https://wiki.teltonika-networks.com/view/Setting_up_a_L2TP_over_IPsec_tunnel_between_RUT_and_Mikrotik_device

Setting up a L2TP over IPsec tunnel between RUT and Mikrotik device

□

Contents

Introduction

Because of the lack of confidentiality inherent in the Layer 2 Networking Protocol (L2TP) protocol, Internet Protocol Security (IPsec) is often used to secure L2TP packets by providing confidentiality, authentication and integrity. The combination of these two protocols is generally known as L2TP over IPsec (or simply L2TP/IPsec).

This article provides a guide on how to configure L2TP/IPsec tunnel between RUTxxx and Mikrotik routers.

Prerequisites

- One RUTxxx router of any type
- One Mikrotik router (this configuration example was created using Mikrotik rb750gr3)
- Server must have a Public Static or Public Dynamic IP address (client can have private or public IP address)
- At least one end device (PC, Laptop) to configure the routers
- WinBox application

Configuration scheme

Mikrotik configuration

Connect to MikroTik by using **WinBox** application and press **New Terminal**.

The first step is to create a PPP Profile on the MikroTik. Use a 192.168.102.1 for the local address (the VPN Gateway), assuming this is not already in use. You will also need to add a DNS Server. Use

this command:

```
/ppp profile add name=ipsec_vpn local-address=192.168.102.1 dns-
server=1.1.1.1
```

Next, you need to add an L2TP-server interface and set the allowed authentication methods, mschap1 and mschap2. Use this command:

```
/interface l2tp-server server set enabled=yes default-profile=ipsec_vpn
authentication=mschap1,mschap2
```

Then you need to define the peering of IPSec and also the default IPsec policy. You will also set the pre-shared-key secret in the process. Use these commands to do so:

```
/ip ipsec policy set [ find default=yes ] src-address=0.0.0.0/0 dst-
address=0.0.0.0/0 protocol=all proposal=default template=yes
```

```
/ip ipsec peer add exchange-mode=main passive=yes name=l2tpserver
```

```
/ip ipsec identity add generate-policy=port-override auth-method=pre-shared-
key secret="password" peer=l2tpserver
```

Next, set the default encryption algorithms:

```
/ip ipsec proposal set default auth-algorithms=sha1 enc-algorithms=3des pfs-
group=modp1024
```

Now, add a user and allocate an IP Address:

```
/ppp secret add name="username" password="password" service=l2tp
profile=ipsec_vpn remote-address=192.168.102.2
```

Open the IPSec ports from the WAN:

```
/ip firewall filter add chain=input action=accept protocol=udp
port=1701,500,4500
```

```
/ip firewall filter add chain=input action=accept protocol=ipsec-esp
```

Now go to **IP > Firewall** and change positions of the 2 Firewall rules you just created (drag it to the top like in the example) in order to move them, press **#** sign.

RUT configuration

Access RUTxxx WebUI and go to **Services > VPN > L2TP'*. There create a new configuration by selecting role* Client*,* writing **New configuration name** and pressing **Add New** button. It should appear after a few seconds. Then press **Edit**.

Then apply the following configuration.

1. **Enable** instance.
2. Write **Server** IP address (MikroTik public IP address).
3. Write **Username** (write the username which you created with this command /ppp secret add name="username" password="password" service=l2tp profile=ipsec_vpn remote-address=192.168.102.2).
4. Write **Password** (write the password which you created with this command /ppp secret add name="username" password="password" service=l2tp profile=ipsec_vpn remote-address=192.168.102.2).
5. Set **Keep alive** (30).
6. Press **Save**.

Now go to **Services > VPN > IPsec**.

1. Write **Pre-shared key** (write the password which you created with this command /ip ipsec identity add generate-policy=port-override auth-method=pre-shared-key secret="password" peer=l2tpserver).
2. Press **Save**.
3. Write **IPsec** interface name and press **Add**.
4. When the interface appears like in the example, press **Edit**.

1. **Enable** instance.
2. Select **Type** (Transport).
3. Write **Remote VPN endpoint** (MikroTik public IP address).
4. Select **DH group** (MODP1024)
5. Set all of the settings in **Phase 2** to be exactly the same as in the **Phase 1**.
6. Press **Save**.

Testing configuration

Go to **Status > Routes** and in the **Active IP Routes** table you should see this new route:

Try to ping the remote VPN endpoint via **CLI** or **SSH** using this command:

```
ping 192.168.102.1
```

Also, you can check whether **IPsec** is working by writing this command to **CLI**:

```
ipsec status
```

It should show:

```
Security Associations (1 up, 0 connecting)
```