

Application Note

WIREGUARD AS A SERVER

MC Technologies GmbH – July 2025

Revision History

Version	Date	Author	Description
1.0	09.07.2025	Ismail Abjou	Initial release of WireGuard as a server setup guide on OpenWRT 24

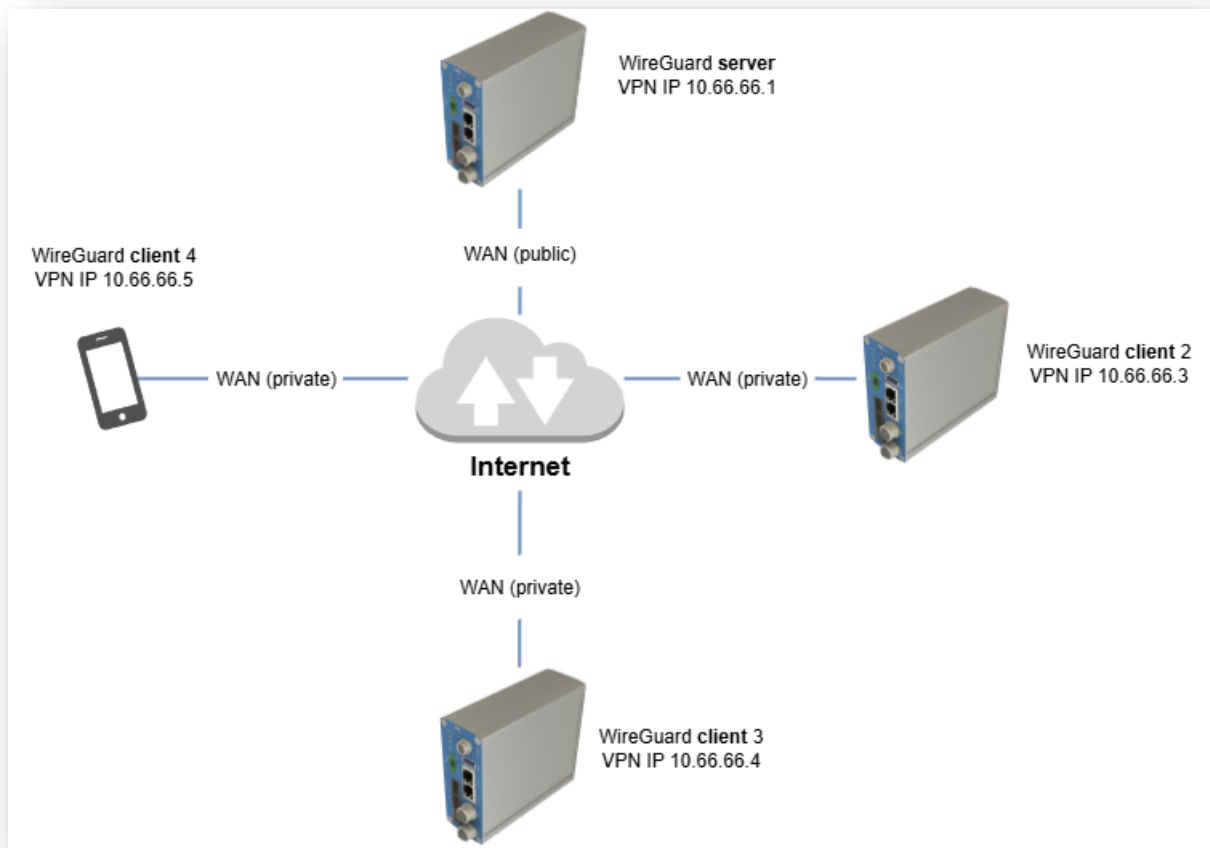
Table of Contents

Inhalt

Revision History	2
Table of Contents	3
Introduction	4
Prerequisites	5
Generate WireGuard Keys	5
Installing Required Packages.....	5
Creating a WireGuard Interface.....	6
On your router (per LuCi):.....	6
Add WireGuard Peer (Client)	7
Adding a Firewall zone	8
Allow Incoming WireGuard Traffic.....	9
Step 6: Test Connection	10
Final Steps	10

Introduction

WireGuard is a lightweight and modern VPN protocol that integrates seamlessly with OpenWrt, providing secure, high-speed communication between networked systems. Its compact and efficient codebase makes it easier to audit, maintain, and deploy compared to traditional VPN solutions like IPsec or OpenVPN.



This application note details the complete process for installing and configuring WireGuard as a server on an MC Technologies router running OpenWRT. It walks you through:

- Installing the necessary WireGuard packages via the LuCI web interface
- Creating and importing a WireGuard interface using your server's configuration
- Defining a dedicated firewall zone to isolate and secure VPN traffic
- Adjusting DNS settings to ensure proper name resolution over the tunnel

Prerequisites

1. MC router running OpenWRT 24 or higher
2. The following packages installed:
 - wireguard-tools
 - luci-proto-wireguard
3. Administrative (root) access to the router
4. Server device will need to have a **Public IP** address or Public Dynamic IP address

Generate WireGuard Keys

1. Log to your router through SSH or PUTTY
2. Run this command:

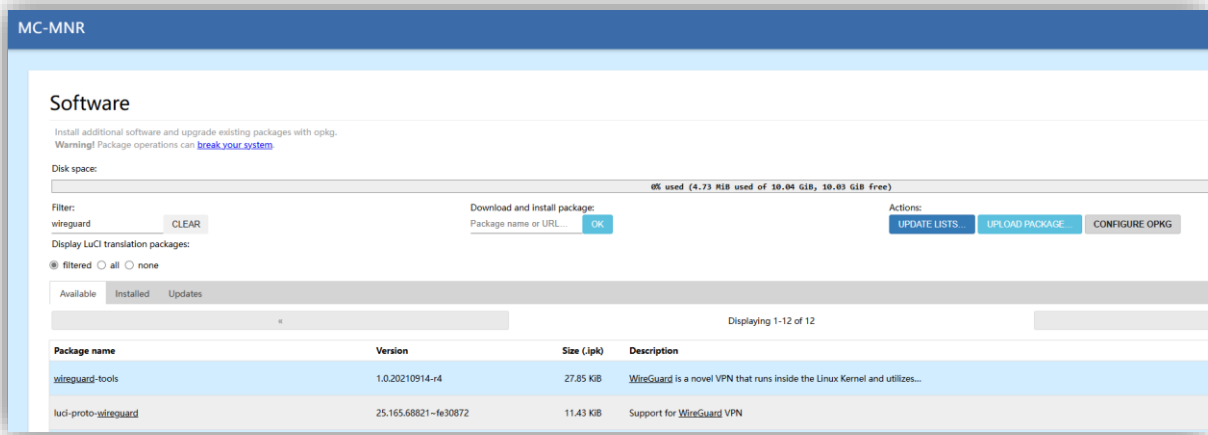
```
wg genkey | tee /etc/wireguard/server_privatekey | wg pubkey > /etc/wireguard/server_publickey
```

You will find the generated keys in /etc/wireguard:

- Private key: /etc/wireguard/server_privatekey (Keep this file secure and do not share it).
- Public key: /etc/wireguard/server_publickey

Installing Required Packages

1. Access your router's web interface
2. Go to System → Software
3. Then click Update lists and wait until the update is complete
4. In the Filter field, type WireGuard
5. Install the following packages:
 - wireguard-tools
 - luci-proto-wireguard
6. Restart your router after installation



Creating a WireGuard Interface

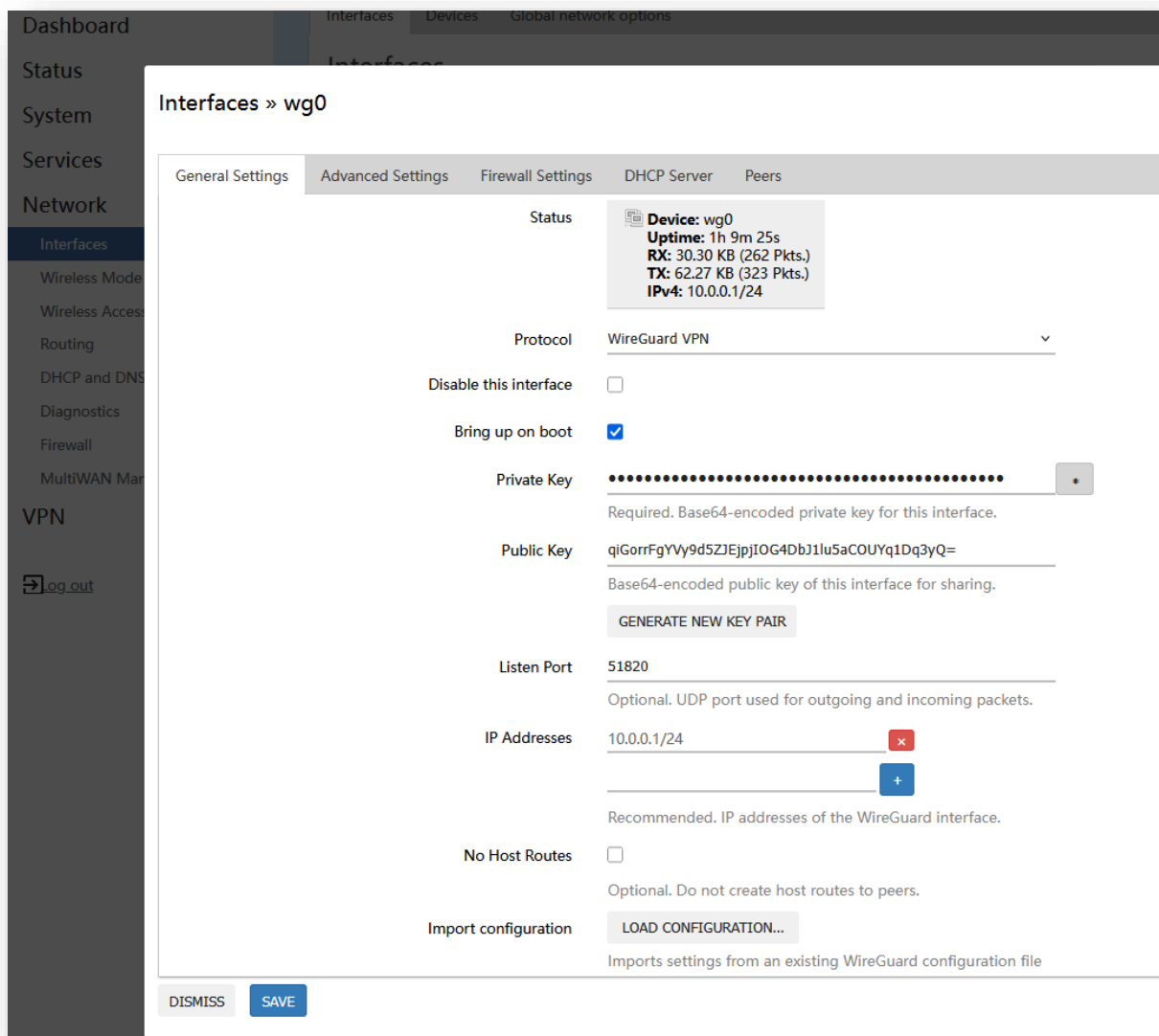
On your router (per LuCi):

1. Navigate to Network → Interfaces.
2. Click Add new interface.
3. Name it (e.g., MNR_Wireguard) and set Protocol to WireGuard VPN.
4. Click Create interface.



Then in general settings:

- Add the generated private key of the server
- Add the listen port
- Add an IP-adress to the Inteface



Add WireGuard Peer (Client)

Under the Peers tab:

- Click Add peer.
- Enable Route Allowed IPs.
- Set Persistent Keep Alive to 25.
- Click Save & Apply.

The screenshot shows the 'Edit peer' configuration page for a WireGuard interface named 'wg0'. The page is divided into several sections with various configuration options:

- Disabled:** A checkbox that is currently unchecked. Below it, a note says 'Enable / Disable peer. Restart wireguard interface to apply changes.'
- Description:** A text field containing 'My Peer'. Below it, a note says 'Optional. Description of peer.'
- Public Key:** A text field containing '+1qWxfXQIGSKMukmU6JRart/SB7Rkc2Kkx4ZbNs+XXI='. Below it, a note says 'Required. Public key of the WireGuard peer.'
- Private Key:** A text field with a small square icon to its right. Below it, a note says 'Optional. Private key of the WireGuard peer. The key is not required for establishing a connection but allows generating a peer configuration file.' A button labeled 'GENERATE NEW KEY PAIR' is located below this section.
- Preshared Key:** A text field with a small square icon to its right. Below it, a note says 'Optional. Base64-encoded preshared key. Adds in an additional layer of symmetric-key cryptography for post-quantum resistance.' A button labeled 'GENERATE PRESHARED KEY' is located below this section.
- Allowed IPs:** Two text fields containing '192.168.2.0/24' and '10.0.0.0/24'. Each field has a red 'x' icon to its right. A blue '+' icon is located below the second field. Below this section, a note says 'Optional. IP addresses and prefixes that this peer is allowed to use inside the tunnel. Usually the peer's tunnel IP addresses and the peer's local IP addresses.'
- Route Allowed IPs:** A checkbox that is checked. Below it, a note says 'Optional. Create routes for Allowed IPs for this peer.'
- Endpoint Host:** A text field containing 'vpn.example.com'. Below it, a note says 'Optional. Host of peer. Names are resolved prior to bringing up the interface.'
- Endpoint Port:** A text field containing '51821'. Below it, a note says 'Optional. Port of peer.'
- Persistent Keep Alive:** A text field containing '25'. Below it, a note says 'Optional. Seconds between keep alive messages. Default is 0 (disabled). Recommended value if this device is behind a NAT is 25.'
- Configuration Export:** A button labeled 'GENERATE CONFIGURATION...'. Below it, a note says 'Generates a configuration suitable for import on a WireGuard peer.'

At the bottom of the page, there are two buttons: 'DISMISS' and 'SAVE'.


Adding a Firewall zone

1. Navigate to Network → Firewall.
2. Click Add and configure as follows:
 - Name: (e.g., Wireguard_fw)
 - Input: Reject
 - Output: Accept
 - Forward: Reject
 - Masquerading: ✓ Checked
 - MSS Clamping: ✓ Checked
 - Covered networks: select your WireGuard interface.
 - Allow forward to destination zones: leave unspecified
 - Allow forward from source zones: select lan
3. Click Save, then Save & Apply.



Firewall - Zone Settings

General Settings | **Advanced Settings** | Contrack Settings

This section defines common properties of "this new zone". The *input* and *output* options set the default policies for traffic entering and leaving this zone.

Name	Wireguard_fw
Input	reject ▼
Output	accept ▼
Intra zone forward	reject ▼
Masquerading	<input checked="" type="checkbox"/>
	Enable network address and port translation IPv4 (NAT4 or NAPT4) for outbound traffic
MSS clamping	<input checked="" type="checkbox"/>
Covered networks	Wireguard_Test:  ▼

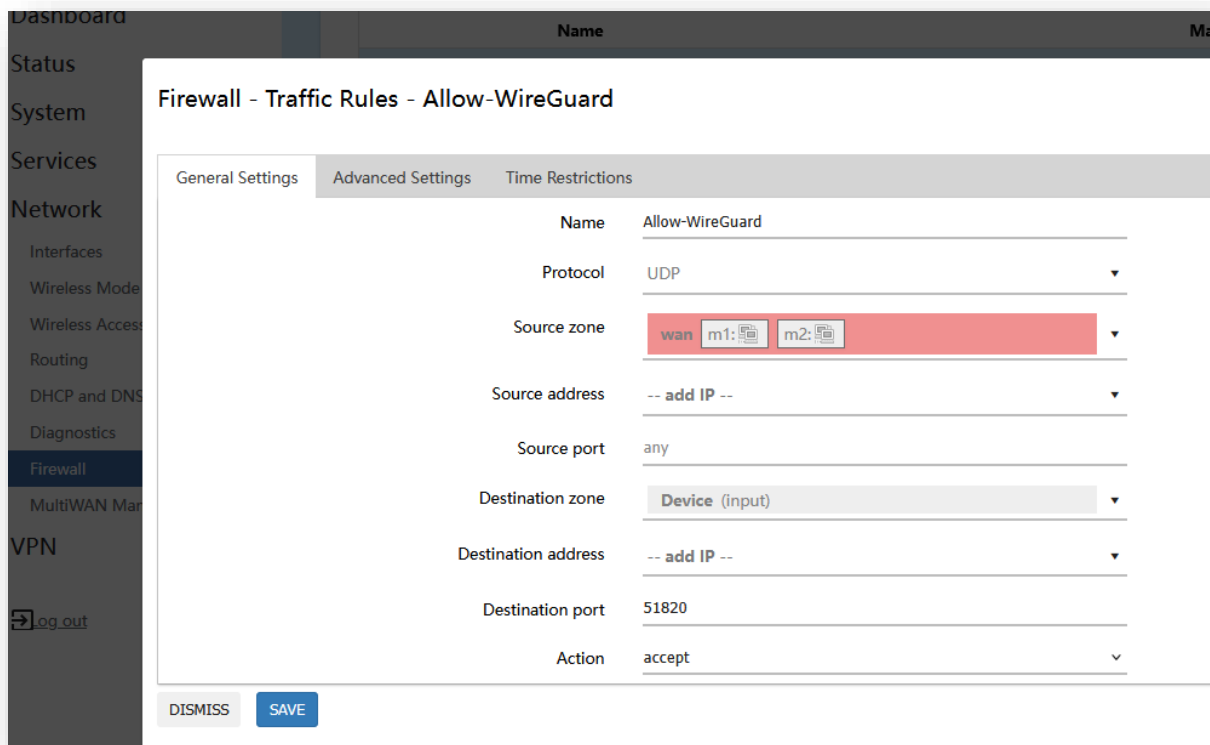
The options below control the forwarding policies between this zone (this new zone) and other zones. *Destination zones* cover forwarded traffic originating from this zone to forward from wan to lan as well.

Allow forward to <i>destination zones</i> :	unspecified ▼
Allow forward from <i>source zones</i> :	lan   ▼

DISMISS **SAVE**

Allow Incoming WireGuard Traffic

1. Navigate to Network → Firewall → Traffic Rules.
2. Click Add and configure as follows:
 - Protocol: UDP
 - The source zone: wan
 - The destination: Device
 - Action: Accept



Step 6: Test Connection

Log to your router through SSH or PUTTY, and ping the client to test the reachability of the client.

```
ping <Client_VPN_IP>
```

Done!

Your MC-MNR is now configured as a WireGuard VPN server.

Final Steps

A reboot is not required but may help confirm everything is working correctly.