

Настройка L2TP IPSEC на Mikrotik

 mikrotiklab.ru/nastrojka/artga-l2tp-ipsec.html

January 30, 2020

Это продолжение предыдущих двух статей ([Первая](#)) и ([Вторая](#)) в которых мы показали как настроить L2TP на MikroTik без IPSec, теперь же прикроем его к нашей конфигурации.

IPSEC – это целый набор протоколов, обеспечивающих защиту данных IP через сеть интернет. Несомненно, он один из самых безопасных реализаций VPN, но ложкой дегтя является сложность настройки. Некоторые модели RouterBOARD имеют встроенные чипы разгрузки для алгоритмов AES, это сделано для того, чтобы не нагружать центральный процессор сложной обработкой. Ознакомиться более подробно со списком оборудования поддерживающих аппаратную разгрузку можно на сайте mikrotik.com.

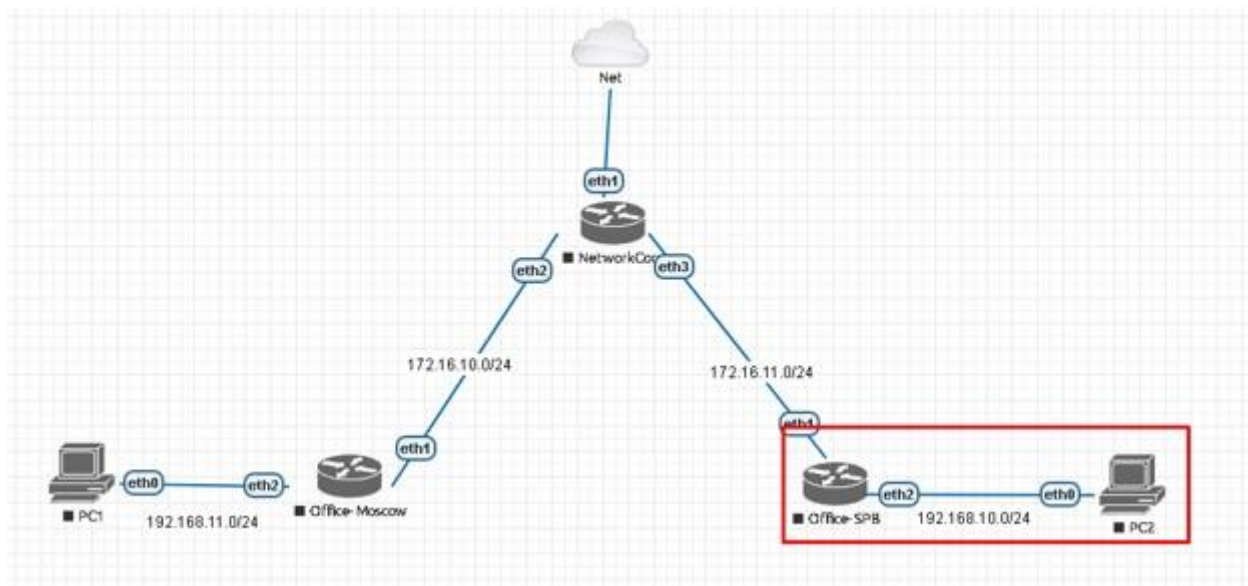
В нижеизложенной инструкции будет продемонстрировано конфигурирование классического IPSEC, а не IKEv2. На основе предыдущих статей я покажу два режима настройки L2TP/IPSec в транспортном режиме на роутере микротик. По сложившейся практике предпочтительно делать именно в транспортном режиме, т.к. удобнее прописать маршруты в локальные сети через адреса в туннелях вместо создания NAT правил. В добавок про NAT отмечу, что IPSEC-у становится дурно, когда он проходит через него. Не плохо реализована поддержка NAT-T. Взяв во внимание вышеизложенную информацию приступим.

Наша команда рекомендует изучить [Наша 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. [Простая настройка](#)
3. [Site to site](#)
4. [Настройка firewall](#)

Схема сети

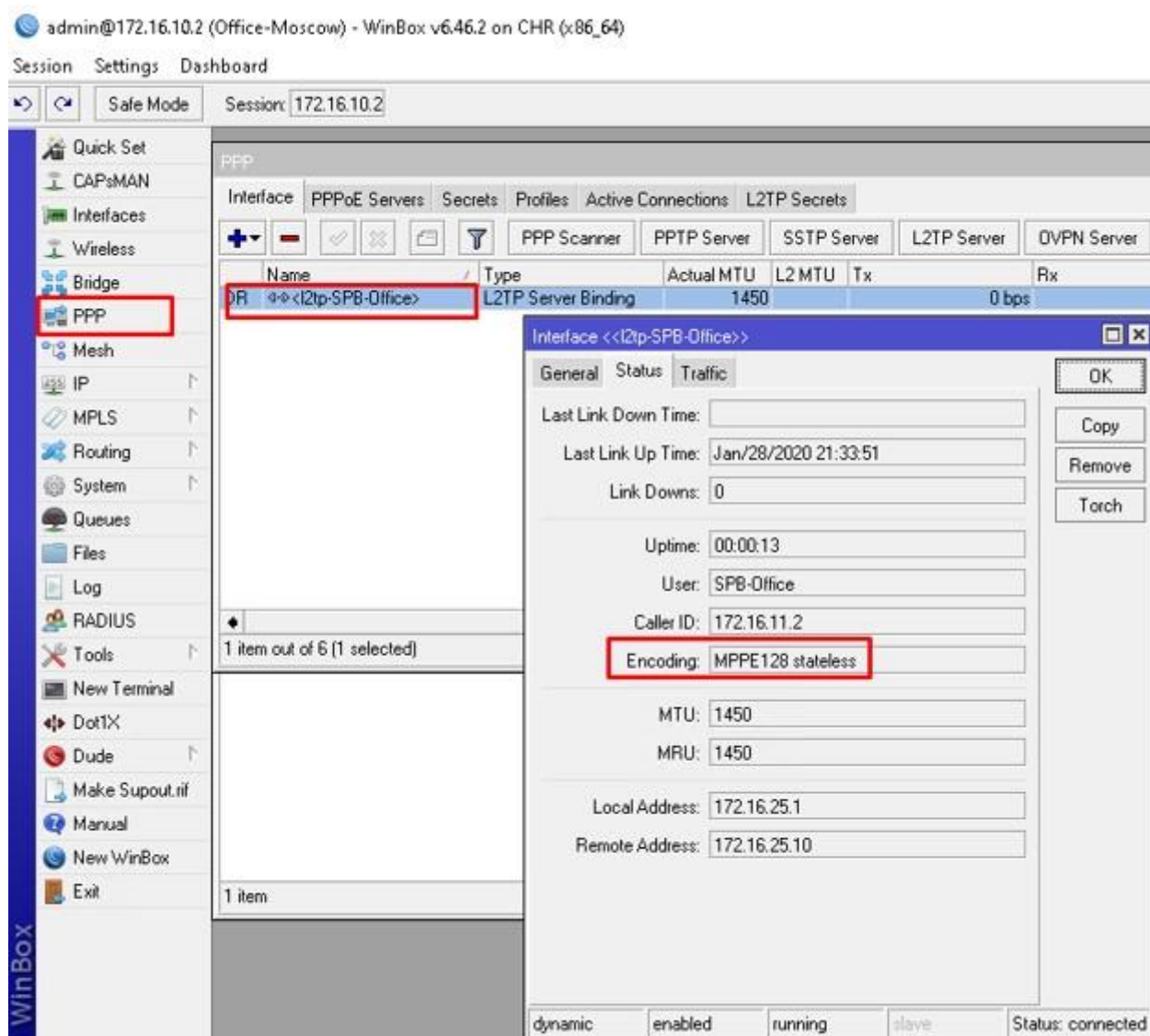


Используем лабораторный стенд с Mikrotik CHR версии 6.46.2 на борту. Мы находимся справа внизу в офисе SPB (Office-SPB). Вводные данные:

- Office-SPB сервер;
- Office-Moscow клиент;
- 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;
- IP ПК в локальной сети Office-Moscow 192.168.11.2;
- IP ПК в локальной сети Office-SPB 192.168.10.2;
- Адресация в VPN сети 172.16.25.0/24;
- Активный L2TP туннель между офисами.

Простая настройка

Предполагает быстрое развертывание на сервере и клиенте. Она более всего подходит для инсталляций, когда вы планируете чтобы к вам подключалось много мобильных устройств или устройств находящихся за NAT-ом. На московском роутере проверим состояние клиентского подключения. Переходим PPP – Interface – SPB-Office – Status.



С соединением все в порядке. В строке Encoding видим стандартное шифрование протокола L2TP. Открываем свойства сервера L2TP. Ставим required на параметре Use IPsec и указываем пароль.

Сохраняем. Клиентское соединение пропадает, т.к. теперь мы требуем согласование протокола IPSEC. Видим соответствующее сообщение в логах сервера. Оно говорит о том, что подключение было отброшено.

L2TP Server

☒ Enabled

Max MTU: 1450

Max MRU: 1450

MRRU:

Keepalive Timeout: 30

Default Profile: L2TP-Server-General

Max Sessions:

Authentication: ☒ mschap2 ☐ mschap1
☐ chap ☐ pap

Use IPsec: required

IPsec Secret: 11111111

Caller ID Type: ip address

☐ One Session Per Host

☐ Allow Fast Path

OK Cancel Apply

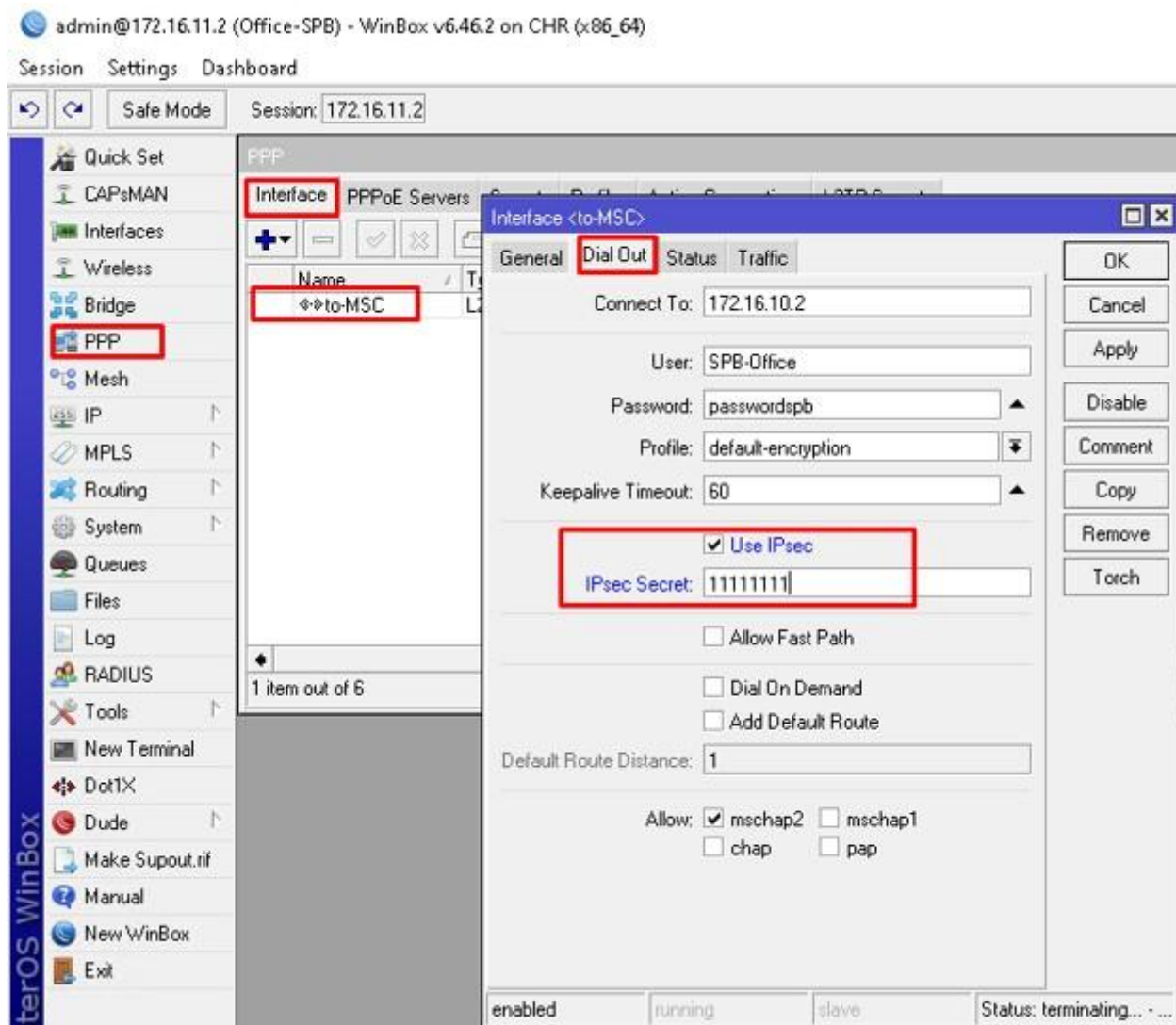
PPP

Interface PPPoE Servers Secrets Profiles Active Connections L2TP Secrets

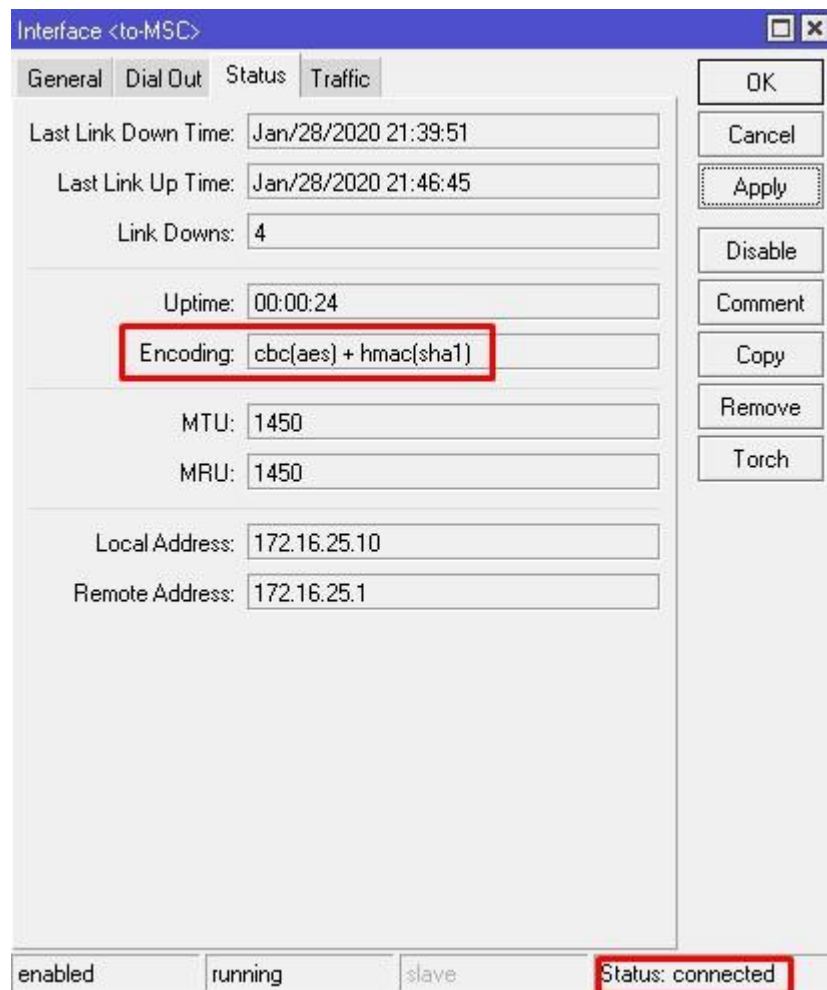
PPP Scanner PPTP Server SSTP Server L2TP Server OVPN Server PPPoE Scan

Name	Type	Actual MTU	L2 MTU	Tx	Rx	Tx Packet [p/																																																																																																																							
<div> <div>L2TP Server</div> <div> <div>Log</div> <div> <div>Freeze</div> <div>all</div> <table border="1"> <tbody> <tr> <td>Jan/28/2020 18:39:52</td> <td>memory</td> <td>l2tp, error</td> <td colspan="4">L2TP connection rejected no IPsec encryption while it was required</td> </tr> <tr> <td>Jan/28/2020 18:39:55</td> <td>memory</td> <td>l2tp, info</td> <td colspan="4">first L2TP UDP packet received from 172.16.11.2</td> </tr> <tr> <td>Jan/28/2020 18:39:55</td> <td>memory</td> <td>l2tp, error</td> <td colspan="4">L2TP connection rejected no IPsec encryption while it was required</td> </tr> <tr> <td>Jan/28/2020 18:40:01</td> <td>memory</td> <td>l2tp, info</td> <td colspan="4">first L2TP UDP packet received from 172.16.11.2</td> </tr> <tr> <td>Jan/28/2020 18:40:01</td> <td>memory</td> <td>l2tp, error</td> <td colspan="4">L2TP connection rejected no IPsec encryption while it was required</td> </tr> <tr> <td>Jan/28/2020 18:40:11</td> <td>memory</td> <td>l2tp, info</td> <td colspan="4">first L2TP UDP packet received from 172.16.11.2</td> </tr> <tr> <td>Jan/28/2020 18:40:11</td> <td>memory</td> <td>l2tp, error</td> <td colspan="4">L2TP connection rejected no IPsec encryption while it was required</td> </tr> <tr> <td>Jan/28/2020 18:40:21</td> <td>memory</td> <td>l2tp, info</td> <td colspan="4">first L2TP UDP packet received from 172.16.11.2</td> </tr> <tr> <td>Jan/28/2020 18:40:21</td> <td>memory</td> <td>l2tp, error</td> <td colspan="4">L2TP connection rejected no IPsec encryption while it was required</td> </tr> <tr> <td>Jan/28/2020 18:40:31</td> <td>memory</td> <td>l2tp, info</td> <td colspan="4">first L2TP UDP packet received from 172.16.11.2</td> </tr> <tr> <td>Jan/28/2020 18:40:31</td> <td>memory</td> <td>l2tp, error</td> <td colspan="4">L2TP connection rejected no IPsec encryption while it was required</td> </tr> <tr> <td>Jan/28/2020 18:40:41</td> <td>memory</td> <td>l2tp, info</td> <td colspan="4">first L2TP UDP packet received from 172.16.11.2</td> </tr> <tr> <td>Jan/28/2020 18:40:41</td> <td>memory</td> <td>l2tp, error</td> <td colspan="4">L2TP connection rejected no IPsec encryption while it was required</td> </tr> <tr> <td>Jan/28/2020 18:40:51</td> <td>memory</td> <td>l2tp, info</td> <td colspan="4">first L2TP UDP packet received from 172.16.11.2</td> </tr> <tr> <td>Jan/28/2020 18:40:51</td> <td>memory</td> <td>l2tp, error</td> <td colspan="4">L2TP connection rejected no IPsec encryption while it was required</td> </tr> <tr> <td>Jan/28/2020 18:41:01</td> <td>memory</td> <td>l2tp, info</td> <td colspan="4">first L2TP UDP packet received from 172.16.11.2</td> </tr> <tr> <td>Jan/28/2020 18:41:01</td> <td>memory</td> <td>l2tp, error</td> <td colspan="4">L2TP connection rejected no IPsec encryption while it was required</td> </tr> </tbody> </table> </div> </div> <div data-bbox="217 1948 1415 2031" data-label="Text"> <p>Если вы установите значение Use IPsec в yes, то все желающие подключиться без использования IPSEC – подключатся.</p> </div> <div data-bbox="1433 2163 1495 2195" data-label="Page-Footer"> <p>4/12</p> </div></div>							Jan/28/2020 18:39:52	memory	l2tp, error	L2TP connection rejected no IPsec encryption while it was required				Jan/28/2020 18:39:55	memory	l2tp, info	first L2TP UDP packet received from 172.16.11.2				Jan/28/2020 18:39:55	memory	l2tp, error	L2TP connection rejected no IPsec encryption while it was required				Jan/28/2020 18:40:01	memory	l2tp, info	first L2TP UDP packet received from 172.16.11.2				Jan/28/2020 18:40:01	memory	l2tp, error	L2TP connection rejected no IPsec encryption while it was required				Jan/28/2020 18:40:11	memory	l2tp, info	first L2TP UDP packet received from 172.16.11.2				Jan/28/2020 18:40:11	memory	l2tp, error	L2TP connection rejected no IPsec encryption while it was required				Jan/28/2020 18:40:21	memory	l2tp, info	first L2TP UDP packet received from 172.16.11.2				Jan/28/2020 18:40:21	memory	l2tp, error	L2TP connection rejected no IPsec encryption while it was required				Jan/28/2020 18:40:31	memory	l2tp, info	first L2TP UDP packet received from 172.16.11.2				Jan/28/2020 18:40:31	memory	l2tp, error	L2TP connection rejected no IPsec encryption while it was required				Jan/28/2020 18:40:41	memory	l2tp, info	first L2TP UDP packet received from 172.16.11.2				Jan/28/2020 18:40:41	memory	l2tp, error	L2TP connection rejected no IPsec encryption while it was required				Jan/28/2020 18:40:51	memory	l2tp, info	first L2TP UDP packet received from 172.16.11.2				Jan/28/2020 18:40:51	memory	l2tp, error	L2TP connection rejected no IPsec encryption while it was required				Jan/28/2020 18:41:01	memory	l2tp, info	first L2TP UDP packet received from 172.16.11.2				Jan/28/2020 18:41:01	memory	l2tp, error	L2TP connection rejected no IPsec encryption while it was required			
Jan/28/2020 18:39:52	memory	l2tp, error	L2TP connection rejected no IPsec encryption while it was required																																																																																																																										
Jan/28/2020 18:39:55	memory	l2tp, info	first L2TP UDP packet received from 172.16.11.2																																																																																																																										
Jan/28/2020 18:39:55	memory	l2tp, error	L2TP connection rejected no IPsec encryption while it was required																																																																																																																										
Jan/28/2020 18:40:01	memory	l2tp, info	first L2TP UDP packet received from 172.16.11.2																																																																																																																										
Jan/28/2020 18:40:01	memory	l2tp, error	L2TP connection rejected no IPsec encryption while it was required																																																																																																																										
Jan/28/2020 18:40:11	memory	l2tp, info	first L2TP UDP packet received from 172.16.11.2																																																																																																																										
Jan/28/2020 18:40:11	memory	l2tp, error	L2TP connection rejected no IPsec encryption while it was required																																																																																																																										
Jan/28/2020 18:40:21	memory	l2tp, info	first L2TP UDP packet received from 172.16.11.2																																																																																																																										
Jan/28/2020 18:40:21	memory	l2tp, error	L2TP connection rejected no IPsec encryption while it was required																																																																																																																										
Jan/28/2020 18:40:31	memory	l2tp, info	first L2TP UDP packet received from 172.16.11.2																																																																																																																										
Jan/28/2020 18:40:31	memory	l2tp, error	L2TP connection rejected no IPsec encryption while it was required																																																																																																																										
Jan/28/2020 18:40:41	memory	l2tp, info	first L2TP UDP packet received from 172.16.11.2																																																																																																																										
Jan/28/2020 18:40:41	memory	l2tp, error	L2TP connection rejected no IPsec encryption while it was required																																																																																																																										
Jan/28/2020 18:40:51	memory	l2tp, info	first L2TP UDP packet received from 172.16.11.2																																																																																																																										
Jan/28/2020 18:40:51	memory	l2tp, error	L2TP connection rejected no IPsec encryption while it was required																																																																																																																										
Jan/28/2020 18:41:01	memory	l2tp, info	first L2TP UDP packet received from 172.16.11.2																																																																																																																										
Jan/28/2020 18:41:01	memory	l2tp, error	L2TP connection rejected no IPsec encryption while it was required																																																																																																																										

Подключаемся к клиентскому Mikrotik в Питере, открываем PPP – Interface – выбираем интерфейс to-MSK и открываем вкладку Dial Out. Ставим галочку на UseIPsec и задаем пароль, установленный на сервере.



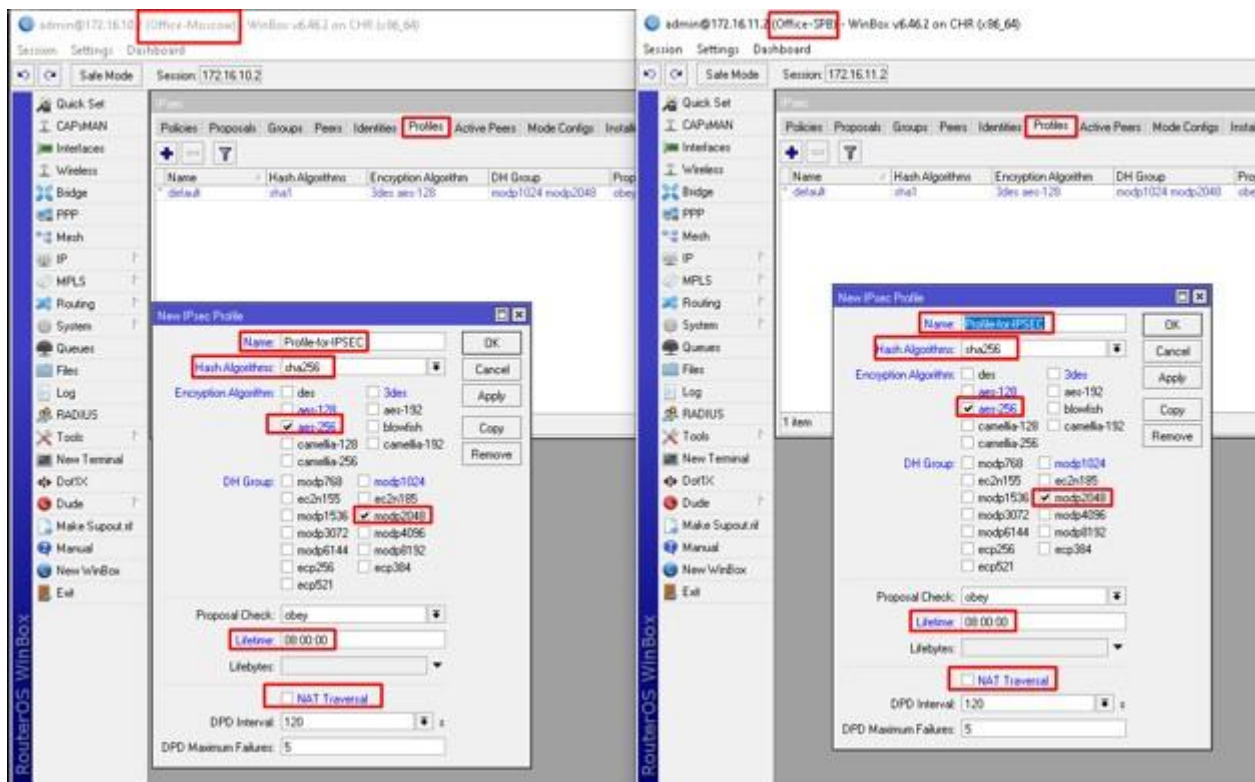
После нажатия кнопки Apply проверим состояние подключения на вкладке Status.



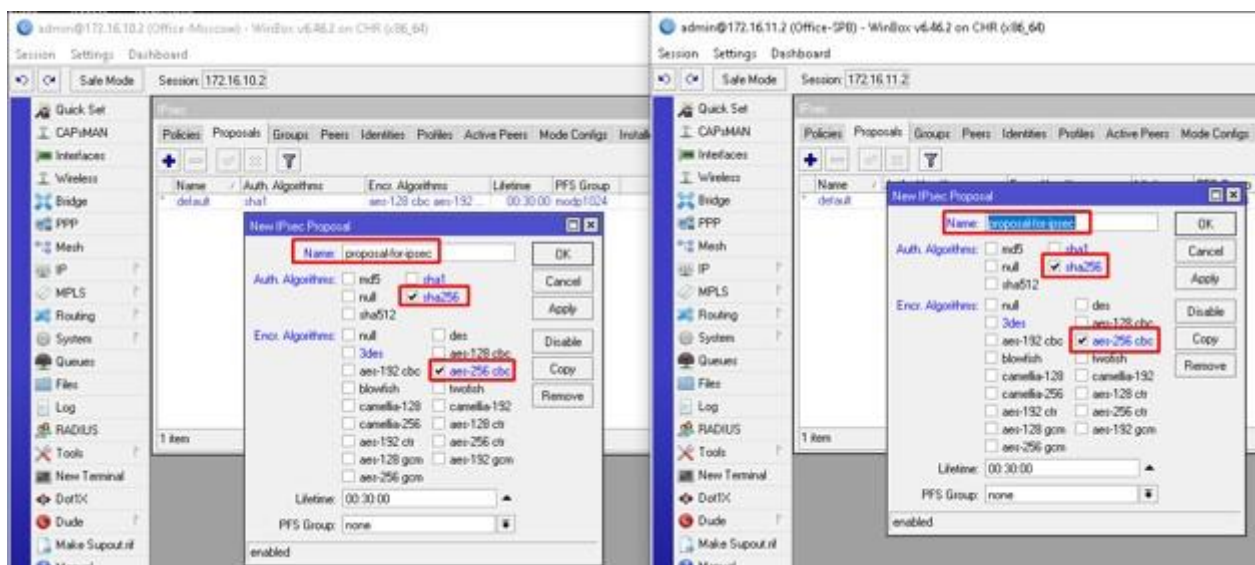
Строка Encoding изменилась на более внушительное значение, что символизирует об успешном согласовании.

Site to site

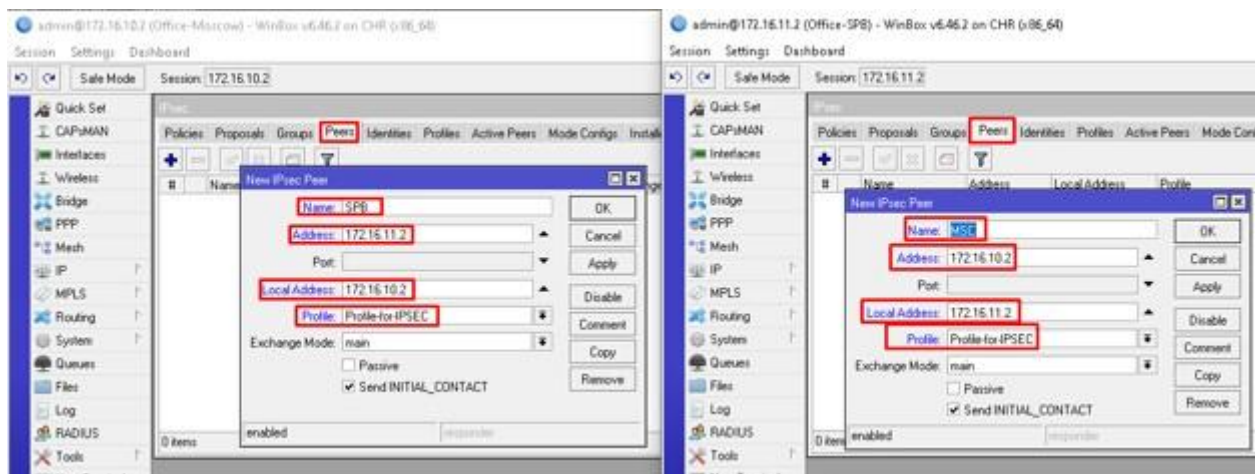
Все настройки находятся в IP – IPSEC. Данный метод предназначен для развёртывания между удаленными площадками. Обязательным условием является наличие статических публичных адресов для обоих участников туннеля. Параметры идентичны, за исключением маленьких деталей. Отлично подходит для голосового трафика, т.к. все данные будут инкапсулированы в UDP. Запасаемся терпением и вниманием. Надеюсь, что все помнят простое правило по неиспользованию стандартных профилей. Создаем одинаковый профиль на обоих устройствах.



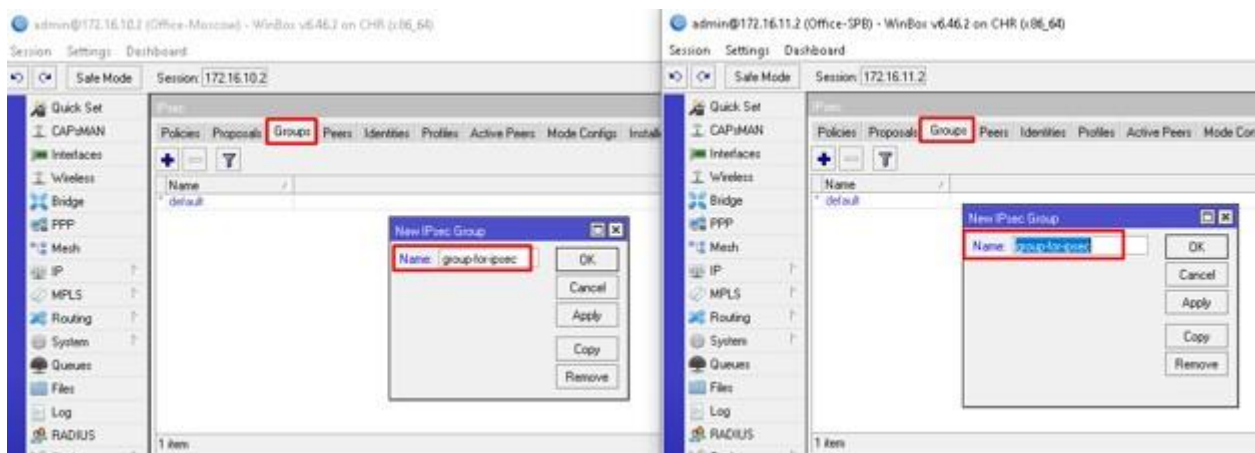
Далее создаем предложения.



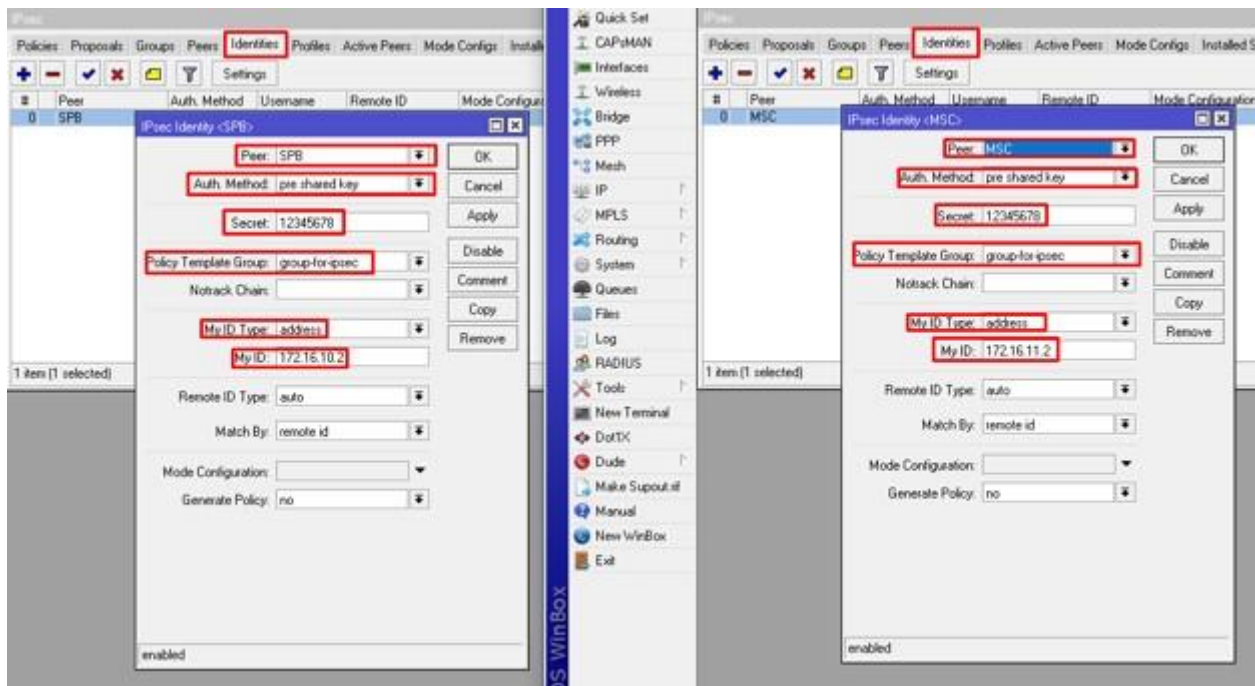
Далее нужно создать пиров. Направляем их друг на друга и указываем раннее созданные профили. Пишем в поле Local Address тот адрес роутера, с которого хотите инициировать соединение. Это особенно актуально если у вас их несколько или нужно инициировать соединение с определенного. Т.к. у нас всего по одному адресу – укажем их.



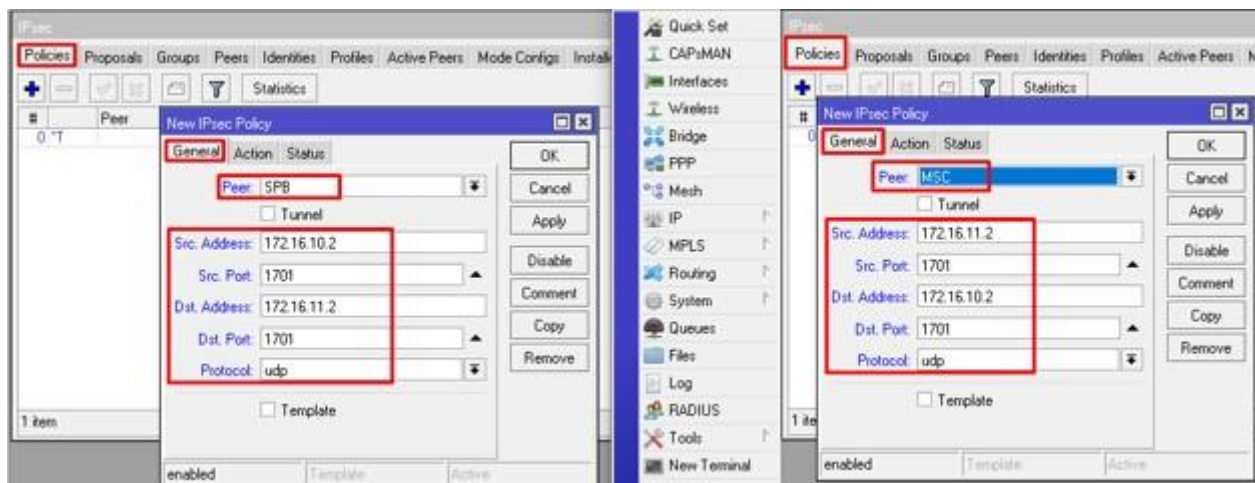
Далее создаем группы.



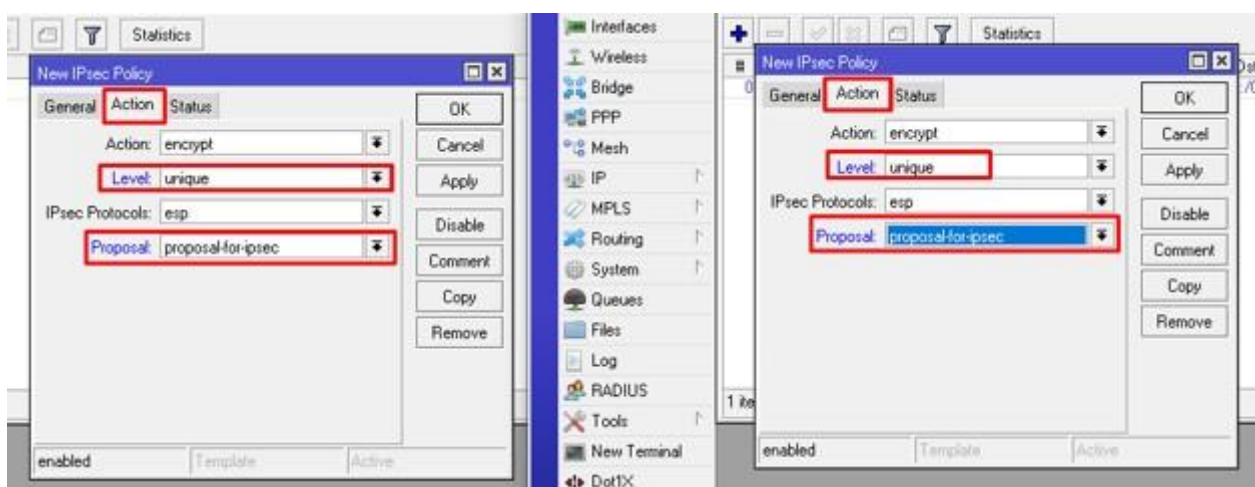
Еще не все. Следующий пункт — Identity.



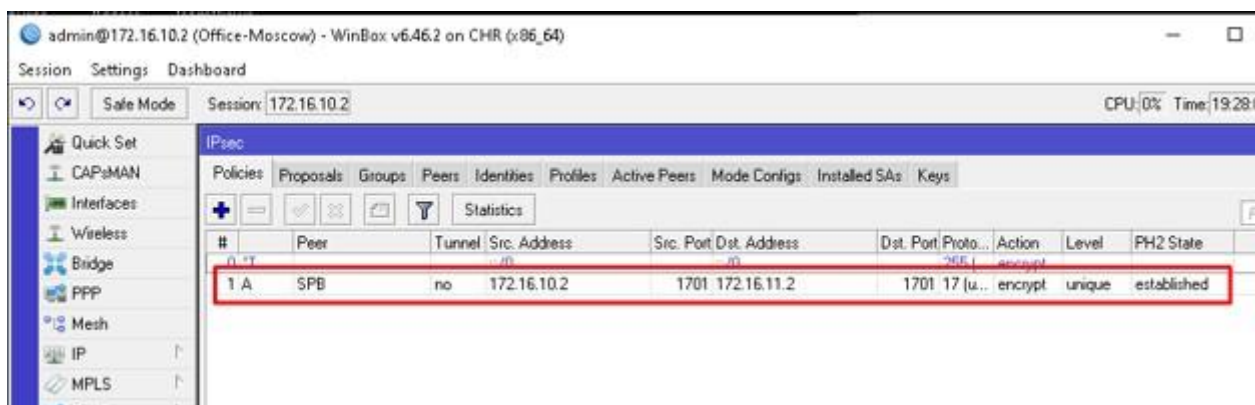
И вишенкой на торте Policies. На вкладке General указываем адреса источника и назначения. Соответственно направляем друг на друга. 1701 это UDP порт L2TP.



Переходим в Action. Обязательно выбираем параметр Level в unique. Особенно полезно будет для тех, кто планирует много зашифрованных туннелей.



Сохраняем и проверяем.



Established в конце строки пира SPB означает что согласование прошло успешно и оно устоялось. Откроем Installed SAs и посмотрим на наши ключики.

IPsec

Policies

Proposals

Groups

Peers

Identities


Profiles

Active Peers

Mode Configs

Installed SAs

Keys



Flush

	SPI	Src. Address	Dst. Address	Auth. Alg...	Encr. Algorit...	Encr. Key Si...	Current B...
E	b3e1661	172.16.10.2	172.16.11.2	sha256	aes cbc	256	472
E	d9cf15a	172.16.11.2	172.16.10.2	sha256	aes cbc	256	444

Все как мы и заказывали. Ну и наконец проверим наше L2TP соединение. Все должно зашифроваться без переподключений.

PPP

Interface

PPPoE Servers

Secrets

Profiles

Active Connections

L2TP Secrets

+

-

✓

✗

📁

🔍

PPP Scanner

PPTP Server

SSTP Server

L2TP Server

VPN Server

Name	Type	Actual MTU	L2 MTU	Tx	Rx
DR <><I2tp-SPB-Office>	L2TP Server Binding	1450			0 bps

1 item out of 6 (1 selected)

Interface <<I2tp-SPB-Office>>

General

Status

Traffic

Last Link Down Time:

Last Link Up Time: Jan/28/2020 22:31:11

Link Downs: 0

Uptime: 00:00:07

User: SPB-Office

Caller ID: 172.16.11.2

Encoding: cbc(aes) + hmac(sha256)

MTU: 1450

MRU: 1450

Local Address: 172.16.25.1

Remote Address: 172.16.25.10

OK

Copy

Remove

Torch

dynamic

enabled

running

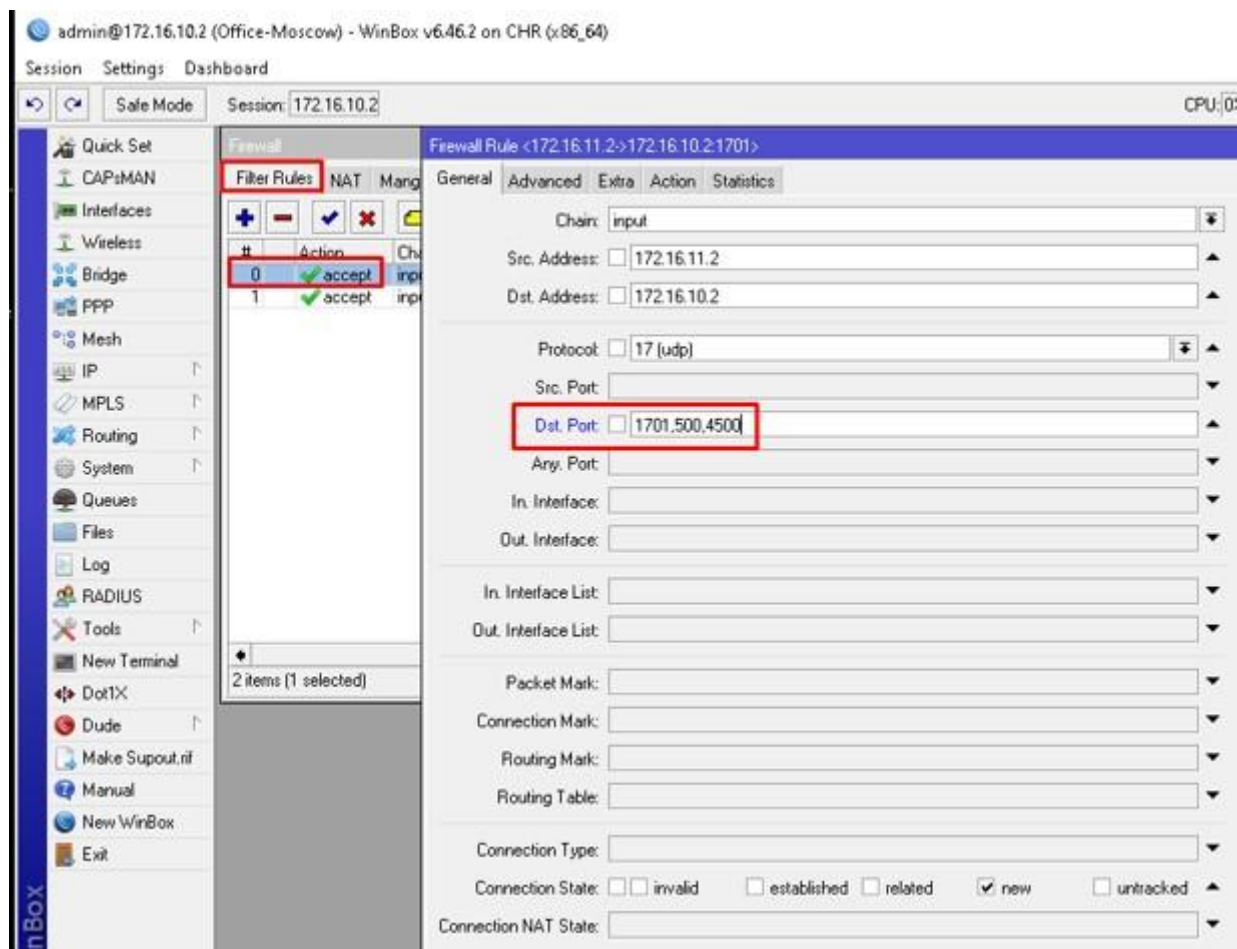
slave

Status: connected

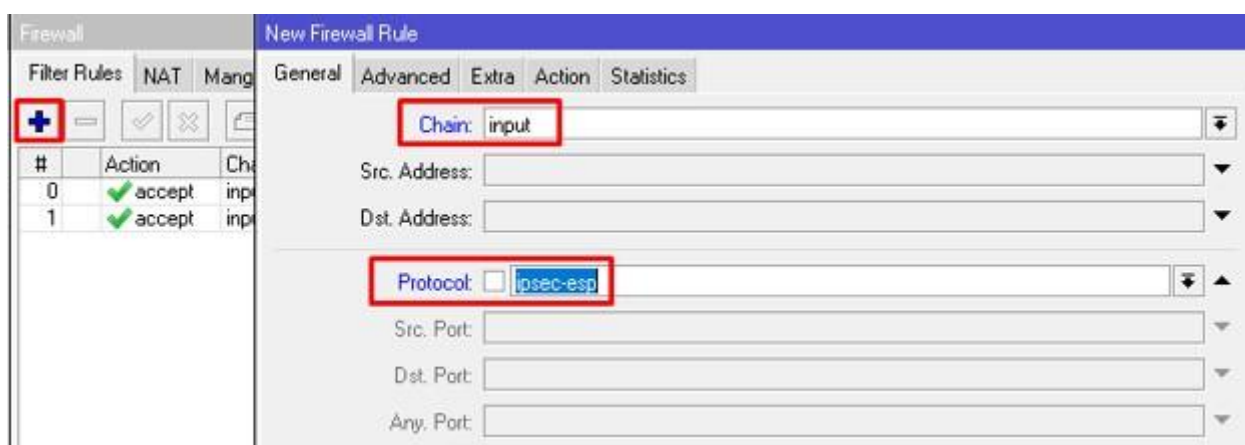
Настройка firewall

Тут также, как и с предыдущим пунктом. Настраиваем одинаково с обеих сторон. Нужно отредактировать созданные правила на московском роутере, а на питерском создаем с нуля аналогичные. В первом правиле кроме порта для L2TP добавляем еще два:

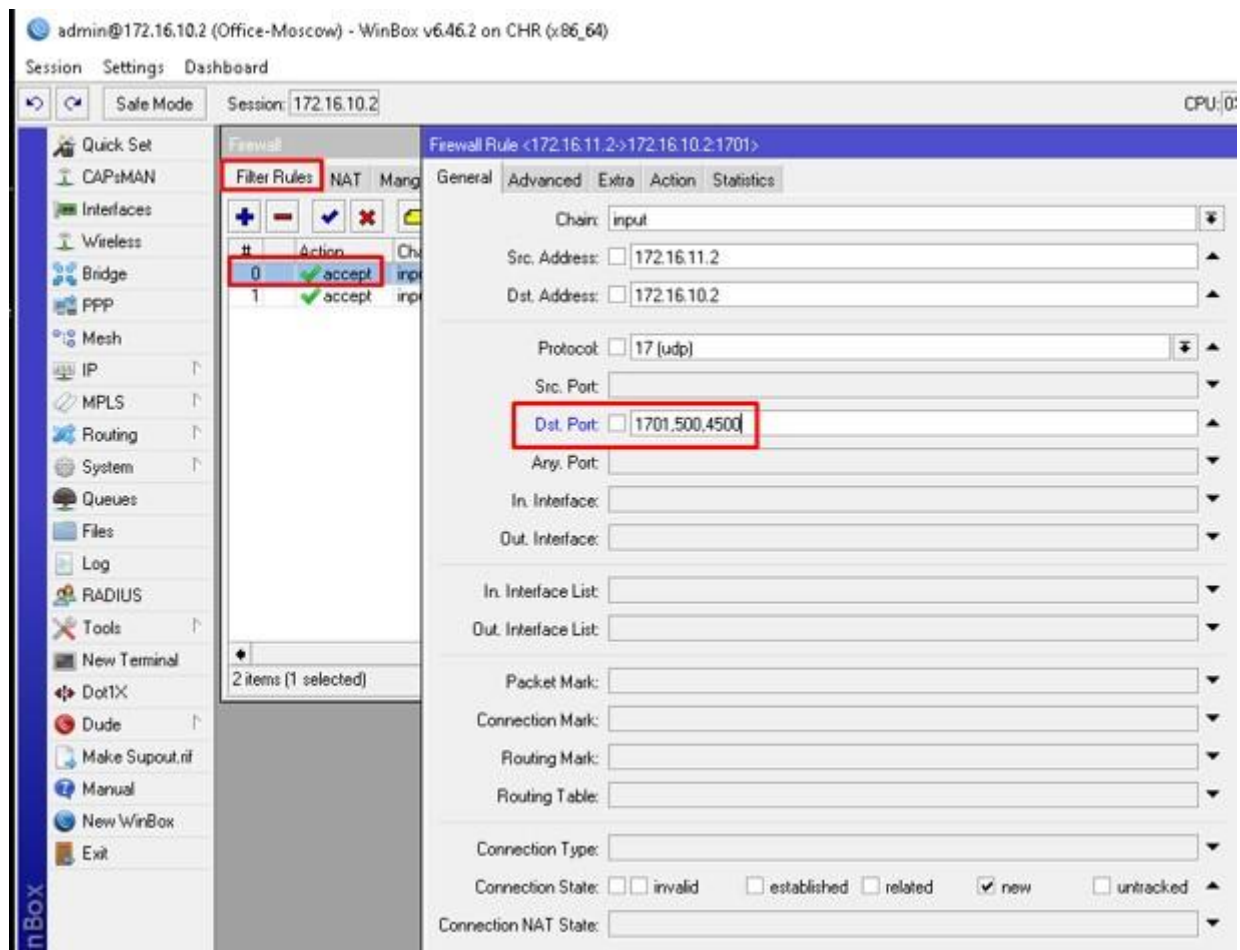
- 500;
- 4500.



Создадим еще одно правило для IPSEC-ESP.



Перемещаем его над последним правилом.



Повторив параметры фаервола на питерском роутере, обязательно проверьте что соединение L2TP подключается и шифруется соответствующими алгоритмами. На этом мы закончили цикл статей про настройку L2TP клиента и сервера как с IPSec так и без него. Если у вас остались вопросы задавайте их в комментариях а лучше в группу Телеграмм.

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 [здесь](#).