Обзор сомнительных технических решений на RouterOS и их разбор

Обзор кейсов и конфигураций.

μTik.pro

http://mtik.pro

Об авторе

- Мартюшев Тимофей
- Более 6 лет работы в провайдерах
- MTCNA (1609NA1077), MTCRE (1606RE139), MTCIPv6E (1703IPv6E034)
- MikroTik certified trainer (TR0422)
- MikroTik Academy Coordinator

Источники

- **Чат MikrotikRu https://t.me/MikrotikRu**
- **Инструкции “экспертов” операторов по настройке RouterOS для рядовых инженеров компании**
- **Личный опыт**

Мои операторы блокируют мой порт, т.к. “видят” много broadcast

- На роутере настроено несколько операторов с балансировкой.
- Интерфейсы в сторону операторов НЕ включены в bridge.

Конфиг

```
/ip route
add gateway=combo1 routing-mark=mark2
add gateway=ether3 routing-mark=mark3
add gateway=pppoe-out routing-mark=mark4
```

Результат

INTERFACE	TIME	NUM	DIR	SRC-MAC	DST-MAC	SRC-ADDRESS	PROTOC
wlan2	58.093	2626	<-	6C:3B:6B:9D:DC:62	FF:FF:FF:FF:FF:FF	10.128.4.14: who has 8.8.8.8?	arp
wlan2	58.173	2627	<-	6C:3B:6B:9D:DC:62	FF:FF:FF:FF:FF:FF	10.128.4.14: who has 149.154.163...	arp
wlan2	58.391	2630	<-	6C:3B:6B:9D:DC:62	FF:FF:FF:FF:FF:FF	10.128.4.14: who has 40.69.218.62?	arp
wlan2	58.653	2632	<-	6C:3B:6B:9D:DC:62	FF:FF:FF:FF:FF:FF	10.128.4.14: who has 64.233.162....	arp
wlan2	58.654	2633	<-	6C:3B:6B:9D:DC:62	FF:FF:FF:FF:FF:FF	10.128.4.14: who has 173.194.32....	arp
wlan2	58.663	2634	<-	6C:3B:6B:9D:DC:62	FF:FF:FF:FF:FF:FF	10.128.4.14: who has 173.194.122...	arp
wlan2	58.663	2635	<-	6C:3B:6B:9D:DC:62	FF:FF:FF:FF:FF:FF	10.128.4.14: who has 74.125.232....	arp
wlan2	58.686	2637	<-	6C:3B:6B:9D:DC:62	FF:FF:FF:FF:FF:FF	10.128.4.14: who has 173.194.222...	arp
wlan2	58.693	2638	<-	6C:3B:6B:9D:DC:62	FF:FF:FF:FF:FF:FF	10.128.4.14: who has 173.194.32....	arp
wlan2	58.703	2639	<-	6C:3B:6B:9D:DC:62	FF:FF:FF:FF:FF:FF	10.128.4.14: who has 173.194.32....	arp
wlan2	58.704	2640	<-	6C:3B:6B:9D:DC:62	FF:FF:FF:FF:FF:FF	10.128.4.14: who has 173.194.113...	arp
wlan2	58.704	2641	<-	6C:3B:6B:9D:DC:62	FF:FF:FF:FF:FF:FF	10.128.4.14: who has 74.125.232....	arp
wlan2	58.713	2642	<-	6C:3B:6B:9D:DC:62	FF:FF:FF:FF:FF:FF	10.128.4.14: who has 173.194.113...	arp
wlan2	58.719	2643	->	64:D1:54:66:B8:2E	01:80:C2:00:00:00		802.2
wlan2	58.723	2644	<-	6C:3B:6B:9D:DC:62	FF:FF:FF:FF:FF:FF	10.128.4.14: who has 173.194.32....	arp
wlan2	58.84	2645	<-	E4:8D:8C:D9:24:4A	FF:FF:FF:FF:FF:FF	192.168.19.254: who has 212.33.2...	arp

Результат

DIR	SRC-MAC	DST-MAC	SRC-ADDRESS	PROTOCOL
<-	6C:3B:6B:9D:DC:62	FF:FF:FF:FF:FF:FF	10.128.4.14: who has 8.8.8.8?	arp
<-	6C:3B:6B:9D:DC:62	FF:FF:FF:FF:FF:FF	10.128.4.14: who has 149.154.163...	arp
<-	6C:3B:6B:9D:DC:62	FF:FF:FF:FF:FF:FF	10.128.4.14: who has 40.69.218.62?	arp
<-	6C:3B:6B:9D:DC:62	FF:FF:FF:FF:FF:FF	10.128.4.14: who has 64.233.162....	arp
<-	6C:3B:6B:9D:DC:62	FF:FF:FF:FF:FF:FF	10.128.4.14: who has 173.194.32....	arp
<-	6C:3B:6B:9D:DC:62	FF:FF:FF:FF:FF:FF	10.128.4.14: who has 173.194.122...	arp
<-	6C:3B:6B:9D:DC:62	FF:FF:FF:FF:FF:FF	10.128.4.14: who has 74.125.232....	arp
<-	6C:3B:6B:9D:DC:62	FF:FF:FF:FF:FF:FF	10.128.4.14: who has 173.194.222...	arp
<-	6C:3B:6B:9D:DC:62	FF:FF:FF:FF:FF:FF	10.128.4.14: who has 173.194.32....	arp
<-	6C:3B:6B:9D:DC:62	FF:FF:FF:FF:FF:FF	10.128.4.14: who has 173.194.32....	arp
<-	6C:3B:6B:9D:DC:62	FF:FF:FF:FF:FF:FF	10.128.4.14: who has 173.194.113...	arp
<-	6C:3B:6B:9D:DC:62	FF:FF:FF:FF:FF:FF	10.128.4.14: who has 74.125.232....	arp
<-	6C:3B:6B:9D:DC:62	FF:FF:FF:FF:FF:FF	10.128.4.14: who has 173.194.113...	arp
->	64:D1:54:66:B8:2E	01:80:C2:00:00:00		802.2
<-	6C:3B:6B:9D:DC:62	FF:FF:FF:FF:FF:FF	10.128.4.14: who has 173.194.32....	arp
<-	E4:8D:8C:D9:24:4A	FF:FF:FF:FF:FF:FF	192.168.19.254: who has 212.33.2...	arp

Вывод

Использовать интерфейс в качестве gateway возможно только на point-to-point соединениях. Например, PPPoE или IPIP.

Ограничение доступа к роутеру

На маршрутизаторе присутствуют публичные IP-адреса, для ограничения доступа на маршрутизатор предлагается использовать:

- ...
- ...

Ограничение доступа к роутеру

Достаточно:

- **использовать не стандартный пароль.**

Ограничение доступа к роутеру

Достаточно:

- использовать не стандартный пароль;
- Добавить ограничение доступа в `/ip service`

Ограничение доступа в /ip service

```
/ip service set [find] address=192.168.88.0/24
```

Ограничение работает на уровне процесса (сервиса), уже после firewall.

Рекомендации уже описаны:

- http://mtik.pro/sec
- https://wiki.mikrotik.com/wiki/Manual:Securing_Your_Router

Рекомендации по защите роутера. Пользователи.

- Не используйте стандартные логины (admin, root, user)
- Используйте сложные пароли. (проверьте ваш пароль: http://mtik.pro/passwd)
- Добавьте ограничения по IP-адресам для системных пользователей

Рекомендации по защите роутера. Сервисы.

- Выключите неиспользуемые сервисы:
  - /ip service
- Добавьте ограничения по IP-адресам для всех сервисов.
- Ограничьте доступ по MAC-адресу
  - `/tool mac-server`
  - `/tool mac-server mac-winbox`
- Выключи или настрой ROMON
  - `/tool romon`

Рекомендации по защите роутера. Сервисы.

- Проверь настройки SNMP:
  - /snmp
  - /snmp community
- Bandwidth Server
  - `/tool bandwidth-server`
- DNS
  - `/ip dns`
- TFTP
  - `/ip tftp`
- Другие
  - `/ip proxy`
  - `/ip socks`

Рекомендации по защите роутера. Физический доступ и функционал.

- Выключите неиспользуемые интерфейсы
- Выключите управление через LCD

- Выключите пакеты, которые не планируете использовать (MPLS?)

Рекомендации по защите роутера. Защищённые соединения.

- Для Winbox – используйте Secure Mode.
- Для SSH – используйте strong crypto
  - `/ip ssh set strong-crypto=yes`

Рекомендации по защите роутера. Firewall

- Настройте Firewall для защиты роутера (input)
- Настройте Firewall для защиты клиентов (forward)
- Не забывайте про настройки Firewall как для Ipv4, так и для Ipv6

Рекомендации по защите роутера. Firewall Filter - input

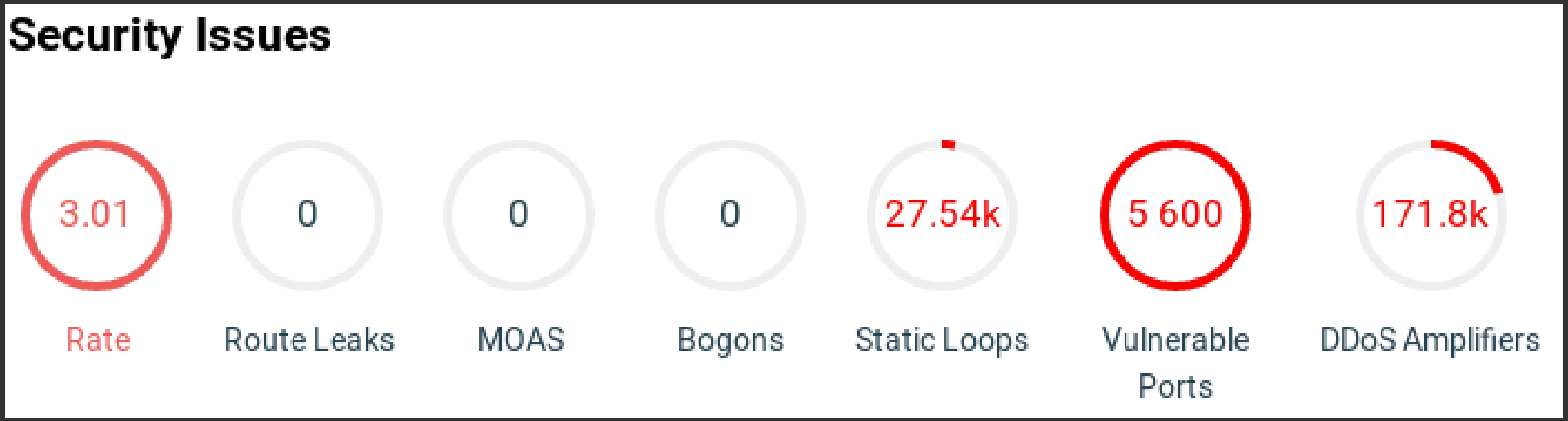
- Порты, на которые стоит обратить внимание:
  - TCP
    - 20-21 (FTP)
    - 22 (SSH)
    - 23 (TELNET)
    - 53 (DNS)
    - 80/443 (HTTP/HTTPS)
    - 1194 (OpenVPN)
    - 1723 (PPTP)
    - 8291 (Winbox)
    - 8728-8729 (API)
    - 2000 (Bandwidth-test)
  - UDP:
    - 53 (DNS)
    - 69 (TFTP)
    - 123 (NTP)
    - 161-162 (SNMP)
    - 1194 (OpenVPN)
    - 1701 (L2TP)
    - 2000 (Bandwidth-test)

Рекомендации по защите роутера. Firewall Filter - forward

- Порты, на которые стоит обратить внимание:
  - UDP (DOS Amplifiers):
    - 53 (DNS)
    - 111 (portmap)
    - 123 (NTP)
    - 161 (SNMP)
    - 520 (RIPv1)
    - 1900 (SSDP)
    - 11211 (memcached)

DoS Amplifiers

- Почему стоит задумываться?
- https://radar.qrator.net/as12389



Рекомендации по защите роутера. Обновление.

- По возможности обновляйте RouterOS.
- Читайте changelog
- Обращайте особое внимание на security bugfix

Схема для операторов:

- Представьте , что вы “маленький” оператор, сеть которого есть только в одном городе.
- У вас есть большой клиент, с множеством филиалов, вы оказываете услуги клиенту на всех его точках.

Схема для операторов:

- Ваш клиент просит добавить новую точку, но точка в близлежащем городе.
- Строить сеть в соседний город не целесообразно.
- Так сложилось, что на конечной точке клиента есть только маленькие локальные операторы, которых нет в вашем городе.

Ограничения оператора

- Биллинг умеет работать только с одним роутером
- Технология авторизации “завязана” на статический Ipv4 у абонента.

Техническая задача

- Организовать L2-канал:
  - от маршрутизатора провайдера в одном городе
  - до оборудования клиента в другом городе

Решение от “Экспертов”:

- Построим туннель через Public Internet.
- Инженеры оператора находят информацию в Интернете об оборудовании RouterBoard с RouterOS и решают запустить схему на этом оборудовании

Конечная схема. Пример.

- Рядом с маршрутизатором оператора ставим устройство RB1100AHx2
- Подключаем к Интернету, получаем статический публичный IP-адрес
- Настраиваем PPTP-сервер
- На PPTP адресах строим EoIP
- VLAN в сторону маршрутизатора и EoIP туннель добавляем в bridge

Конечная схема. Пример.

- На удалённой точке клиента ставим устройство RB951Ui-2HnD
- Подключаем к Интернету, получаем динамический публичный IP-адрес
- Строим PPTP туннель
- На PPTP адресах строим EoIP
- Порты в сторону клиента и EoIP туннель добавляем в bridge

Сложности

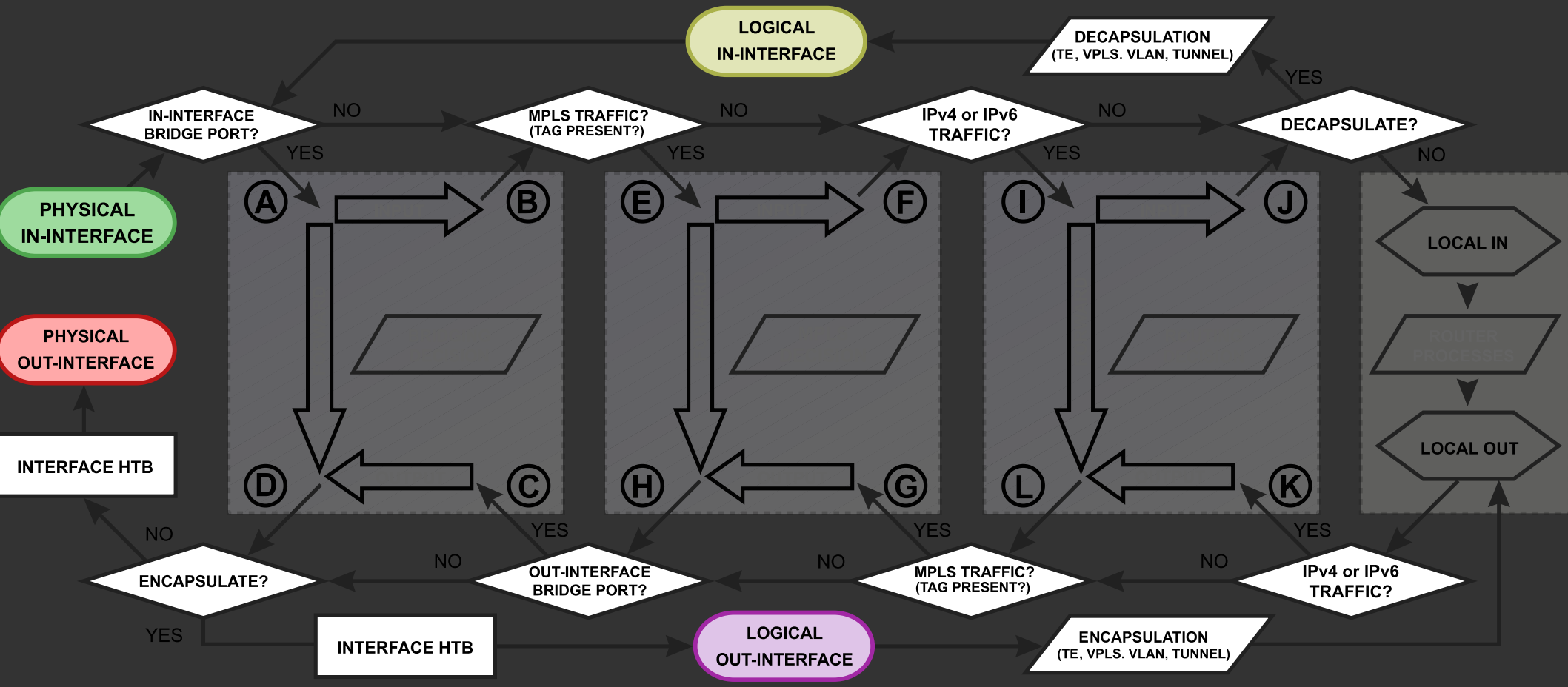
- Удалённых точек становится много
- Часть из них имеет серый адрес
- Несколько PPTP тунелей не работает через один NAT (ограничение GRE)
- На части точек нет проводного Интернета

Усложнение схемы

- Вместо PPTP иногда используем L2TP
- … а иногда SSTP…
- Иногда используем мобильный интернет.

Что получилось:

					L2 клиента	IP клиента	payload
				EoIP			
			GRE (PPTP)				
Ethernet	L2 для туннеля	IP для туннеля					
Mobile NET	ppp	Private IP для туннеля					


LOGICAL
IN-INTERFACE
DECAPSULATION
(TE, VPLS. VLAN, TUNNEL)
IN-INTERFACE
BRIDGE PORT?
NO
MPLS TRAFFIC?
(TAG PRESENT?)
NO
IPv4 or IPv6
TRAFFIC?
NO
DECAPSULATE?
YES
YES
YES
YES
NO
PHYSICAL
IN-INTERFACE
PHYSICAL
OUT-INTERFACE
INTERFACE HTB
A
B
C
D
E
F
G
H
I
J
K
L
LOCAL IN
ROUTER
PROCESSES
LOCAL OUT
NO
YES
NO
YES
NO
YES
NO
YES
ENCAPSULATE?
OUT-INTERFACE
BRIDGE PORT?
MPLS TRAFFIC?
(TAG PRESENT?)
IPv4 or IPv6
TRAFFIC?
YES
INTERFACE HTB
LOGICAL
OUT-INTERFACE
ENCAPSULATION
(TE, VPLS. VLAN, TUNNEL)

Как исправить

- На удалённых точках использовать только статический публичный IP, это позволит использовать только туннель EoIP
- Если невозможно, использовать PPTP + BCP
- Считать MTU, “продавать” клиенту сразу MTU, которое вы можете предоставить

Спасибо за Внимание.

μTik.pro

http://mtik.pro