RutOS NordVPN configuration example

[Main Page](#) > [General Information](#) > [Configuration Examples](#) > [VPN](#) > **RutOS NordVPN configuration example**

☐
Contents

☒

Introduction

Virtual private networks (VPNs) are affordable, easy to use, and a vital component in your PC and smartphone set up. Along with a firewall and antivirus/anti-malware solution, you should have a VPN installed to keep every moment you spend online completely private. NordVPN is a personal virtual private network (VPN) service provider. It is supported on various different Teltonika Networks devices. This article contains step-by-step instructions on how to set up **NordVPN** VPN connection using RUTX routers.

Prerequisites

You will need:

- One Teltonika Networks router (RUTX11 routers will be used in this example)
- An end device to configure the router (PC, Laptop, Tablet, Smartphone)
- NordVPN account and subscription

Please bear in mind that from June 14th, 2023, you will no longer be able to use your NordVPN email/username and password to authenticate your connection, and you will need to set up service credentials manually on your Nord Account. More details about the changes to the login process can be found **[here](#)**.

Choosing and downloading server files

In order to set up your router to connect to NordVPN server you will need to download OVPN configuration files. Those can be found at [NordVPN website](#). It is necessary to choose a server which can provide the best possible performance, visit this [website](#) and it will automatically show you which server will provide you the best experience. Also when it comes to choosing TCP or UDP you need to decide what you are trying to achieve. TCP is reliable, data sent using this protocol is guaranteed to be delivered to the receiver. If data is lost in transit it will recover the data and resend it. TCP will also check packets for errors and track packets so that data is not lost or corrupted, but that effects internet speed. UDP is unreliable, it does not provide guaranteed delivery and a datagram packet may become corrupt or lost in transit, but you will get greater internet speed.

Home network configuration (RUTX)

Access RUTX WebUI and go to **Services > VPN > OpenVPN**. There create a new configuration by writing **New configuration name**, 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. **Enable OpenVPN config from file** feature.
3. Upload **OpenVPN configuration file** (the one you downloaded from [NordVPN website](#)).
4. Allow **Upload OpenVPN authentication files**.
5. Set **Authentication** to **Password**.
6. NordVPN service **username**.
7. NordVPN service **password**.
8. Press **Save & Apply**.

You will be forwarded back to **OpenVPN configuration** window. There you will find connection status indicator. If you applied the configuration correctly it should indicate as **connected**. (It might not connect instantly so please wait for a moment).

In order to increase your anonymity you will need to set your router to use custom DNS servers (in this example we used NordVPN DNS servers). In order to do that go to **Network > WAN**, there click **Edit** on a WAN source you are using (in this example we used mobile WAN source).

Now to set DNS servers follow the steps below:
1. Go to **Advanced settings**.
2. Disable **DNS servers advertised by peer**.
3. Add first DNS server: **103.86.96.100**.
4. Add second DNS server: **103.86.99.100**.
5. Press **Save & Apply**.

Results

If configured correctly all of your internet traffic now should go through VPN server. One of the easiest ways to check whether everything is working correctly is to check whether your public IP address has changed. You can do so by simply visiting a website such as www.whatismyipaddress.com and comparing your IP address before and after you connect to server also there you can find information about IP location, so when you connect to server it should change to a different address/country. Or you can visit [NordVPN website](#) and there on the very top of the website you can indicate whether you are protected or not.

External links

[NordVPN homepage](#)

Disclaimer:

Any of the trademarks, service marks, collective marks, design rights or similar rights that are mentioned, used or cited in the articles are the property of their respective owners.