

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/neighbours internet.

Index

| | |
|---|---|
| Introduction..... | 1 |
| General Remarks..... | 1 |
| Server setup..... | 3 |
| Installation..... | 3 |
| Create WireGuard Interface..... | 3 |
| Firewall Setup..... | 5 |
| 1. Opening up the port (55443 in this example) with a traffic rule..... | 5 |
| 2. Allowing traffic for the wgserver the interface..... | 6 |
| Peer Setup..... | 6 |
| References..... | 9 |

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`

Add new interface...

| | |
|----------|--|
| Name | <input type="text" value="wgserver"/> |
| Protocol | <input type="text" value="WireGuard VPN"/> |

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

Choose as Protocol `WireGuard VPN`

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

Interfaces » wgserver

General Settings Advanced Settings Firewall Settings DHCP Server Peers

| | |
|------------------------|--|
| Status | <div>Device: wireguard-wgserver RX: 0 B (0 Pkts.) TX: 0 B (0 Pkts.)</div> |
| Protocol | <input type="text" value="WireGuard VPN"/> |
| Disable this interface | <input type="checkbox"/> |
| Bring up on boot | <input checked="" type="checkbox"/> |
| Private Key | <input type="text"/> Required. Base64-encoded private key for this interface. |
| Public Key | <input type="text"/> Base64-encoded public key of this interface for sharing. <input type="button" value="Generate new key pair"/> |
| Listen Port | <input type="text" value="random"/> Optional. UDP port used for outgoing and incoming packets. |
| IP Addresses | <input type="text"/> Recommended. IP addresses of the WireGuard interface. |
| No Host Routes | <input type="checkbox"/> Optional. Do not create host routes to peers. |

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

General Settings

Advanced Settings

Firewall Settings

DHCP Server

Peers

Status

Device: wgserver

Uptime: 0h 1m 41s

RX: 0 B (0 Pkts.)

TX: 0 B (0 Pkts.)

IPv4: 172.22.22.1/24

IPv6: fd8f:de49:19f1:ffff::1/64

Protocol

WireGuard VPN

Disable this interface

☐

Bring up on boot

☒

Private Key

.....*

Required. Base64-encoded private key for this interface.

Public Key

ML5BqgOUmKMklzhXGSXnmFWeTVD1gI

Base64-encoded public key of this interface for sharing.

Generate new key pair

Listen Port

55443

Optional. UDP port used for outgoing and incoming packets.

IP Addresses

172.22.22.1/24-

fd8f:de49::1/64-

+

Recommended. IP addresses of the WireGuard interface.

Save and then Save & Apply

wgserver



wgserver

Protocol: WireGuard VPN

Uptime: 0h 2m 41s

RX: 0 B (0 Pkts.)

TX: 0 B (0 Pkts.)

IPv4: 172.22.22.1/24

IPv6: fd8f:de49:19f1:ffff::1/64

Restart

Stop

Edit

Delete

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-55442

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

Firewall - Traffic Rules - Unnamed rule

General Settings Advanced Settings Time Restrictions

| | |
|---------------------|------------------------------|
| Name | allow-55443 |
| Protocol | UDP |
| Source zone | wan wan: wan6: wg_proton_nl: |
| Source address | -- add IP -- |
| Source port | any |
| Destination zone | Device(input) |
| Destination address | -- add IP -- |
| Destination port | 55443 |
| Action | accept |

Save the rule and the result looks like this:

| | | | |
|-------------|--|--------------|-------------------------------------|
| allow-55443 | Incoming <i>IPv4</i> and <i>IPv6</i> , protocol <i>UDP</i> | | |
| | From wan | Accept input | <input checked="" type="checkbox"/> |
| | To this device , port 55443 | | <div>Edit Clone Delete</div> |

2. Allowing traffic for the wgserver the interface

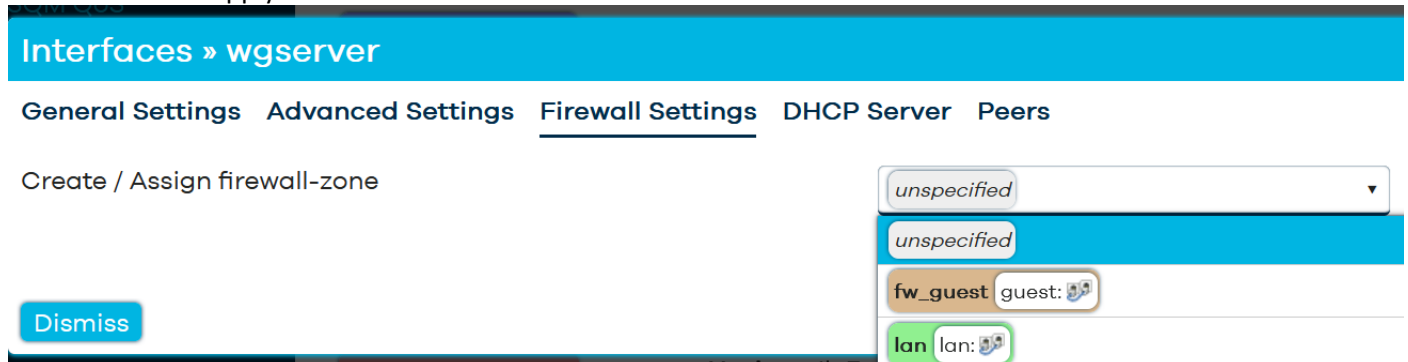
The easiest method is to edit the wg server interface.

Network > Interfaces and click the edit button on the wgserver interface

Goto 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



Peer Setup

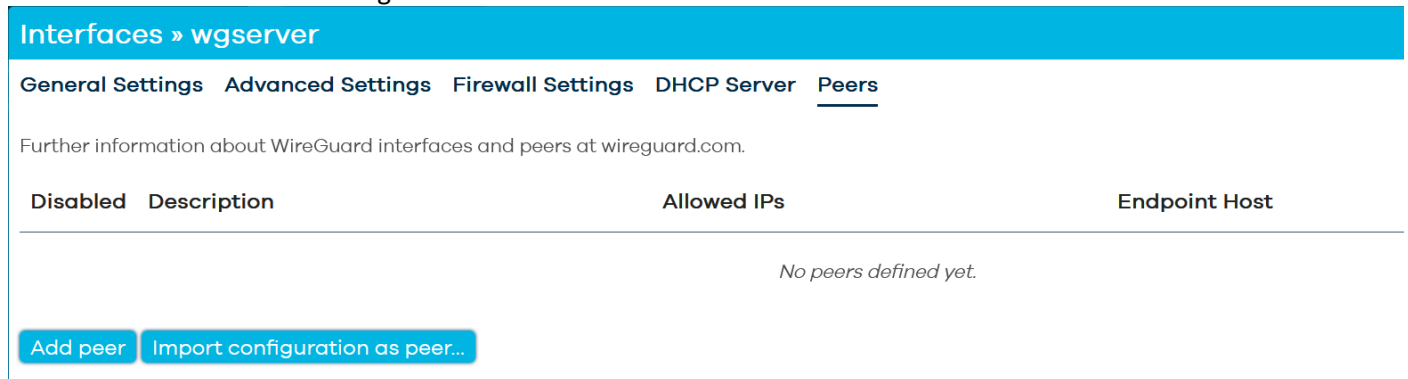
Next we are going to setup the peers for our server.

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



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.

Route Allowed IPs: Enable, Always enable this

Endpoint host: Leave blank

Endpoint port: 554433, this is the listening port of the wgserver

Persistent keep alive: 25, most clients are behind NAT so to keep the connection open use persistent keep alive

Interfaces » wgserver » Edit peer

Disabled

☐

Enable / Disable peer. Restart wireguard interface to apply changes.

Description

My Phone

Optional. Description of peer.

Public Key

t+VWHP9T7as9/woFpKJldEEP/fftnKt9DE

Required. Public key of the WireGuard peer.

Private Key

.....*

Optional. Private key of the WireGuard peer. The key is not required for es allows generating a peer configuration or QR code if available. It can be r has been exported.

Generate new key pair

Preshared Key

.....*

Optional. Base64-encoded preshared key. Adds in an additional layer of : post-quantum resistance.

Generate preshared key

Allowed IPs

172.22.22.2/32

.....+

Optional. IP addresses and prefixes that this peer is allowed to use inside tunnel IP addresses and the networks the peer routes through the tunnel.

Route Allowed IPs

☒

Optional. Create routes for Allowed IPs for this peer.

Endpoint Host

vpn.example.com

Optional. Host of peer. Names are resolved prior to bringing up the interf

Endpoint Port

55443

Optional. Port of peer.

Persistent Keep Alive

25

Optional. Seconds between keep alive messages. Default is 0 (disabled). f is behind a NAT is 25.

Configuration Export

Generate configuration...

Generates a configuration suitable for import on a WireGuard peer

Save

Open the peer again by clicking on Edit.

Click Generate configuration

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 your router might not listen on the wgserver interface so to be sure that you have got DNS resolution use 1.1.1.1

Address: do not change

Interfaces » wgserver » Edit peer » Generate configuration

The generated configuration can be imported into a WireGuard client application to set up a connection towards this device.

Connection endpoint

192.168.0.5

The public hostname or IP address of this system. It can be a public IP address, a static hostname or a DDNS domain.

Allowed IPs

0.0.0.0/0

::/0

-- Please choose --

IP addresses that are allowed inside the tunnel. The addresses matching this list will route back to the peer.

DNS Servers

192.168.5.1

DNS servers for the remote clients using this tunnel. This can be set to a list of DNS servers.

Addresses

172.22.22.2/32

-- Please choose --

IP addresses for the peer to use inside the tunnel. These addresses will be routed to the peer.



```
[Interface]
PrivateKey = kM0R4CKnMNx18mOWsfZQQ1t7xa0+e8XhLxeiI+AnVVM=
Address = 172.22.22.2/32
ListenPort = 55443
DNS = 192.168.5.1

[Peer]
PublicKey = ML5BqgOUmKMklzhXGSXnmFWeTVD1gDn15SEB8f/T5zo=
# PresharedKey not used
AllowedIPs = 0.0.0.0/0, ::/0
Endpoint = 192.168.0.5:55443
PersistentKeepAlive = 25
```

If you setup WireGuard on your phone (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 172.22.0/24 (the wg servers subnet), or masquerade this traffic

References