Лабораторная работа №2

Настройка L2TP Сервера на Mikrotik

Цель работы: конфигурация протокола L2TP на устройствах Mikrotik в клиент-серверном режиме.

1. L2TP – протокол туннелирования второго уровня. Используется для поддержки виртуальных частных сетей. Отличительной особенностью, является, возможность работы не только в IP сетях, но и в ATM, X.25 и Frame Relay. Клиент-серверный протокол, всегда есть клиент и сервер. Использует на транспортном уровне UDP порт 1701 – большой плюс для трафика, которому не нужно подтверждение каждого пакета (IP телефония, видеонаблюдение), а значит работает быстрее. Но и в этом его минус, шифрование пакетов алгоритмом MPPE 128bit RC4 никого не напугаешь.

Для конфигурации используется сегмент лабораторного стенда, оставшийся после выполнения лабораторной работы №1, выделенный на рис.1. Далее в тексте встречаются программные команды, их выполнение не обязательно, команды дублируют графическую конфигурацию.

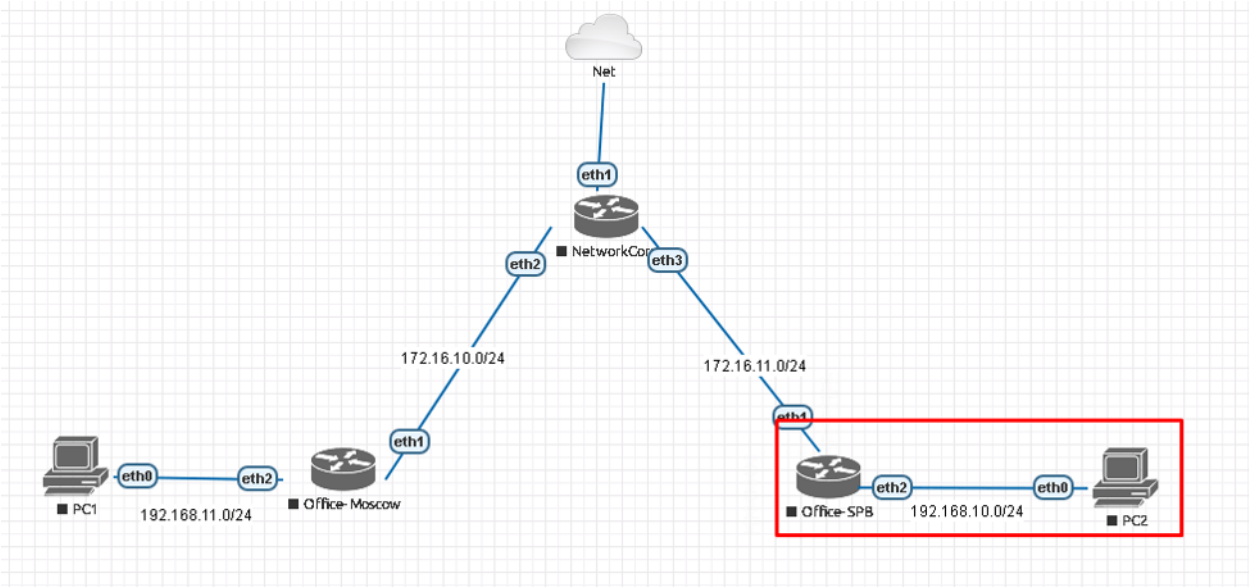

Рисунок 1 – Схема лабораторного стенда

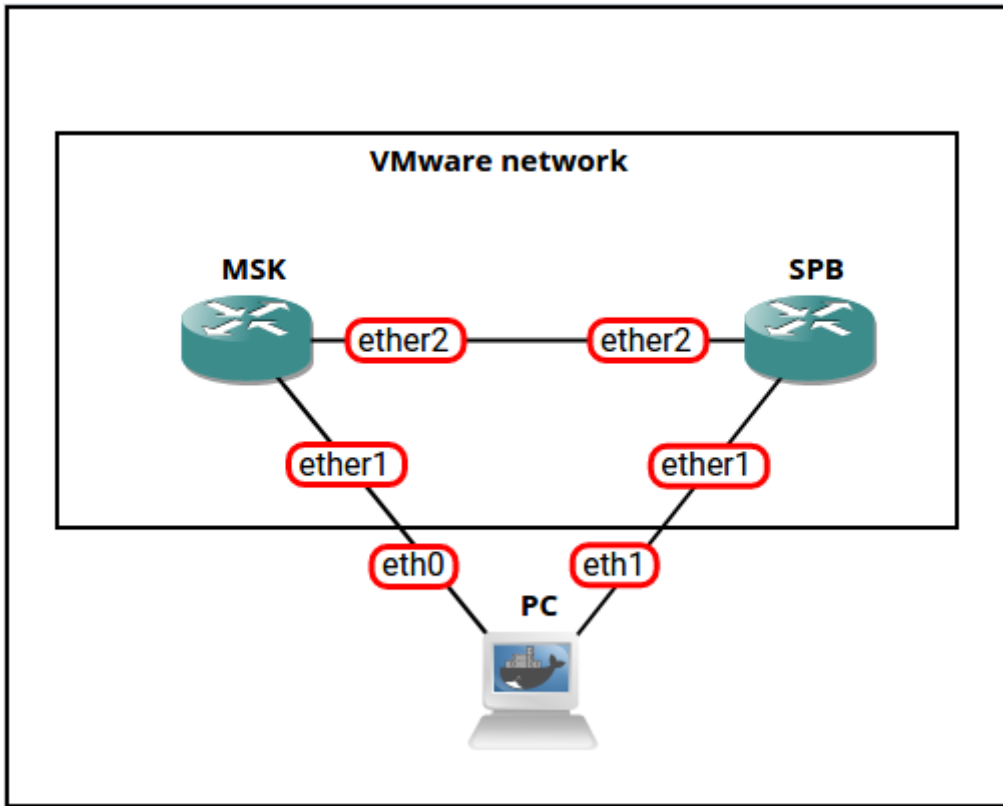

Рисунок 2 – Упрощенная схема стенда с использованием гипервизора VMware

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.

2. Конфигурация протокола L2TP

2.1 Создание IP пула

На оборудовании Mikrotik есть особенность с клиент серверными протоколами VPN – соединение не установится до тех пор, пока мы не назначим IP адреса с обоих сторон, в предыдущей лабораторной адрес устанавливался статически. Создадим пул для VPN клиентов. Подключаемся к «московскому» роутеру и открываем IP-Pool.

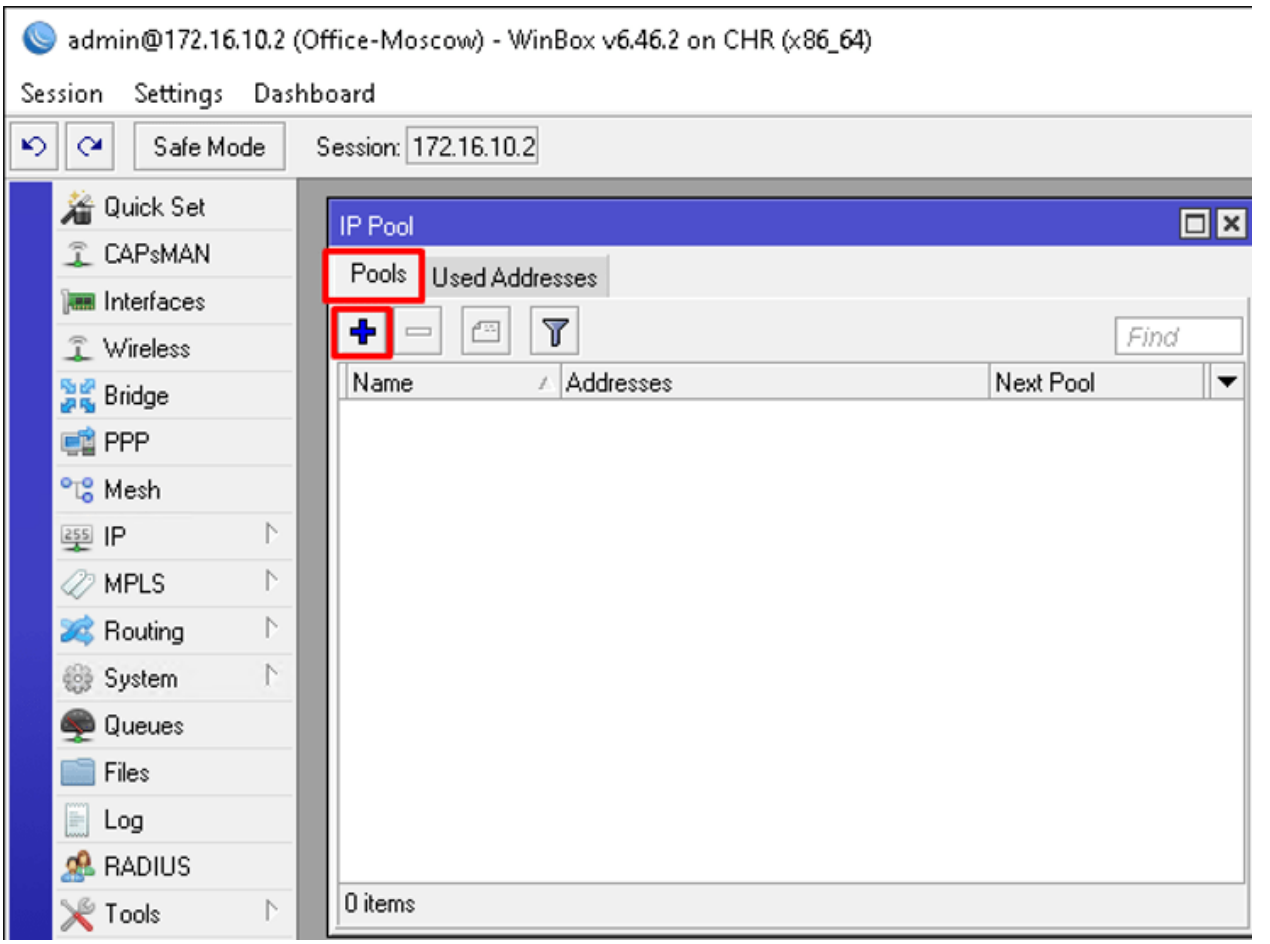

Рисунок 3 – Добавление IP пула

Добавляем пул, задаем имя и адреса.

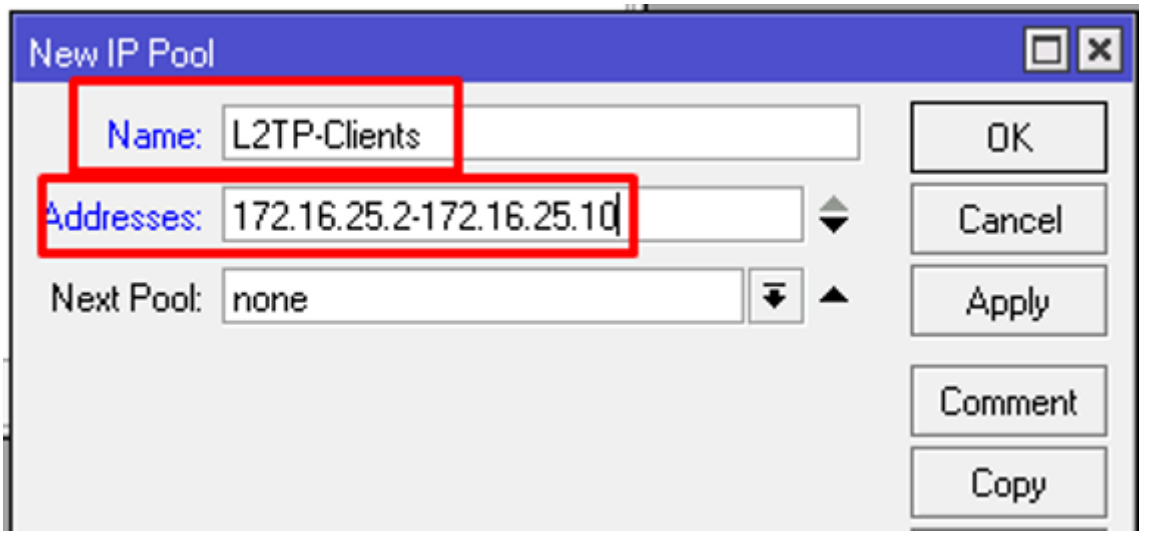

Рисунок 4 – Конфигурация IP пула

Next Pool указывать не будем. Так же отметим, что в работе будем использовать в VPN /32 маску подсети.

CLI:

/ip pool add name=L2TP-Clients ranges=172.16.25.2-172.16.25.10

2.2 Создание профиля подключения

Переходим к созданию профиля L2TP для нашего сервера. Создаем его в PPP – Profiles.

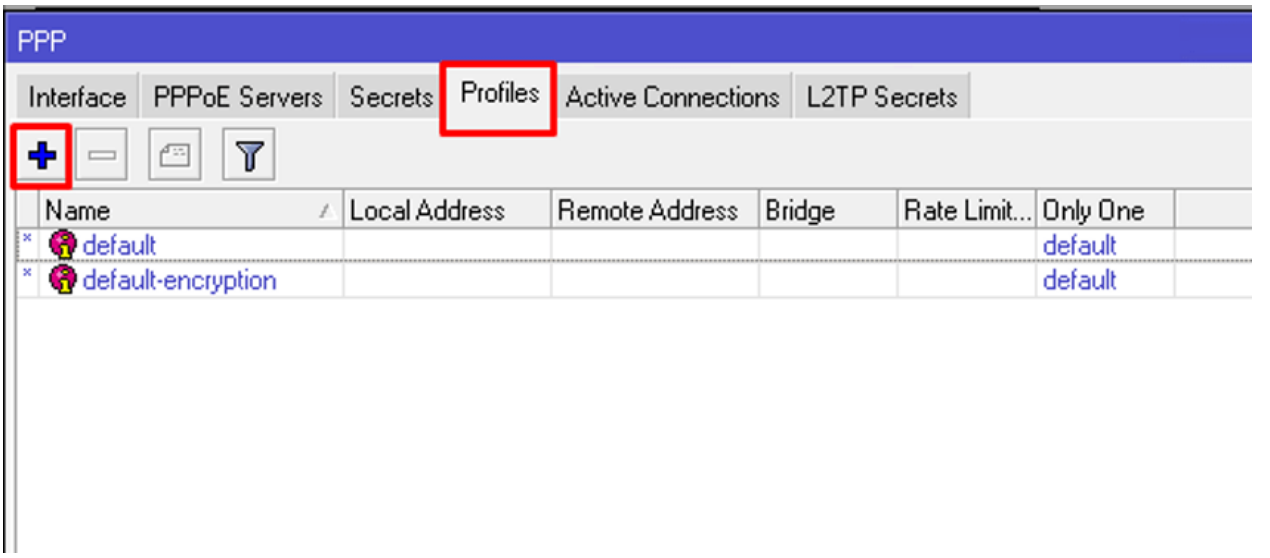

Рисунок 5 – Создание профиля L2TP

Создаем профайл. Указываем:

– Имя профиля;

– Local Address – следует указать статический адрес внутри VPN, в нашем случае 172.16.25.1;
– Remote Address – созданный на предыдущем шаге пул из выпадающего списка;
– Change TCP MSS – No;
– Use UPnP – No.

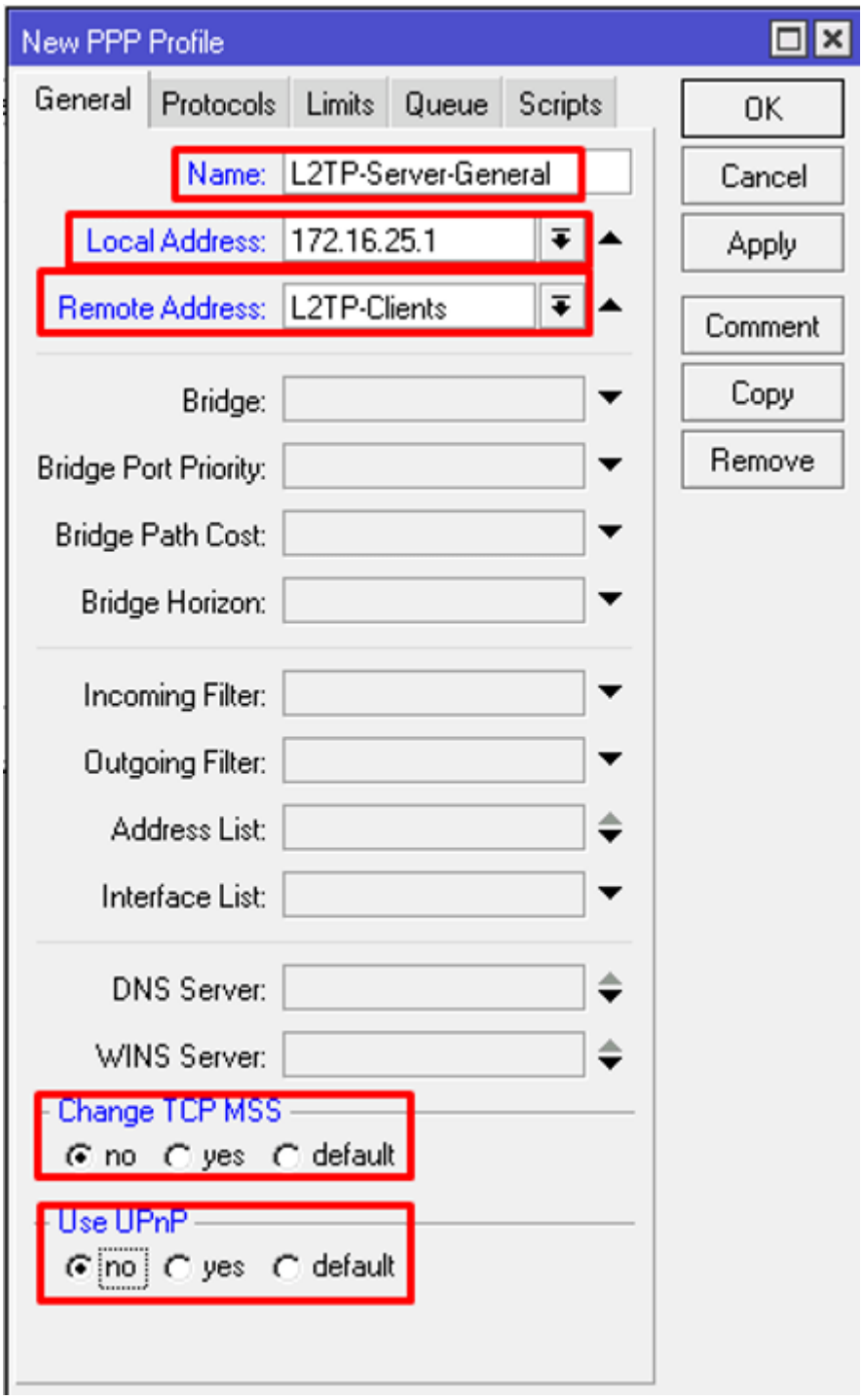

Рисунок 6 – Конфигурация профиля L2TP

Переходим на вкладку Protocols, ставим значения:

- Use MPLS – No;
- Use Compressions – Yes;
- Use Encryption – Yes.

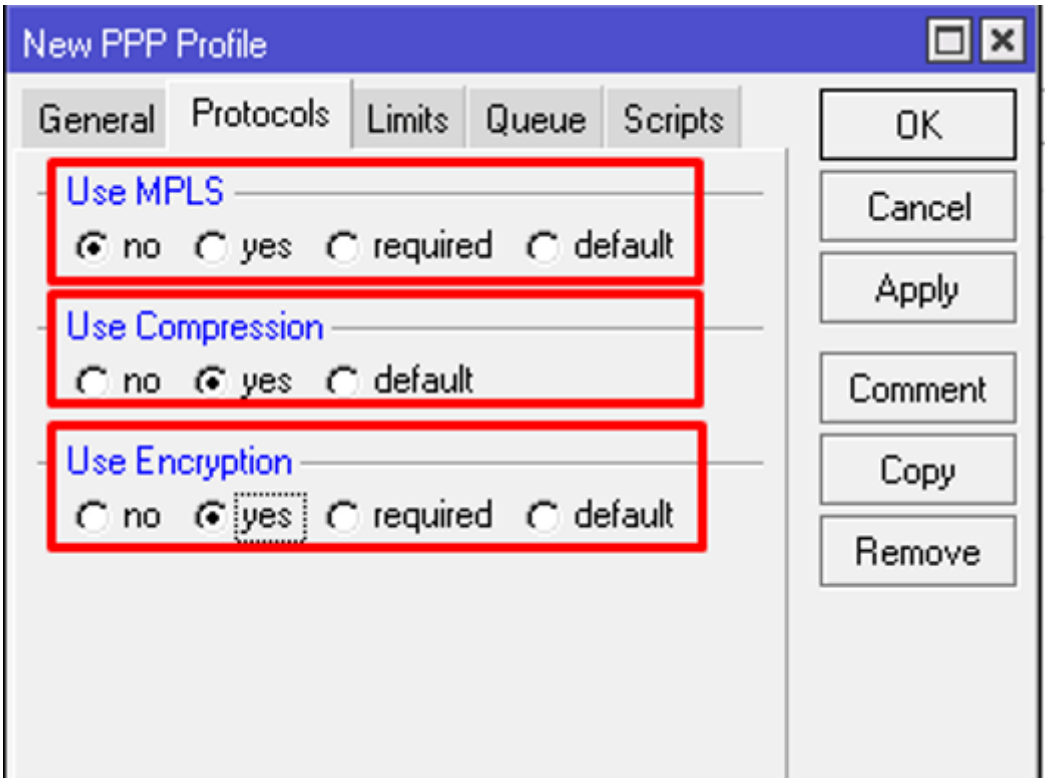

Рисунок 7 – Конфигурация профиля L2TP

Переходим в Limits, выставляем значение Only One в No.

Сохраняем и проверяем результат.

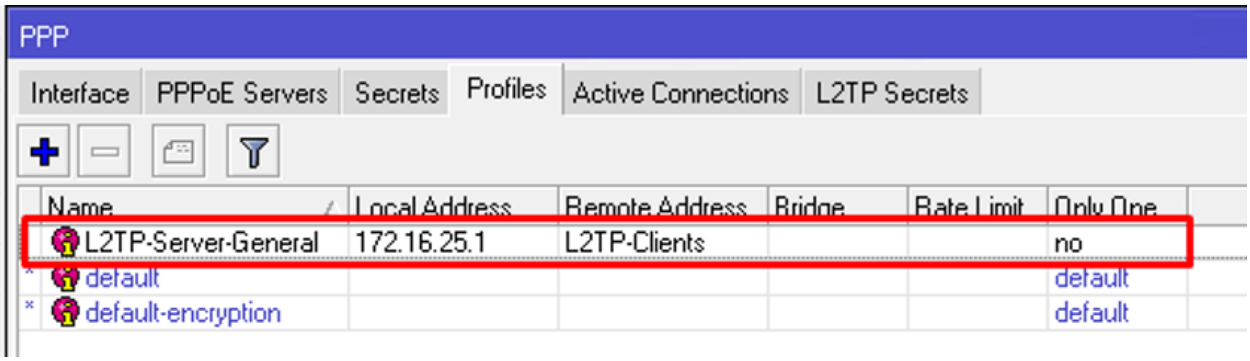

Рисунок 8 – Отображение профиля L2TP в окне PPP

CLI:

/ppp profile add change-tcp-mss=no local-address=172.16.25.1 name=L2TP-Server-General only-one=no remote-address=L2TP-Clients use-compression=yes use-encryption=yes use-mpls=no use-upnp=no

2.3 Включение L2TP сервера

Будем ориентироваться на повышение безопасности аутентификации и отключим старые протоколы. Если у вас есть устройства не поддерживающие современные протоколы аутентификации, то не забудьте включить их обратно. Переходим в PPP – Interface – L2TP Server.

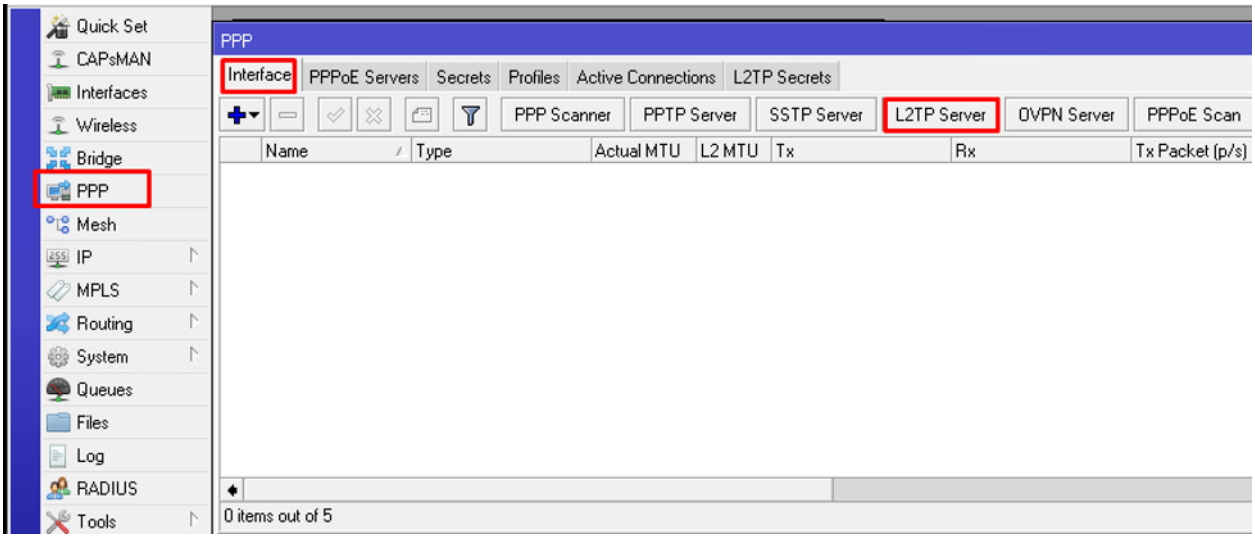

Рисунок 9 – Включение L2TP

Выставляем следующее параметры:

- Enable – ставим галочку;
- Default Profile – L2TP-Server-General;
- mschapv1, chap, pap – снимаем галочки;
- Use IPsec – ничего не ставим, т.к. мы не будем использовать IPSEC.

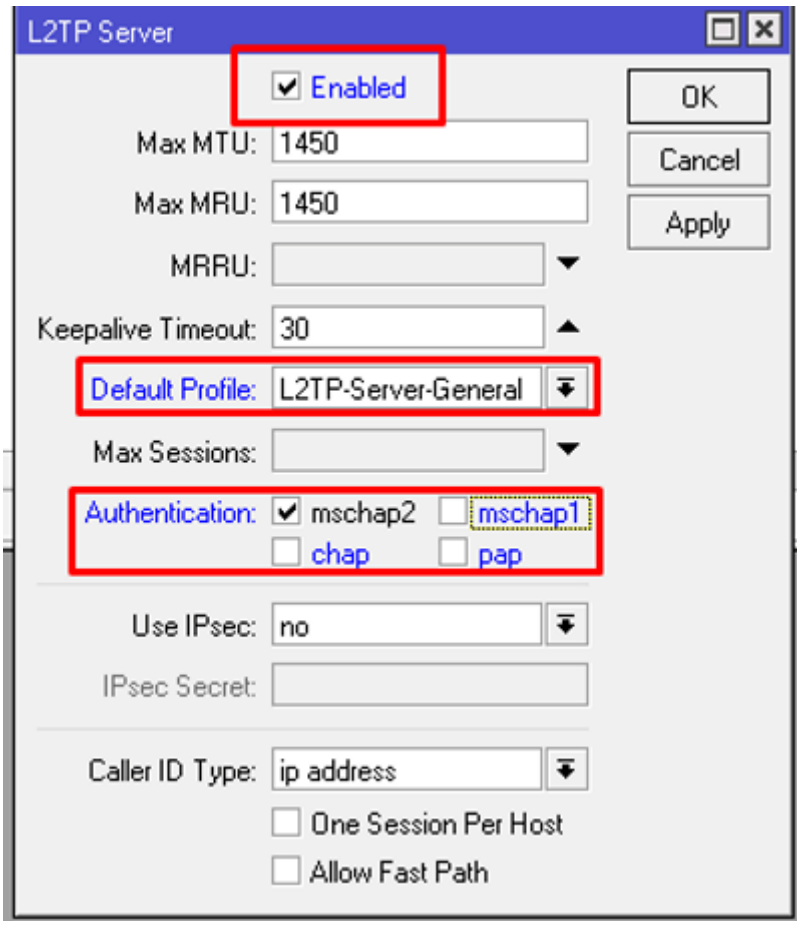

Рисунок 10 – Конфигурация L2TP

Сохраняем и переходим далее.

CLI: /interface l2tp-server server set authentication=mschap2 default-profile=L2TP-Server-General enabled=yes

2.4 Настройка firewall

Необходимо создать разрешающее правило входящего трафика L2TP на нашем mikrotik в firewall для UDP порта 1701. Приступим к реализации. IP – Firewall – Filter создаем новое правило.

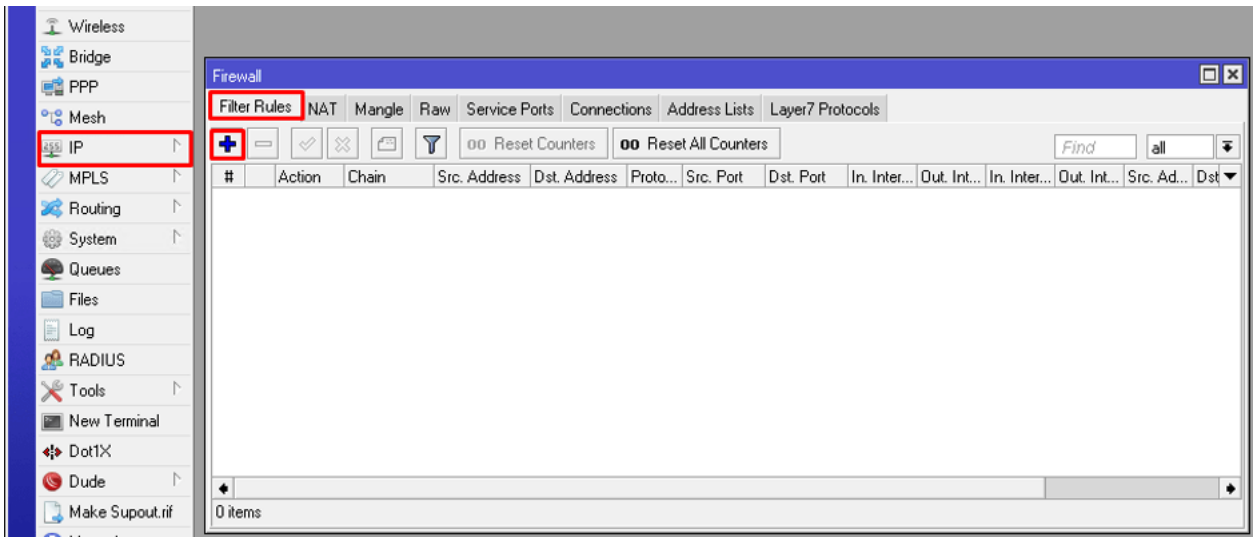

Рисунок 11 – Конфигурация межсетевого экрана

На вкладке General необходимо изменить следующие параметры:

- Chain – input;
- Protocol – UDP;
- Dst. Port – 1701;
- Connection State – New.

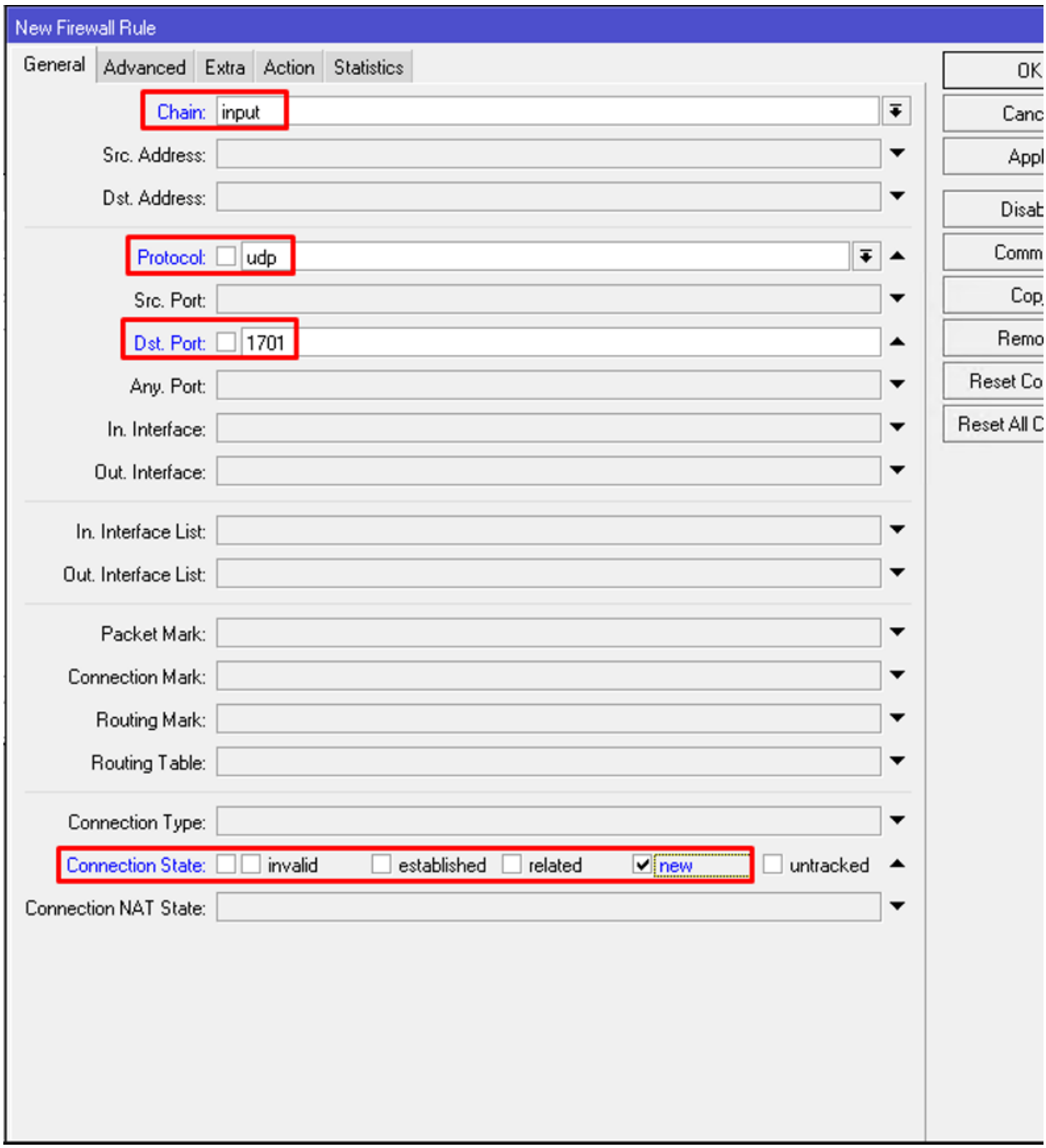

Рисунок 12 – Конфигурация межсетевого экрана

На вкладке «Action» указать действие «accept» и сохранить.

CLI:

```
/ip firewall filter
add action=accept chain=input connection-state=new dst-port=1701 protocol=udp
add action=accept chain=input connection-state=established,related
```

На самом деле, данное правило будет работать только для новых пакетов пришедших на роутер, для остальных пакетов – нет, а значит сессия не запустится.

Чтобы сессии работали корректно нужно еще одно правило, которое разрешает все устоявшиеся входящие соединения. Создаем еще одно правило.

- Chain – input;
- Connection State – established, related;
- Action – accept.

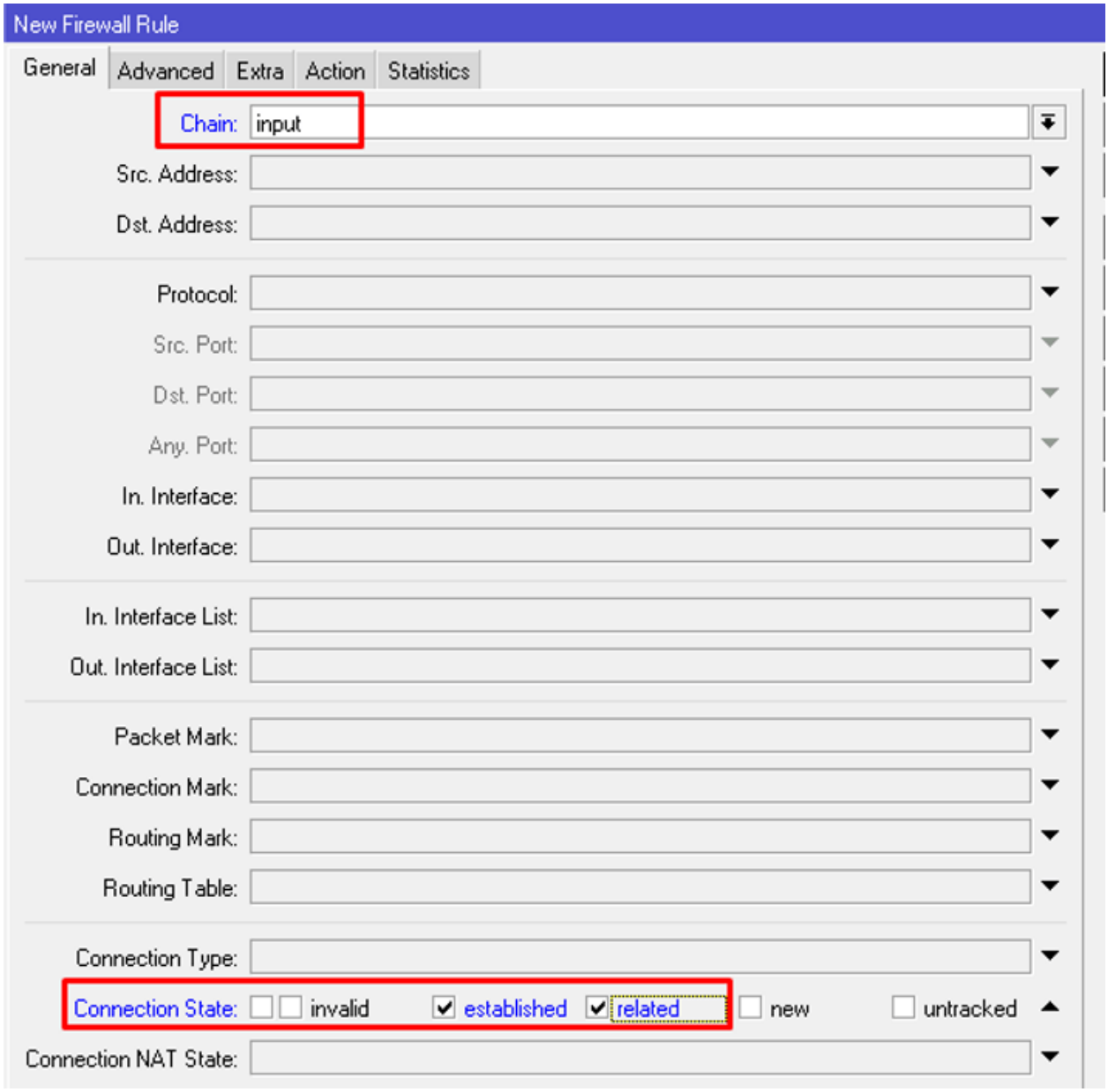

Рисунок 13 – Конфигурация межсетевого экрана

На этом настройка сервера L2TP завершена.

В отчет включить конфигурацию роутера в виде текстового файла, получить конфигурацию можно выполнив команду:

```
/export file=backup-test compact
```