

Setting up an OpenVPN tunnel between RUT and Mikrotik device



Contents

- [1 Introduction](#)
- [2 Prerequisites](#)
- [3 Configuration scheme](#)
- [4 Server \(Mikrotik\) configuration](#)
- [5 Client \(RUTxxx\) configuration](#)
- [6 Testing configuration](#)

Introduction

OpenVPN is an open-source software application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities.

This guide provides a configuration example with details on how to configure OpenVPN connection between MikroTik and RUTxxx routers. The server will be MikroTik device and the client will be our RUTxxx router.

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
- At least one end device (PC, Laptop) to configure the routers
- WinBox application

Configuration scheme



Server (Mikrotik) configuration

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



Now create certificates by using these commands (these will be valid for 10 years):

```
/certificate
```

```
add name=ca-template common-name=example.com days-valid=3650 key-size=2048
key-usage=crl-sign,key-cert-sign
```

```
add name=server-template common-name=*.example.com days-valid=3650 key-
size=2048 key-usage=digital-signature,key-encipherment,tls-server
```

```
add name=client-template common-name=client.example.com days-valid=3650 key-
size=2048 key-usage=tls-client
```

Created certificates will need signing, use these commands:

```
sign ca-template name=ca-certificate
```

```
sign server-template name=server-certificate ca=ca-certificate
```

```
sign client-template name=client-certificate ca=ca-certificate
```

Now you need to export those certificates:

```
/certificate
```

```
export-certificate ca-certificate export-passphrase=""
```

```
export-certificate client-certificate export-passphrase=12345678
```

Now go to **Files** and export those certificates by simply dragging them to your desktop.



Now go back to **Terminal** and create a separate pool of IP addresses for clients by using this command:

```
/ip
```

```
pool add name="vpn-pool" ranges=192.168.8.10-192.168.8.99
```

Instead of editing the default encrypted profile, we need to create a new one. Assumption is your MikroTik will also be a DNS server. And while at it, create a bit more secure user/password:

```
/ppp
```

```
profile add name="vpn-profile" use-encryption=yes local-address=192.168.8.250
dns-server=192.168.8.250 remote-address=vpn-pool
```

```
secret add name=user profile=vpn-profile password=password
```

Adjust firewall by using this command:

```
/ip firewall filter
```

```
add chain=input protocol=tcp dst-port=1194 action=accept place-before=0
comment="Allow OpenVPN"
```

Now enable OpenVPN server interface:

```
/interface vpn-server server
```

```
set default-profile=vpn-profile certificate=server-certificate require-  
client-certificate=yes auth=sha1 cipher=aes128,aes192,aes256 enabled=yes
```

Client (RUTxxx) configuration

Access RUTxxx WebUI and go to **Service > VPN > OpenVPN**. 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. Select **Protocol** (TCP).
3. Select **Authentication** (TLS/Password).
4. Select **Encryption** (AES-128-CBC 128).
5. Write **Remote host/IP address** (MikroTik public IP address).
6. Write **Keep alive** (10 120).
7. Write **Remote network IP address** (192.168.8.0).
8. Write **Remote network IP netmask** (255.255.255.0).
9. Write **User name** and **Password** which you created on Mikrotik (you created it by using this command: `secret add name=user profile=vpn-profile password=password`).
10. Upload **Certificate authority**, **Client certificate**, **Client key** (use those exported files).
11. Write **Private key decryption password** (you created it by using this command: `export-certificate client-certificate export-passphrase=12345678`).
12. Press **Save**.

Testing configuration

Go to **Status > Routes** and in the **Active IP Routes** table you should see these two new routes.



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

```
ping 192.168.8.250
```

