https://wiki.teltonika-networks.com/view/Template:Networking_rutos_configuration_example_openvpn_bridge_wifi_ap_use_case

Template:Networking rutos configuration example openvpn bridge wifi ap use case

Contents

Configuration overview and prerequisites

Prerequisites:

- Two RUTX routers (only the versions, which have WiFi)
- A Public Static or Public Dynamic IP address
- An end device to configure the router (PC, Laptop, Tablet, Smartphone)

The topology above depicts the OpenVPN scheme. The router with the Public IP address (**RUTX**) acts as the **OpenVPN server** and other **RUTX** acts as **client**. OpenVPN connects the networks of **HQ Office** and **Remote Office**. **Remote Office** will also have a separate WiFi AP for guests.

When the scheme is realized, remote office workers will be able to reach HQ's internal network with all internal systems by connecting to the router via LAN port or by connecting to a WiFi AP, which is used for work. All traffic apart guest WiFi is going to travel through VPN tunnel. Guest network traffic will go directly to WAN, it will give visitors access to the Internet connection, but nothing else making your company a lot more secure.

Configuring HQ office router

Before you start configuring the router **turn on "Advanced WebUI" mode**. You can do that by clicking the "Basic" button under "Mode", which is located at the top-right corner of the WebUI.

Note: You will need to do that in both, HQ and remote office routers.

OpenVPN

Generating Static key

Login to the router's WebUI, navigate to the **Services → CLI** page and do the following:
1. Enter username ***root*** .
2. Write the **Password** of your router.

Write the following commands to create OpenVPN **Static key**, which will be used for authentication:

```
1) cd /etc/easy-rsa
2) openvpn --genkey --secret static.key
```

Extracting the key

Linux

If you are using a Linux-based OS, extracting files from the router is simple. Just go to the directory on your PC where you want to relocate the files, right click anywhere and choose the **Open in Terminal** option. In the Terminal command line use the **Secure Copy** (**scp**) command to copy the files from the router. The full command should look something like this:

```
$ scp root@192.168.1.1:/etc/easy-rsa/static.key ./
```

The **root@192.168.1.1:/etc/easy-rsa/static.key** specifies the path to where the Static key is located (replace the IP address with your router's LAN IP); the **./** denotes that you want to copy the contents to the directory you are in at the moment.

Windows

If you are using Windows, you can copy files from the router using **WinSCP**, an Open source freeware SFTP, SCP and FTP client for Windows OS. Use the same login information with WinSCP as with CLI or SSH.
Please note: You must select **SCP** as File Protocol in WinSCP Session settings.

Once you've connected to the router with WinSCP, copying the files should be simple enough: just go to **/etc/easy-rsa/**, select the Static key file and drag it to directory on your PC where you would like to store it.

Configuring OpenVPN server

Go to **Services → VPN → OpenVPN**. There create a new configuration by writing **New configuration name** (you can type anything you want), selecting role **Server** and pressing **Add** button. It should appear after a few seconds. Then press **Edit**.

Now apply the following configuration:
1. **Enable** instance.
2. Set **TUN/TAP** to **TAP (bridged)**.
3. Enable **LZO**.
4. Select **Authentication: Static key**.
5. Add **Keep alive** interval: **10 120**.
6. Upload **Static pre-shared key**.
7. **Save** the changes.

Configuring remote office router

Before you start configuring the remote office router, set a static IP address on the device you are configuring the router with (e.g. 192.168.1.10). You can find instructions on how to do that here:

Ubuntu

Windows

Note: make sure to switch back to automatic DNS and IP address obtaining when you are done configuring the router.

OpenVPN

LAN

Go to **Network → Interfaces** and press **Edit** next to your LAN interface:

Apply the following steps:
1. Change your **LAN IP address** to: **192.168.1.2**
2. Disable **DHCP**.
3. **Save** the changes.

Configuring OpenVPN client

Go to **Services → VPN → OpenVPN**. There create a new configuration by writing **New configuration name** (you can type anything you want), selecting role **Client** and pressing **Add** button. It should appear after a few seconds. Then press **Edit**.

Now apply the following configuration:
1. **Enable** instance.
2. Set **TUN/TAP** to **TAP (bridged)**.
3. Enable **LZO**.
4. Select **Authentication: Static key**.
5. Write **Remote host/IP address** (RUTX OpenVPN server public IP).
6. Add **Keep alive** interval: **10 120**.
7. Upload **Static pre-shared key**.
8. **Save** the changes.

Guest WiFi

Creating a new WiFi AP

Go to **Network → Wireless**. There create a new **WiFi Access Point** by pressing **Add** button (you can use either, 2.4GHz or 5GHz WiFi). Then you will be forwarded to the configuration window.

Apply the following steps:
1. Disable **LAN**.
2. Create a new **Network** for guest WiFi.
3. **Save** the changes.

Now go to **Network → Interfaces** and press **Edit** next to your newly created LAN interface:

Apply the following steps:
1. Set **Protocol** to **Static**.
2. Press **Switch Protocol** and then more configuration options will appear.

Now apply the following steps:
1. Set **IPv4 Address** to **192.168.5.1**.
2. Select **IPv4 netmask: 255.255.255.0**.
3. Press **Setup DHCP Server**, after that more configuration options will appear, but you can leave those as default or change it to your own liking.
4. **Save** the changes.

Editing Firewall rules

Navigate to **Network → Firewall → General Settings**. There create a new **Zone** rule by pressing **Add** button. Then you will be forwarded to the configuration window.

Now apply the following steps:
1. At **Covered Networks** section select your newly created LAN interface.
2. Set WAN at **Allow Forward To Destination Zones** section.
3. Set WAN at **Allow Forward From Destination Zones** section.
4. **Save** the changes.

Go to **Network → Firewall → Traffic Rules**. There create a new **Forward** rule by writing a **Name**, selecting **Source Zone (newzone)**, **Destination Zone (lan)** and pressing **Add** button. Then you will be forwarded to the configuration window.

Now apply the following steps:
1. Set **Protocol** to **Any**.
2. Select **Action: Drop**.
3. **Save** the changes.

Results

Remote office should now be able to access HQ network resources. To verify the connection you can ping remote RUTX (HQ server) LAN IP and if you get a reply, you have successfully connected to HQ's internal network. Also, all LAN addresses, that belong to the work network (192.168.1.0/24), should now be leased to LAN devices by HQ router.

In order to check the guest WiFi, you simply need to connect to the newly created WiFi AP, then check whether you have internet connectivity and try to ping OpenVPN server LAN IP - if everything is set up correctly, you should not be able to do that.