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

Creating OpenVPN access server and connecting RUTX to it

□

Contents

Introduction

OpenVPN Access Server is a set of installation and configuration tools that comes in one package, it simplifies the rapid deployment of a VPN remote access solution. At its core it is based on the popular OpenVPN open source software and maintains compatibility with it, making the deployed VPN immediately compatible with OpenVPN client software across multiple platforms and devices.

This article provides an extensive configuration example with details on how to install an **OpenVPN Access Server** in a virtual machine connected to a RUTX device, also provides the RUTX OpenVPN client configuration.

Prerequisites

- Two RUTX routers.
- At least one router must have a **Public Static** or **Public Dynamic IP** address.
- One PC to configure the OpenVPN access server and routers.

Configuration scheme

Installing OpenVPN Access Server

First of all we will need to have working **OpenVPN Access Server** on PC, which would act as server.

Note: Please keep in mind that for PC to act as any kind of server it **MUST** have either **Public Static** or **Public Dynamic** IP address.

If you're using Windows, we recommend installing OpenVPN Access Server in a virtual machine with Linux Ubuntu 18.04.1.

For this manual we will assume you are working with Linux Ubuntu 18.04.1 on your virtual machine.

- Login to your Linux machine.
- Open the terminal (Ctrl + Alt + t).
- Type the following commands into your virtual Linux machine to install **OpenVPN Access Server** (one at a time):

```
sudo apt update && apt -y install ca-certificates wget net-tools gnupg
```

It will ask for a password, it's the same one you use to login into your Linux Ubuntu.

```
sudo –i
```

```
wget -qO - https://as-repository.openvpn.net/as-repo-public.gpg | apt-key add
-
```

```
echo "deb http://as-repository.openvpn.net/as/debian bionic
main">/etc/apt/sources.list.d/openvpn-as-repo.list
```

```
exit
```

```
apt update && apt -y install openvpn-as
```

Setting administrator password

After installation restart the Linux machine, once the reboot is done, open terminal and set the password for OpenVPN Access Server administrator account, in order to do that use the following commands:

```
sudo passwd openvpn
```

Enter Linux machine password and then the password for OpenVPN Access Server administrator account, (see picture below):

If everything was done correctly, you should be able to access OpenVPN Access Server via virtual Linux machine from the web browser by entering: https://localhost:943

Probably you will get a warning: **"Potential Security Risk Ahead"**, simply accept the risks and **Continue**.

If for some reason the OpenVPN Access Server installation failed on your virtual machine, we

recommend you to visit these pages, it could help you to solve the issue: Installing openvpn access server on a linux system and VPN Software Packages

Note: Installed OpenVPN Access Server only provides 2 VPN connections.

OpenVPN Access Server configuration

After installing OpenVPN Access Server on your virtual machine you will need to change some settings to get *.ovpn* configuration file and allow Teltonika Networking devices to connect as clients to this server.

- Login to your OpenVPN Access Server as administrator by entering this link into your web browser: https://localhost:943
- By default username is: **openvpn**
- The Password is the same as you have configured previously.

Once you are connected, scroll down and click on **Admin** button to get access to VPN configuration (it could ask to login again).

You will need to set up some details into the OpenVPN Access Server:

- Create new OpenVPN Access Server user (Username and password).
- Set up the Public IP address.
- Once the new user is created, you will need to login with these credentials and download the .openvpn client file (it will be used in the RUTX router).

Adding new user to OpenVPN Access Server

In order to manage your users on OpenVPN Access Server navigate to **User Management -> User Permissions**

1. Type the **Username**.
2. Select **Allow Auto-login**.
3. Click on **More Settings**.
4. Add a **Password**.
5. Click on **Save Settings**.

Click on **Update Running Server** (it should pop-up at the top of configuration window):

Network settings

Presuming that **OpenVPN Access Server** will be running on Windows PC (virtual machine with Linux installed) and assuming that Teltonika RUTX device will be providing a public IP address for Windows PC you will need to configure OpenVPN Access Server, virtual machine and RUTX device to allow connection to OpenVPN Access Server.

Setting IP address

Now Windows PC and Linux systems will be getting public IP from Teltonika RUTX device, so it is required to make one more configuration to OpenVPN Access Server.

1. To get the IP address, login into your RUTX device and check your WAN IP Address.

1. Connect to the OpenVPN Access Server as **Administrator** https://localhost:943
    1. *Username:* ***openvpn***
    2. *Password: The password you configured above in the* ***Setting administrator password*** *step.*
2. Navigate to **Configuration -> Network Settings -> Hostname or IP address**.
3. Enter the public IP address of the Teltonika RUTX device:
4. Save the settings and update the running server.

This way, the clients .ovpn configuration files will be successfully downloaded from the server.

Virtual machine configuration

Now you will need to configure virtual machine network settings.

- Open the virtual machine and go to **Devices → Network → Network Settings**

1. Click on **Advanced**.
2. Click on **Port Forwarding** and add the following rules.

1. Click on **Add** new rule.
2. Type the Port Forwarding rule name.
3. Select the protocol to use.
4. Type the ports in **Host port** and **Guest port** fields.
5. Click on **OK**.

RUTX configuration

Also, you need to configure port forwarding on the RUTX device. So the client could connect to OpenVPN Access Server. For this configuration example we will be using a RUTX device, to configure port forwarding:

- Navigate to **Network -> Firewall -> Port Forwarding**
- Add three port forwarding rules (See the picture below)

Note: The destination IP **"Forward to IP"** should be your Windows PC IP address on which virtual machine is running.

Keep in mind that port 443 is also used for HTTPS, if you want to use a different port for **OpenVPN Access Server** when using TCP connection, try configuring the Access Server. With this configuration you will be able to connect to OpenVPN Access Server from internet side.

Getting OpenVPN client configuration file

Now, assuming that both Linux virtual machine and Teltonika Networking device are configured correctly, we need to get OpenVPN client configuration file (.ovpn).

- Connect to OpenVPN Access Server https://localhost:943
- Login with your recently added user credentials.

- Scroll down and click on the link **Yourself(autologin profile)** located in the tab "Available Connection Profiles"

- Download and save the .ovpn file.

Now with the downloaded **.ovpn** configuration file you will be able to connect as client to OpenVPN Access Server. The configuration file can be used on any device which supports OpenVPN configuration from file.

Uploading .opvn file to RUTX device

At this point you should have configured OpenVPN Access Server and you should have the .ovpn configuration file. Now you will need to upload it to the RUTX device OpenVPN configuration.

Connect to RUTX WebUI, navigate to **Services → VPN → OpenVPN** and do the following:

1. Type the **New Configuration Name**.
2. Select **Role: Client**.
3. Click **ADD**.
4. New configuration should appear after a few seconds. Then press **Edit**.

Now apply the following configuration:

1. Click on **Enable**.
2. Click on **Enable OpenVPN config from file**.
3. Upload the .opvn client configuration file.
4. Press **Save & Apply**.

Wait for a about a minute and the RUTX should connect to the OpenVPN Server Access, to confirm it

go to OpenVPN instance **Status** and it should be as **"Connected"**.

Note: The same .opvn configuration file should work on other devices.

Testing the configuration

In order to check whether your configuration is correct access your OpenVPN Access Server and go to **Status --> Current Users**:

- The OpenVPN instance should appear and display its IP addresses.

- Enter **VPN IP Address** to your internet browser and you should be able to reach the RUTX WebUI.