OpenWRT WireGuard Server Setup guide using LuCi

Introduction

WireGuard is an open-source VPN solution written in C by Jason Donenfeld and others, aiming to fix many of the problems that have plagued other modern server-to-server VPN offerings like IPSec/IKEv2, OpenVPN, or L2TP.
It many ways it can be seen as a replacement for OpenVPN.
It has three advantages over OpenVPN, it is much faster especially on lower-spec hardware such as Soho routers (my own R7800 goes from 85 Mb/s on OpenVPN to 300 Mb/s with WireGuard), it is easy to setup if you know how, the guides will help you with that and it has a very small code base (about 4000 lines) so that it can easily be reviewed and checked for vulnerabilities.

Some key points about WireGuard:

- Layer 3 only no bridging
- UDP only punches through firewall
- Like SSH authenticated keys
- Executes in Linux Kernel
- Static routing

This is guide is to setup WireGuard as a server.
A server is the WireGuard interface listening for incoming connections e.g. from your phone/laptop from outside.
A client setup is making an outbound connection to a WireGuard server.
But as WireGuard basically is a point-to-point connection it can be both "client" and "server" at the same time, and if you have this setup between two routers we are talking about a site-to-site setup

This guide is based upon OpenWRT 24.10 but also should work on 23.05 and Main builds and uses LuCi to set things up but the resulting config files are also listed.

General Remarks

The most important parts of WireGuard are the public/private keys and the Allowed IP.

The public key is distributed to the peers.
The Allowed IP serves two roles, the first is that the allowed IP is used to know which of the peers public keys (if there is more than one peer) should be used to encrypt the packets.
Therefore the Allowed IP's must be unique for each peer!
The second one is security, if WireGuard detects a source IP which is not in the Allowed IP's the packets are discarded.
The keys are 32 bytes long and can be easily represented in Base64 encoding in 44 *characters the last character is always an =.*

As WireGuard is a routed solution all three involved subnets have to be different. So the Servers subnet, the WG subnet and the Clients subnet all have to be different!
As you often cannot choose the subnet of the client it is best to avoid using frequently used subnet for your routers IP address of e.g. 192.168.1.1/24 or 192.168.0.1/24

Furthermore proper testing can only be done from outside e.g. with your phone or laptop on cellular data or from a friends/neighbors internet.

Index

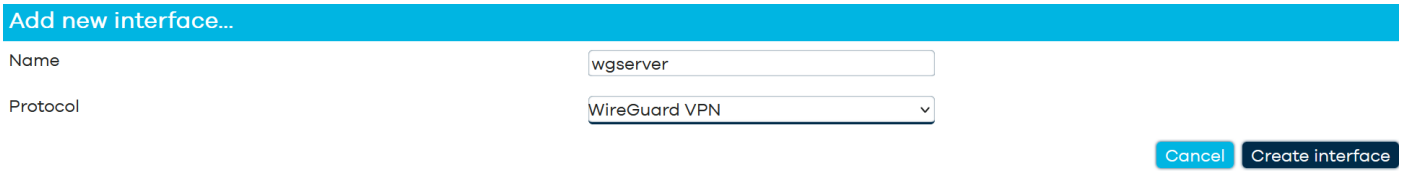
Server setup

Installation

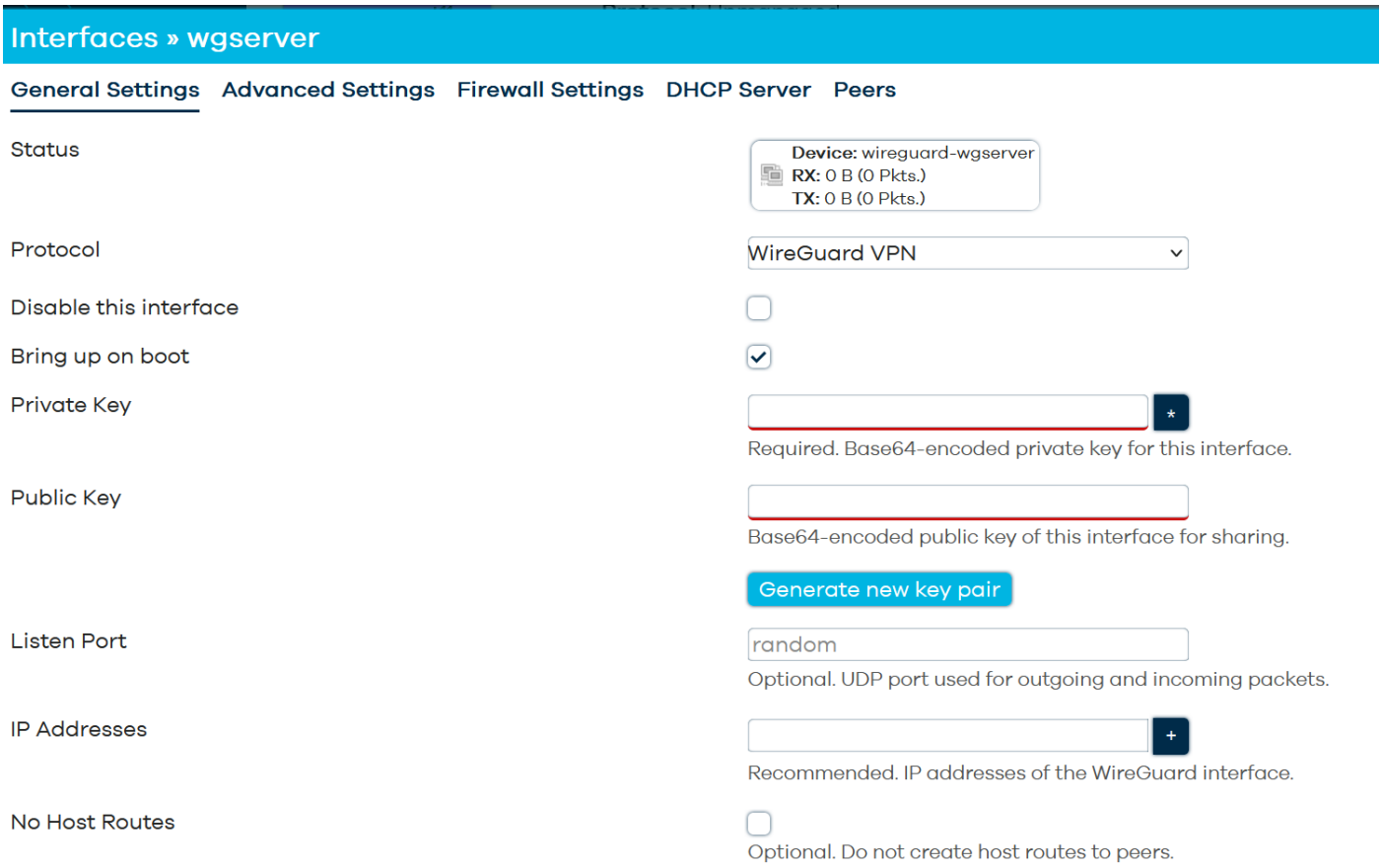
Install WireGuard:
LuCi > System > Software: click `*Update Lists*` to get the latest packages for your build
Install: `*luci-proto-wireguard*`, `*wireguard-tools*` and `*wg-installer-client*` (only necessary if you later want to install a client)

Create WireGuard Interface

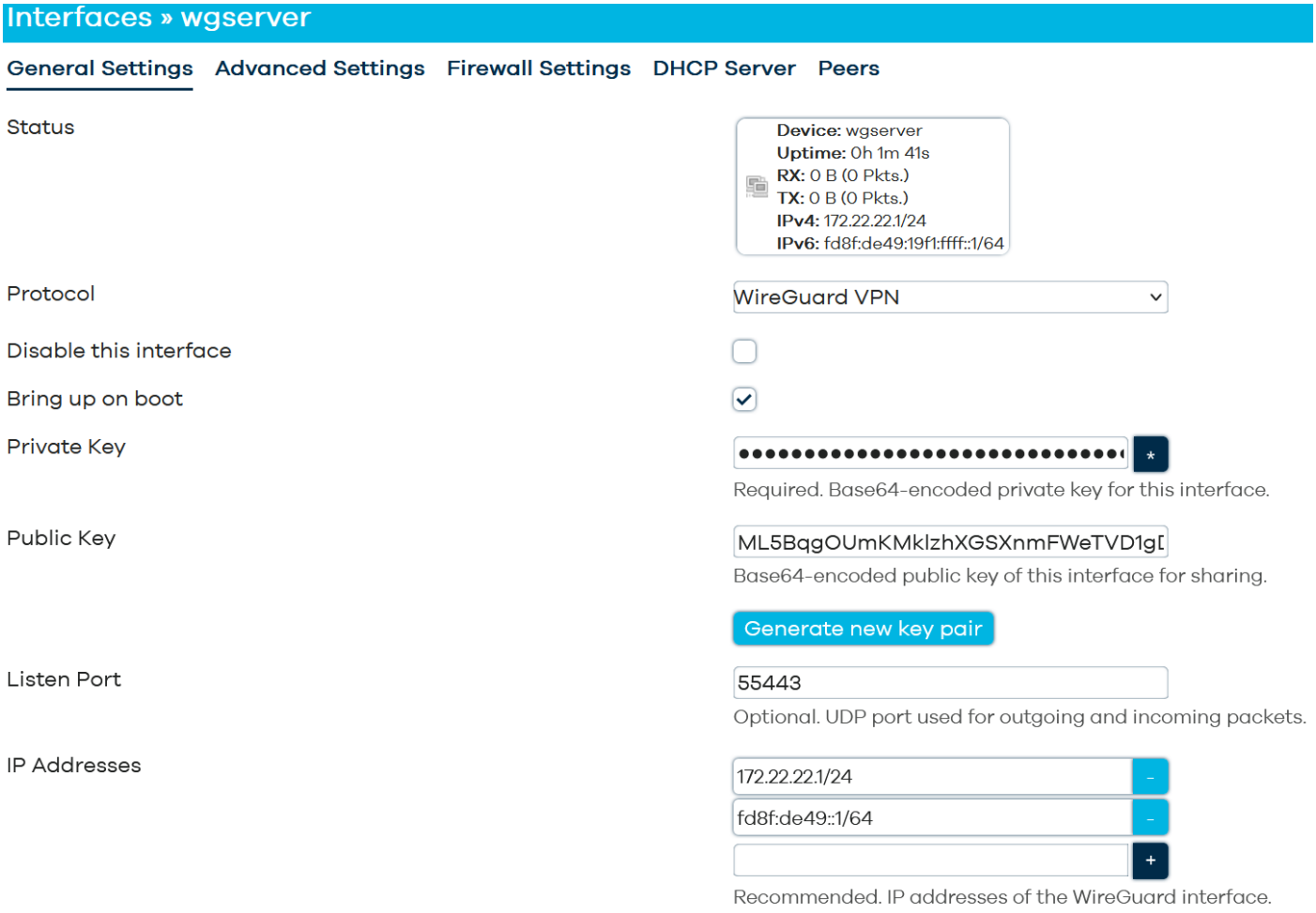
Next up we are going to create the WireGuard Interface:
Network > Interfaces on the bottom click: `Add New interface`



Name: give the interface a name (hyphens are not allowed and the name has to be below 15 characters!)
Protocol: *WireGuard VPN*
Click: *Create interface* and the Interface configuration screen should appear:



Click: *Generate new key pair*
Listen port: *55443* , you can use any port with is not already taken.
IP Addresses: *172.22.22.1/24*, if you also want IPv6 use a ULA address e.g.: *fd8f:de49::1/64*, you can use an ULA calculator if you want



Save and then Save & Apply

/etc/config/network:

```
config interface 'wgserver'
        option proto 'wireguard'
        option private_key 'MIShxrFJZqAQ4UG/pql2Y+xgs+QP5FyAl57s3M7lhW0='
        option listen_port '55443'
        list addresses '172.22.22.1/24'
        list addresses 'fd8f:de49::1/64'
```

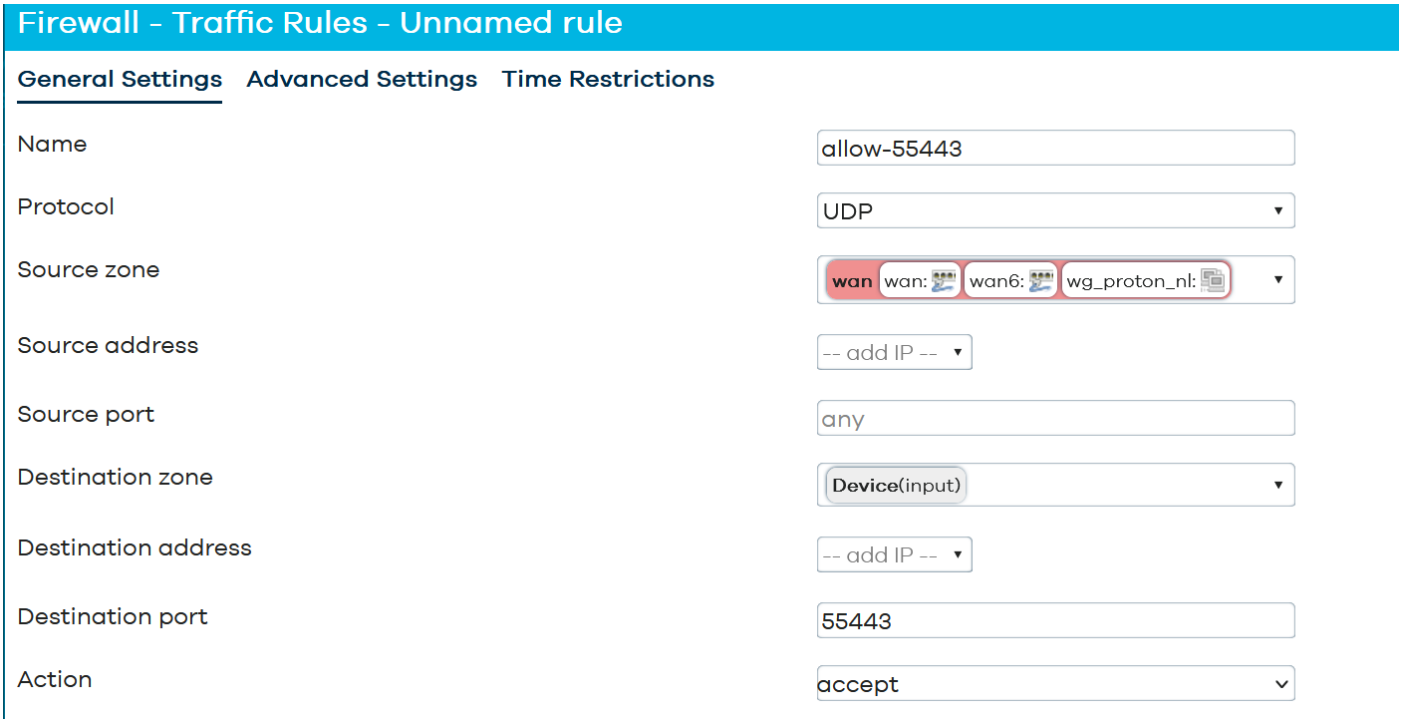
Firewall Setup

The firewall setup consist of three things:
1. Opening up the port (55443 in this example) with a traffic rule
2. Allowing traffic for the wgserver the interface

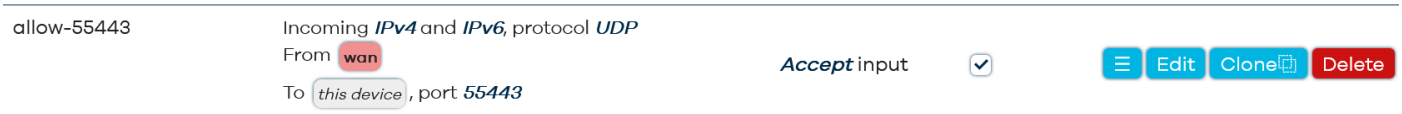
1. Opening up the port (55443 in this example) with a traffic rule

Network > Firewall > Traffic Rules
Add new traffic rule
Name: *allow-55443*
Protocol: *UDP*, click drop down button and disable TCP
Source zone: *WAN*
Destination zone: *Device (input)*
Destination port: *55443* , the port the wgserver interface listens on

The traffic rule will by default applies to IPv4 and IPv6, you can restrict the rule to IPv4 on the Advanced Tab



Save the rule and the result looks like this:



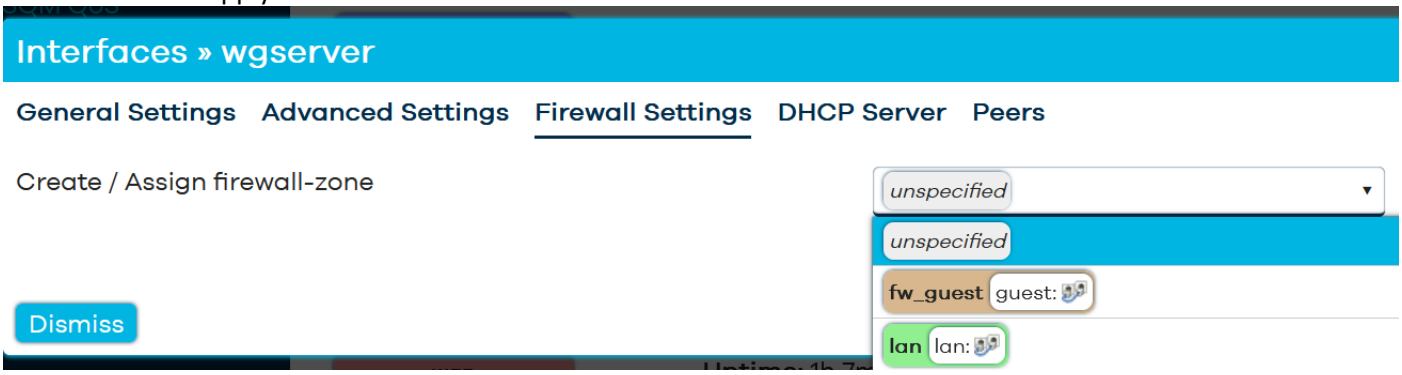
/etc/config/firewall:

```
config rule
        option name 'allow-55443'
        list proto 'udp'
        option src 'wan'
        option dest_port '55443'
        option target 'ACCEPT'
```

2. Allowing traffic for the wgserver's the interface

The easiest method is to edit the wg server interface.
Network > Interfaces and click the *edit* button on the *wgserver interface*

Go to Firewall settings:
Click on the drop down button and click on lan, this will add the wgserver interface to the lan zone
Save and Save & Apply



/etc/config/firewall:

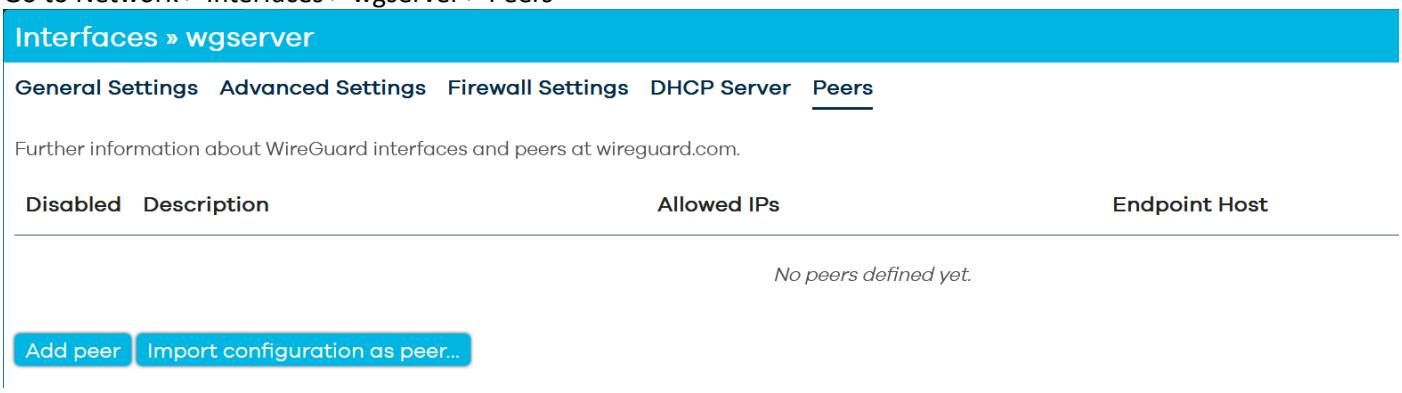
```
config zone
        option name 'lan'
        option input 'ACCEPT'
        option output 'ACCEPT'
        option forward 'ACCEPT'
        list network 'lan'
        list network 'wgserver'
```

Peer Setup

Next we are going to setup the peers for our server.
These are the clients which connects from outside our home to our wgserver.
There are WireGuard clients for almost operating systems.

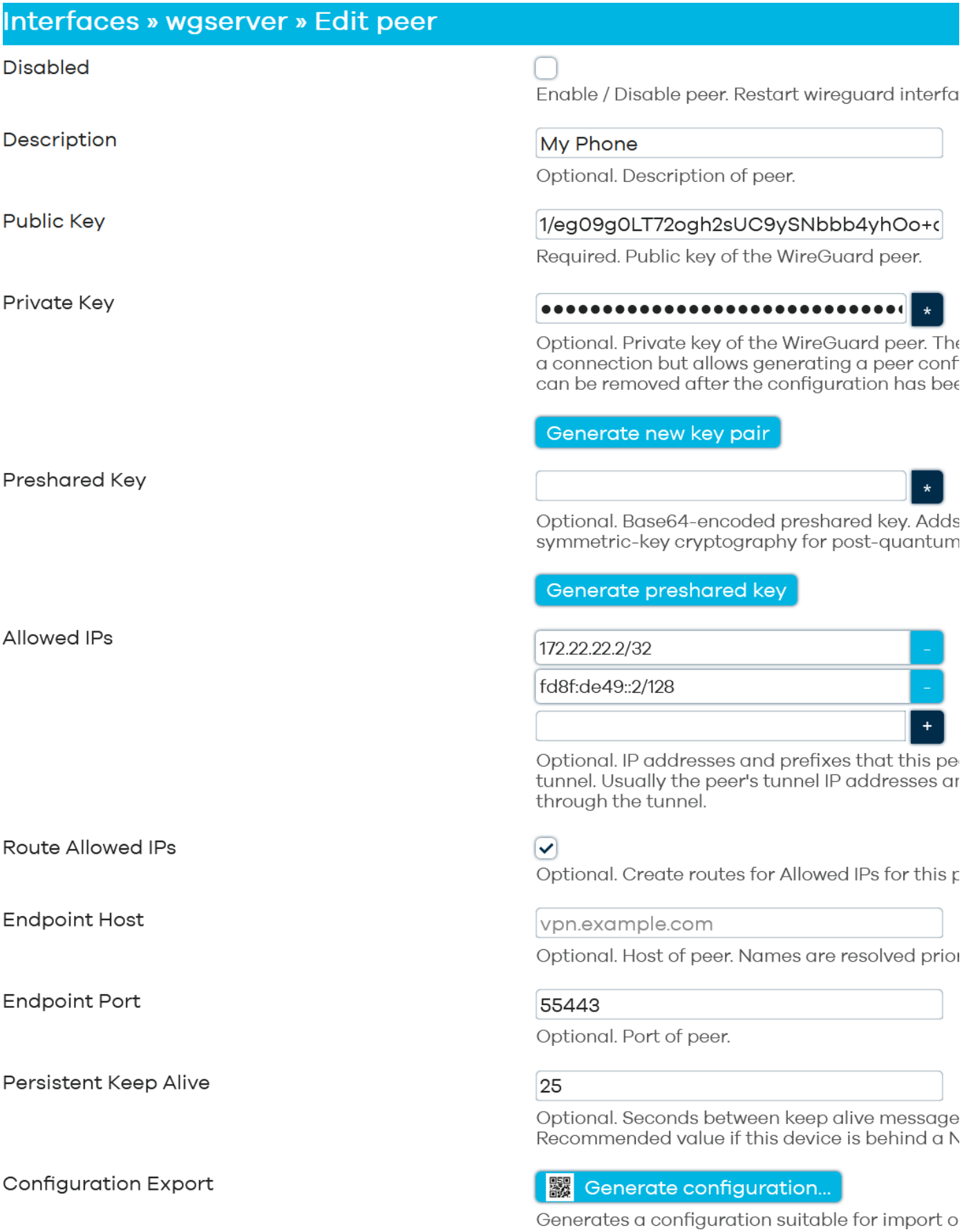
We are going to setup one Peer but you can of course add as many as you want, note that you can reuse this one peer for multiple clients but you can only connect one at a time!

Go to Network > Interfaces > wgserver > Peers



Click: *Add Peer*
Description: give a name for your Peer
Click *Generate new key pair*, the keys for the peer will be filled in.
Allowed IPs: *172.22.22.2/32*, the wgserver has this address 172.22.22.1/24, all peers should have an address in this subnet so for this peer use 172.22.22.2/32, note the /32 mask. Subsequent peers will use .3/32 etc.
For IPv6 you add: *fd8f:de49::2/128*, note the /128 mask
Route Allowed IPs: *Enable*, Always enable this
Endpoint host: Leave blank

Endpoint port: *554433*, this is the listening port of the wgserver, only used to make your config
Persistent keep alive: *25*, most clients are behind NAT so to keep the connection open use persistent keep alive, only used to make your config

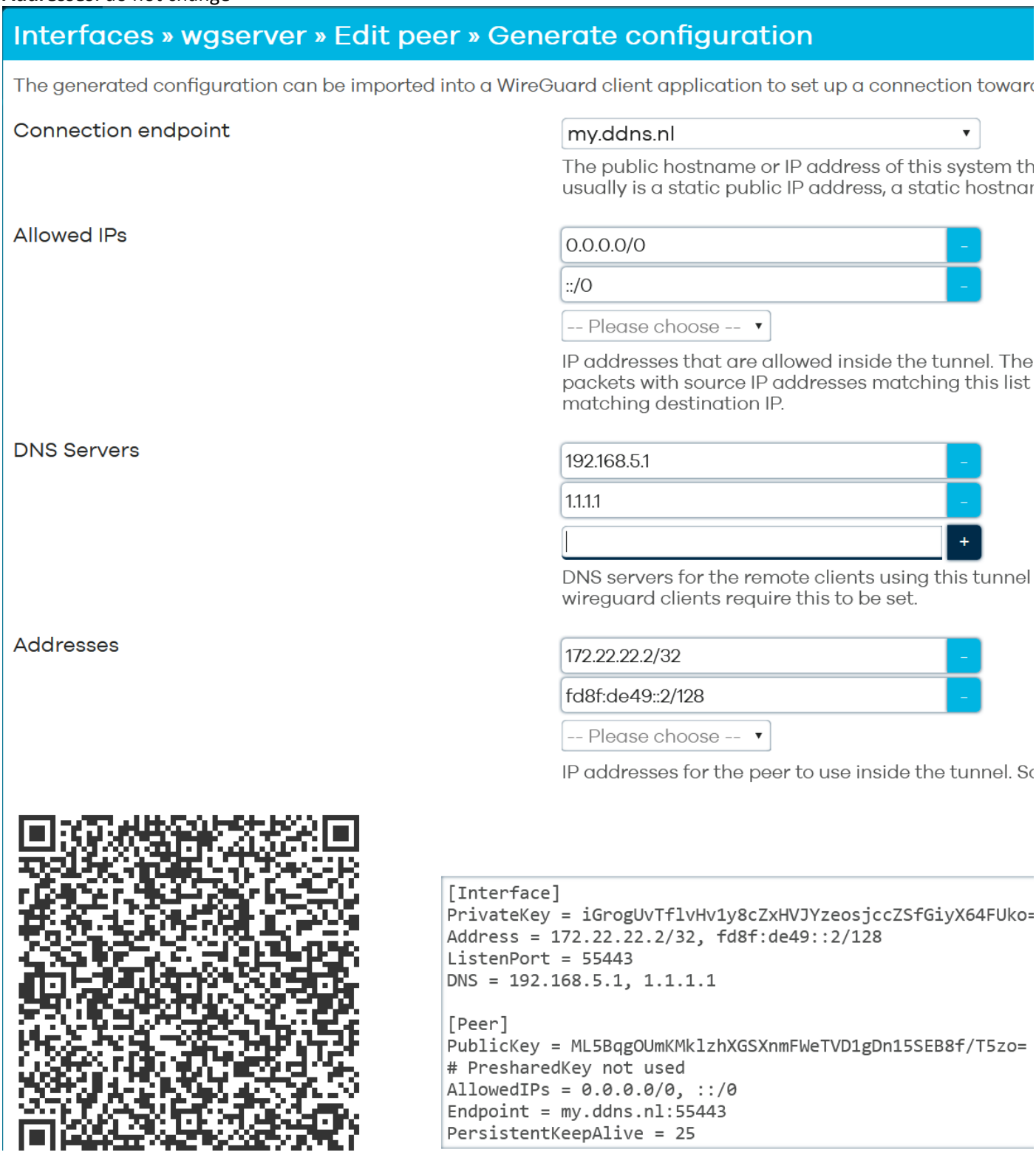


Save

Open the peer again by clicking on *Edit*.

Click: *Generate configurations*

Connection Endpoint: this is the WAN IP address or DDNS address your wgserver listens on
Allowed IPs: standard 0.0.0.0/0, ::/0, which means all traffic from your wg client will use the tunnel
DNS server: standard your routers IP address, not all clients can deal with this and you router might not listen on the wgserver interface so to be sure that you have got DNS resolution use 1.1.1.1
Addresses: do not change




```
[Interface]
PrivateKey = iGrogUvTflvHv1y8cZxHVJYzeosjccZSfGiyX64FUko=
Address = 172.22.22.2/32, fd8f:de49::2/128
ListenPort = 55443
DNS = 192.168.5.1, 1.1.1.1

[Peer]
PublicKey = ML5BqgOUmKMklzhXGSXnmFWeTVD1gDn15SEB8f/T5zo=
# PresharedKey not used
AllowedIPs = 0.0.0.0/0, ::/0
Endpoint = my.ddns.nl:55443
PersistentKeepAlive = 25
```

/etc/config/network:

```
config wireguard_wgserver
        option description 'My Phone'
        option public_key '1/eg09g0LT72ogh2sUC9ySNbbb4yhOo+q7kmDaAv1gM='
        option private_key 'iGrogUvTflvHv1y8cZxHVJYzeosjccZSfGiyX64FUko='
        list allowed_ips '172.22.22.2/32'
        list allowed_ips 'fd8f:de49::2/128'
        option route_allowed_ips '1'
        option endpoint_port '55443'
        option persistent_keepalive '25'
```

Setup WireGuard on your Client

Setup WireGuard on your client (phone/laptop etc) by downloading the WireGuard app via play store or apple store. You can import the settings with the QR code.
Otherwise copy the text and paste in a file, name it *peer-172.22.22.2.conf* which can be used to import in your wg client

Finish by Saving and Applying everything and do a reboot!

Now see if you can connect from outside e.g. with your phone or laptop on cellular.

Note that your LAN clients will not always allow traffic from a foreign subnet, in that case you have to tweak the firewall of said lan clients to allow traffic from 172.22.22.0/24 (the wg servers subnet), or masquerade this traffic

References