

Обзор сомнительных технических решений на RouterOS и их разбор

Обзор кейсов и конфигураций.



<http://mtik.pro>

Об авторе

- **Мартюшев Тимофей**
- **Более 6 лет работы в провайдерах**
- **MTCNA, MTCIPv6E, MTCRE, MTCINE**
- **MikroTik certified trainer (TR0422)**
- **MikroTik Academy Coordinator**

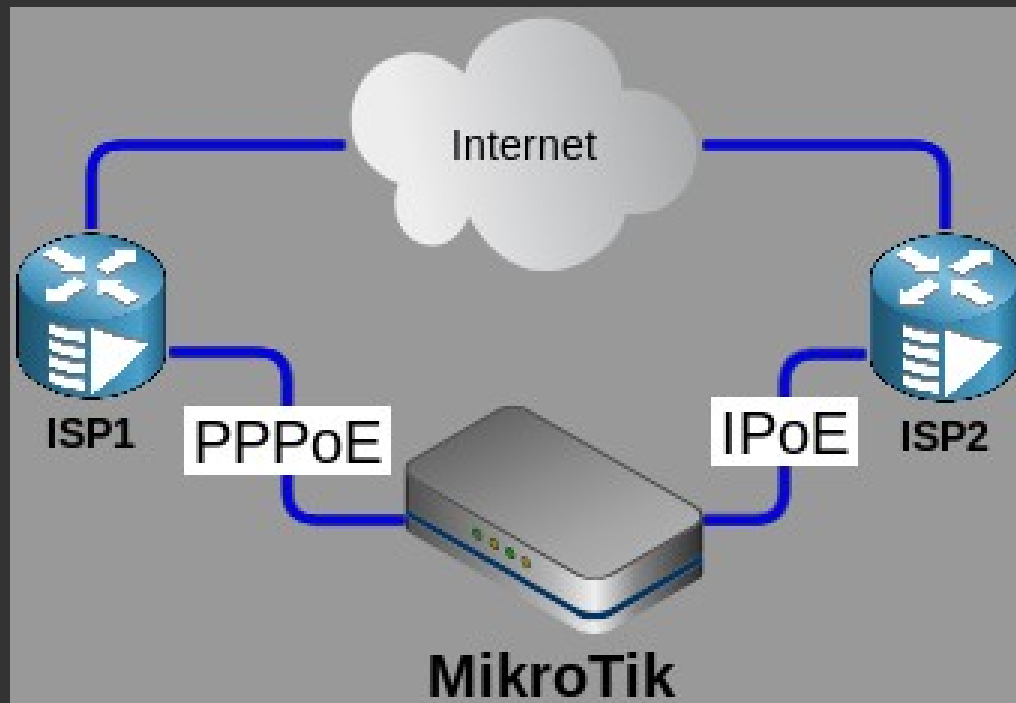
Источники

- Чат MikrotikRu
<https://t.me/MikrotikRu>
- Инструкции “экспертов” крупных и не очень операторов по настройке RouterOS для рядовых инженеров
- 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.

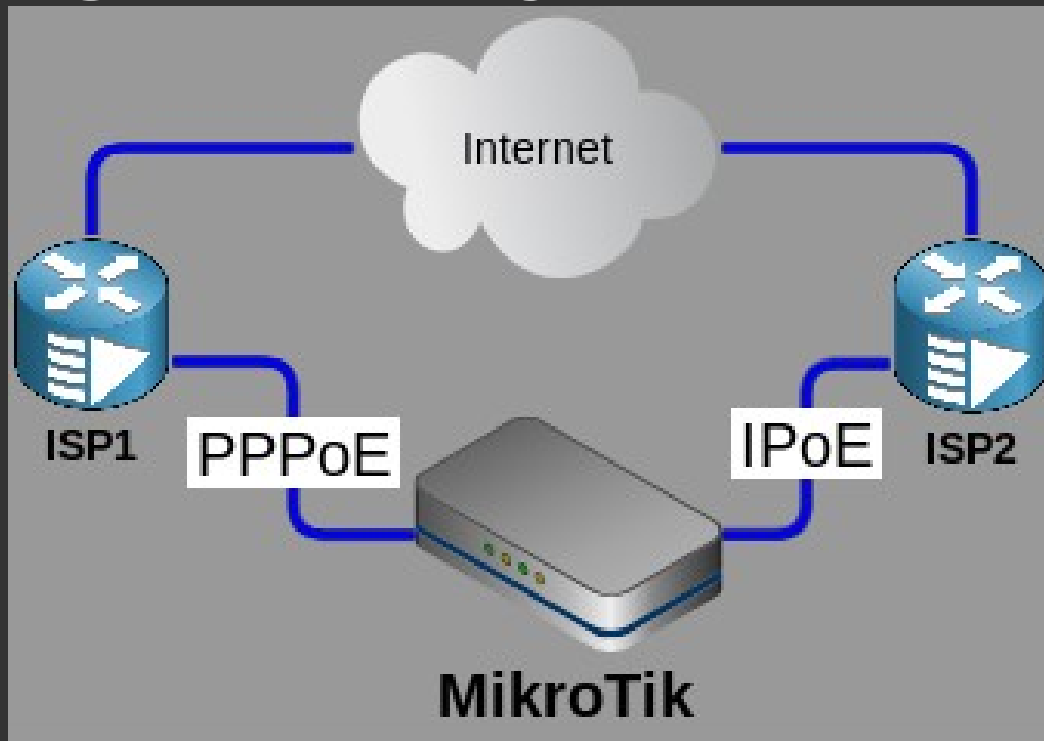


Конфиг

```
/ip route
```

```
add gateway=pppoe-out . . .
```

```
add gateway=ether3 . . .
```



Результат

/tool sniffer quick

INTERFACE	SRC-MAC	DST-MAC	SRC-ADDRESS	PROTOCOL
ether3	6C:3B:6B:9D:DC:62	FF:FF:FF:FF:FF:FF	10.128.4.14: who has 40.69.218.62?	arp
ether3	6C:3B:6B:9D:DC:62	FF:FF:FF:FF:FF:FF	10.128.4.14: who has 8.8.8.8?	arp
ether3	6C:3B:6B:9D:DC:62	FF:FF:FF:FF:FF:FF	10.128.4.14: who has 1.1.1.1?	arp
ether3	6C:3B:6B:9D:DC:62	FF:FF:FF:FF:FF:FF	10.128.4.14: who has 8.8.8.8?	arp
ether3	...	FF:FF:FF:FF:FF:FF	...: who has ... ?	arp

Результат

INTERFACE	TIME	NUM	DIR	SRC-MAC	DST-MAC	SRC-ADDRESS	PROTOCOL
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

Вывод

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

2

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>, <https://monitor.firefox.com/>)
- 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)
- 2828 (uPnP)

- UDP:

- 53 (DNS)
- 69 (TFTP)
- 123 (NTP)
- 161-162 (SNMP)
- 1194 (OpenVPN)
- 1701 (L2TP)
- 2000 (Bandwidth-test)
- 1900 (uPnP)

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 - март

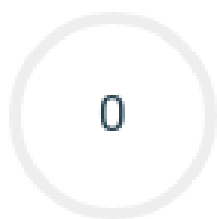
- Почему стоит задумываться?
- <https://radar.qrator.net/as12389>

Security Issues



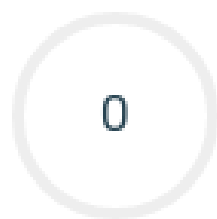
3.01

Rate



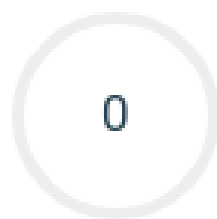
0

Route Leaks



0

MOAS



0

Bogons



27.54k

Static Loops



5 600

Vulnerable
Ports



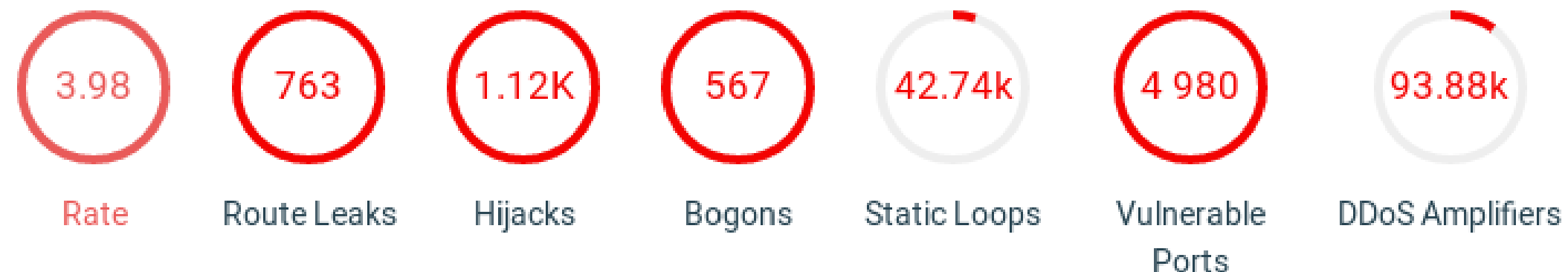
171.8k

DDoS Amplifiers

DoS Amplifiers – сентябрь

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

Security Issues



Рекомендации по защите роутера. Обновление.

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

Что если не обновлять?

Добрый день!

Микротик обновился до 6.42.7 и теперь пасс админа не подходит

Не подскажете как сбросить пасс не сбрасывая конфиг?

Бэкапа нет ((

Приветствую. Сам обновился?

Да... Я не обновлял

И сам ребутнулся 5 дней назад

CCR1009

3

Игра в угадайку

Port Properties		
ifIndex	Port	ifType / Status
1	ether12 FREE	Ethernet disabled / down
2	ether13 FREE	Ethernet disabled / down
3	ether1 ether1_WAN-MGMT	Ethernet enabled / up
4	ether2 ether2_Clients_EOIP_Port-2-Vlan	Ethernet enabled / up
5	ether3 ether3_MBS001_NAME1	Ethernet enabled / up
6	ether4 ether4_MBS001_NAME2	Ethernet enabled / up
7	ether5 ether5_MBS001_NAME3	Ethernet enabled / up
8	ether6 ether6_MBS001_NAME4	Ethernet enabled / up
9	ether7_AN003_NAME,15	Ethernet enabled / up
10	ether7	Ethernet enabled / up
11	ether8 ether9_free	Ethernet enabled / up
12	ether10 FREE	Ethernet disabled / down
13	ether11 FREE	Ethernet disabled / down

Именованние интерфейсов

(Примеры)

- 55555
- bridge_880_10.74.251.1_некоторое обш ZADACHA-15
- Lombard_1991_br
- bridge_v1581_ISP1/Pochta_to_ul.Uralskaya d.1
- Vlan100
- Vlan100_1

Вывод

- Договоритесь с коллегами об именовании интерфейсов (и не только интерфейсов)
- Опишите правила именования
- Покажите ваши правила именования внешнему специалисту

Будут ли они понятны новичку?

- Избегайте неоднозначности
- Помните про комментарии

Именованние интерфейсов

(один из вариантов)

Вариант именованния:

- **VLAN** – <ifName>.<svlan>[.<cvlan>]

Пример: ether5.100 , sfp1.15.300

- **Bridge** – bridge-<comment>

Пример: bridge-pppoe, bridge-l2vpn-id12389

- **IPIP** – ipip-<comment> (аналогично для **GRE/EoIP**)

Пример: gre-prk , ipip-parentshome

- **BONDING** - bond<N>

4

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 туннелей не работает через один NAT (ограничение GRE)
- На части точек нет проводного Интернета

Усложнение схемы

- Вместо РРТР иногда используем L2TP
- ... а иногда SSTP...
- Иногда используем мобильный интернет.

Что получилось:

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

Вопросы по схеме

- Если у конечного клиента Интернет с полосой 10 Мбит/сек, сможет ли он получить её, если на его точке для туннелей Интернет с полосой 10 Мбит/сек?
- Как посчитать полосу для туннелей?
 - +0%
 - +15%
 - +1 Мбит/сек

Как исправить

- На удалённых точках использовать статический публичный IP, это позволит использовать только туннель EoIP
- Если невозможно, использовать PPTP + VSP или L2TP + VSP
- Считать MTU, “продавать” клиенту сразу MTU, которое вы можете предоставить

5

Схема для операторов:

- Ваш клиент просит добавить новую точку, но точка в близлежащем городе.
- Строить сеть в соседний город не целесообразно.
- Есть возможность взять L2VPN у стороннего оператора

Дополнительные требования

- Требуется мониторить стык с конечным клиентом
- Очень хочется поставить клиенту оборудование с логотипом своей компании

Техническая задача

- “Внутри” L2VPN от стороннего оператора:
 - Предоставить услугу конечному клиенту (PPPoE, IроE, IPv6oE, L2VPN)
 - Организовать IP связность с оборудованием, установленным у клиента
 - Изолировать каналы

Решение от “Экспертов”:

- На конечную точку ставим hAP lite
- Поднимаем “серую” адресацию
- Построим туннель EoIP туннель на серых адресах до RB1100AHx2
- Клиентский трафик будет “ходить” внутри туннеля

Усложнение схемы

На конечной точке клиенту требуется несколько услуг:

- Используем VLAN внутри EoIP
- или
- Используем несколько EoIP (`tunnel-id`)

Что получилось:

				L2 клиента	IP клиента	payload
			EoIP (GRE)			
Ethernet	L2 для туннеля	IP для туннеля				

Как исправить:

- “Отдать весь L2-канал для трафика клиента
- Для управления использовать VLAN внутри L2-канала
- Явно уменьшить MTU на интерфейсах управления

Как исправить:

Ethernet		L2 клиента	IP клиента	payload
	VLAN MGMT	L2 MGMT	IP MGMT	payload MGMT

Спасибо за Внимание.
