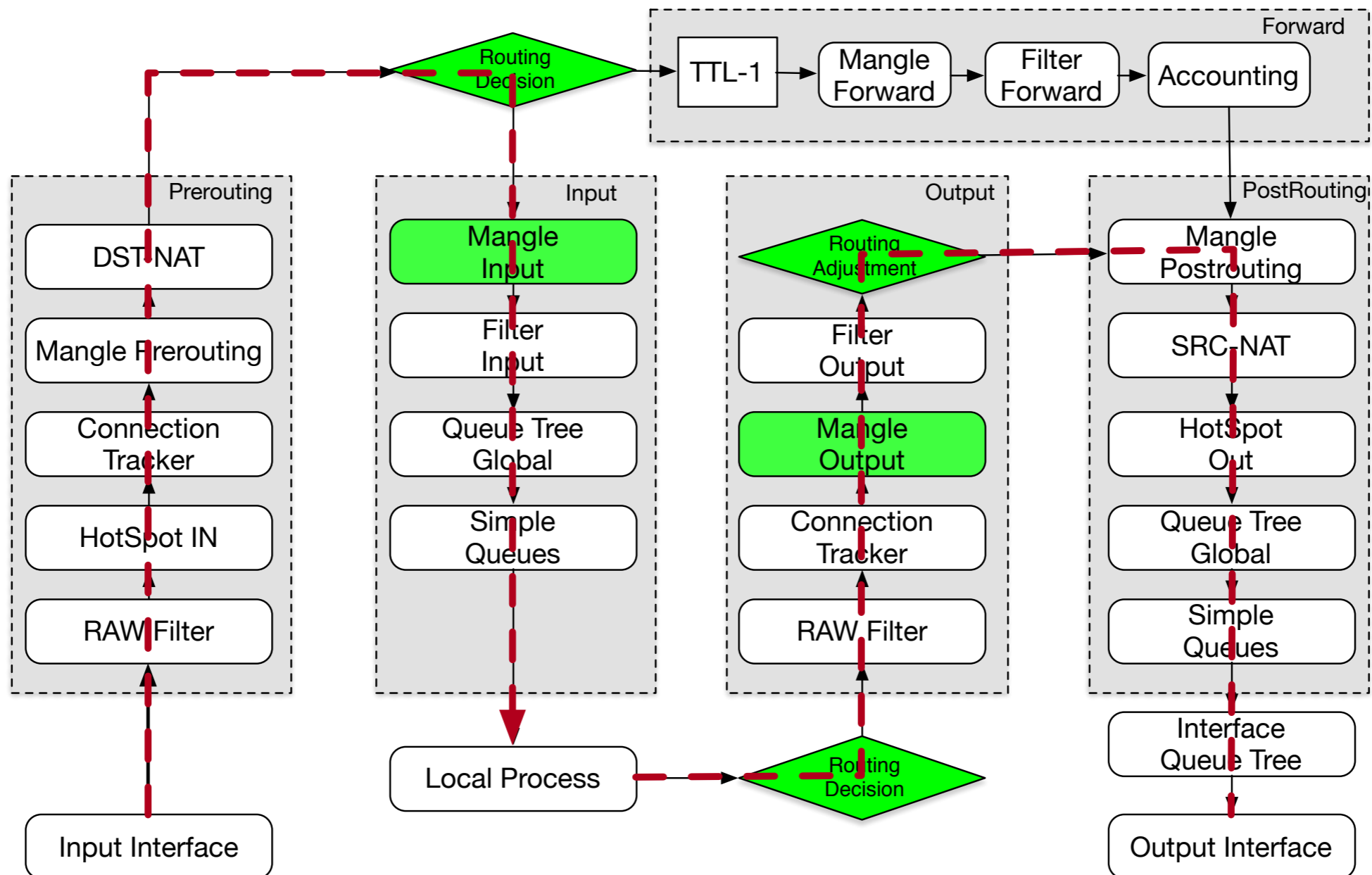


Solution.
Production.
Warranty.

Официальный
дистрибьютор Mikrotik
В России

8 800 700 97 66
www.spw.ru info@spw.ru

Ответ маршрутизатора с правильного интерфейса



Solution.
Production.
Warranty.

Официальный
дистрибьютор Mikrotik
в России

8 800 700 97 66
www.spw.ru info@spw.ru

Ответ маршрутизатора с правильного интерфейса

```
/ip firewall mangle
add action=mark-connection chain=input in-interface=ether1-WAN1 \
    new-connection-mark=con-WAN1 passthrough=yes
add action=mark-connection chain=input in-interface=ether2-WAN2 \
    new-connection-mark=con-WAN2 passthrough=yes
add action=mark-routing chain=output connection-mark=con-WAN1 \
    new-routing-mark=WAN1 passthrough=yes
add action=mark-routing chain=output connection-mark=con-WAN2 \
    new-routing-mark=WAN2 passthrough=yes

/ip route
add distance=1 gateway=1.1.1.1 routing-mark=WAN1
add distance=1 gateway=2.2.2.1 routing-mark=WAN2
add distance=1 gateway=1.1.1.1
add distance=2 gateway=2.2.2.1
```



Solution.
Production.
Warranty.

Официальный
дистрибьютор Mikrotik
в России

8 800 700 97 66
www.spw.ru info@spw.ru

Ответ маршрутизатора с правильного интерфейса

- Типовой ошибкой при этом является отсутствие немаркированного маршрута по умолчанию
- Например если таблица маршрутизации будет иметь такой вид, то нормальный доступ к роутеру с внешних адресов будет невозможен.
- Так же будет невозможен доступ в Интернет с маршрутизатора

```
/ip route  
add distance=1 gateway=1.1.1.1 routing-mark=WAN1  
add distance=1 gateway=2.2.2.1 routing-mark=WAN2
```



Solution.
Production.
Warranty.

Официальный
дистрибьютор Mikrotik
В России

8 800 700 97 66
www.spw.ru info@spw.ru

Ответ маршрутизатора с правильного интерфейса

- Это связано с тем, что для попадания пакета в mangle output пакет должен пройти routing decision, при этом на пакете еще нету маркировки маршрута
- Поэтому необходимо иметь хотя бы один маршрут по умолчанию без маркировки, даже если этот маршрут никогда не будет использоваться

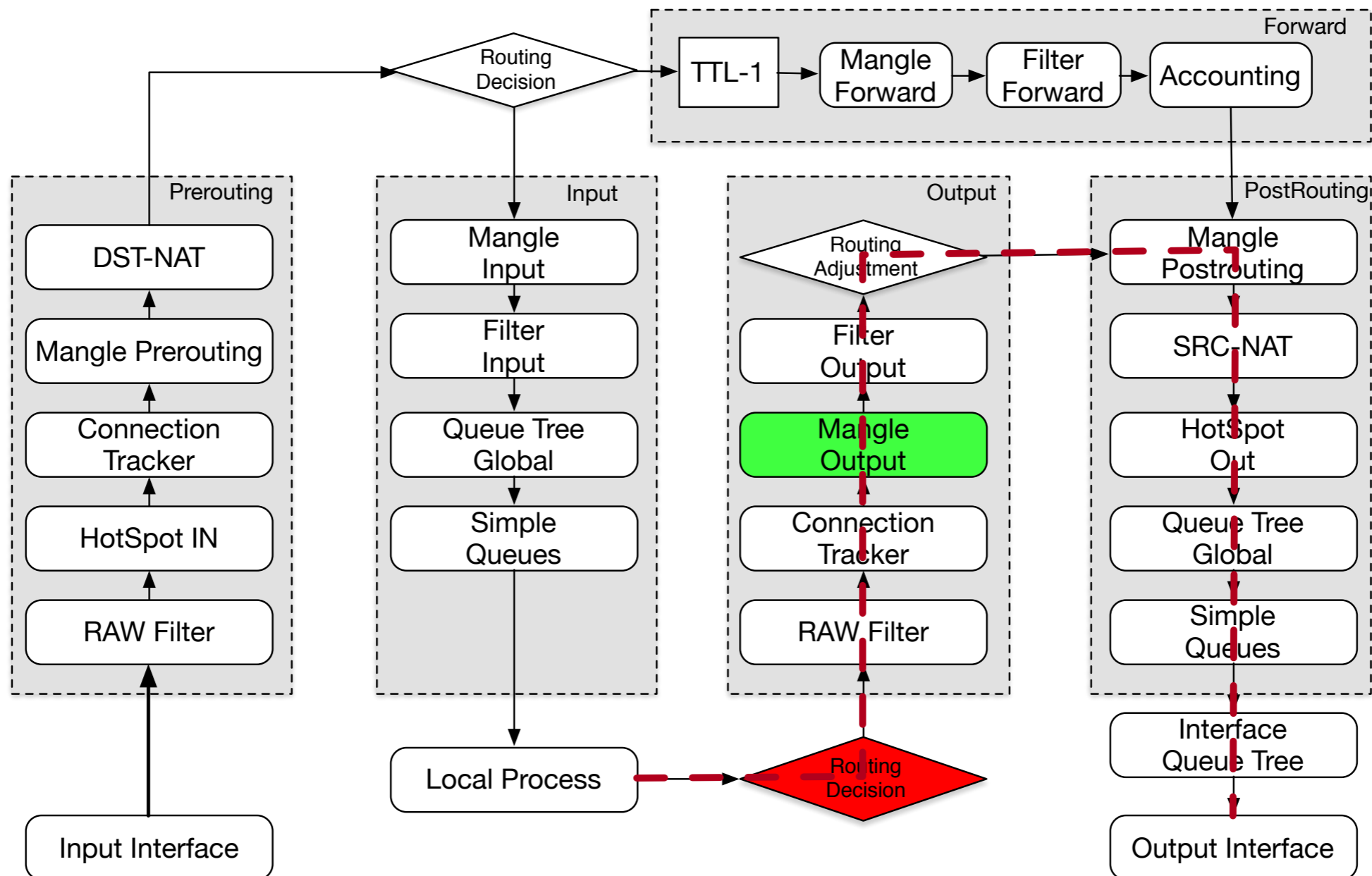


Solution.
Production.
Warranty.

Официальный
дистрибьютор Mikrotik
В России

8 800 700 97 66
www.spw.ru info@spw.ru

Ответ маршрутизатора с правильного интерфейса



Solution.
Production.
Warranty.

Официальный
дистрибьютор Mikrotik
в России

8 800 700 97 66
www.spw.ru info@spw.ru

Построение туннелей на маршрутизаторе с MultiWAN

- Часто, при необходимости обеспечить бесперебойный доступ к удаленной площадке, удобно построить до нее одновременно несколько туннелей с разных WAN-интерфейсов.
- В GRE, IpIP и EoIP туннелях есть параметр source-address
- Однако только этого недостаточно



Solution.
Production.
Warranty.

Официальный
дистрибьютор Mikrotik
В России

8 800 700 97 66
www.spw.ru info@spw.ru

Построение туннелей на маршрутизаторе с MultiWAN

- Пример ошибочной конфигурации
- При этом туннель gre-tunnel2 построится не так, как ожидается

```
/interface gre
add local-address=1.1.1.2 name=gre-tunnel1 remote-address=5.5.5.5
add local-address=2.2.2.2 name=gre-tunnel2 remote-address=6.6.6.6
```

```
/ip route
add distance=1 gateway=1.1.1.1
add distance=10 gateway=2.2.2.1
```

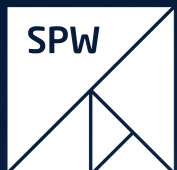
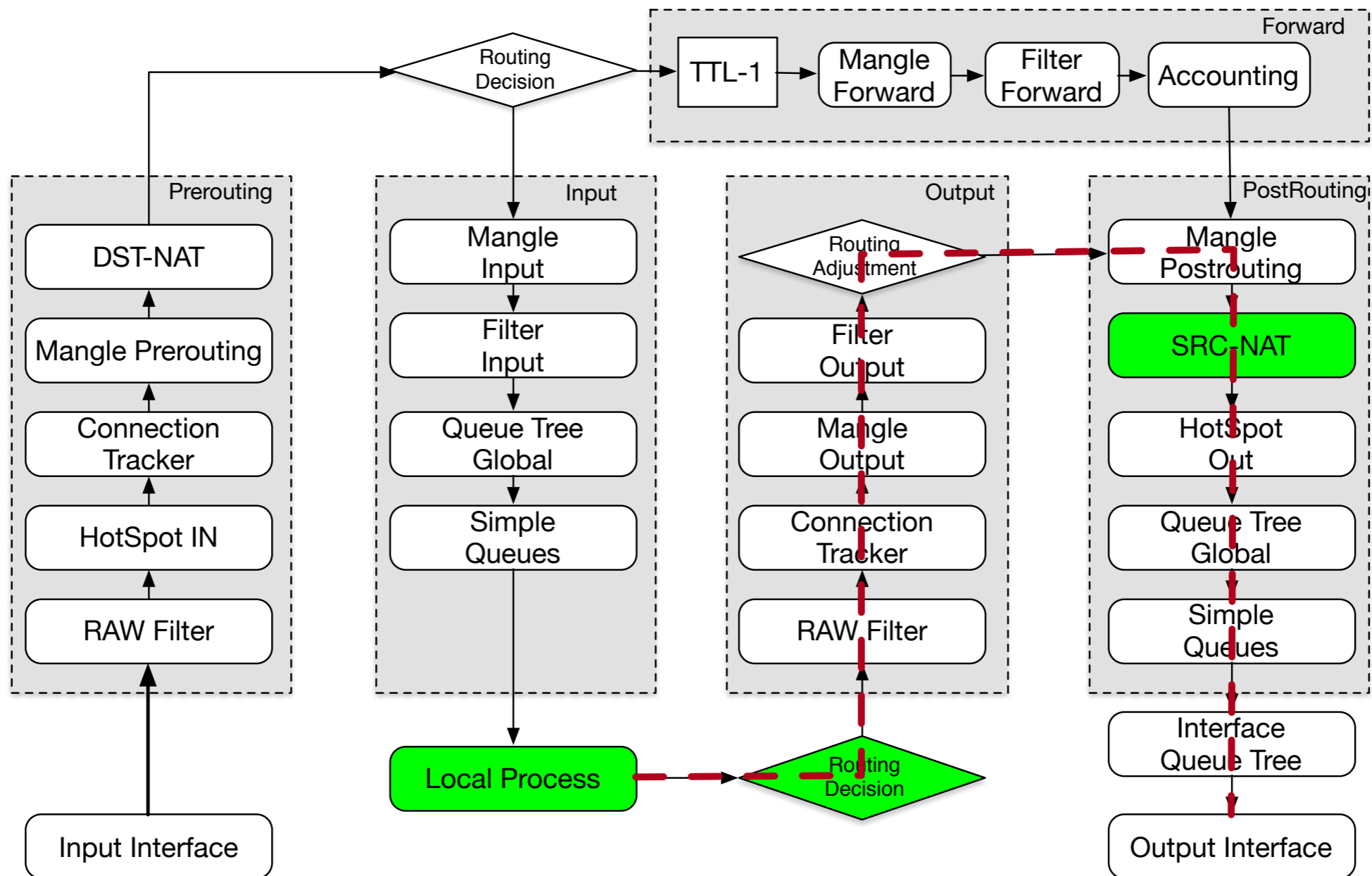


Solution.
Production.
Warranty.

Официальный
дистрибьютор Mikrotik
В России

8 800 700 97 66
www.spw.ru info@spw.ru

Построение туннелей на маршрутизаторе с MultiWAN



Solution.
Production.
Warranty.

Официальный
дистрибьютор Mikrotik
в России

8 800 700 97 66
www.spw.ru info@spw.ru

Построение туннелей на маршрутизаторе с MultiWAN

- Для корректной конфигурации необходимо заблокировать возможность построения туннеля не со «своего» интерфейса
- Удобнее всего это делать при помощи `/ip route rule action=lookup-only-in-table`

```
/ip route
add distance=1 gateway=1.1.1.1 routing-mark=only-WAN1
add distance=1 gateway=2.2.2.1 routing-mark=only-WAN2
add distance=1 gateway=1.1.1.1
add distance=2 gateway=2.2.2.1
/ip route rule
add action=lookup-only-in-table src-address=1.1.1.2/32 table=only-WAN1
add action=lookup-only-in-table src-address=2.2.2.2/32 table=only-WAN2
```



Solution.
Production.
Warranty.

Официальный
дистрибьютор Mikrotik
В России

8 800 700 97 66
www.spw.ru info@spw.ru

MultiWAN и Destination NAT

- При необходимости публикации сервисов за маршрутизатором, кроме ответа самого маршрутизатора с «правильного» интерфейса, необходимо это же обеспечить для сервисов за NAT
- В этой ситуации необходимо маркировать и соединения и маршруты в mangle prerouting
- Очень важно исключить маркировку маршрутов при поступлении пакета с WAN интерфейса
- Модифицируем предыдущую конфигурацию. Для удобства используем interface list

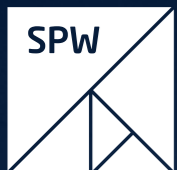
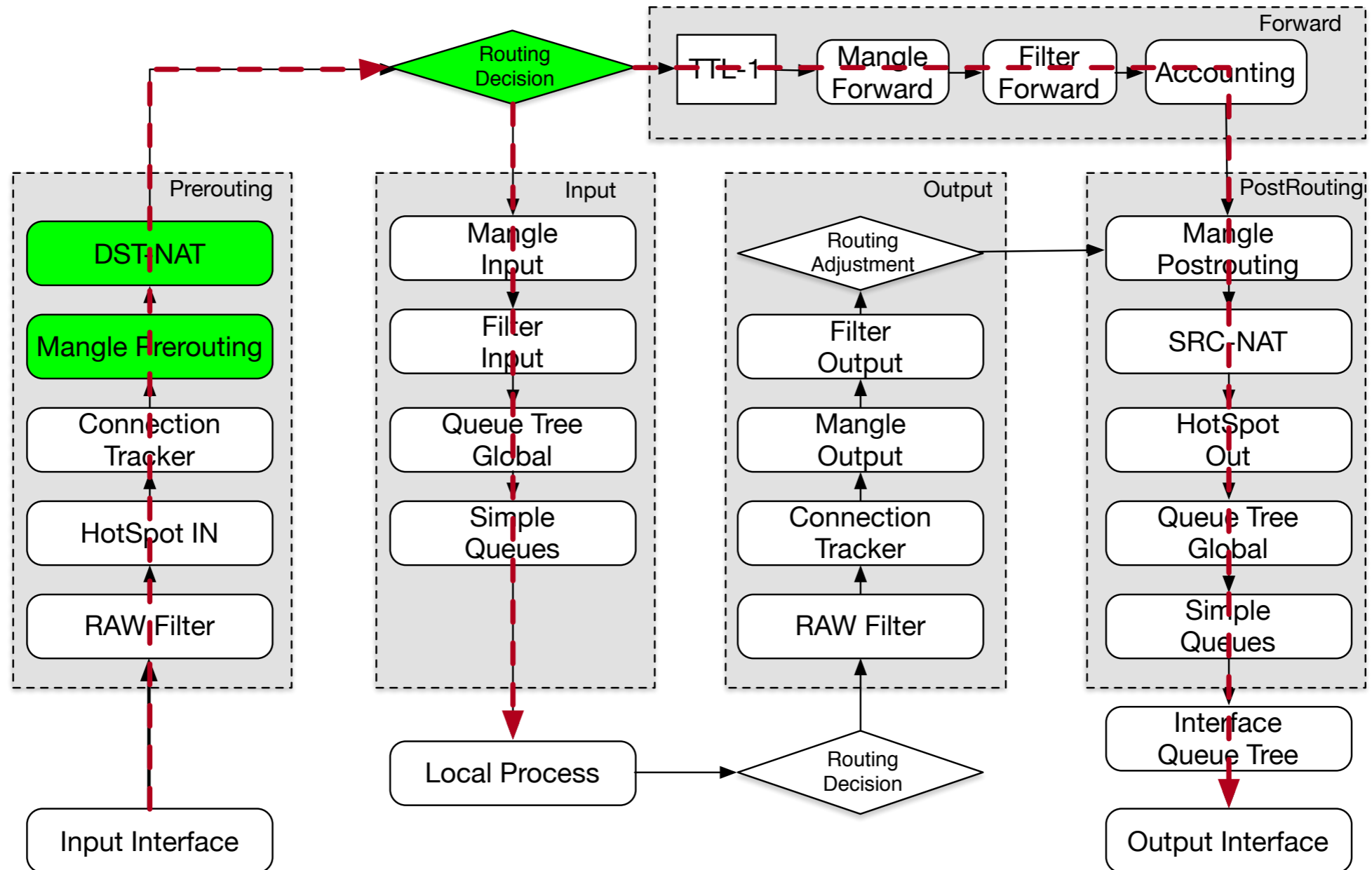


Solution.
Production.
Warranty.

Официальный
дистрибьютор Mikrotik
В России

8 800 700 97 66
www.spw.ru info@spw.ru

MultiWAN и Destination NAT



Solution.
Production.
Warranty.

Официальный
дистрибьютор Mikrotik
в России

8 800 700 97 66
www.spw.ru info@spw.ru

MultiWAN и Destination NAT

```
/interface list
add name=lst-WAN
/interface list member
add interface=ether1-WAN1 list=WAN
add interface=ether2-WAN2 list=WAN

/ip firewall mangle
add action=mark-connection chain=prerouting connection-mark=no-mark \
  in-interface=ether1-WAN1 new-connection-mark=con-WAN1
add action=mark-connection chain=prerouting connection-mark=no-mark \
  in-interface=ether2-WAN2 new-connection-mark=con-WAN2
add action=mark-routing chain=prerouting connection-mark=con-WAN1 \
  in-interface-list=!lst-WAN new-routing-mark=WAN1
add action=mark-routing chain=prerouting connection-mark=con-WAN2 \
  in-interface-list=!lst-WAN new-routing-mark=WAN2
add action=mark-routing chain=output connection-mark=con-WAN1 new-routing-mark=WAN1
add action=mark-routing chain=output connection-mark=con-WAN2 new-routing-mark=WAN2
```



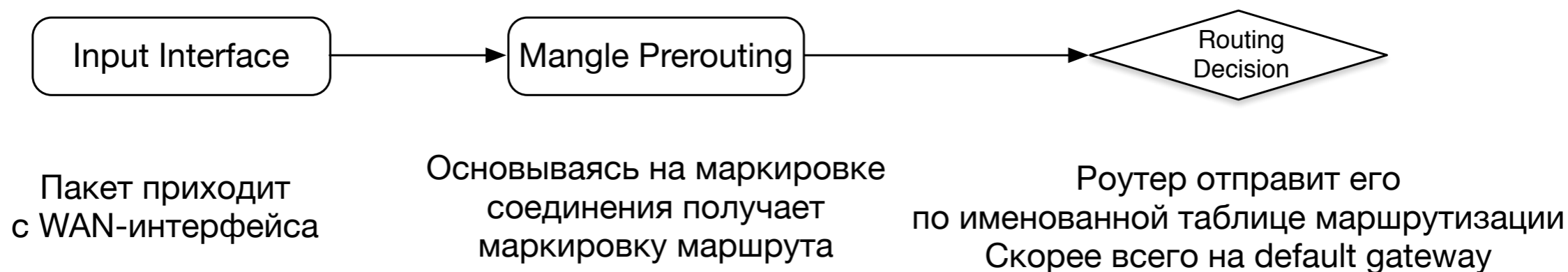
Solution.
Production.
Warranty.

Официальный
дистрибьютор Mikrotik
в России

8 800 700 97 66
www.spw.ru info@spw.ru

Зачем исключили WAN-интерфейсы из маркировки?

- Если этого не сделать, пакет пришедший из Интернет и относящийся к маркированному соединению не будет доставлен в LAN



Solution.
Production.
Warranty.

Официальный
дистрибьютор Mikrotik
В России

8 800 700 97 66
www.spw.ru info@spw.ru

Распределение нагрузки по каналам



Solution.
Production.
Warranty.

Официальный
дистрибьютор Mikrotik
В России

8 800 700 97 66
www.spw.ru info@spw.ru

Алгоритмы распределения нагрузки

- Статический (по адресам, протоколам, портам и их комбинациям)
- Per Connection Classifier (PCC)
- Nth
- Equal Cost Multi Path (ECMP)
- Random



Solution.
Production.
Warranty.

Официальный
дистрибьютор Mikrotik
В России

8 800 700 97 66
www.spw.ru info@spw.ru

Статическое распределение трафика

- Обычно базируется на маркировке маршрутов в `mangle prerouting` на основании адресов отправителя/получателя пакета, протоколов, портов и т.п.
- В случае простых правил, можно воспользоваться `/ip route rule`
- В некоторых случаях можно воспользоваться `action=route` в `mangle prerouting`. Но при этом вы лишитесь части функционала маршрутизации (например `route distance`)



Solution.
Production.
Warranty.

Официальный
дистрибьютор Mikrotik
В России

8 800 700 97 66
www.spw.ru info@spw.ru

Статическое распределение трафика

- В этом примере мы определяем что адреса из первой половины LAN выходят в Интернет через WAN1
- Вторая половина сети выходит в Интернет через WAN2
- Хост 192.168.88.50 являясь почтовым сервером работает по протоколу SMTP (TCP Port=25) через WAN3



Solution.
Production.
Warranty.

Официальный
дистрибьютор Mikrotik
В России

8 800 700 97 66

Статическое распределение трафика

```
# Создаем списки адресов
/ip firewall address-list
add address=192.168.88.0/25 list=First-NET
add address=192.168.88.128/25 list=second-NET
# Маркируем соединения
/ip firewall mangle
add action=mark-connection chain=prerouting new-connection-mark=con-WAN1 \
src-address-list=First-NET
add action=mark-connection chain=prerouting new-connection-mark=con-WAN2 \
src-address-list=Second-NET
add action=mark-connection chain=prerouting dst-port=25,110,143 \
new-connection-mark=con-WAN3 protocol=tcp src-address=192.168.88.50
# Маркируем маршруты
add action=mark-routing chain=prerouting connection-mark=con-WAN1 \
in-interface-list=!lst-WAN new-routing-mark=WAN1 passthrough=yes
add action=mark-routing chain=prerouting connection-mark=con-WAN2 \
in-interface-list=!lst-WAN new-routing-mark=WAN2 passthrough=yes
add action=mark-routing chain=prerouting connection-mark=con-WAN3 \
in-interface-list=!lst-WAN new-routing-mark=WAN3 passthrough=yes
```



Solution.
Production.
Warranty.

Официальный
дистрибьютор Mikrotik
В России

8 800 700 97 66
www.spw.ru info@spw.ru

Per Connection Classifier

- Позволяет выбрать классификатор соединения (src-address, dst-address, оба адрес в комбинации с портами или без них)
- Для каждого соединения маршрутизатор рассчитывает 32-битный хеш
- Для распределения нагрузки, достаточно решить несложную пропорцию



Solution.
Production.
Warranty.

Официальный
дистрибьютор Mikrotik
В России

8 800 700 97 66
www.spw.ru info@spw.ru

Per Connection Classifier

- Задача, распределить трафик на основании адреса отправителя, в соотношении 1:2 (например имеются каналы WAN1=10 Мбит и WAN2=20 Мбит)

```
/ip firewall mangle
add action=mark-connection chain=prerouting in-interface=LAN \
    new-connection-mark=con-WAN1 passthrough=yes per-connection-classifier=\
    src-address:3/0
add action=mark-connection chain=prerouting in-interface=LAN \
    new-connection-mark=con-WAN2 passthrough=yes per-connection-classifier=\
    src-address:3/1
add action=mark-connection chain=prerouting in-interface=LAN \
    new-connection-mark=con-WAN2 passthrough=yes per-connection-classifier=\
    src-address:3/2
add action=mark-routing chain=prerouting connection-mark=con-WAN1 \
    in-interface-list=!lst-WAN new-routing-mark=WAN1 passthrough=yes
add action=mark-routing chain=prerouting connection-mark=con-WAN2 \
    in-interface-list=!lst-WAN new-routing-mark=WAN2 passthrough=yes
```



Solution.
Production.
Warranty.

Официальный
дистрибьютор Mikrotik
в России

8 800 700 97 66
www.spw.ru info@spw.ru

Nth

- Еще один механизм RouterOS позволяющий распределить трафик по каналам
- Функционально похож на PCC, но не имеет возможности управления классификатором трафика
- Обычно используется для динамического заполнения списков адресов (address-list) в файрволе, на основании которых в дальнейшем осуществляется распределение маршрутов



Solution.
Production.
Warranty.

Официальный
дистрибьютор Mikrotik
В России

8 800 700 97 66

ECMP

- **Equal Cost Multi Path Route** маршрут в котором имеется более одного шлюза
- В одном маршруте один и тот же шлюз можно указать несколько раз
- Для каждого нового соединения маршрутизатор вычисляет хеш на основании `src-address+port` и `dst-address+port` и «привязывает» это к одному из шлюзов указанных в маршруте



Solution.
Production.
Warranty.

Официальный
дистрибьютор Mikrotik
В России

8 800 700 97 66

ЕСМР

- При этом раз в 10 минут маршрутизатор «выравнивает» количество соединений между шлюзами
- Это не позволяет работать этой технологии совместно с NAT
- Проверка доступности шлюза (check-gateway) для этого маршрута не имеет смысла, потому что хотя бы один из шлюзов обычно доступен



Solution.
Production.
Warranty.

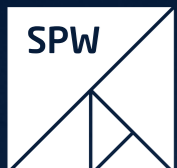
Официальный
дистрибьютор Mikrotik
В России

8 800 700 97 66

ECMP

- Пример ECMP-маршрута и маршрутов с проверкой доступности Gateway

```
/ip route  
add distance=1 gateway=1.1.1.1,1.1.1.1,2.2.2.2  
add check-gateway=ping distance=100 gateway=1.1.1.1  
add check-gateway=ping distance=100 gateway=2.2.2.2
```



Solution.
Production.
Warranty.

Официальный
дистрибьютор Mikrotik
В России

8 800 700 97 66

ЕСМР и NAT

- Так как ЕСМР может «переместить» соединение на другой шлюз без учета NAT, совместно с NAT использовать эту технологию не получится
- Если вы все-таки хотите ее использовать, то необходимо «привязать» соединение к конкретному шлюзу
- Для этого удобно использовать маркировку соединения в mangle forward и затем маркировку маршрутов

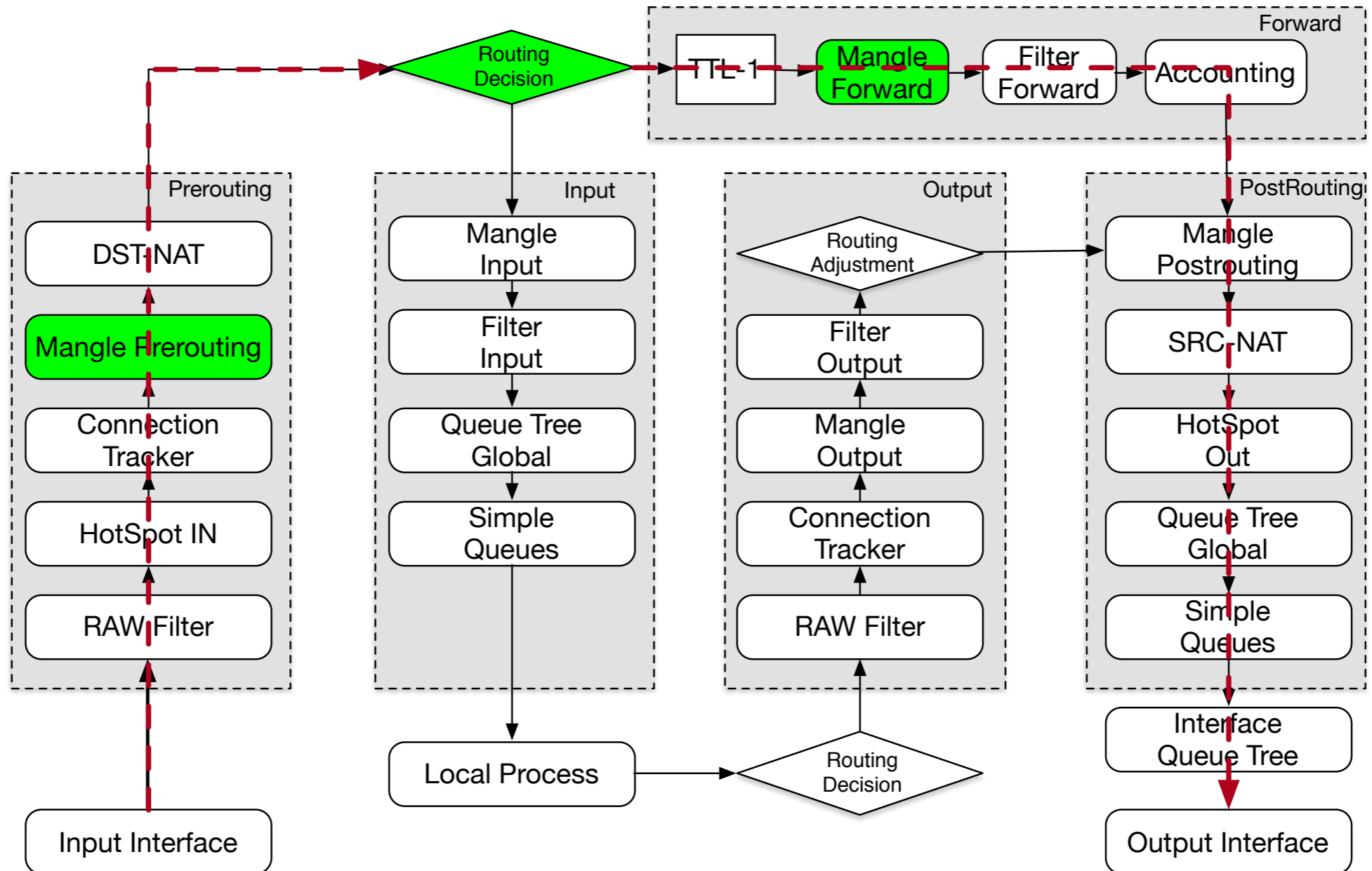


Solution.
Production.
Warranty.

Официальный
дистрибьютор Mikrotik
В России

8 800 700 97 66

ЕСМР и NAT



Solution.
Production.
Warranty.

Официальный
дистрибьютор Mikrotik
в России

8 800 700 97 66

ECMP и NAT

```
/ip firewall mangle
```

```
add action=mark-connection chain=forward connection-mark=no-mark \  
new-connection-mark=con-WAN1 out-interface=ether1-WAN1 passthrough=yes  
add action=mark-connection chain=forward connection-mark=no-mark \  
new-connection-mark=con-WAN2 out-interface=ether2-WAN2 passthrough=yes  
add action=mark-routing chain=prerouting connection-mark=con-WAN1 \  
in-interface-list=!lst-WAN new-routing-mark=WAN1 passthrough=yes  
add action=mark-routing chain=prerouting connection-mark=con-WAN2 \  
in-interface-list=!lst-WAN new-routing-mark=WAN2 passthrough=yes
```

```
/ip route
```

```
add distance=1 gateway=1.1.1.1 routing-mark=WAN1  
add distance=1 gateway=2.2.2.1 routing-mark=WAN2  
add distance=1 gateway=1.1.1.1,1.1.1.1,2.2.2.1  
add check-gateway=ping distance=100 gateway=2.2.2.1  
add check-gateway=ping distance=100 gateway=1.1.1.1
```



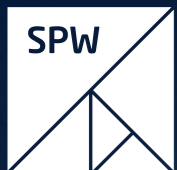
Solution.
Production.
Warranty.

Официальный
дистрибьютор Mikrotik
в России

8 800 700 97 66

Random

- Для распределения нагрузки между каналами так же можно использовать функцию Random
- Данная функция является производной от генератора псевдослучайной последовательности срабатывая с вероятностью задаваемой в процентах
- Это позволяет «относительно честно» распределить подключения по каналам



Solution.
Production.
Warranty.

Официальный
дистрибьютор Mikrotik
В России

8 800 700 97 66

Random

- Предположим у вас есть каналы на 100 и на 10 мбит
- Вы хотите 10% «неудачников» привязать к более медленному каналу
- «Неудачники» выбираются случайным образом

```
/ip firewall mangle
add action=mark-connection chain=prerouting connection-mark=no-mark \
    in-interface=ether3-LAN new-connection-mark=con-WAN1 passthrough=yes \
    random=10
add action=mark-connection chain=prerouting connection-mark=no-mark \
    in-interface=ether3-LAN new-connection-mark=con-WAN2 passthrough=yes
add action=mark-routing chain=prerouting connection-mark=con-WAN1 \
    in-interface-list=!lst-WAN new-routing-mark=WAN1 passthrough=yes
add action=mark-routing chain=prerouting connection-mark=con-WAN2 \
    in-interface-list=!lst-WAN new-routing-mark=WAN2 passthrough=yes
```



Solution.
Production.
Warranty.

Официальный
дистрибьютор Mikrotik
в России

8 800 700 97 66

Сложные сценарии

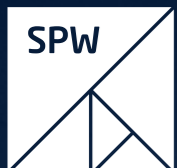
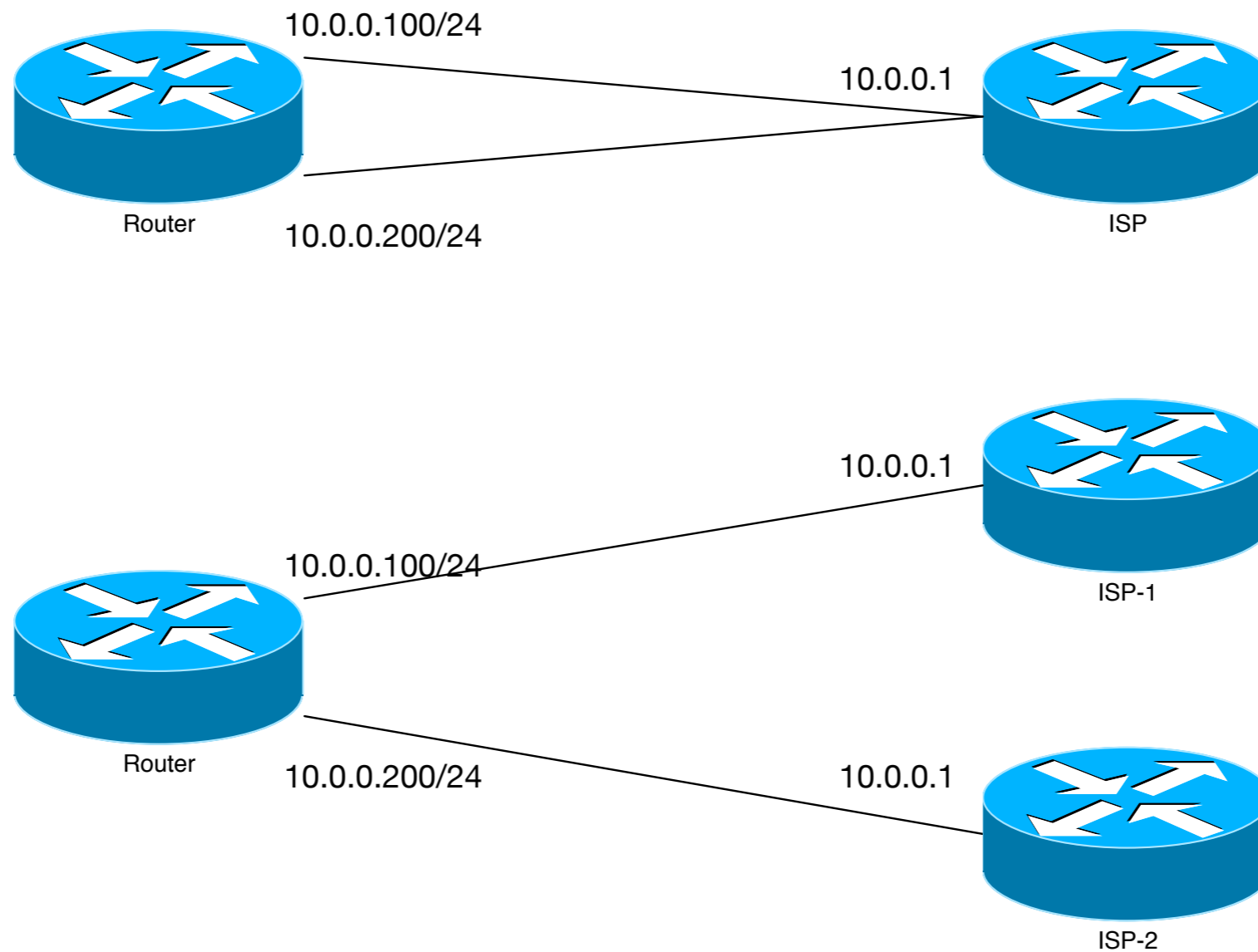


Solution.
Production.
Warranty.

Официальный
дистрибьютор Mikrotik
В России

8 800 700 97 66

Несколько Интерфейсов с одним и тем же шлюзом



Solution.
Production.
Warranty.

Официальный
дистрибьютор Mikrotik
в России

8 800 700 97 66

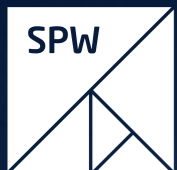
2 Интерфейса с одним и тем же шлюзом

- В этой ситуации помогает специальный вариант указания шлюза (gateway) в таблице маршрутизации в виде `address%interface`

- Например

```
/ip route
add distance=1 gateway=10.0.0.1%ether1-WAN1
add distance=2 gateway=10.0.0.1%ether2-WAN2
add distance=1 gateway=10.0.0.1%ether1-WAN1 routing-mark=WAN1
add distance=1 gateway=10.0.0.1%ether2-WAN2 routing-mark=WAN2
```

- Далее используя маркировки балансируем нагрузку



Провайдер по DHCP

- Когда провайдер отдает адрес по DHCP, то на момент написания конфигурации нам неизвестен адрес default gateway и невозможно написать маркированный маршрут
- Тогда можно использовать
- Dhcp-client script
- VRF



Solution.
Production.
Warranty.

Официальный
дистрибьютор Mikrotik
В России

8 800 700 97 66

DHCP-Client Script

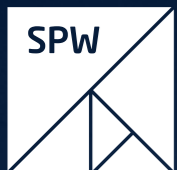
- Данный скрипт (пример из Wiki), при получении адреса создает маркированный маршрут с маркировкой WAN1
- Если поставить add-default-route=yes то будет так же создан немаркированный маршрут

```
/ip dhcp-client
add add-default-route=no dhcp-options=hostname,clientid disabled=no interface=ether1-WAN1 script="{\r\
\n :local rmark \"WAN1\"\r\
\n :local count [/ip route print count-only where comment=\"WAN1\"]\r\
\n :if (\$bound=1) do={\r\
\n :if (\$count = 0) do={\r\
\n /ip route add gateway=\$\"gateway-address\" comment=\"WAN1\" routing-mark=\$rmark\r\
\n } else={\r\
\n :if (\$count = 1) do={\r\
\n :local test [/ip route find where comment=\"WAN1\"]\r\
\n :if ([/ip route get \$test gateway] != \$\"gateway-address\") do={\r\
\n /ip route set \$test gateway=\$\"gateway-address\"\r\
\n }\r\
\n } else={\r\
\n :error \"Multiple routes found\"\r\
\n }\r\
\n }\r\
\n } else={\r\
\n /ip route remove [find comment=\"WAN1\"]\r\
\n }\r\
\n}\r\
\n"
```



VRF

- VRF это Virtual Routing and Forwarding
- Представляет собой изолированную независимую таблицу маршрутизации
- В VRF можно указать интерфейсы
- Если такой интерфейс получит адрес по DHCP, все маршруты тоже будут в этом VRF
- Так как в RouterOS VRF построена на маркировках, можно используя mangle отправлять пакеты в эту таблицу маршрутизации где они будут обработаны



Solution.
Production.
Warranty.

Официальный
дистрибьютор Mikrotik
В России

8 800 700 97 66

VRF

- Так как VRF это изолированная таблица, при приходе пакетов на интерфейс WAN1 их надо принудительно отправлять в таблицу маршрутизации MAIN иначе они будут обработаны внутри таблицы VRF

```
/ip route vrf
add interfaces=ether1-WAN1 routing-mark=WAN1

/ip dhcp-client
add dhcp-options=hostname,clientid disabled=no interface=ether1-WAN1

/ip firewall mangle
add action=mark-connection chain=prerouting in-interface=ether3-LAN \
    new-connection-mark=con-WAN1 passthrough=yes random=20
add action=mark-routing chain=prerouting connection-mark=con-WAN1 in-interface=\
    ether3-LAN new-routing-mark=WAN1 passthrough=yes
add action=mark-routing chain=prerouting in-interface=ether1-WAN1 new-routing-mark=\
    main passthrough=yes
```



Solution.
Production.
Warranty.

Официальный
дистрибьютор Mikrotik
В России

8 800 700 97 66

Check Gateway

- Check Gateway это функция проверки шлюза
- При включении этой опции RouterOS раз в 10 секунд выполняет ping или arp-запрос на шлюз
- Если шлюз не ответил в течении двух проверок, он считается недоступным и все маршруты ассоциированные с ним становятся неактивными
- Проблема в том, что обычно Default gateway это адрес ближнего к вам устройства провайдера, доступность которого не гарантирует доступность доступа в Интернет



Solution.
Production.
Warranty.

Официальный
дистрибьютор Mikrotik
В России

8 800 700 97 66

Check Gateway

- Можно проверять доступность не непосредственно шлюза, а какого-либо реального адреса в сети Интернет (например, адреса центрального офиса из филиала)
- Для этого можно воспользоваться утилитой NetWatch или рекурсивной маршрутизацией



Solution.
Production.
Warranty.

Официальный
дистрибьютор Mikrotik
В России

8 800 700 97 66

NetWatch

- Утилита, проверяющая доступность хоста в сети
- При его доступности выполняется скрипт UP
- При его недоступности выполняется скрипт Down
- Скрипт исполняется один раз, при изменении состояния
- Данный скрипт проверяет доступность узла 8.8.8.8 и если он не доступен перезагружает USB-модем

```
/tool netwatch  
add down-script="/system routerboard usb power-reset duration=3» host=8.8.8.8
```



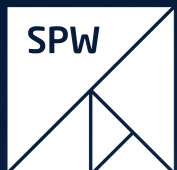
Solution.
Production.
Warranty.

Официальный
дистрибьютор Mikrotik
В России

8 800 700 97 66

Recursive Routing

- Позволяет указать в качестве шлюза любой произвольный адрес в сети
- При этом этот адрес распознается через другой шлюз
- Управляется при помощи параметров маршрута `score` и `target-score` (маршрут определяется через другие маршруты, чей `score` меньше или равен `target-score` этого маршрута)



Solution.
Production.
Warranty.

Официальный
дистрибьютор Mikrotik
В России

8 800 700 97 66

Recursive Routing

```
/ip route
add distance=1 gateway=8.8.8.8 target-scope=20
add distance=1 dst-address=8.8.8.8/32 gateway=192.168.0.1 scope=20
```

	Dst. Address	Gateway	Distance	Routing Mark
AS	▶ 0.0.0.0/0	8.8.8.8 recursive via 192.168.0.1 ether3-LAN	1	
AS	▶ 8.8.8.8	192.168.0.1 reachable ether3-LAN	1	

- Более подробно, см. статью [Advanced Failover Without Scripting](https://wiki.mikrotik.com/wiki/Advanced_Routing_Failover_without_Scripting) [https://wiki.mikrotik.com/wiki/Advanced Routing Failover without Scripting](https://wiki.mikrotik.com/wiki/Advanced_Routing_Failover_without_Scripting)



Solution.
Production.
Warranty.

Официальный
дистрибьютор Mikrotik
в России

8 800 700 97 66

Dynamic Routing

- Использование протоколов динамической маршрутизации (RIP, OSPF, BGP), особенно совместно с BFD позволяют ускорить определение недоступного шлюза
- К сожалению провайдер обычно предоставляет подключение со статической маршрутизацией



Solution.
Production.
Warranty.

Официальный
дистрибьютор Mikrotik
В России

8 800 700 97 66

MultiWAN на входе

- К сожалению при обеспечении резервирования канала для доступа снаружи, обычно мы остаемся привязанными к внешним IP-адресам выданным провайдером
- При недоступности канала, становятся также недоступны ассоциированные с ним IP-адреса
- Есть 2 способа избежать этого
- Вынос внешнего роутера на отдельную площадку (Tier3 ДЦ)
- Получение AS и установление BGP-сессий с несколькими провайдерами



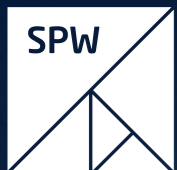
Solution.
Production.
Warranty.

Официальный
дистрибьютор Mikrotik
В России

8 800 700 97 66

Роутер на внешней площадке

- Идея заключается в выносе маршрутизатора во внешний ДЦ, который имеет высокий уровень резервирования
- Это наиболее дешевый вариант (несколько тысяч рублей в месяц за юнит или несколько сотен рублей за VPS)
- Вся работа с внешним миром переносится на роутер в ДЦ
- Так как между офисом и ДЦ нет необходимости использовать NAT, облегчается балансировка нагрузки и при неисправности канала не происходит разрыва сессии
- Это решение так же прекрасно сочетается с динамической маршрутизацией

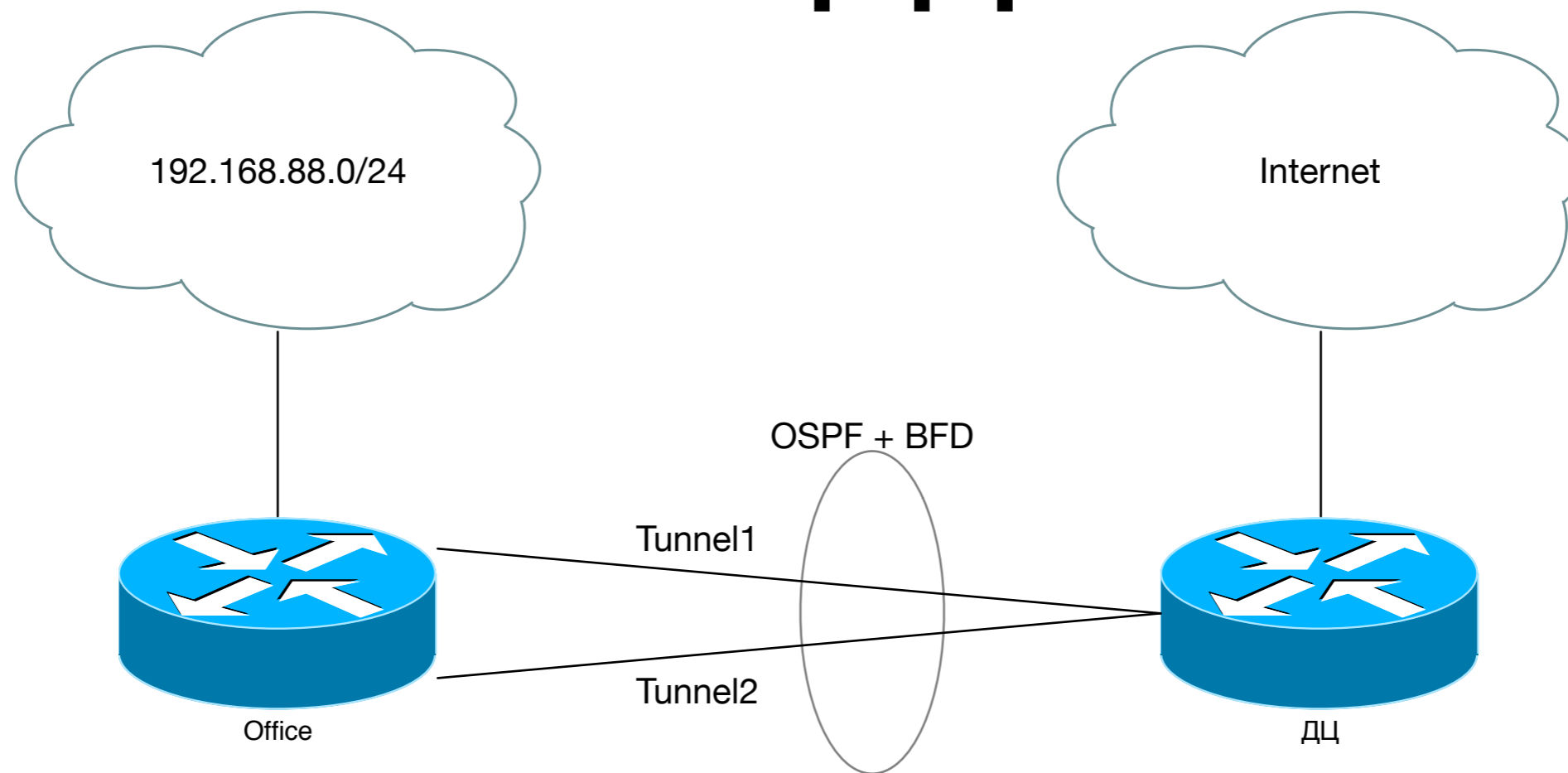


Solution.
Production.
Warranty.

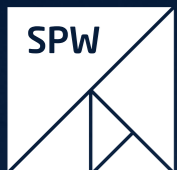
Официальный
дистрибьютор Mikrotik
В России

8 800 700 97 66

Роутер на внешней площадке



- В этой схеме NAT и основной файрвол находятся на маршрутизаторе в ДЦ
- Офисный роутер только обеспечивает балансировку нагрузки между туннелями



Solution.
Production.
Warranty.

Официальный
дистрибьютор Mikrotik
В России

8 800 700 97 66

BGP + AS

- Получение своей автономной системы позволяет получить провайдеронезависимый блок адресов и обеспечить его доступность через нескольких провайдеров
- Минимальный блок адресов при этом /24
- Требуются знания протокола BGP
- Достаточно высокая стоимость владения



Solution.
Production.
Warranty.

Официальный
дистрибьютор Mikrotik
в России

8 800 700 97 66
www.spw.ru info@spw.ru

СПАСИБО ЗА ВНИМАНИЕ, ЗАДАВАЙТЕ ВОПРОСЫ

АВТОР ДОКЛАДА: ИЛЬЯ КНЯЗЕВ