

Настройка L2TP Сервера на Mikrotik

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

January 29, 2020

Добрый день коллеги. Сегодня я покажу на деле как настроить L2TP Server на оборудовании Mikrotik. Конфигурация будет простая, без наворотов типа IPSEC. Но не стоит этим пренебрегать, т.к. стандартное шифрование весьма слабое и строить линки site-to-site без IPSEC я бы не рекомендовал.

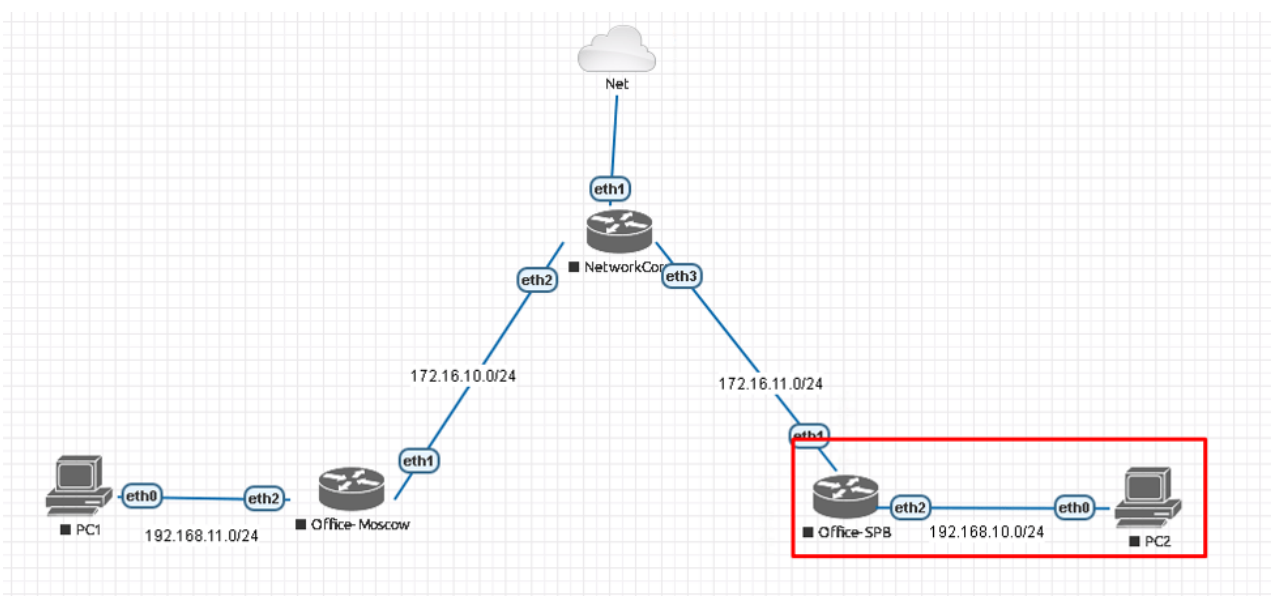
Содержание

1. Немного о протоколе L2TP
2. Конфигурирование
3. Создание IP пула
4. Создание профиля подключения
5. Включение L2TP сервера
6. Настройка firewall

Немного о протоколе L2TP

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.

Конфигурирование



Используем наш уже знакомый лабораторный стенд с Mikrotik CHR версии 6.46.2 на борту. Мы находимся справа внизу в офисе SPB (Office-SPB).

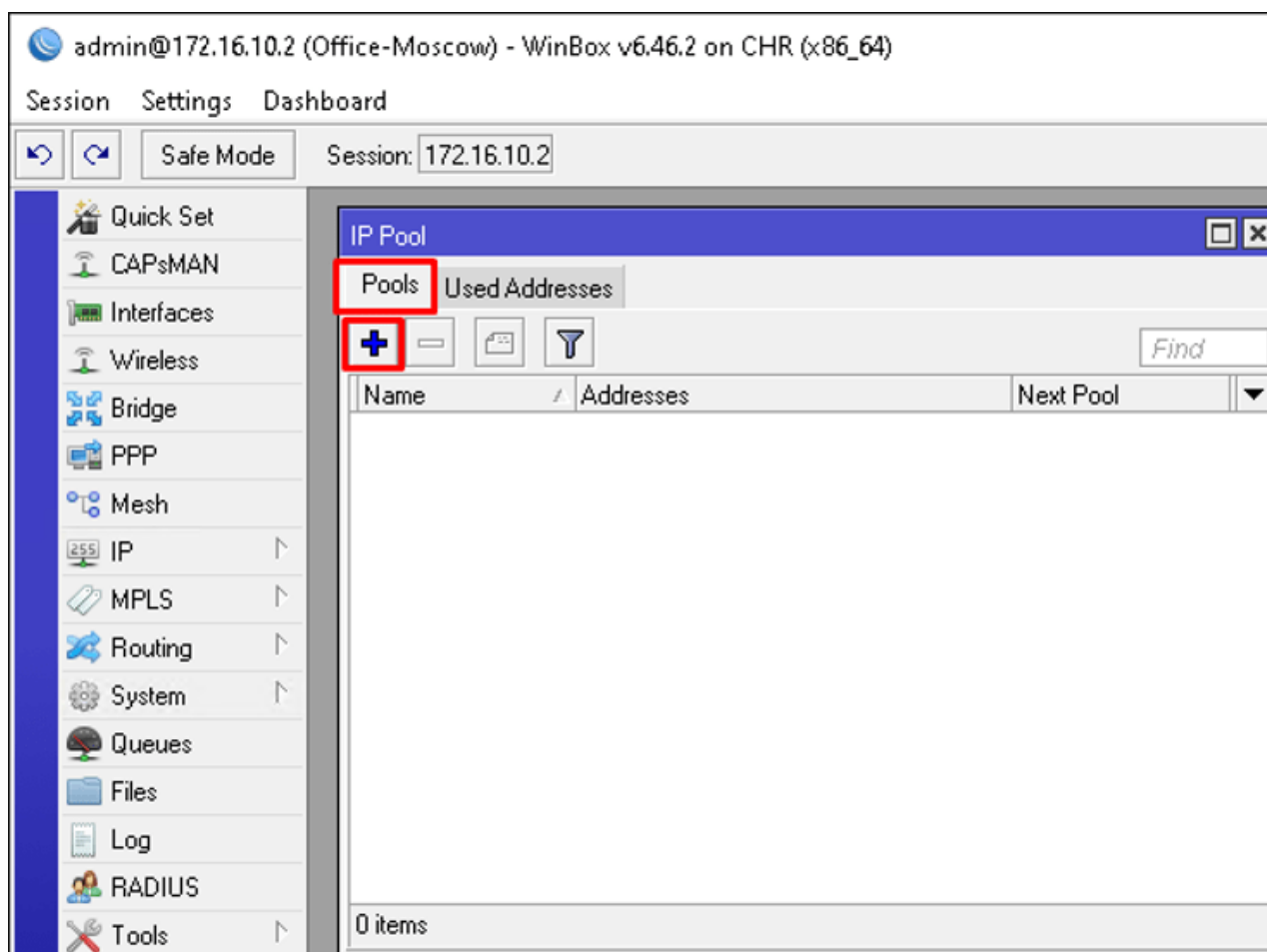
Вводные данные:

- 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.

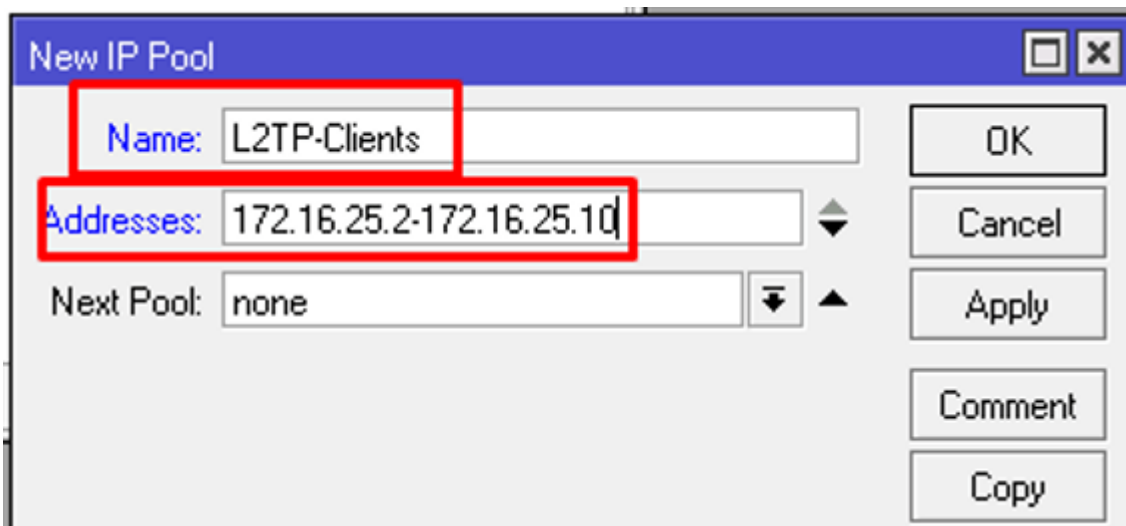
Наша команда рекомендует изучить Наша команда рекомендует изучить углубленный курс по администрированию сетевых устройств MikroTik В курсе много лабораторных работ по итогам которых вы получите обратную связь. После обучения вы получите диплом гос. образца РФ. Подробности и доступ к началу курса бесплатно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

Создание IP пула

На оборудовании Mikrotik есть нюанс с клиент серверными протоколами VPN – соединение не установится до тех пор, пока мы не назначим IP адреса с обеих сторон. Поэтому создадим пул для VPN клиентов. Подключаемся к московскому роутеру и открываем IP-Pool.



Добавляем пул, задаем имя и адреса.



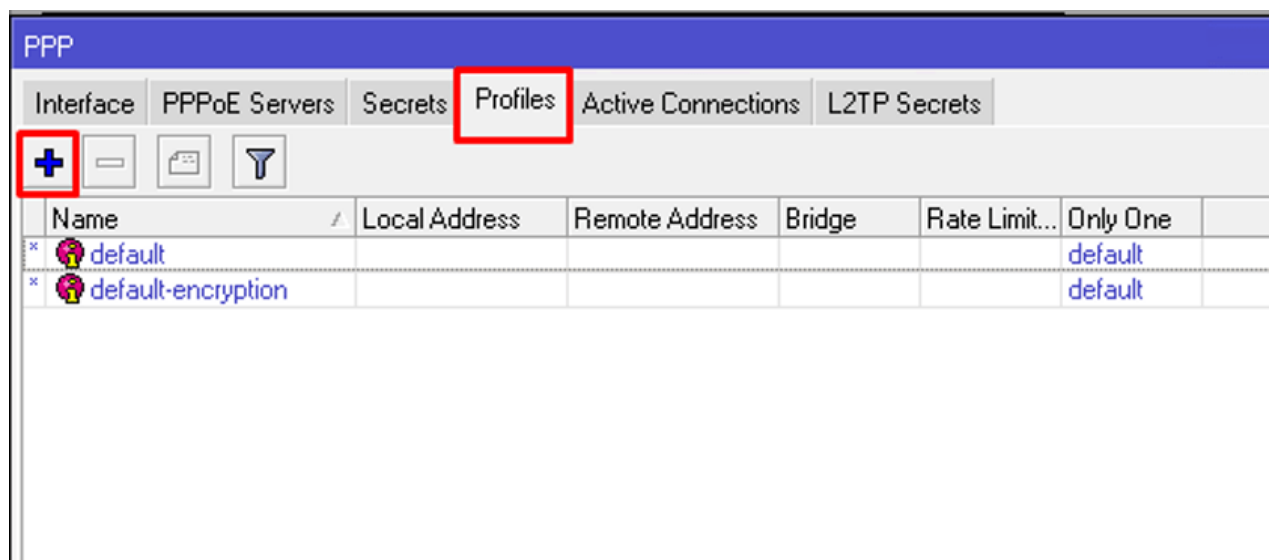
Next Pool указывать не будем. Так же отмечу, что используем мы в VPN /32 маску подсети.

CLI:

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

Создание профиля подключения

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



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.

New PPP Profile

General Protocols Limits Queue Scripts

Name: L2TP-Server-General

Local Address: 172.16.25.1

Remote Address: L2TP-Clients

Bridge:

Bridge Port Priority:

Bridge Path Cost:

Bridge Horizon:

Incoming Filter:

Outgoing Filter:

Address List:

Interface List:

DNS Server:

WINS Server:

Change TCP MSS

☒ no ☐ yes ☐ default

Use UPnP

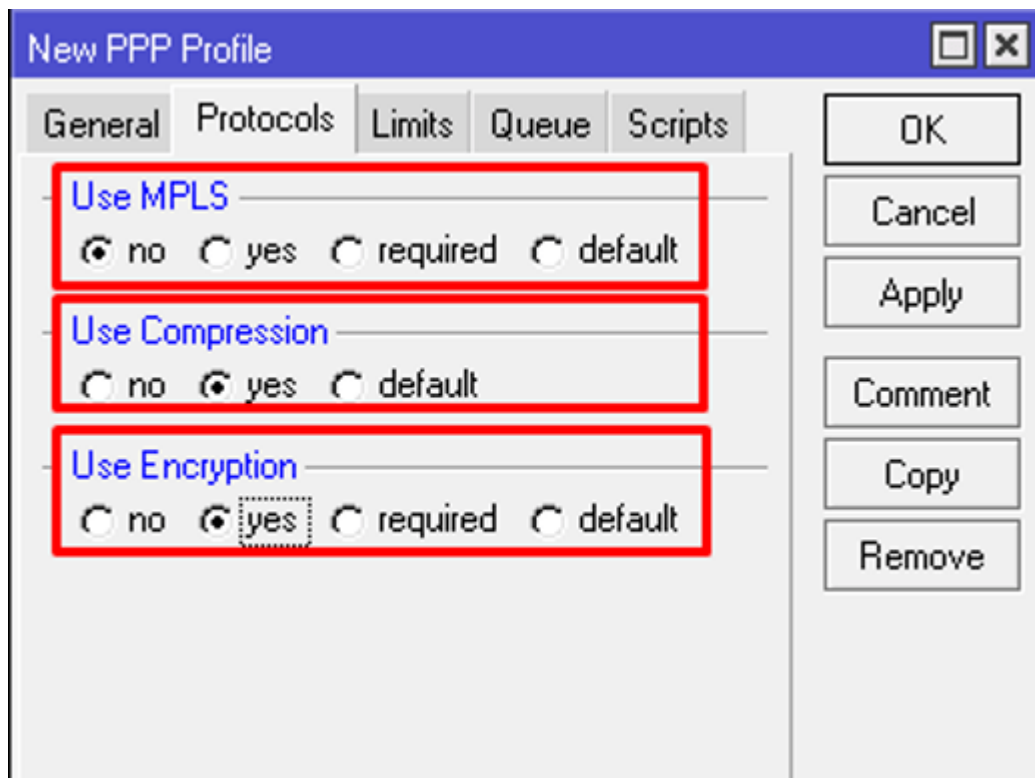
☒ no ☐ yes ☐ default

OK Cancel Apply Comment Copy Remove

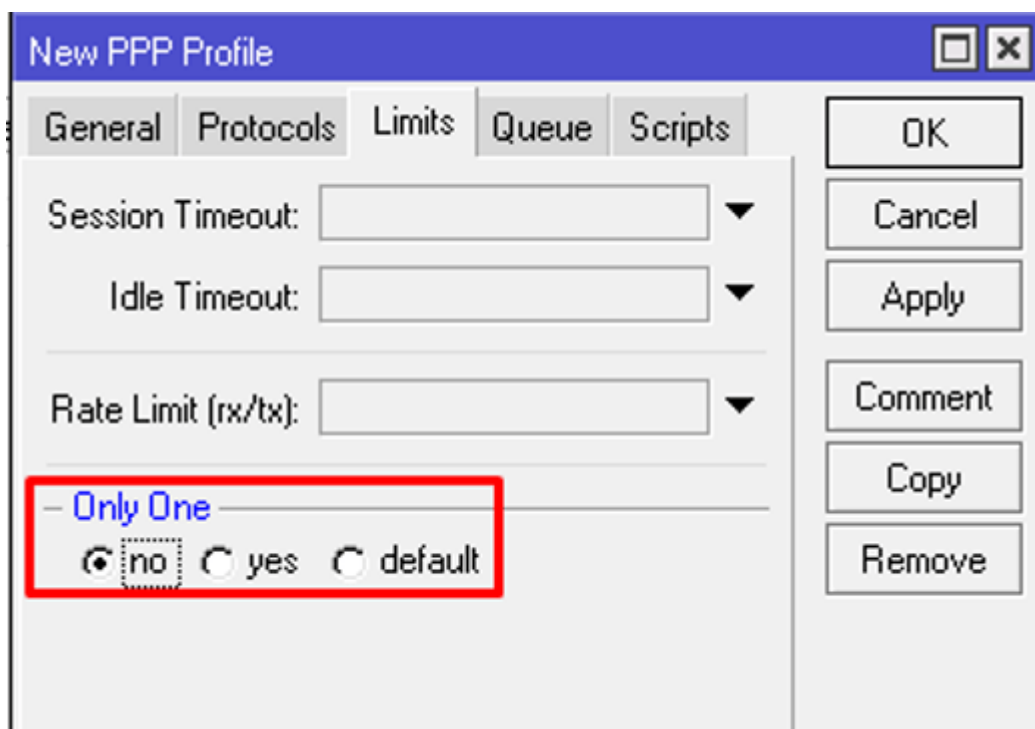
Переходим на вкладку Protocols, ставим значения:

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





Переходим в Limits, выставляем значение Only One в No.



Сохраняем и смотрим на результат.

PPP

Interface

PPPoE Servers

Secrets




Profiles

Active Connections

L2TP Secrets

+

-

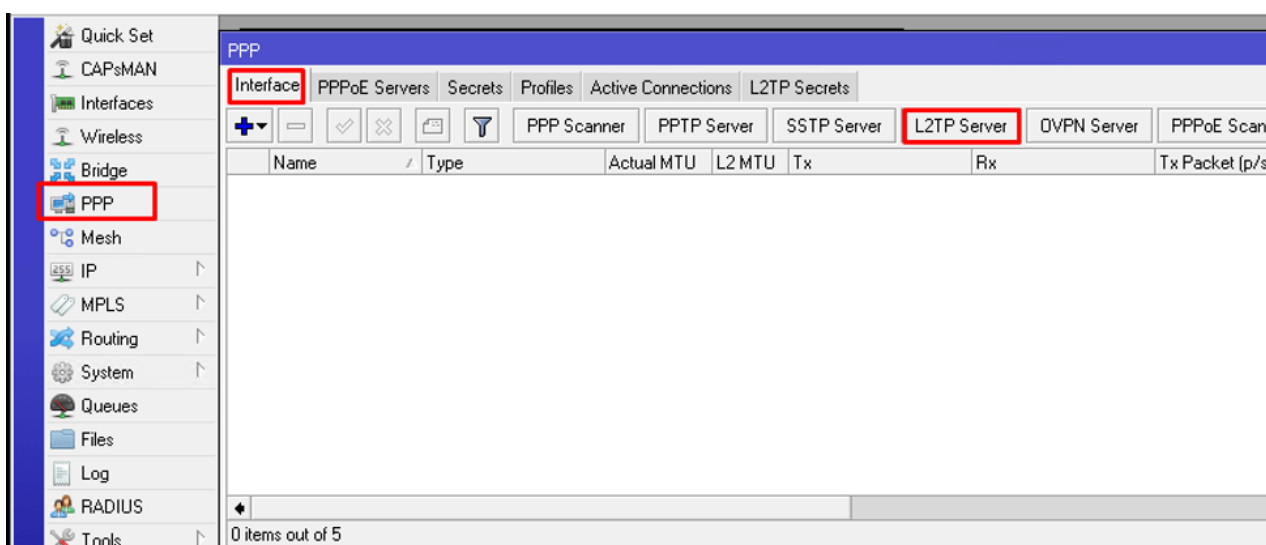
Name	Local Address	Remote Address	Bridge	Rate Limit	Only One
 L2TP-Server-General	172.16.25.1	L2TP-Clients			no
*  default					default
*  default-encryption					default

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-mpsl=no use-upnp=no
```

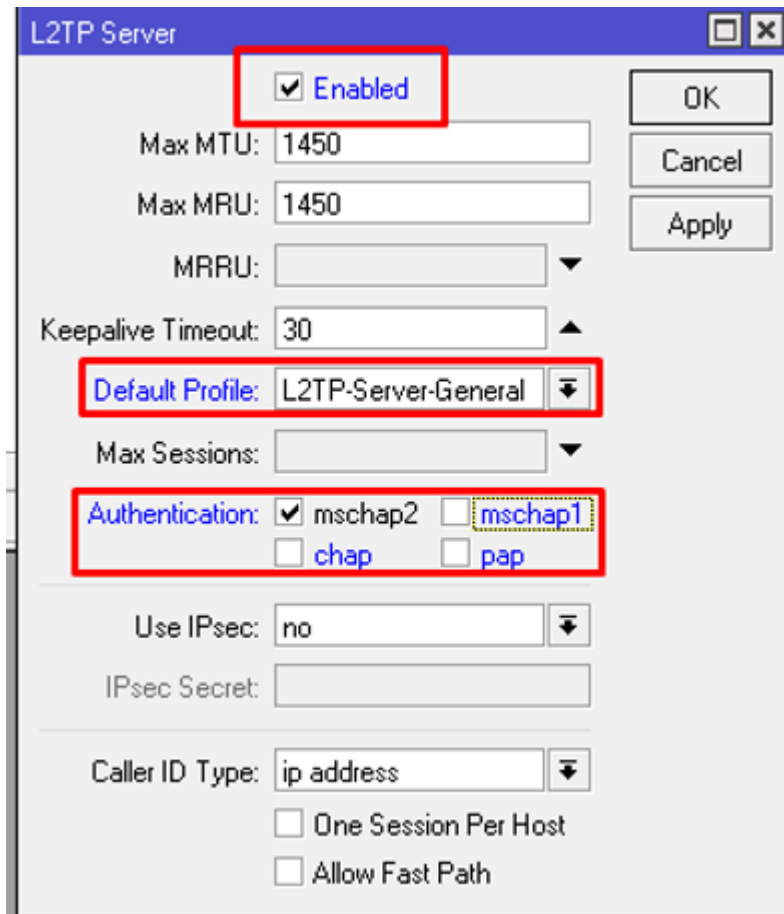
Включение L2TP сервера

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.



Выставляем следующие 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.



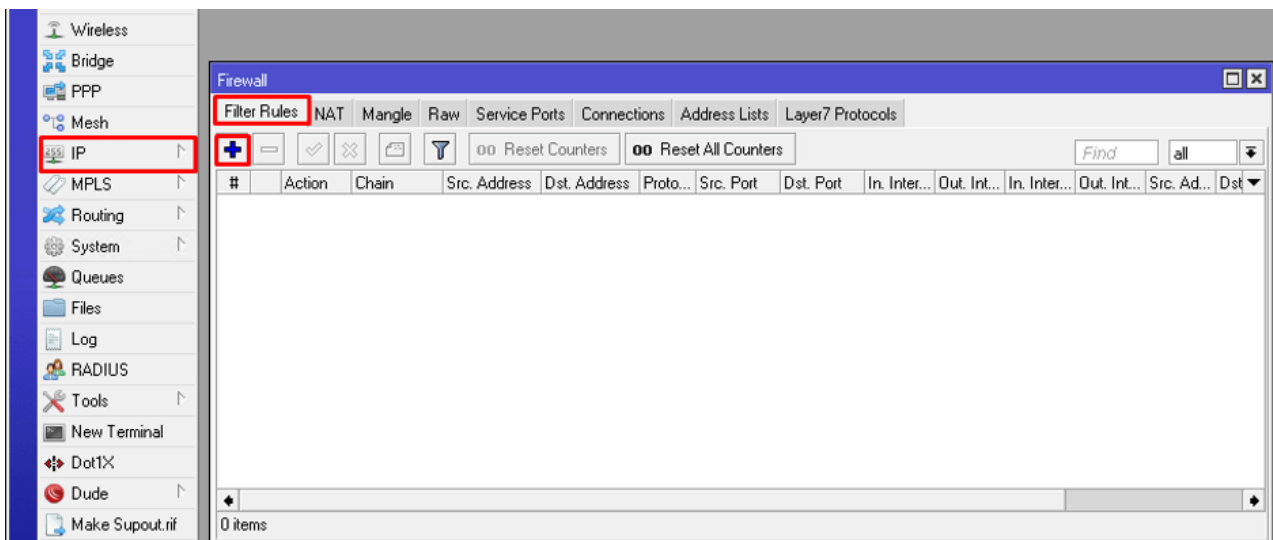
Сохраняем и переходим далее.

CLI:

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

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.



В General нас интересует:

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

New Firewall Rule

General Advanced Extra Action Statistics

Chain: input

Src. Address:

Dst. Address:

Protocol: ☐ udp

Src. Port:

Dst. Port: ☐ 1701

Any. Port:

In. Interface:

Out. Interface:

In. Interface List:

Out. Interface List:

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

Connection Type:

Connection State: ☐ invalid ☐ established ☐ related ☒ new ☐ untracked

Connection NAT State:

OK Cancel Apply Disable Commit Copy Remove Reset Config Reset All Config

На вкладке Action нас интересует accept.

New Firewall Rule

General Advanced Extra **Action** Statistics

Action: **accept**

☐ Log

Log Prefix:

Сохраняем.

Firewall

Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols

+ - ✓ ✗ [icon] [icon] oo Reset Counters oo Reset All Counters

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	n. Inte
0	✓ acc...	input			17 (udp)		1701	

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 оживет. Чтобы сессии жили и им было хорошо нужно еще одно правило, которое разрешает все устоявшиеся входящие соединения. Создаем еще одно правило.

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

New Firewall Rule

General Advanced Extra Action Statistics

Chain: input

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

In. Interface:

Out. Interface:

In. Interface List:

Out. Interface List:

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

Connection Type:

Connection State: ☐ invalid ☒ established ☒ related ☐ new ☐ untracked

Connection NAT State:

New Firewall Rule

General Advanced Extra Action Statistics

Action: accept

☐ Log

Log Prefix:

На этом, пожалуй, все. Настройка сервера L2TP завершена.

Несколько слов про блокировку L2TP – из практики, есть такие товарищи — провайдеры, которые блокируют L2TP. Допустим Билайн в некоторых регионах уже начал блокировать весь L2TP без IPSEC. Обращайте на это внимание, если вы

сделали все правильно, но соединение не проходит, значит дело в провайдере.

Далее мы рассмотрим настройку L2TP-клиента и конечно же всеми любимый IPSEC.

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](#).