

OpenWRT Installing WireGuard client with Luci

Install WireGuard:

LuCi > System > Software: click `Update Lists`

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

Download a WireGuard configuration file from your provider or WireGuard server

In this example I will download a WireGuard configuration file from Proton which is free but it will expire after a week.

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 = vH2i8RY1qc66XfqwrrixBpvH4K9GYJatkugJj0GHgoUQ=
AllowedIPs = 0.0.0.0/0
Endpoint = 217.23.3.76:51820
...
```

We are going to 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`
```

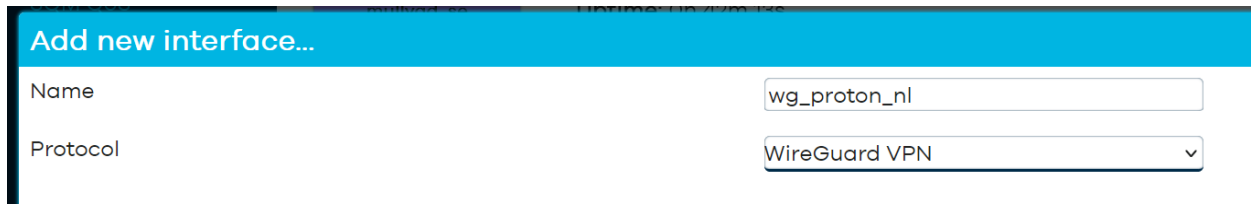
So in the end we have:

...

```
[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 = vH2i8RY1qc66XfqwrrixBpvH4K9GYJatkugJj0GHgoUQ=
AllowedIPs = 0.0.0.0/0, ::0/0
Endpoint = 217.23.3.76:51820
PersistentKeepalive = 25
...
```

Next up we are going to create the WireGuard Interface:
Network > Interfaces on the bottom click: `Add New interface`

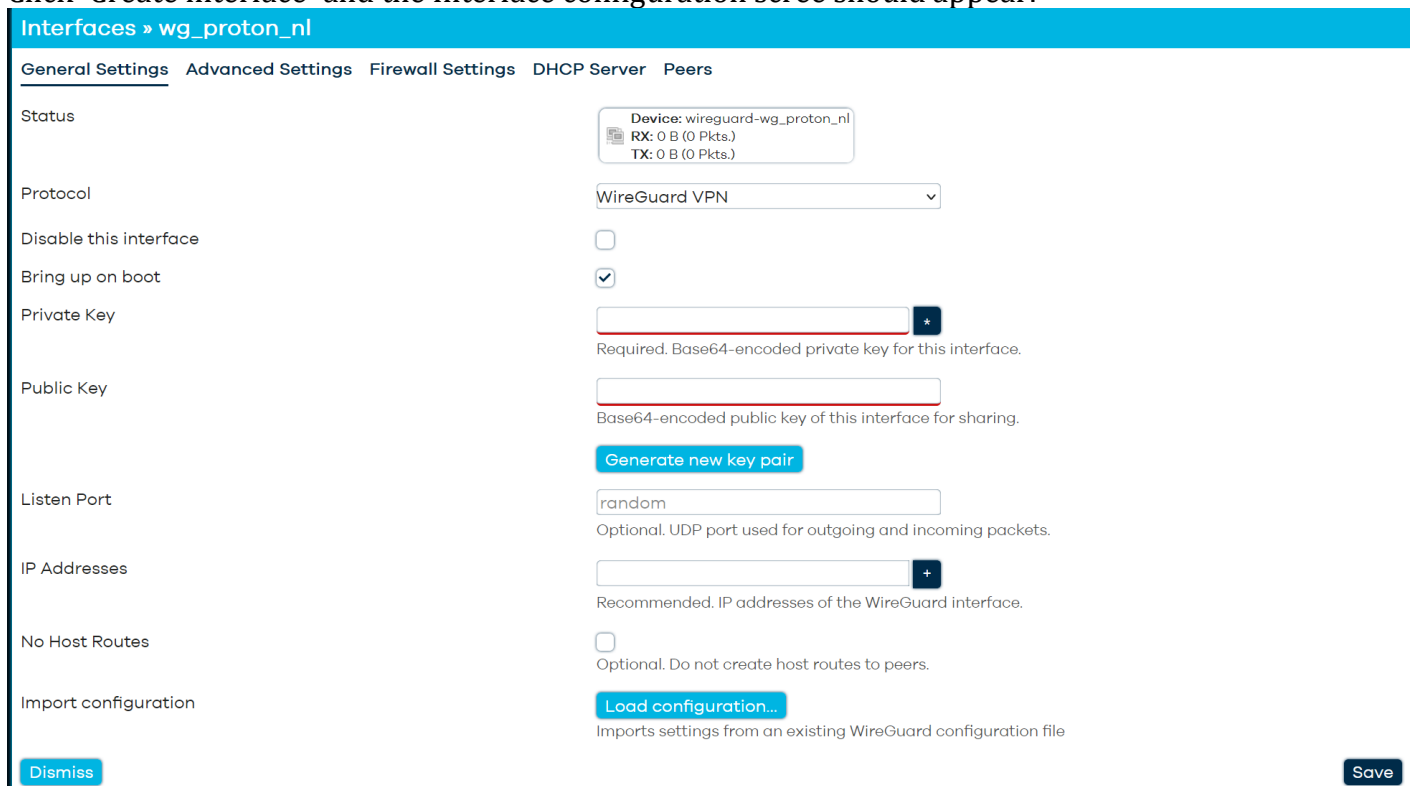


The screenshot shows a form titled "Add new interface...". It has two input fields: "Name" with the value "wg_proton_nl" and "Protocol" with a dropdown menu showing "WireGuard VPN".

Give the interface a name (hyphens are not allowed and the name has to be below 15 chracters!)

Choose as Protocol `WireGuard VPN`

Click `Create interface` and the Interface configuration scree should appear:



The screenshot shows the "Interfaces » wg_proton_nl" configuration page. It has a sidebar with tabs: "General Settings", "Advanced Settings", "Firewall Settings", "DHCP Server", and "Peers". The "General Settings" tab is active. The main content area has the following fields and options:

- Status: Device: wireguard-wg_proton_nl, RX: 0 B (0 Pkts.), TX: 0 B (0 Pkts.)
- Protocol: WireGuard VPN (dropdown)
- 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: [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)

At the bottom, there are "Dismiss" and "Save" buttons.

As we have installed the `wg-installer-client` we can Import our configuration file by clicking the button `Load configuration`

After clicking the button `Load configuration` we get a box to drop our configuration file from the file manager into this box and automagically the settings should appear into our `Interface 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

1rMnp6/8iXg4uMdFNgkzWrSgLbl4uSqa6

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

+

Next up is configuring the `Peers` section, click on `Peers` in the menu

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	<div>⋮</div> <div>Edit</div>
<div>Add peer</div> <div>Import configuration as peer...</div>				
<div>Dismiss</div>				

Click on the `Edit` button:

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 generating a peer configuration or QR code is available. It can be exported.
	<input type="button" value="Generate new key pair"/>	
Preshared Key	<input type="text"/> 	Optional. Base64-encoded preshared key. Adds in an additional layer of post-quantum resistance.
	<input type="button" value="Generate preshared key"/>	
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 interface.
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:

Tick/Enable `Route Allowed IPs`:

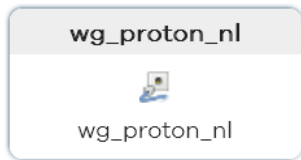
Route Allowed IPs	<input checked="" type="checkbox"/>	Optional. Create routes for Allowed IPs for this peer.
-------------------	-------------------------------------	--

Click `Save`

In the next window click `Save` again

In the Interface window click `Save & Apply`

After a few moments we can see that the interface is up and traffic is flowing both Tx and RX indicating the setup is correct:



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 no be traffic yet.

Next up Firewall

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

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 the 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: wg_proton_nl:

Under Covered Networks add wg_proton_nl:

Covered networks



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`