Настройка L2TP Клиента на MikroTik

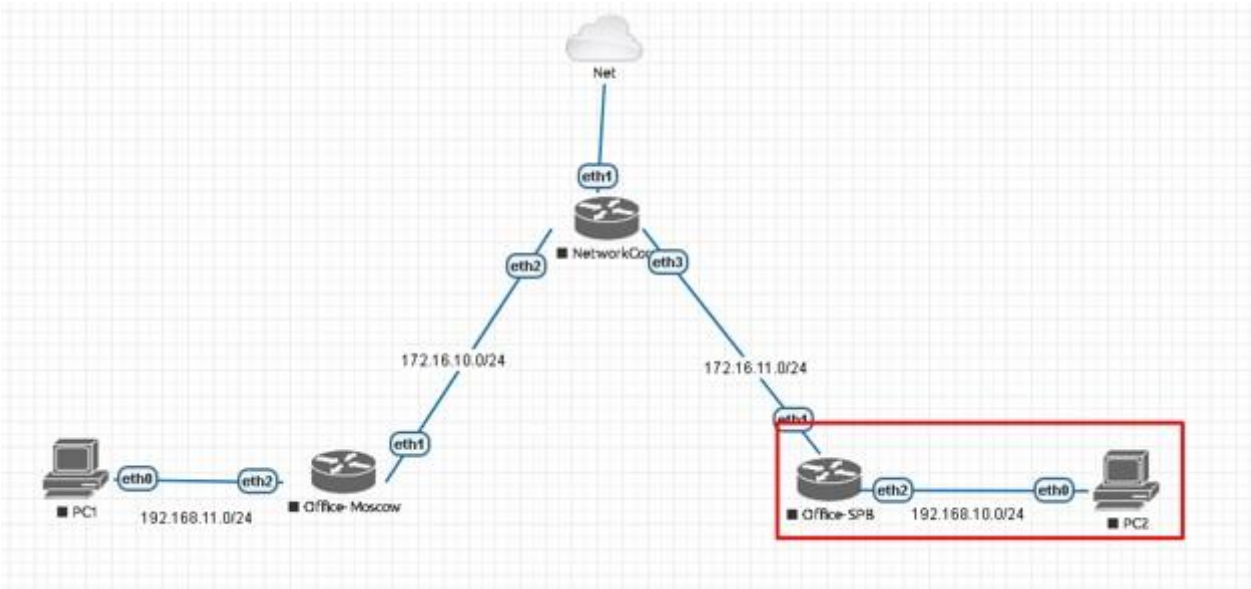
mikrotiklab.ru/nastrojka/artga-l2tp-client.html

January 29, 2020

Сегодня сделаем настройку L2TP Client на MikroTik, это продолжение предыдущей статьи в которой мы рассмотрели базовую конфигурацию серверной части L2TP. Подготовили профиль, включили сервер и настроили фаервол. Нам осталось создать пользователя и подключить клиентскую часть. Также немного разберем вопросы безопасности и защитим нашу VPN сеть от ненужных товарищей. Но обо всем этом по порядку.

Содержание

Конфигурирование



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

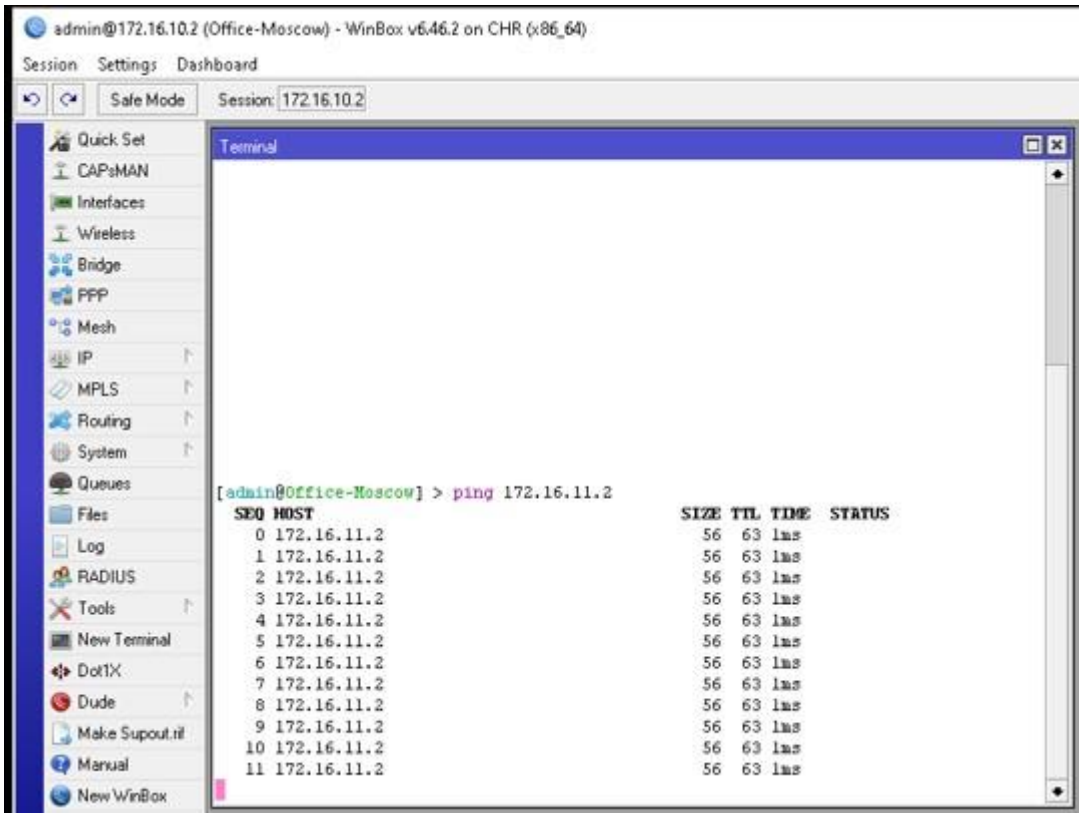
- Office-SPB клиент;
- Office-Moscow сервер;
- NetworkCore выполняет роль провайдера, он будет заниматься обычной маршрутизацией;
- Office-Moscow ether1 смотрит в интернет 172.16.10.2/24;
- Office-SPB ether1 смотрит в интернет 172.16.11.2/24;

- 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.

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.

Тестирование связи

На нашем стенде, как вы заметили, я использую статические частные (серые) IP адреса. В действительности необходим хотя бы один публичный (белый) IP адрес. Он должен быть на том оборудовании, которое выполняет роль сервера. Самым лучшим решением – это использование публичных адресов со всех устройств которые будут подключаться к VPN. Цена в таком решении — это абонентская плата, а результат – улучшенная безопасность на нескольких уровнях. Проверим связь между устройствами. Отправляю ping-запросы между 172.16.10.2 и 172.16.11.2 с московского роутера.



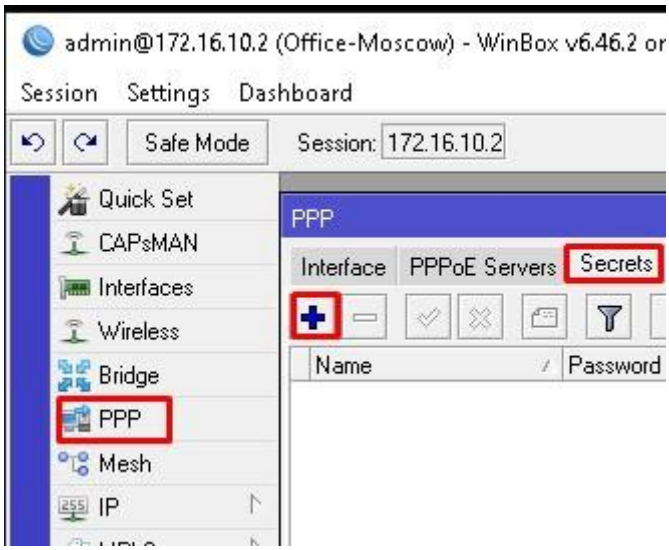
Ping-и идут стабильно, можно идти дальше.

Создание пользователя

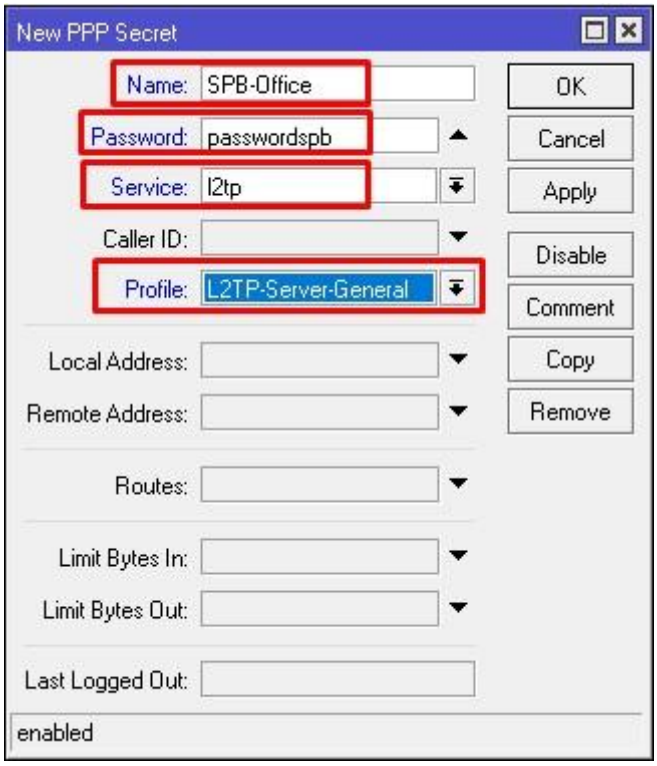
Не отключаясь от роутера Office-Moscow создадим пользователя. Переходим в PPP – Secrets.

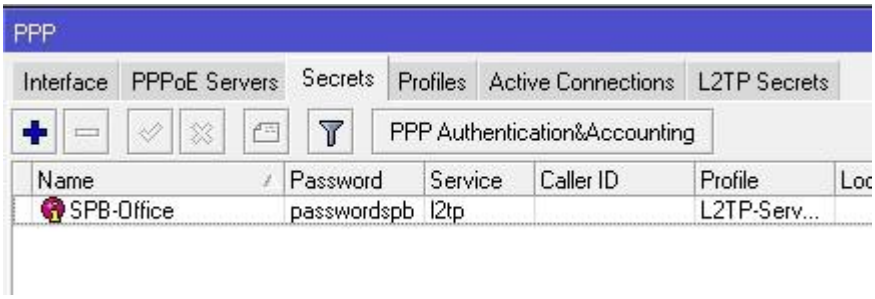
Задаем следующие параметры:

- Name – SPB-Office — Имя учетной записи;
- Password – passwordspb – пароль;
- Service – l2tp – сервис, который разрешен данной учетной записи;
- Profile – L2TP-Server-General – созданный ранее профиль сервера.



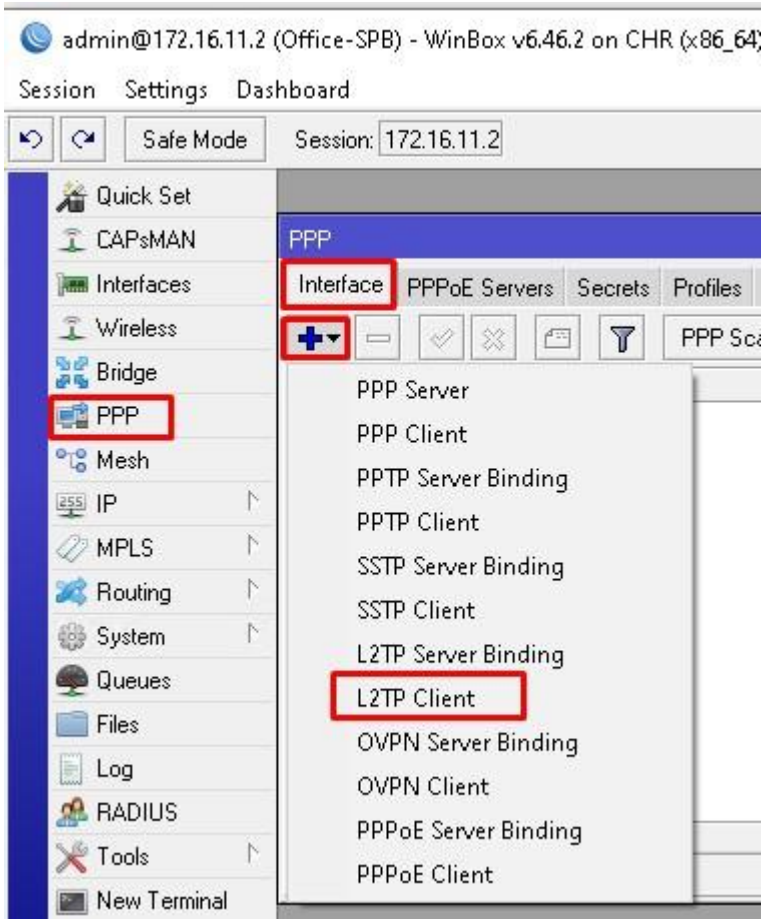
Сохраняем и проверяем результат.





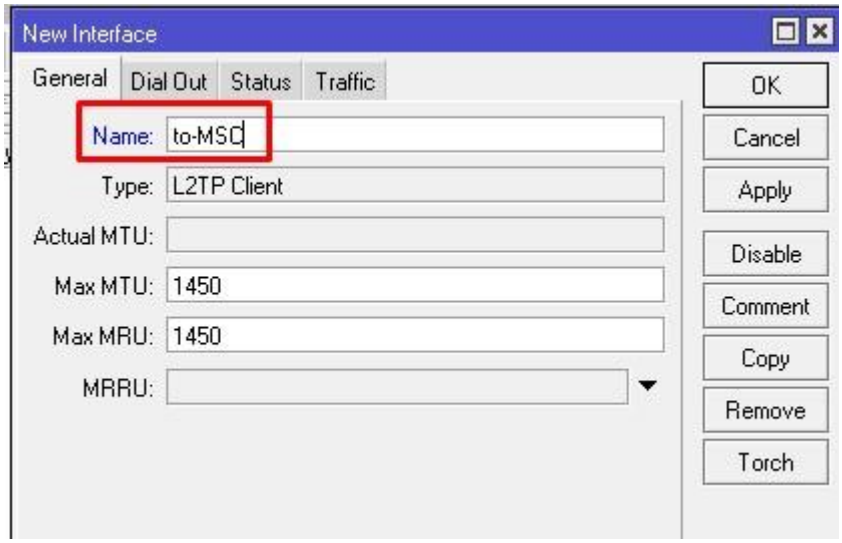
Создание клиентского интерфейса

Подключаемся к клиентскому Mikrotik Office-SPB. Создаем интерфейс в PPP – Interface.



Указываем параметр Name на вкладке General. Я обычно указываю направление, в которое будет подключаться роутер.

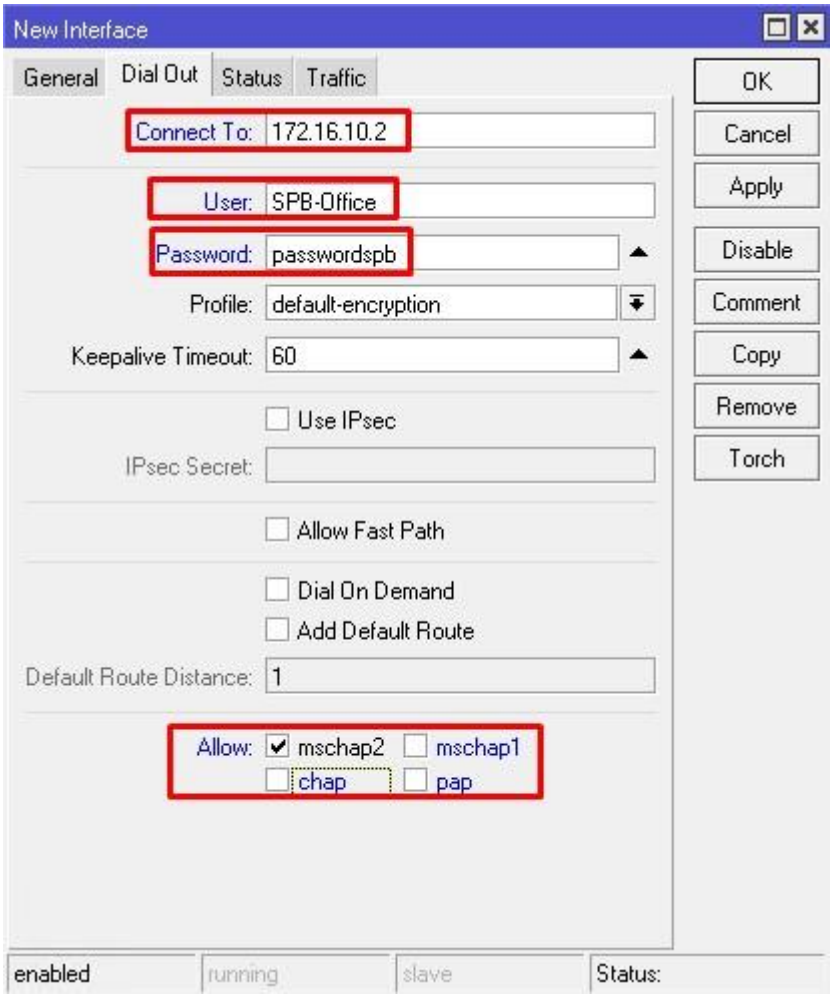
> Задавайте понятные имена интерфейсов на английском языке, чтобы вам было все ясно при диагностики неисправностей.



На вкладке Dial Out указываем:

- Connect To – 172.16.10.2 – IP или DNS имя сервера Mikrotik;

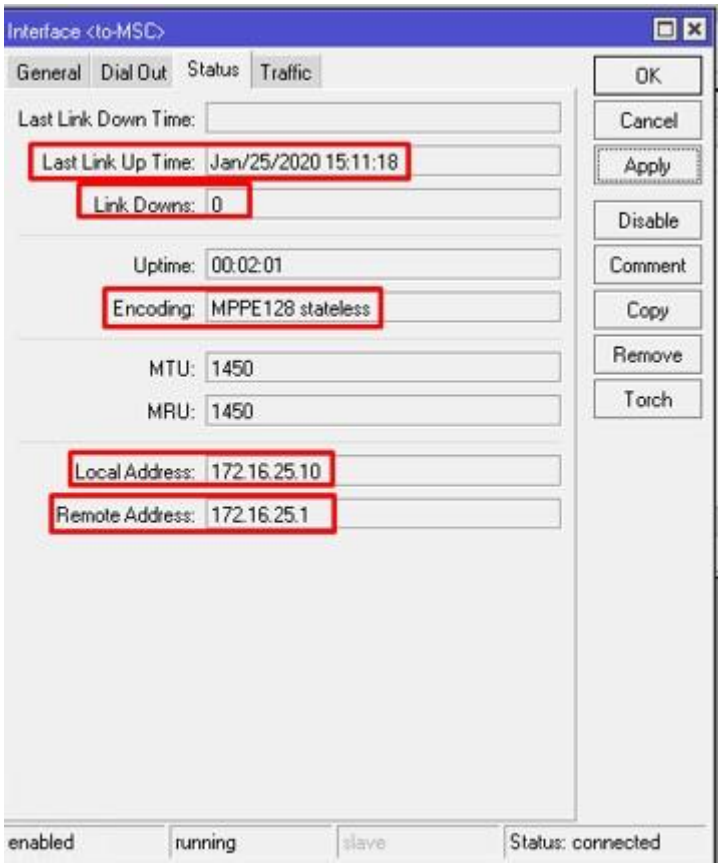
- User — SPB-Office – созданный на прошлом шаге пользователь;
- Password – passwordspb – пароль от учетной записи;
- Allow – mschap2 – протокол аутентификации.

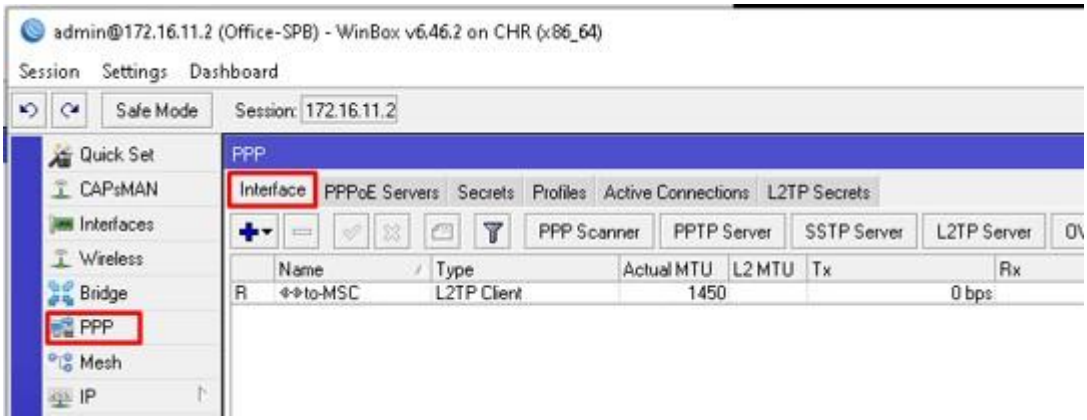


Жмем Apply и смотрим на статус в правом нижнем углу, он должен быть connected.

Это символизирует об успешном подключении. Открываем вкладку Status. Взглянем на состояние.

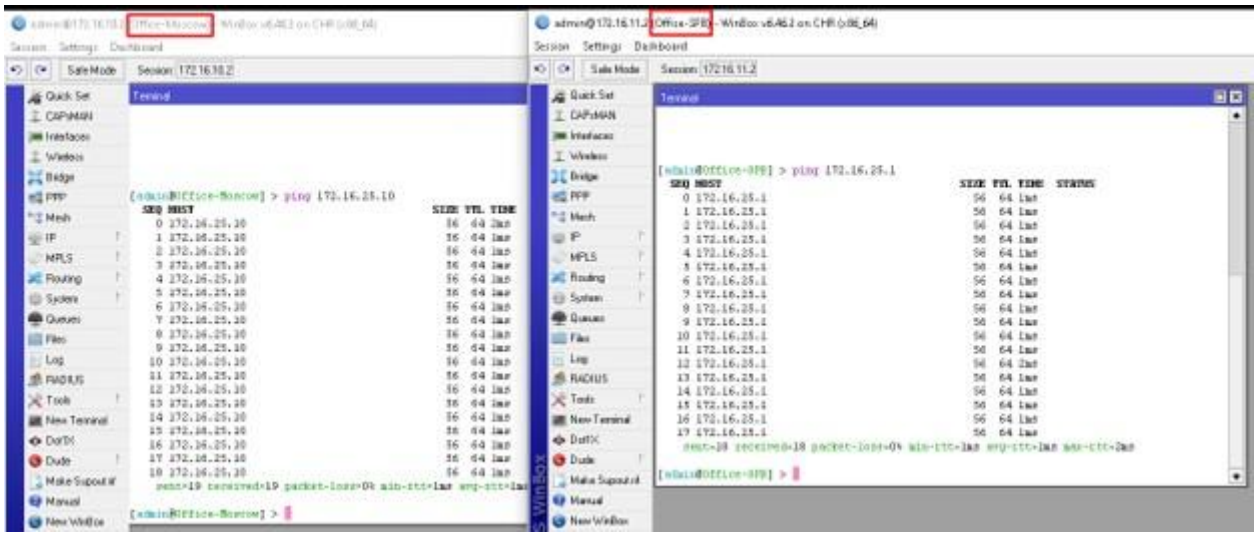
Мы видим, что наш клиент подключился последний раз 25 января 2020 года в 15:11:18, ни одного разрыва с момента подключения, шифрование MPPE 128, адрес клиента в туннеле 172.16.25.10 и шлюза 172.16.25.1. Если ваш провайдер блокирует L2TP без IPSEC, то у вас либо не поднимется соединение, либо будет расти счетчик Link Downs. Так же стоит проверить, создался ли сам интерфейс.





Проверка соединения

Перейдем к проверке связи. Будем тестировать ping-запросами. Отправим их внутри туннеля.

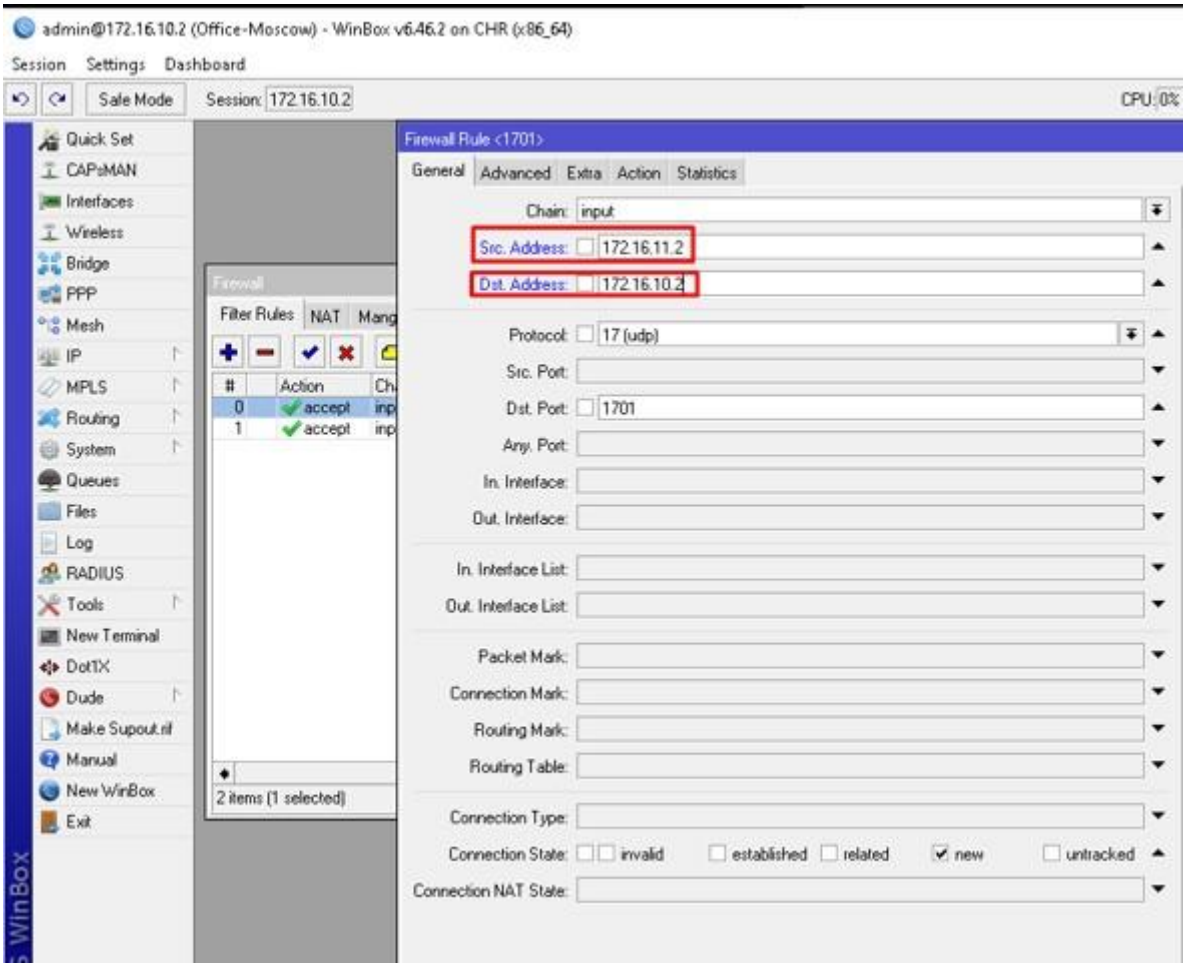


Убедившись, что запросы по направлению друг к другу отрабатывают корректно, займемся настройкой безопасности.

Настройка firewall

> Вы можете пропустить данный пункт если ваш роутер, который выполняет роль клиента имеет динамический IP.

Брутфорс – зло! Но нас не проведешь. В предыдущей статье мы сделали базовую настройку фаервола сервера. Мы знаем, что клиент будет подключаться с 172.16.11.2. Проведем не большие изменения для увеличения безопасности подключения. Подключаемся на московский роутер и открываем ранее созданное правило фаервола для порта UDP 1701.



Данное правило можно читать следующим образом: если новое соединение с 172.16.11.2 на 172.16.10.2 на сокет UDP:1701 – разрешить. Все устоявшиеся соединения будут жить, т.к. уже есть второе разрешающее правило ниже. Идем дальше PPP – Secrets. Открываем пользователя SPB-Office и указываем адрес в Caller ID, с которого он будет подключаться.

Читаем правильно – пользователь SPB-Office, с паролем passwordspb, с адреса 172.16.11.2 к сервису L2TP – назначить параметры, указанные в профиле. Подключиться не удастся если хотя бы одно условие не выполнится. На этом все, настройка и подключение l2pt клиента завершено, теперь у нас есть стабильный канал связи. В следующий статье мы прикрутить ко всему этому IPSec для еще большей безопасности.

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.