https://wiki.teltonika-networks.com/view/Connecting_two_same_subnet_office_networks_using_OpenVPN_bridge_(TAP)_on_RUT2xx

Connecting two same subnet office networks using OpenVPN bridge (TAP) on RUT2xx

Contents

Configuration overview and prerequisites

Prerequisites:

- Two RUTxxx routers
- A Public Static or Public Dynamic IP addresses
- 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 (**RUT**) acts as the **OpenVPN server** and other **RUT** acts as **client**. OpenVPN connects the networks of **HQ Office** and **Remote Office**.

When the scheme is realized, remote office workers will be able to reach HQ's internal network with all internal systems, allowing working from remote office to be possible. All remote office's WAN and LAN traffic is going to travel through VPN tunnel.

Configuring HQ office router

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

Now go to **Services → VPN → OpenVPN**. There create a new configuration by selecting role **Server**, writing **New configuration name** and pressing **Add New** 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.

LAN

Go to **Network → LAN** and apply the following steps:
1. Change your **LAN IP address** to: **192.168.1.2**
2. Disable **DHCP**.
3. **Save** the changes.

OpenVPN

Configuring OpenVPN client

Go to **Services → 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**.

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** (RUT OpenVPN server public IP).
6. Add **Keep alive** interval: **10 120**.
7. Upload **Static pre-shared key**.
8. **Save** the changes.

Results

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