

Настройка GRE over IPSEC на Микротик

 mikrotiklab.ru/nastrojka/artga-gre-ipsec.html

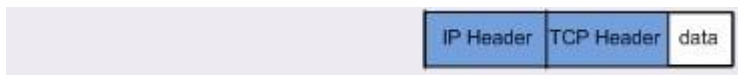
February 14, 2020

В данной статье поговорим как настроить GRE туннель over IPSEC на роутере Микротик. Но сначала немного теории, GRE – это туннельный протокол разработанный компанией Cisco. Основная задача – инкапсуляция большого количества протоколов через виртуальный point-to-point линк. Работает на сетевом уровне TCP/IP и не имеет порта. Для лучшего понимания можно провести аналогию его с протоколами без отслеживания состояния, а именно IPIP и EoIP.

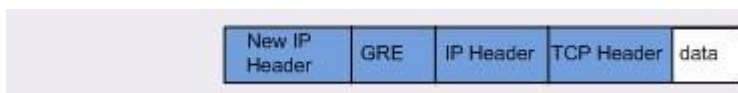
Это означает, что, если ваш линк на одной из сторон упадет, вы не сможете этого понять, находясь на другой стороне – это классика. Но компания Mikrotik добавила компонент keeralive. Теперь можно отслеживать состояние линка отправляя тем самым keeralive запросы. Отсутствует шифрование по понятным причинам, но это не беда, ведь у нас есть IPSEC. GRE туннель может пересылать только IPv4 и IPv6 пакеты. Не используйте «Check gateway» опцию «agr».

В своей практике, данное решение использую крайне редко, хоть он и используется в PPTP.

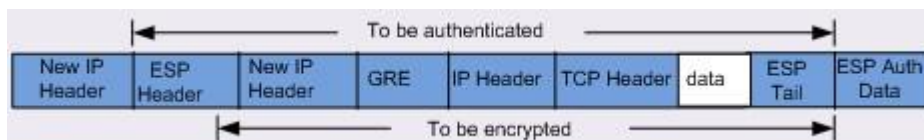
Взглянем на обычный IP пакет.



Теперь посмотрим с GRE.



И еще с IPSEC в туннельном режиме.

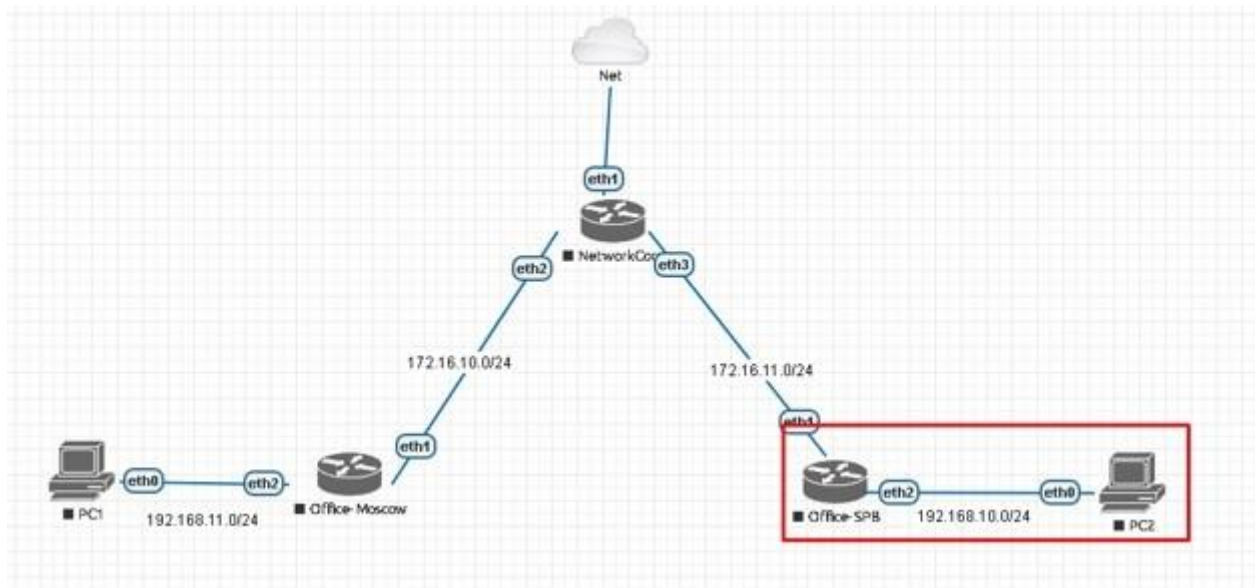


Наша команда рекомендует изучитьНаша команда рекомендует изучить [углубленный курс по администрированию сетевых устройств MikroTik](#) В курсе много лабораторных работ по итогам которых вы получите обратную связь. После обучения вы получите диплом гос. образца РФ. Подробности и доступ к началу курса бесплатно [ТУТ](#).

Содержание

1. [Схема сети](#)
2. [Настройка GRE](#)
3. [Настройка GRE IPSEC](#)

Схема сети



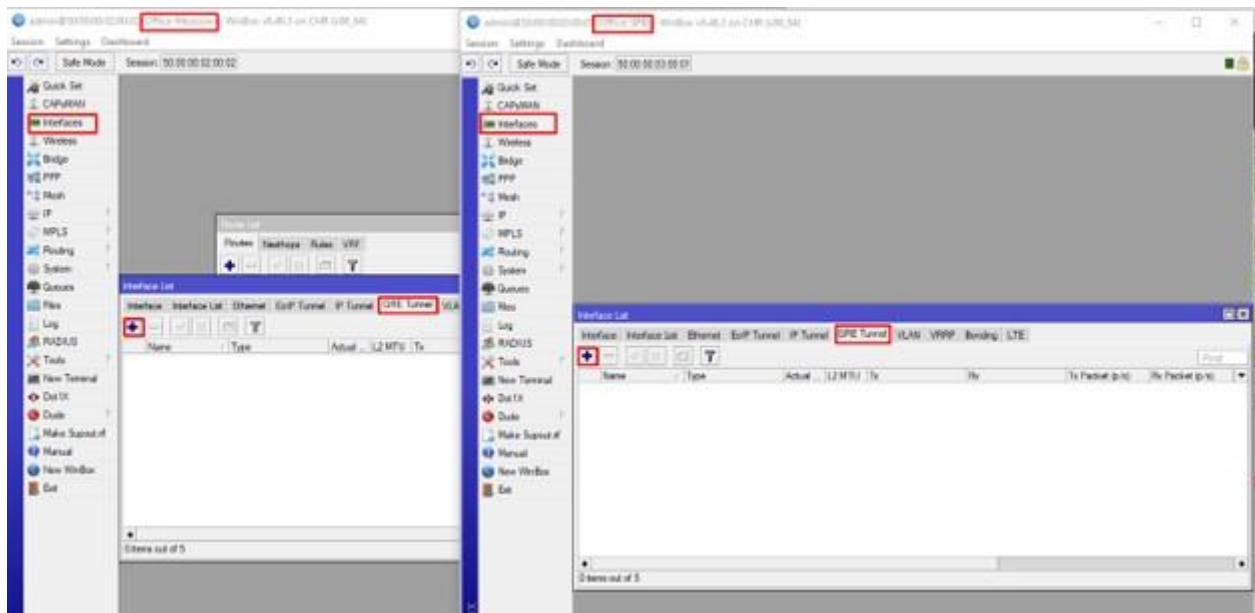
Используем лабораторный стенд с Mikrotik CHR версии 6.46.3 на борту. Мы находимся справа внизу в офисе SPB (Office-SPB). Вводные данные:

- Office-SPB GRE пир;
- Office-Moscow GRE пир;
- NetworkCore выполняет роль провайдера, он будет заниматься обычной маршрутизацией;
- Office-Moscow ether1 смотрит в интернет 172.16.10.2/24;
- Office-SPB ether1 смотрит в интернет 172.16.11.2/24;
- Office-Moscow имеет bridge “General-Bridge” в локальной сети 192.168.11.1/24;
- Office-SPB имеет bridge “General-Bridge” в локальной сети 192.168.10.1/24;
- Адресация сети в туннеле 172.16.25.0/24.

Настройка GRE

Первым шагом рассмотрим простую настройку gre туннеля. Вся она будет одинакова на обоих роутерах. Подключившись к нажим железкам через Winbox и перейдем в Interfaces – GRE Tunnel.

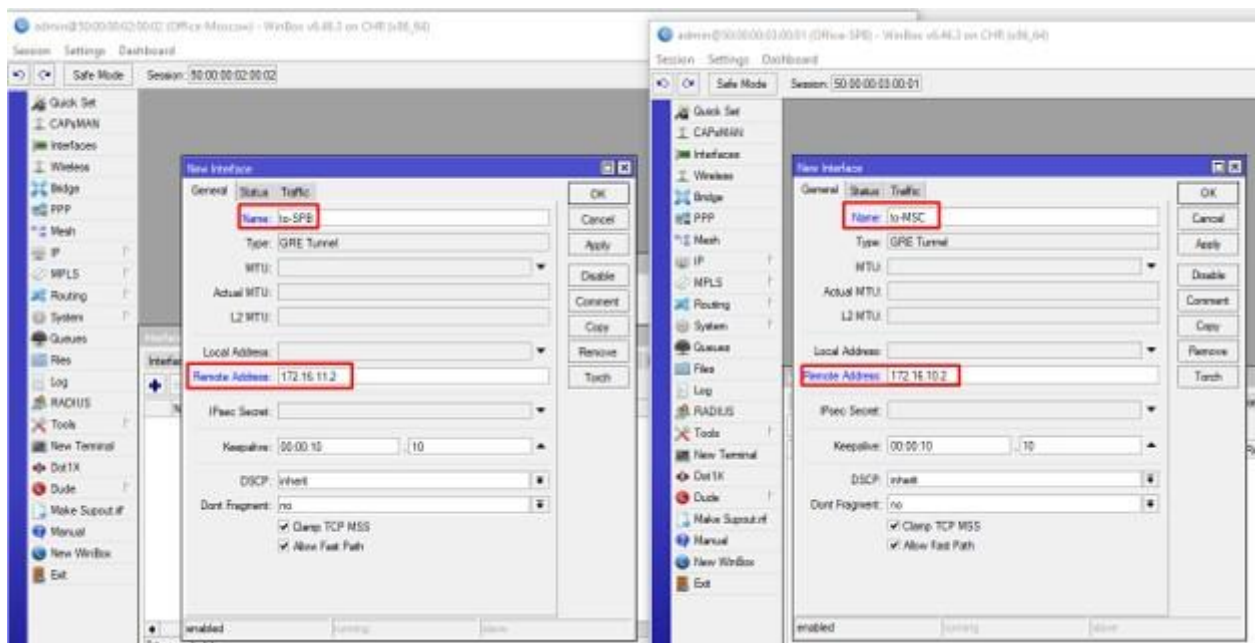











Создадим по интерфейсу. Укажем следующие параметры:

- Name – понятное имя;
- Remote Address – адрес соседа по туннелю. Основной принцип — направляем роутеры друг на друга;

Keepalive – тот самый параметр отслеживания состояния. Можно ничего не менять. Он означает следующее – если в течении 10 попыток по 10 секунд не отвечает удаленная сторона, считать туннель не активным.



Сохраняем настройки и смотрим на состояние.

Interface List					
Interface	Interface List	Ethernet	EoIP Tunnel	IP Tunnel	GRE Tunnel
					
	Name	Type	Actual ...	L2 MTU	Tx
R	 to-SPB	GRE Tunnel	1476	65535	

Как мы видим, интерфейс в состоянии running. Назначим адреса. Переходим в IP – Addresses.

admin@50:00:00:02:00:02 (Office-Moscow) - WinBox v6.46.3 on CHR (x86_64)

Session Settings Dashboard

Safe Mode Session: 50:00:00:02:00:02

- Quick Set
- CAPsMAN
- Interfaces
- Wireless
- Bridge
- PPP
- Mesh
- IP**
- MPLS
- Routing
- System
- Queues
- Files
- Log
- RADIUS
- Tools
- New Terminal
- Dot1X
- Dude

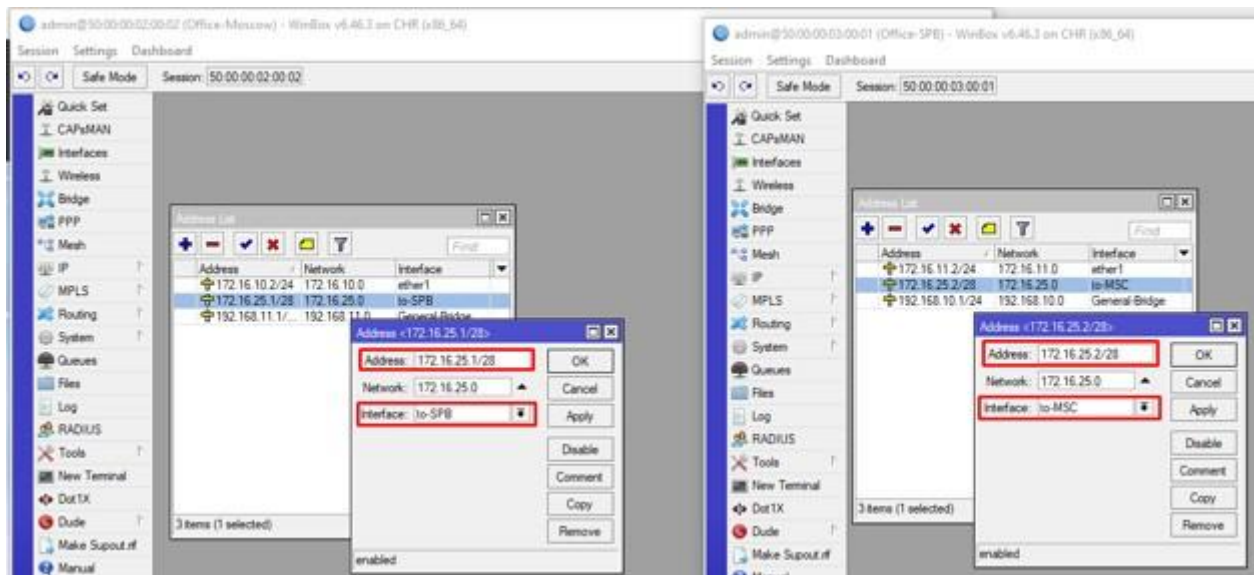
Address List

Find

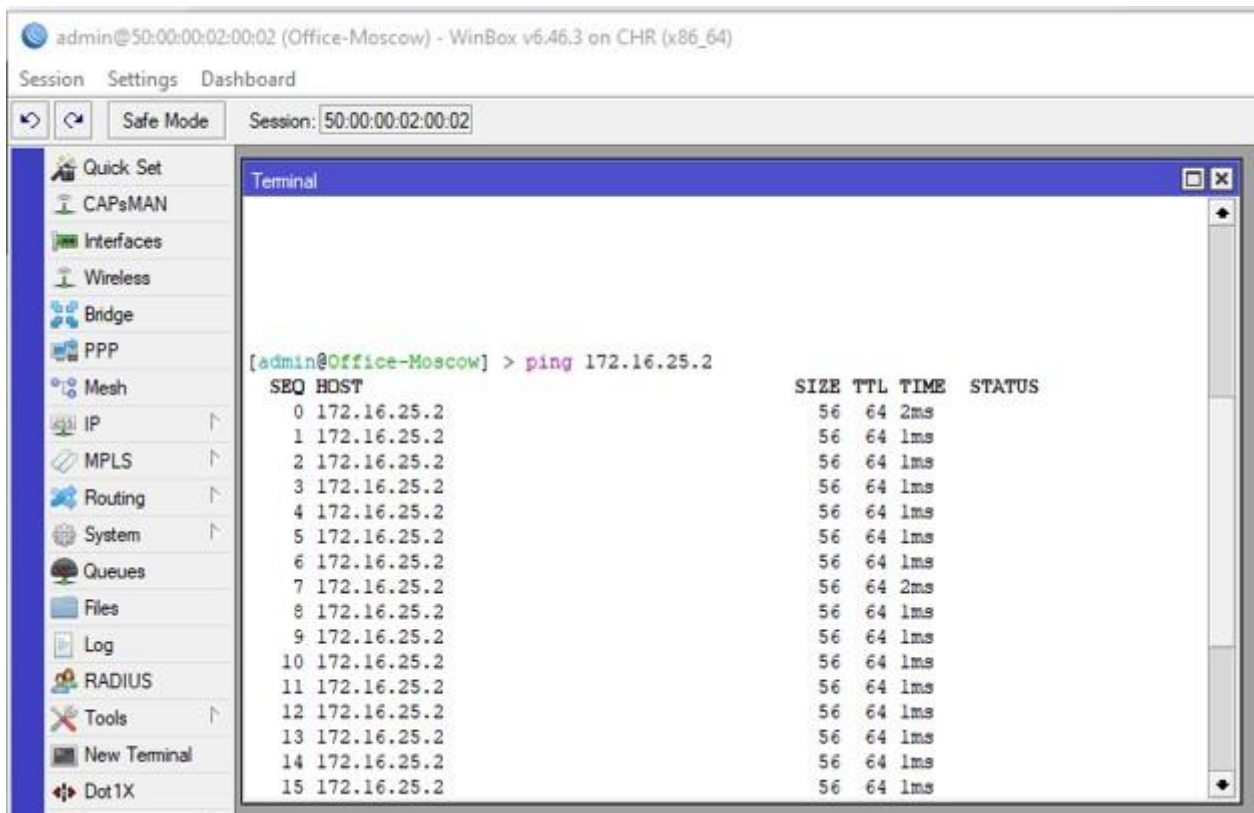
Address	Network	Interface
172.16.10.2/24	172.16.10.0	ether1
192.168.11.1/...	192.168.11.0	General-Bridge

2 items (1 selected)

Зададим адрес 172.16.25.1 для московского роутера и 172.16.26.2 для питерского.



Для проверки связи запустим ping запросы.



Пинги идут – все хорошо. Далее пропишем маршруты в локальные сети. Открываем IP – Routes на московском.

Route List						
<div> <div>Routes</div> <div>Nexthops</div> <div>Rules</div> <div>VRF</div> </div> <div> <div>+</div> <div>-</div> <div>✓</div> <div>✗</div> <div>📄</div> <div>🔍</div> <div>Find</div> <div>all</div> <div>▼</div> </div>						
	Dst. Address	/	Gateway	Distance	Routing Mark	Pref. Source
AS	▶ 0.0.0.0/0		172.16.10.1 reachable ether1	1		
DAC	▶ 172.16.10.0/24		ether1 reachable	0		172.16.10.2
DAC	▶ 172.16.25.0/28		to-SPB reachable	0		172.16.25.1
DAC	▶ 192.168.11.0/24		General-Bridge reachable	0		192.168.11.1
4 items						

Добавляем новый маршрут:

- Dst. Address – 192.168.10.0/24;
- Gateway – 172.16.25.2.

New Route		OK
General		Cancel
Attributes		Apply
Dst. Address:	192.168.10.0/24	Disable
Gateway:	172.16.25.2	Comment
Check Gateway:		Copy
Type:	unicast	Remove
Distance:		
Scope:	30	
Target Scope:	10	
Routing Mark:		
Pref. Source:		
enabled	active	

Сохраняем и проделываем аналогичную операцию только на питерском роутере.

Route <192.168.11.0/24>

General Attributes

Dst. Address: 192.168.11.0/24

Gateway: 172.16.25.1 reachable to-MSK

Check Gateway:

Type: unicast

Distance: 1

Scope: 30

Target Scope: 10

Routing Mark:

Pref. Source:

enabled active

OK Cancel Apply Disable Comment Copy Remove

Основной принцип – прописать маршруты в сети через адреса в туннелях.
Проверим ping до адреса бриджа Mikrotik в Москве.

admin@50:00:00:03:00:01 (Office-SPB) - WinBox v6.46.3 on CHR (x86_64)

Session Settings Dashboard

Safe Mode Session: 50:00:00:03:00:01

Quick Set CAPsMAN Interfaces Wireless Bridge PPP Mesh IP MPLS Routing System Queues Files Log RADIUS Tools New Terminal Dot1X

Terminal

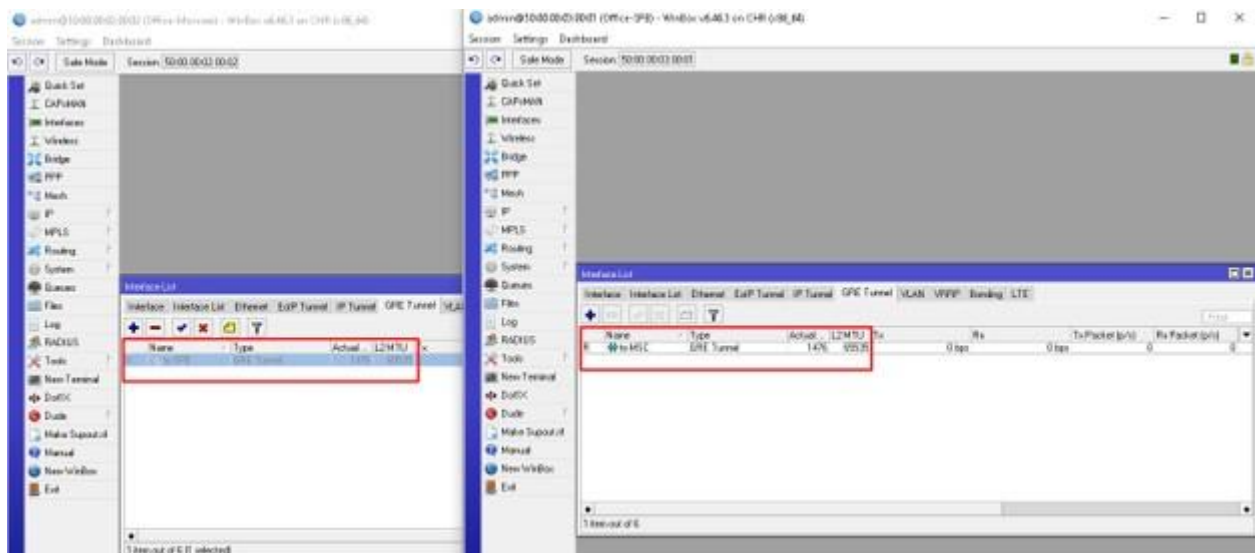
```
[admin@Office-SPB] > ping 192.168.11.1
```

SEQ	HOST	SIZE	TTL	TIME	STATUS
0	192.168.11.1	56	64	1ms	
1	192.168.11.1	56	64	1ms	
2	192.168.11.1	56	64	2ms	
3	192.168.11.1	56	64	1ms	
4	192.168.11.1	56	64	1ms	
5	192.168.11.1	56	64	1ms	
6	192.168.11.1	56	64	1ms	

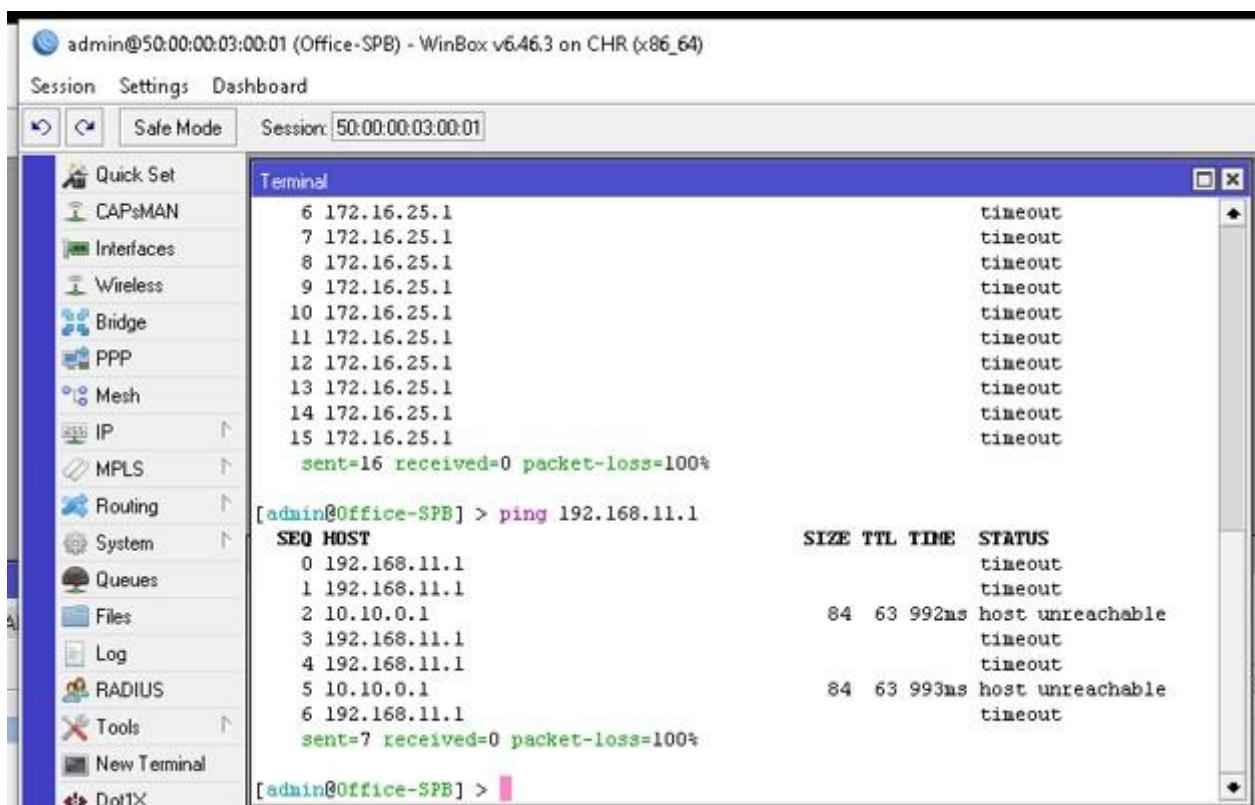
sent=7 received=7 packet-loss=0% min-rtt=1ms avg-rtt=1ms max-rtt=2ms

[admin@Office-SPB] >

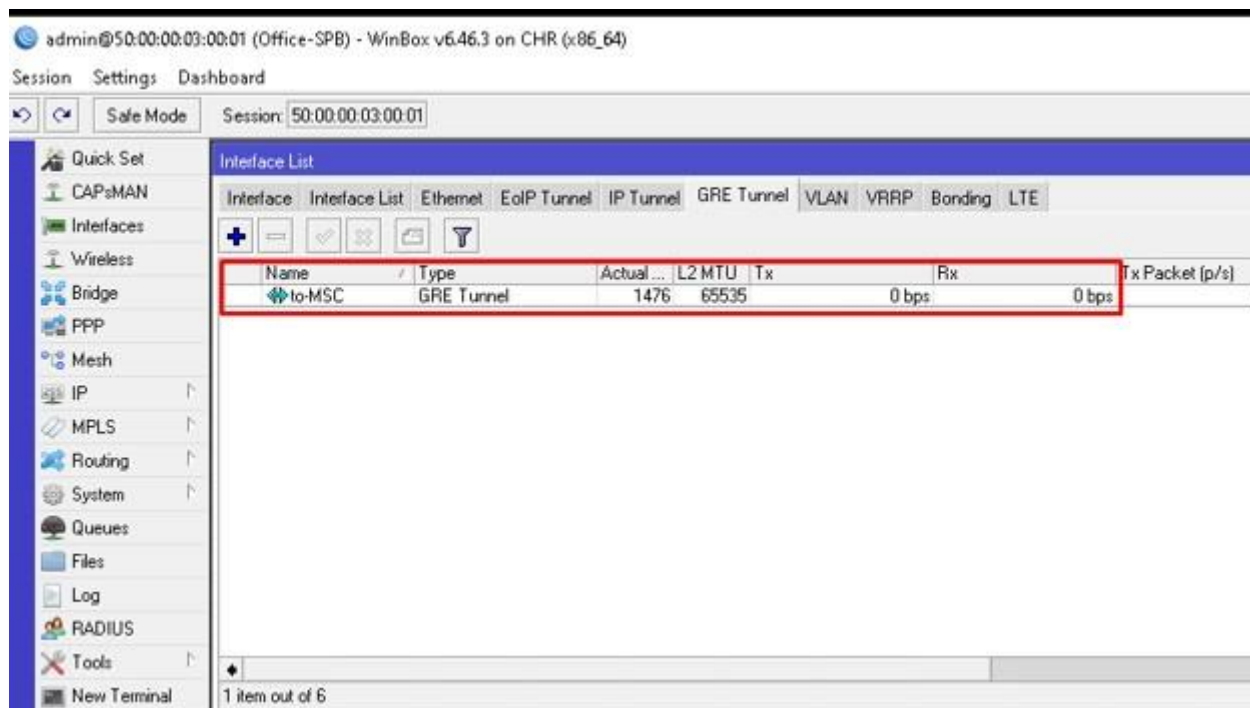
Все отлично – значит мы правильно сделали. В целях демонстрации я отключу интерфейс в Москве, выжду интервал в 100 секунд и посмотрим на состояние туннеля.



Интересная ситуация, в одном офисе интерфейс активный, а в другом нет. Попробуем проверить связь.



Пингов нет, а туннель активен. Спустя какое-то время, Mikrotik в Питере понимает, что связи через gre туннель нет и меняют статус на интерфейс.

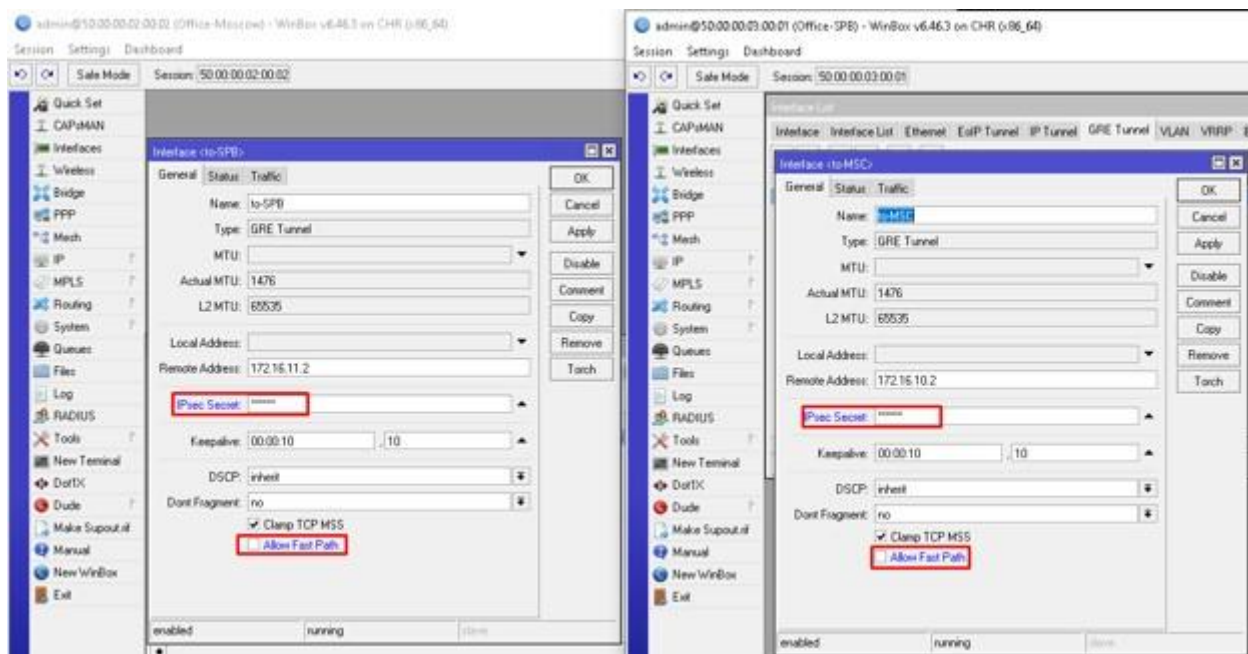


Тут-то и помогла доработка Mikrotik с keepalive. К чему этот эксперимент спросите вы? Во-первых – для демонстрации, во-вторых – если есть те, кто еще используют данный протокол для своих задач, имейте ввиду, что маршруты в routes будут активны то время, которое вы указали в keepalive. Только по истечении этого времени маршруты и адрес станут не активны.

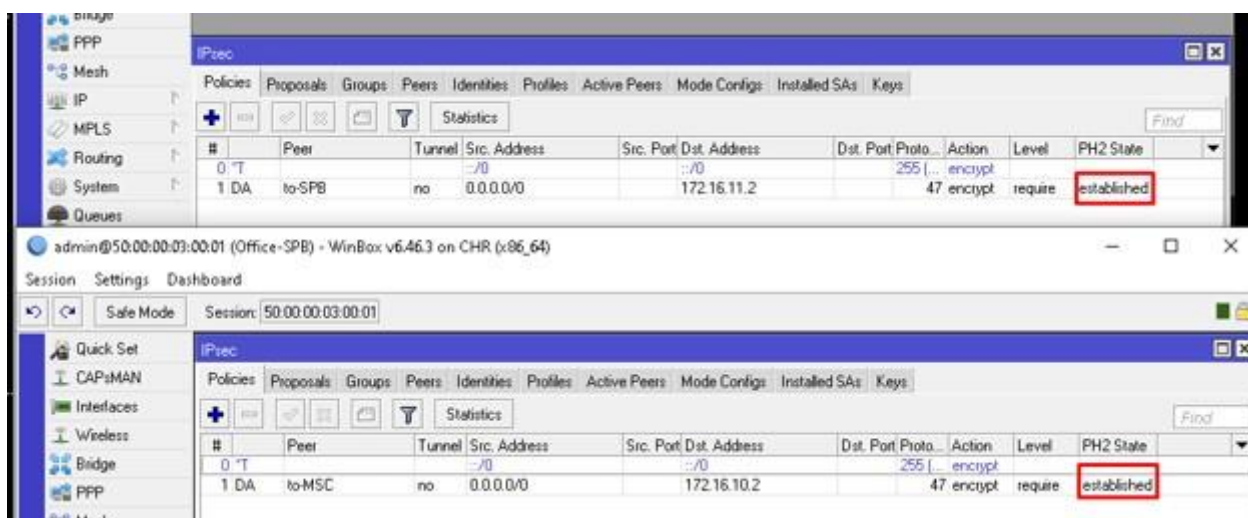
Настройка GRE IPSEC

Более подробно с IPSEC можно познакомиться в [одной из наших статей](#). Напомню только то, что нам необходимо вернуть московский в состояние активный и дождаться установки соединения. Далее переходим в настройки интерфейса и меняем следующие параметры:

- IPsec Secret – общий ключ (пароль);
- Allow Fast Path – снимаем галочку.



Сохраняем и проверяем.



Указав общий ключ, наши микротики согласуют стандартный IPSEC (не IKEv2) и инкапсулирует в него GRE. На этом настройка завершена. Спасибо за внимание и не забываем про safe mode.

Вы хорошо разбираетесь в Микротиках? Или впервые недавно столкнулись с этим оборудованием и не знаете, с какой стороны к нему подступиться? В обоих случаях вы найдете для себя полезную информацию в углубленном курсе «Администрирование сетевых устройств MikroTik». В курсе много практических лабораторных работ по результату выполнения которых вы получите обратную связь. После окончания обучения вы получите диплом гос. образца РФ. Подробности и доступ к началу курса бесплатно [тут](#).