

OpenWRT WireGuard Client Setup guide using Luci

Index

OpenWRT WireGuard Client Setup guide using Luci.....	1
Install WireGuard.....	1
Download configuration.....	1
Create WireGuard interface.....	4
Create WireGuard Peers section.....	5
Firewall.....	7

Install WireGuard

LuCi > System > Software: click *Update Lists*

Install: luci-proto-wireguard, wireguard-tools and wg-installer-client

Download configuration

Download a WireGuard configuration file from your provider or WireGuard server.

In this example we are going to download a WireGuard configuration file from Proton which is free but it will expire after a week or so:

Create an account on <https://protonvpn.com/>

Login

Go to Downloads and scroll to the bottom for the WireGuard configuration.

Give a name to your config and choose router for your Platform :

WireGuard configuration

These configurations are provided to work with WireGuard routers and official clients.

1. Give a name to the config to be generated

Device/certificate name ⓘ

wg_proton_nl

2. Select platform

☐ Android ☐ iOS ☐ Windows ☐ macOS ☐ GNU/Linux ☒ Router

3. Select VPN options

☐ NAT-PMP (Port Forwarding) [Learn more](#)

☒ VPN Accelerator [Learn more](#)

4. Select a server to connect to


Use the best server according to current load and position: **NL-FREE#70**


Create

Or select a particular server:

☐ Standard server configs ☒ Free server configs ☐ Secure Core configs

Scroll down to the server you want to connect to and Choose Create:

^  Netherlands

Name	Status	Action
NL-FREE#1	 63%	Create

Download the config file to your computer, the config file (wg_proton_nl-NL-FREE-1.conf) looks like this:

```
[Interface]
# Key for wg_proton_nl
# Bouncing = 3
# NAT-PMP (Port Forwarding) = off
# VPN Accelerator = on
PrivateKey = UJmovcwC7KQ/vfgnradTHoHD30WJ6SonkvXYg23ex0A=
Address = 10.2.0.2/32
DNS = 10.2.0.1
[Peer]
# NL-FREE#1
PublicKey = vH2i8RY1qc66XfqwrixBpvH4K9GYJatkugJj0GHgoUQ=
AllowedIPs = 0.0.0.0/0
Endpoint = 217.23.3.76:51820
```

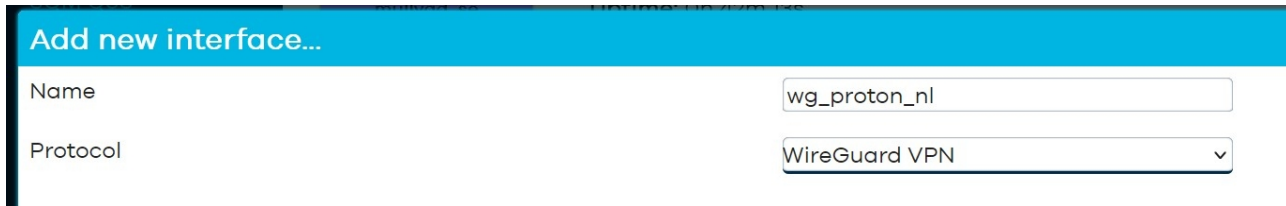
Add the `PersistentKeepAlive` so that the connection stays open:
PersistentKeepalive = 25 and if you use IPv6 add `::0/0` to allowed IPs:
AllowedIPs = 0.0.0.0/0, ::0/0

The result:

```
[Interface]
# Key for wg_proton_nl
# Bouncing = 3
# NAT-PMP (Port Forwarding) = off
# VPN Accelerator = on
PrivateKey = UJmovcwC7KQ/vfgnradTHoHD30WJ6SonkvXYg23ex0A=
Address = 10.2.0.2/32
DNS = 10.2.0.1
[Peer]
# NL-FREE#1
PublicKey = vH2i8RY1qc66XfqwrixBpvH4K9GYJatkugJj0GHgoUQ=
AllowedIPs = 0.0.0.0/0, ::0/0
Endpoint = 217.23.3.76:51820
PersistentKeepalive = 25
```

Create WireGuard interface

Network > Interfaces on the bottom **click:** *Add New interface*



Add new interface...

Name: wg_proton_nl

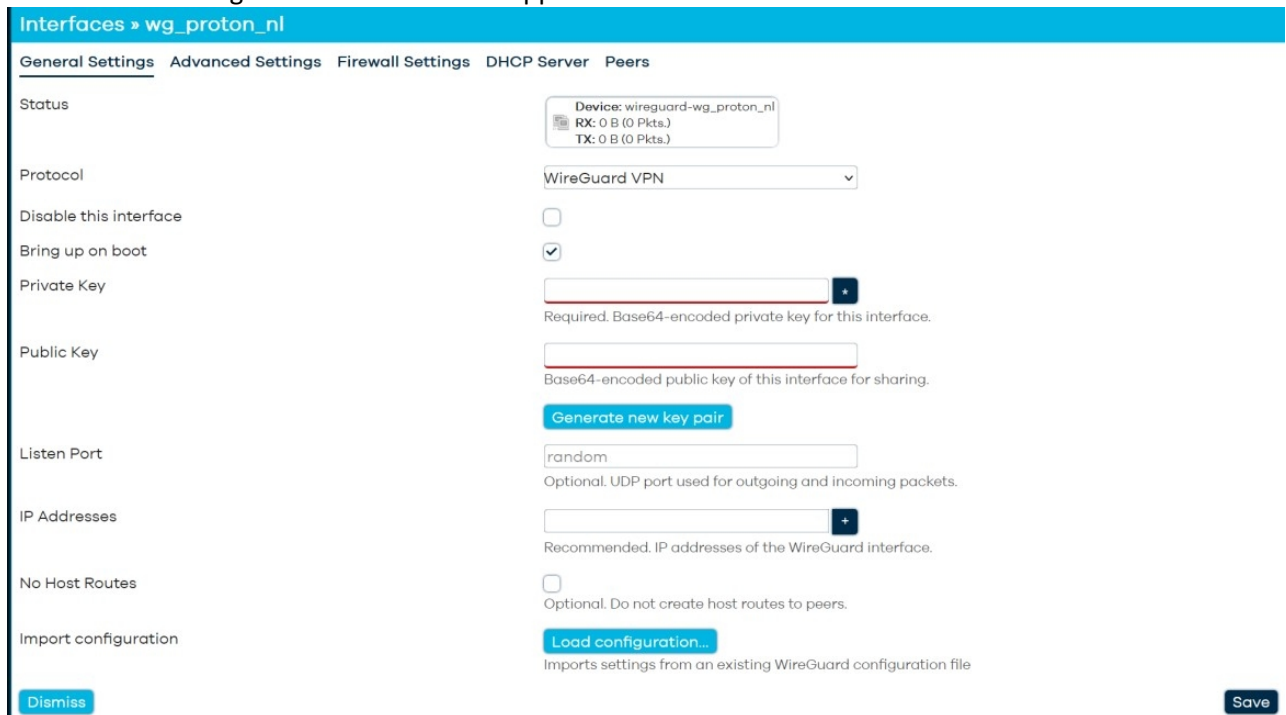
Protocol: WireGuard VPN

Name: give a descriptive name, hyphens are not allowed and the name has to be less than 15 characters!

Protocol: *WireGuard VPN*

Click: *Create interface*

The Interface configuration screen should appear:



Interfaces > wg_proton_nl

General Settings | Advanced Settings | Firewall Settings | DHCP Server | Peers

Status: Device: wireguard-wg_proton_nl
RX: 0 B (0 Pkts.)
TX: 0 B (0 Pkts.)

Protocol: WireGuard VPN

Disable this interface: ☐

Bring up on boot: ☒

Private Key: +
Required. Base64-encoded private key for this interface.

Public Key:
Base64-encoded public key of this interface for sharing.

Generate new key pair

Listen Port: random
Optional. UDP port used for outgoing and incoming packets.

IP Addresses: +
Recommended. IP addresses of the WireGuard interface.

No Host Routes: ☐
Optional. Do not create host routes to peers.

Import configuration: Load configuration...
Imports settings from an existing WireGuard configuration file

Dismiss Save

As the *wg-installer-client* is installed we can import our configuration file by clicking the button *Load configuration*

Click: Load configuration
Drop the configuration file from the file manager into this box and automagically the settings should appear into the Interfaces configuration:

Interfaces » wg_proton_nl

General Settings

Advanced Settings

Firewall Settings

DHCP Server

Peers

Status

Device: wireguard-wg_proton_nl
RX: 0 B (0 Pkts.)
TX: 0 B (0 Pkts.)

Protocol

WireGuard VPN

Disable this interface

☐

Bring up on boot

☒

Private Key

.....*

Required. Base64-encoded private key for this interface.

Public Key

1rMnp6/8iXg4uMdFNgkzWrSgLbI4uSqa6

Base64-encoded public key of this interface for sharing.

Generate new key pair

Listen Port

random

Optional. UDP port used for outgoing and incoming packets.

IP Addresses

10.2.0.2/32

-

+

Create WireGuard Peers section

Network > Interfaces > wg_proton_nl : **click edit**
Go to *Peers* section:

Interfaces » wg_proton_nl

General Settings

Advanced Settings

Firewall Settings

DHCP Server

Peers

Further information about WireGuard interfaces and peers at wireguard.com.

Disabled	Description	Allowed IPs	Endpoint Host
<input type="checkbox"/>	<div>wg_proton_nl-NL-FREE-1.conf</div> <div>vH2i8_HgoUQ=</div>	<div>0.0.0.0/0</div> <div>:::0/0</div>	217.23.3.76:51820

Add peer

Import configuration as peer...

Dismiss

Click: *Edit* and the Peers section will open:
Interfaces » wg_proton_nl » Edit peer

Disabled	<input type="checkbox"/>	Enable / Disable peer. Restart wireguard interface to apply changes.
Description	<input type="text" value="wg_proton_nl-NL-FREE-1.conf"/>	Optional. Description of peer.
Public Key	<input type="text" value="vH2i8RY1qc66XfqwrixBpvH4K9GYJatkug"/>	Required. Public key of the WireGuard peer.
Private Key	<input type="text"/> *	Optional. Private key of the WireGuard peer. The key is not required if you allow generating a peer configuration or QR code if available. It can also be exported.
	<button>Generate new key pair</button>	
Preshared Key	<input type="text"/> *	Optional. Base64-encoded preshared key. Adds in an additional layer of post-quantum resistance.
	<button>Generate preshared key</button>	
Allowed IPs	<div><input type="text" value="0.0.0.0/0"/> -</div> <div><input "::0="" 0"="" type="text" value=""/> -</div> <div><input type="text"/> +</div>	Optional. IP addresses and prefixes that this peer is allowed to use to tunnel IP addresses and the networks the peer routes through the interface.
Route Allowed IPs	<input type="checkbox"/>	Optional. Create routes for Allowed IPs for this peer.
Endpoint Host	<input type="text" value="217.23.3.76"/>	Optional. Host of peer. Names are resolved prior to bringing up the peer.
Endpoint Port	<input type="text" value="51820"/>	Optional. Port of peer.
Persistent Keep Alive	<input type="text" value="25"/>	Optional. Seconds between keep alive messages. Default is 0 (disabled) if behind a NAT is 25.

Now the most important part which is often overlooked:
Route Allowed IPs: *Enable (tick)*


Route Allowed IPs	<input checked="" type="checkbox"/>	Optional. Create routes for Allowed IPs for this peer.
-------------------	-------------------------------------	--

Click: *Save*

In the next window **Click: *Save again***

In the Interface window click ***Save & Apply***

After a few moments the interface appears and should be up and traffic should flow, both Tx and RX indicating the setup is correct:

<div><div>wg_proton_nl</div><div></div><div>wg_proton_nl</div></div>	Protocol: WireGuard VPN Uptime: 0h 1m 37s RX: 300 B (5 Pkts.) TX: 8.87 KB (30 Pkts.) IPv4: 10.2.0.2/32
---	---

However this is depending on your default firewall setting with OUTPUT Accept, if not there will not be traffic yet.
Next up Firewall

Firewall

Easiest method is to just add the `wg_proton_nl` interface to the WAN zone

Network > Firewall > WAN zone > **Click: edit:**

Firewall - Zone Settings

General Settings

Advanced Settings

Conntrack Settings

This section defines common properties of "wan". The *input* and *output* options set the default policies for traffic entering and leaving the zone. *Covered networks* specifies which available networks are covered by this zone.

Name	wan
Input	reject
Output	accept
Intra zone forward	reject
Masquerading	<input checked="" type="checkbox"/> Enable network address and port translation IPv4 typically enabled on the <i>wan</i> zone.
MSS clamping	<input checked="" type="checkbox"/>
Covered networks	wan: wan6:

Covered Networks: add `wg_proton_nl`

Covered networks

wan: wan6: wg_proton_nl:

Click: *Save* and click *Save & Apply*

This should give you a working WireGuard Client

Check from the routers console with `curl ipinfo.io` and/or from your LAN clients with `ipleak.net`