Лабораторная работа №3

Настройка L2TP Клиента на MikroTik

Целью лабораторной работы является конфигурация L2TP VPN клиента и проверка его работоспособности на основе предыдущей лабораторной работы.

В лабораторной работе №2 мы рассмотрели базовую конфигурацию серверной части L2TP, подготовили профиль подключения, активировали L2TP сервер и настроили межсетевой экран. Таким образом, осталось создать пользователя и подключить клиентскую часть. Также в процессе выполнения лабораторной работы будут разбираться основные вопросы безопасности и защиты VPN сети от несанкционированного доступа.

1. Конфигурация L2TP

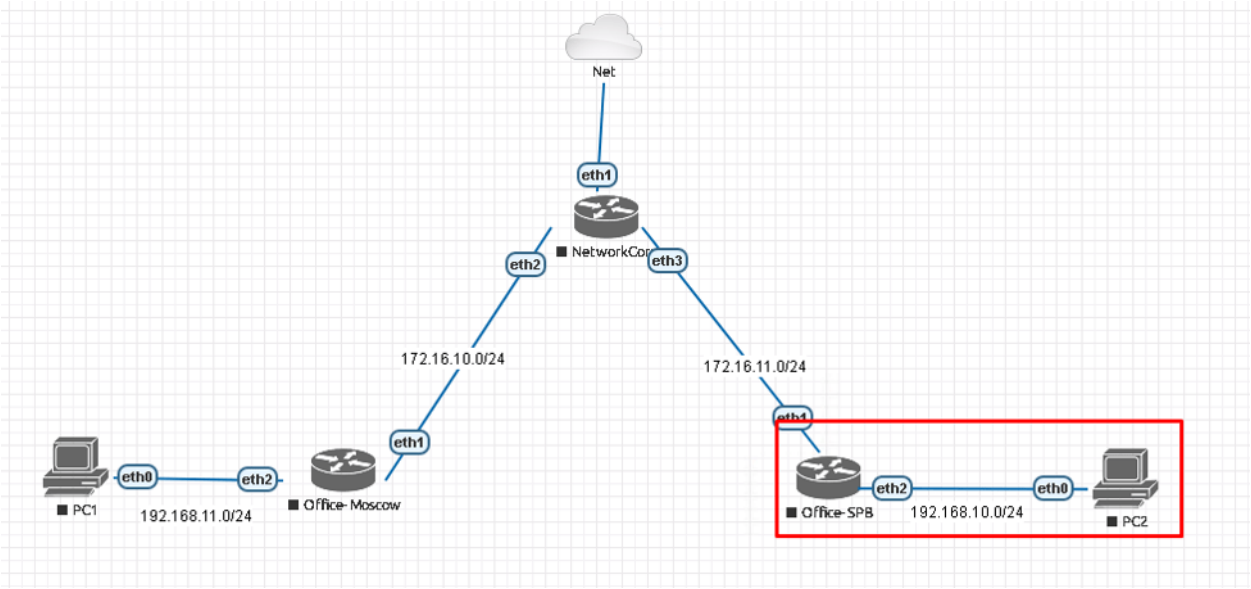

Рисунок 1 – Схема лабораторного стенда

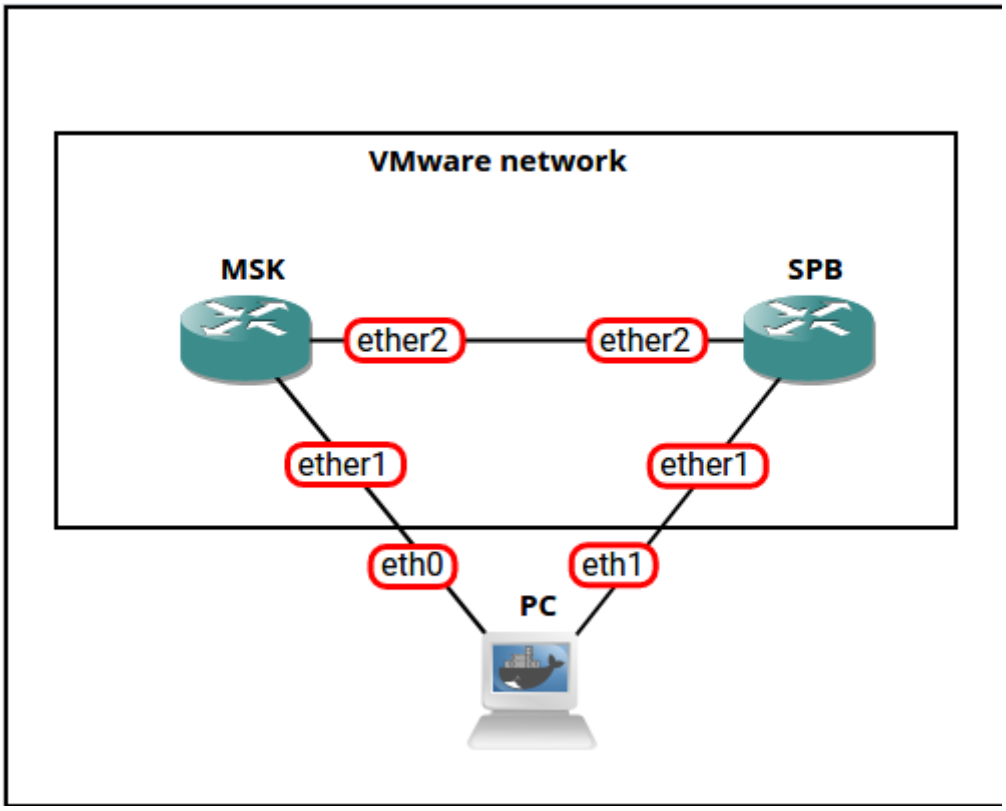

Рисунок 2 – Упрощенная схема стенда с использованием гипервизора VMware

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.

Схема адресации может быть изменена на усмотрение студента. Ввиду упрощения исходной схемы все компьютеры и маршрутизаторы могут быть подключены к локальной сети Вашего основного устройства (компьютера) напрямую. Рекомендованным решением адресации устройств является создание дополнительной сети типа Host-only для соединения маршрутизаторов между собой.

2. Тестирование связи

Для реализации тестового соединения VPN на виртуальном стенде, как вы заметили, мы используем статические частные (серые) IP адреса. В действительности необходим хотя бы один публичный (белый) IP адрес. Он должен быть на том оборудовании, которое выполняет роль VPN 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. Отправляем ping-запросы между 172.16.10.2 и 172.16.11.2 с «московского» роутера.

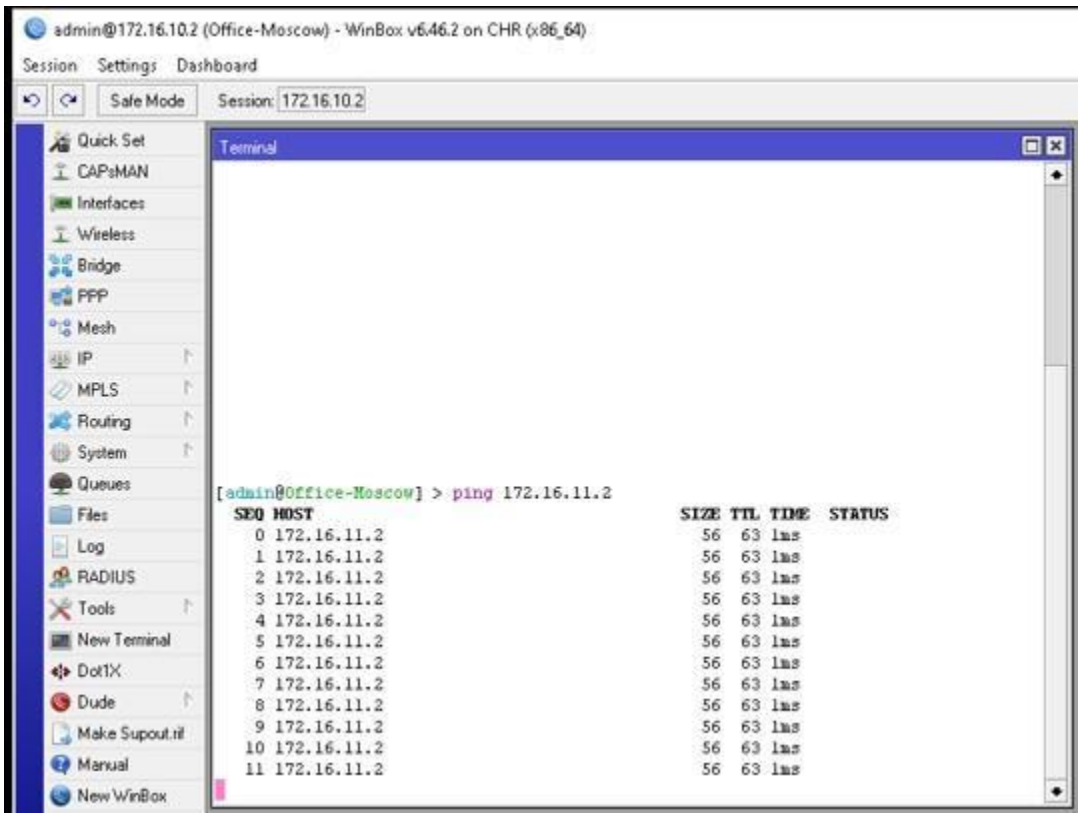

Рисунок 3 – Проверка соединения между маршрутизаторами

Ping-и идут стабильно, можно идти дальше, если нет – требуется проверка сетевых интерфейсов виртуального стенда: режима их работы, подключенной виртуальной сети, сетевых адресов.

2.1 Создание пользователя

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

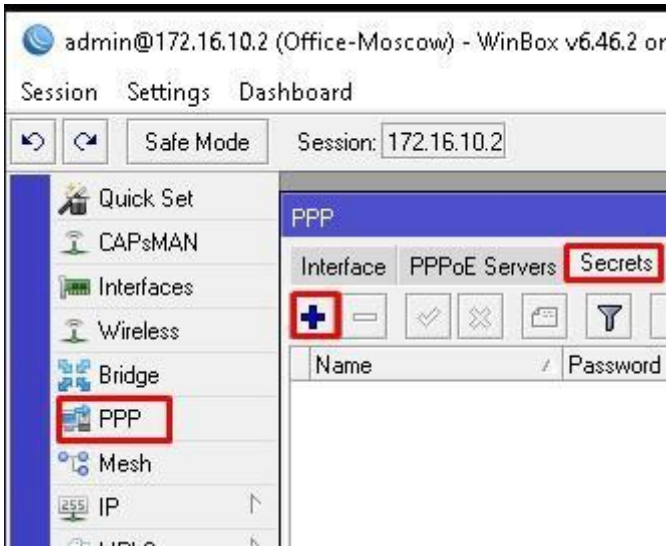

Рисунок 4 – Создание пользователя

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.

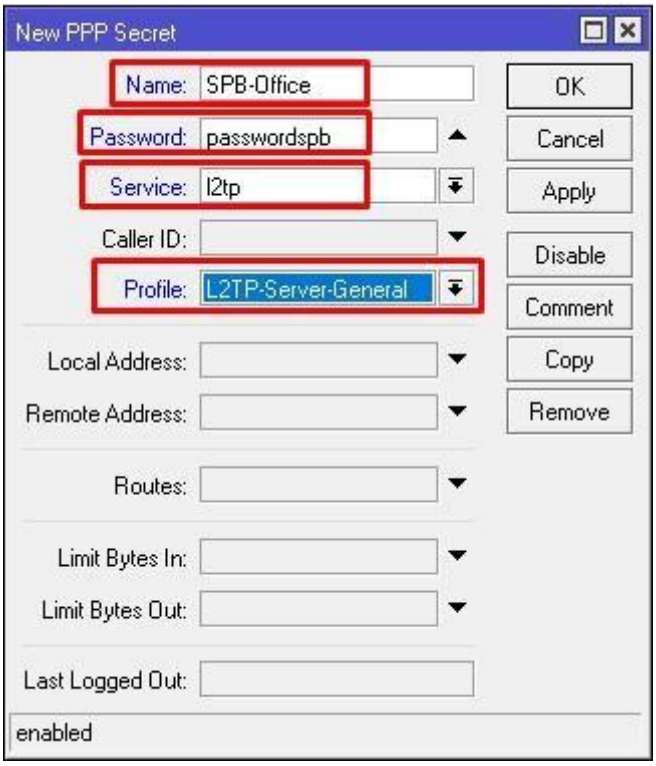

Рисунок 5 – Настройка пользователя

Сохраняем и проверяем результат.

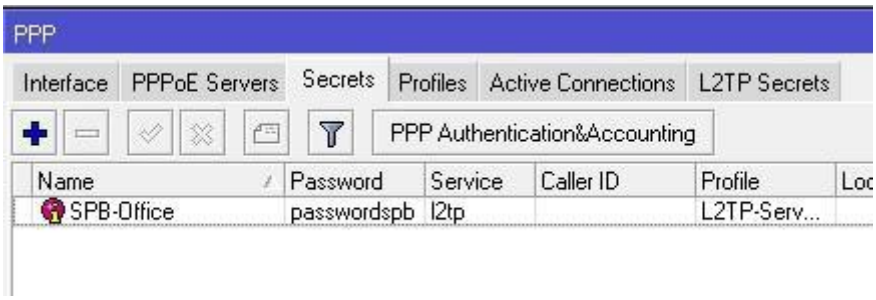

Рисунок 6 – Проверка сохранения параметров

2.2 Создание клиентского интерфейса

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

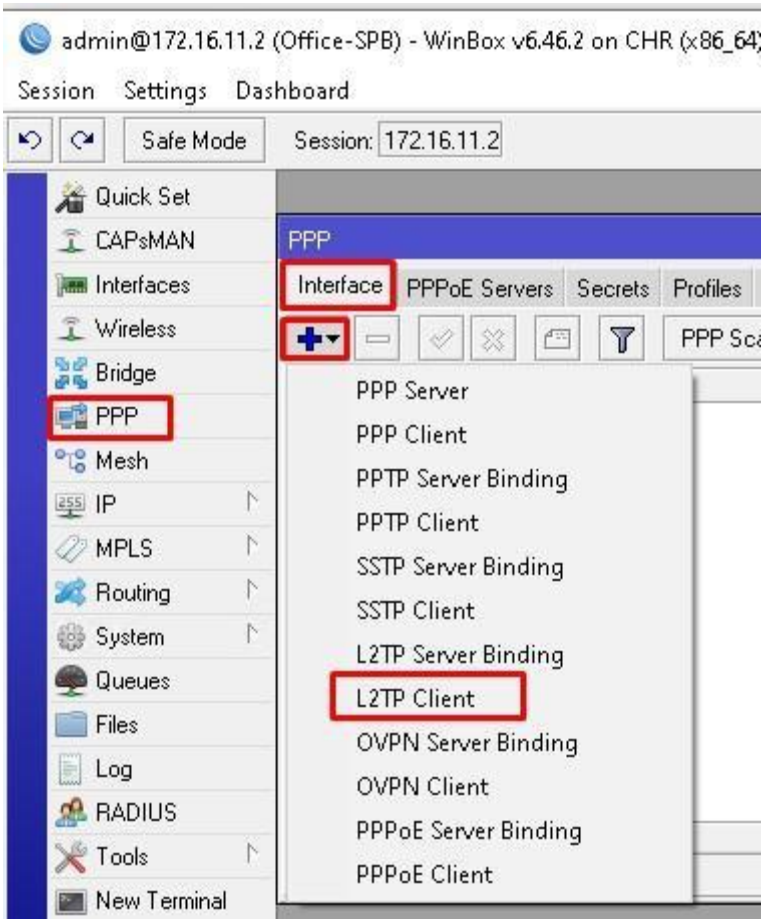

Рисунок 7 – Создание интерфейса L2TP клиента

Указываем параметр Name на вкладке General. Можно указать направление, в котором будет подключаться роутер.

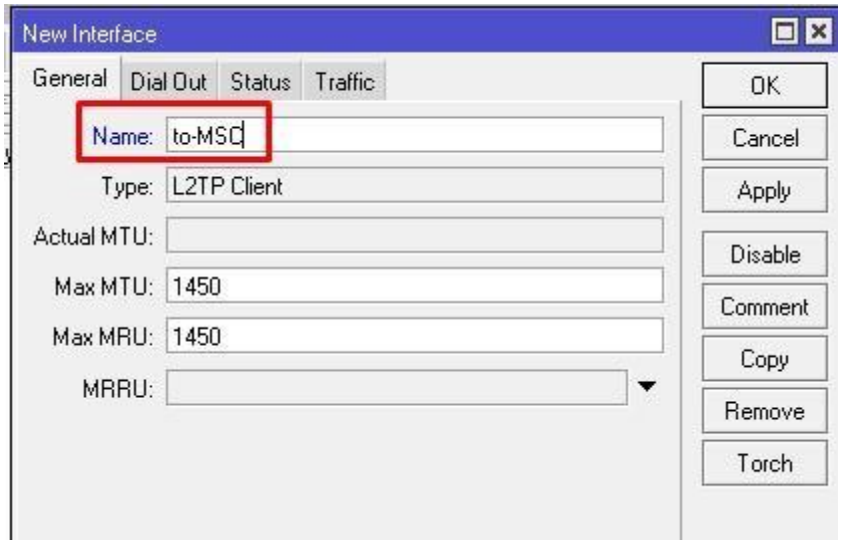

Рисунок 8 – Создание интерфейса L2TP клиента

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 (из лабораторной №2);
- Allow – mschap2 – протокол аутентификации.

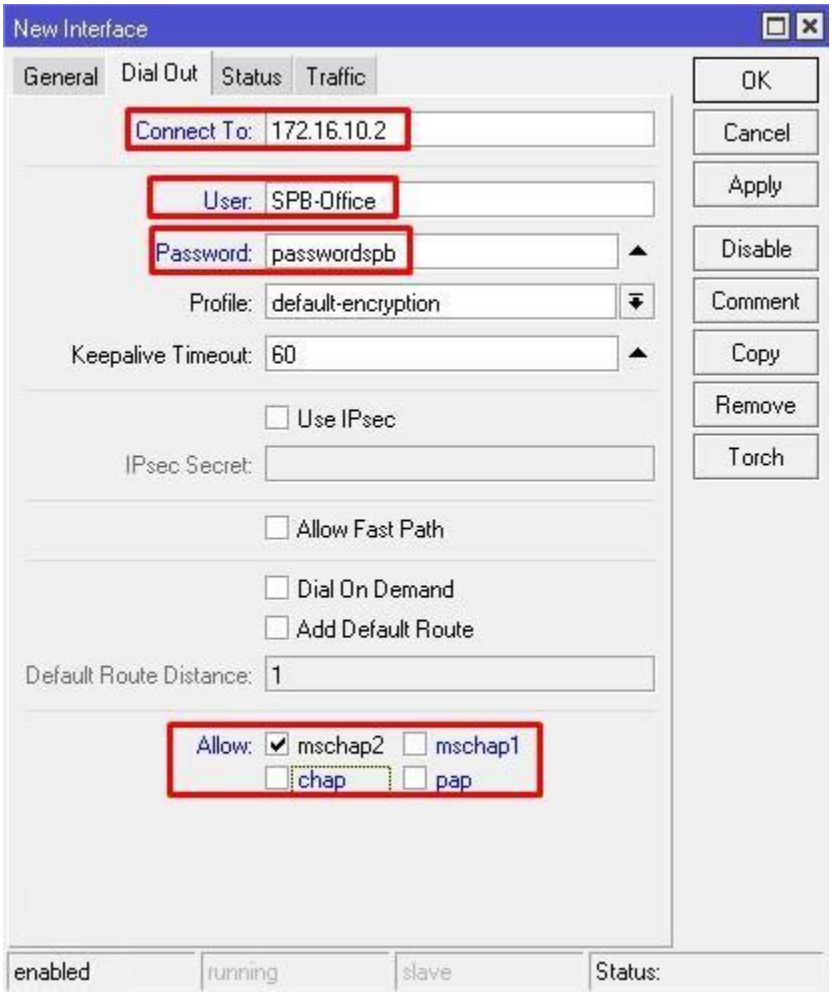

Рисунок 9 – Конфигурация L2TP клиента

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

Рисунок 10 – Проверка подключения

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

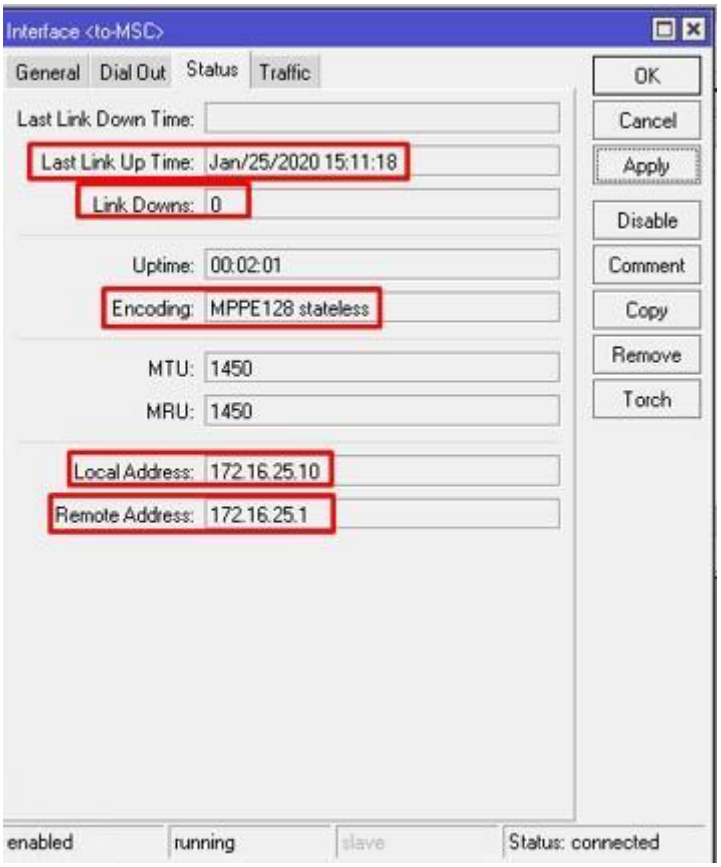

Рисунок 11 – Статус подключения

Из открытой вкладки следует, что клиент подключился последний раз 25 января 2020 года в 15:11:18 (Информация с рисунка 11), 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.

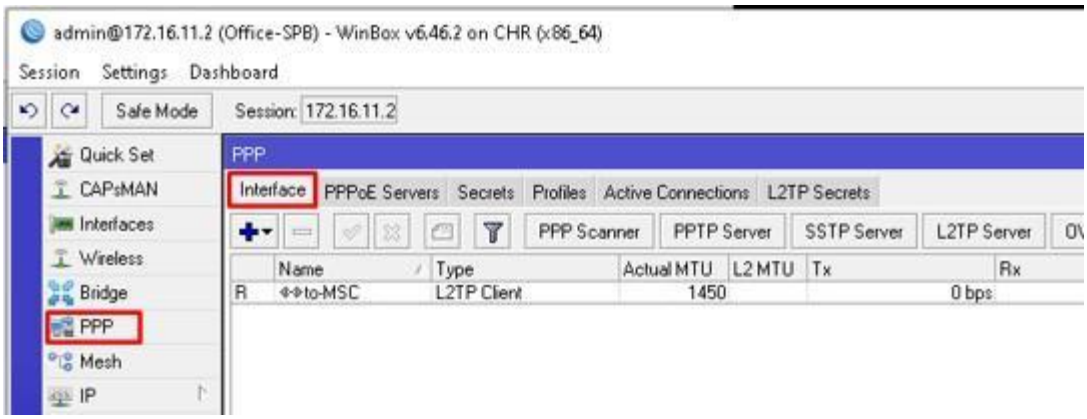

Рисунок 12 – Проверка интерфейса

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.

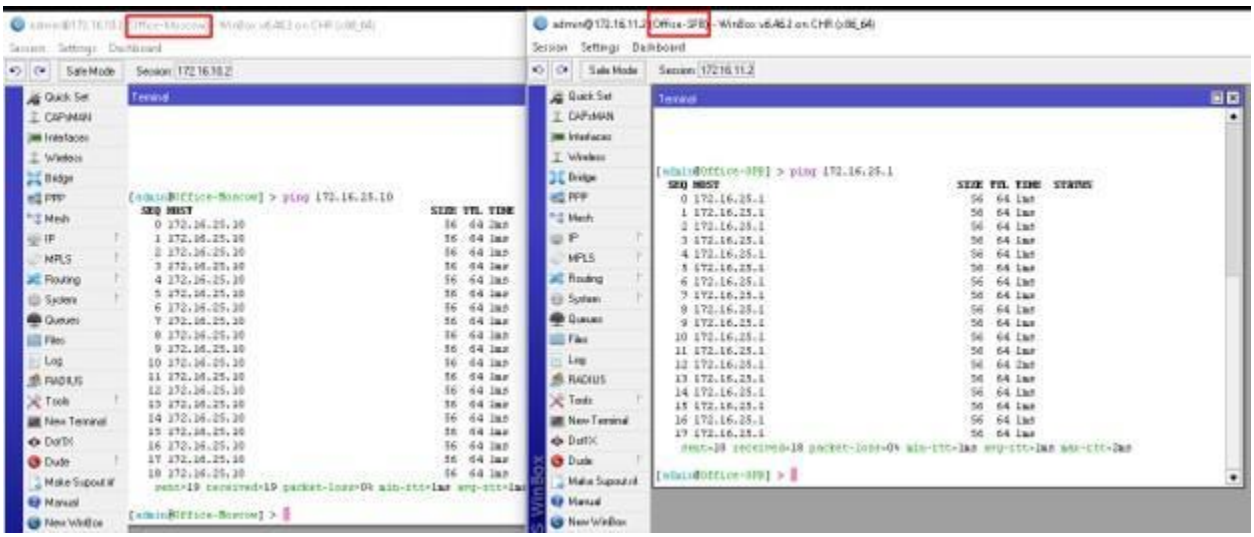

Рисунок 13 – Проверка соединения

2.3 Настройка firewall

Поскольку маршрутизатор с высокой вероятностью получает сетевой адрес динамически, в реальной конфигурации такой подход не имеет логического обоснования, поскольку после получения нового адреса устройством VPN перестанет работать, таким образом, если при выполнении лабораторной

устройство получит новый адрес – проверьте его правильность и в конфигурации межсетевого экрана.

В предыдущей работе была проведена базовая настройка фаервола сервера. Учитываем, что клиент будет подключаться с 172.16.11.2. Проведем небольшие изменения для увеличения безопасности подключения. Подключаемся на московский роутер и открываем ранее созданное правило фаервола для порта UDP 1701.

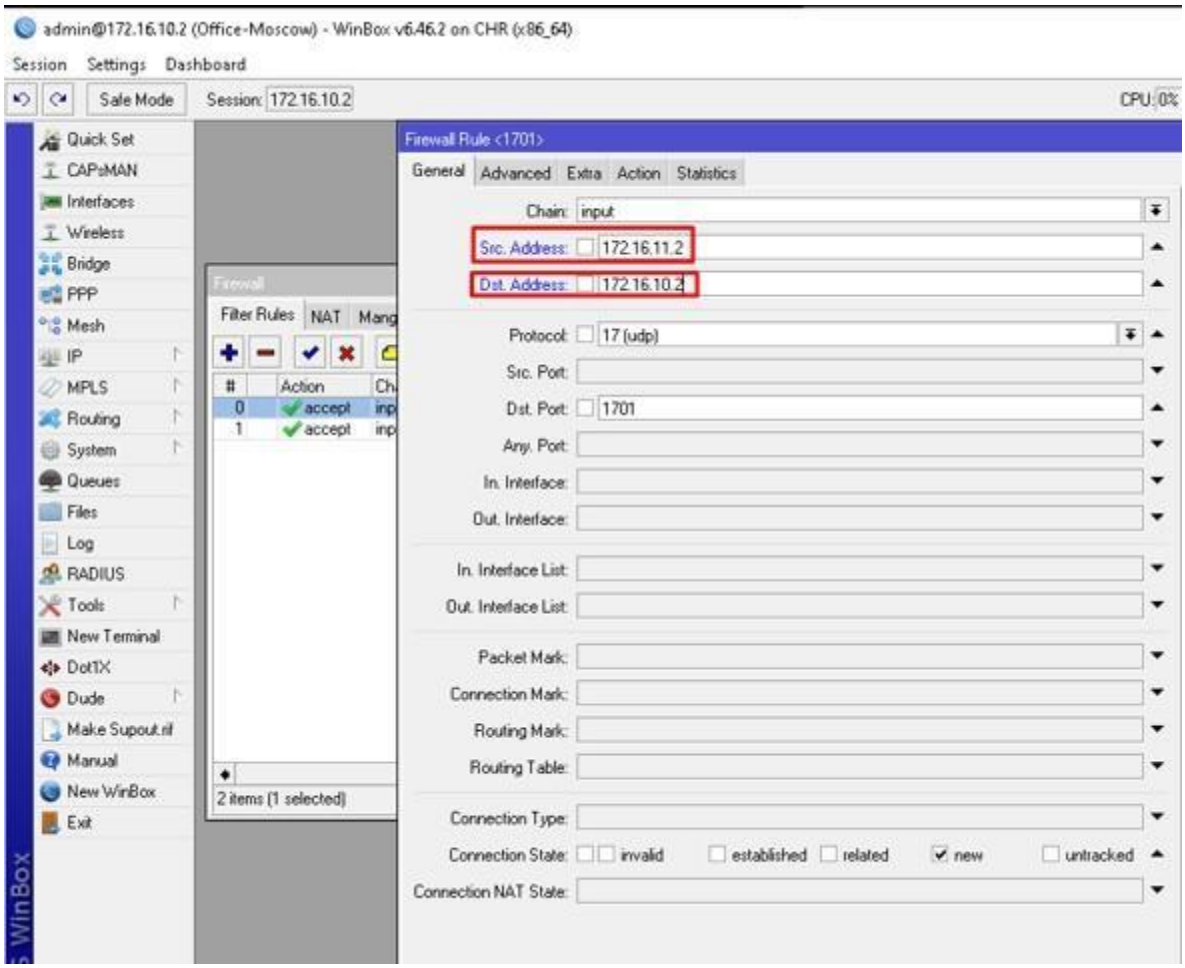

Рисунок 14 – Настройка правила фаервола

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 работать, 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 (указать требуется реальные адреса устройств).

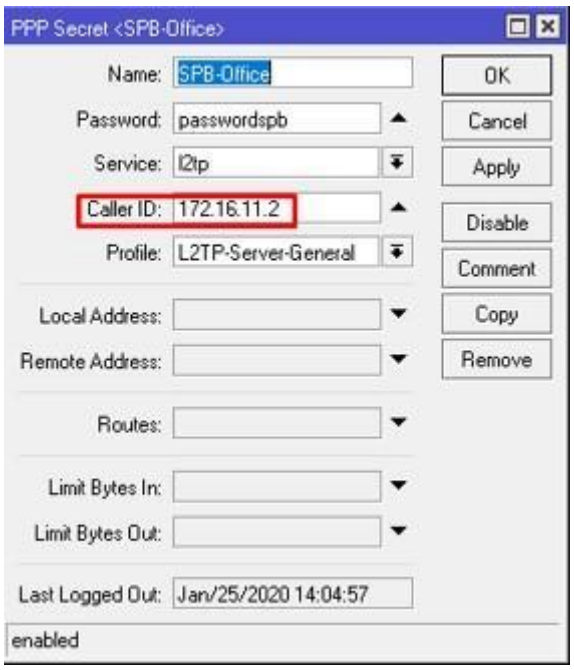

Рисунок 15 – Конфигурация Caller ID

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 L2TP клиента завершено, теперь у нас есть стабильный канал связи.

2.4 Проверка скорости соединения

Далее можно проверить, как меняется скорость передачи данных с использованием L2TP VPN. Для этого используем встроенную утилиту bandwidth-test. Сама утилита представляет собой клиент-серверное решение, поэтому требуется ее включение на L2TP сервере выполнением команд или в соответствующих вкладках графического интерфейса :

```
[admin@MikroTik] /tool bandwidth-server> set enabled=yes
authenticate=no
[admin@MikroTik] /tool bandwidth-server> print
                  enabled: yes
             authenticate: no
  allocate-udp-ports-from: 2000
             max-sessions: 100
[admin@MikroTik] /tool bandwidth-server>
```

А на стороне клиента – инициализация передачи данных с установленными параметрами, сами параметры можно взять из приведенного ниже примера и выполнить в консольном или графическом режиме в соответствующих вкладках интерфейса (адрес нужно вписать аналогично VPN):

```
[admin@MikroTik] /tool> bandwidth-test 10.0.0.32 duration=15s \
\... direction=both local-udp-tx-size=1000 protocol=udp \
\... remote-udp-tx-size=1000 user=admin
                status: done testing
              duration: 15s
            tx-current: 272.8Mbps
  tx-10-second-average: 200.3Mbps
      tx-total-average: 139.5Mbps
            rx-current: 169.6Mbps
  rx-10-second-average: 164.8Mbps
      rx-total-average: 117.0Mbps
          lost-packets: 373
           random-data: no
             direction: both
               tx-size: 1000
               rx-size: 1000
[admin@MikroTik] /tool>
```

После этого можно выключить VPN сервер и повторить процедуру.

Как изменилась скорость передачи данных с активным и неактивным L2TP VPN? Приведите реальные значения, постройте график зависимости скорости передачи данных проведя несколько тестов подряд с различными параметрами.