WireGuard Configuration Example

□

Contents

Introduction

WireGuard is simple, fast, lean, and modern VPN that utilizes secure and trusted cryptography. This page will show you an example on how to configure a basic tunnel between WireGuard interface and its peers.

Note: WireGuard is additional software that can be installed from the **System → Package Manager** page.

Prerequisites

For this example you need:

1. Two RUTOS devices (this example will be written with RUTX09 and TRB141 in particular)
2. An end device to configure devices (PC, Laptop, Tablet or Smartphone)
3. One of the RUTOS devices must have **Public** IP address

End results

In the end there will be created a tunnel between RUTX09 and TRB141. RUTX09 will have 10.0.0.1 and TRB141 will have 10.0.0.2 tunnel IP addresses.

WireGuard Instances

To create Instance enter its name and click the **Add** button. Then click the **Edit** button to configure it.

In this example Instance is named by its device name to make it easier to follow images.

RUTX09 Example

TRB141 Example

Instance Configuration

The following part of example applies to both devices.

Before editing any fields click button to generate Public and Private keys.

After that you need to Enable this instance and in the **Listen Port** field enter your desired port. WireGuard by default uses **51820** port which will be used in this example.

Lastly you need to enter IP Address for instance. As mentioned in the beginning, RUTX09 will have 10.0.0.1 and TRB141 will have 10.0.0.2 IP addresses.

Note: enter IP address **and** its mask e.g. **10.0.0.1/24**

RUTX09 Example

Note: fields with numbers **1** and **2** will be used later when configuring remote peers.

TRB141 Example

Note: fields with numbers **3** and **4** will be used later when configuring remote peers.

Peers

Until now you have configured WireGuard instance itself, now you need to configure Peers which are

going to connect to those instances.

To create Peer enter its name and click the **Add** button. Then click the **Edit** button to configure it.

One Peer for each device will be created:

4. **RUTX09** will have a Peer named **trb1peer**
5. **TRB141** will have a Peer named **rutxpeer**

RUTX09 Example

TRB141 Example

Peers Configuration

General Setup

In the **General Setup** section you need to enter **Public Key** and **Allowed IPs** from the Remote instance you want to connect to.

In this example a peer from RUTX09 (named **trb1peer**) needs to connect to TRB141, which means **trb1peer** will enter Public Key and Allowed IPs from TRB141.

Note: the numbers in the images below represent a *number of field* from which that value was taken from the images in Instance Configuration.

RUTX09 Example

TRB141 Example

Advanced Setup

Lastly atleast one device has to enter Public IP address from Remote instance. Enter IP address, save and move to the Testing Configuration.

If in the Instance Configuration you specified port other than 51820 then you also need to specify it here.

Testing Configuration

To initiate connection and test it you need to open Command Line Interface (Services → CLI) and login. Then type

```
wg
```

If you see **latest handshake** line then it means you have established a connection between your devices and you are able to communicate via IP addresses specified in number **2** and **4** fields from the images in Instance Configuration.

If you dont see **latest handshake** line, then ping the **Public IP address** you specified in **Endpoint Host** field, this will initiate handshake.

```
ping XX.XX.XX.XX
```