

Application Note

WIREGUARD

MC Technologies GmbH – July 2025

Revision History

Version	Date	Author	Description
1.0	27.06.2025	ismail.abjou@mc-technologies.com	Initial release of WireGuard as a client setup guide on OpenWRT 24

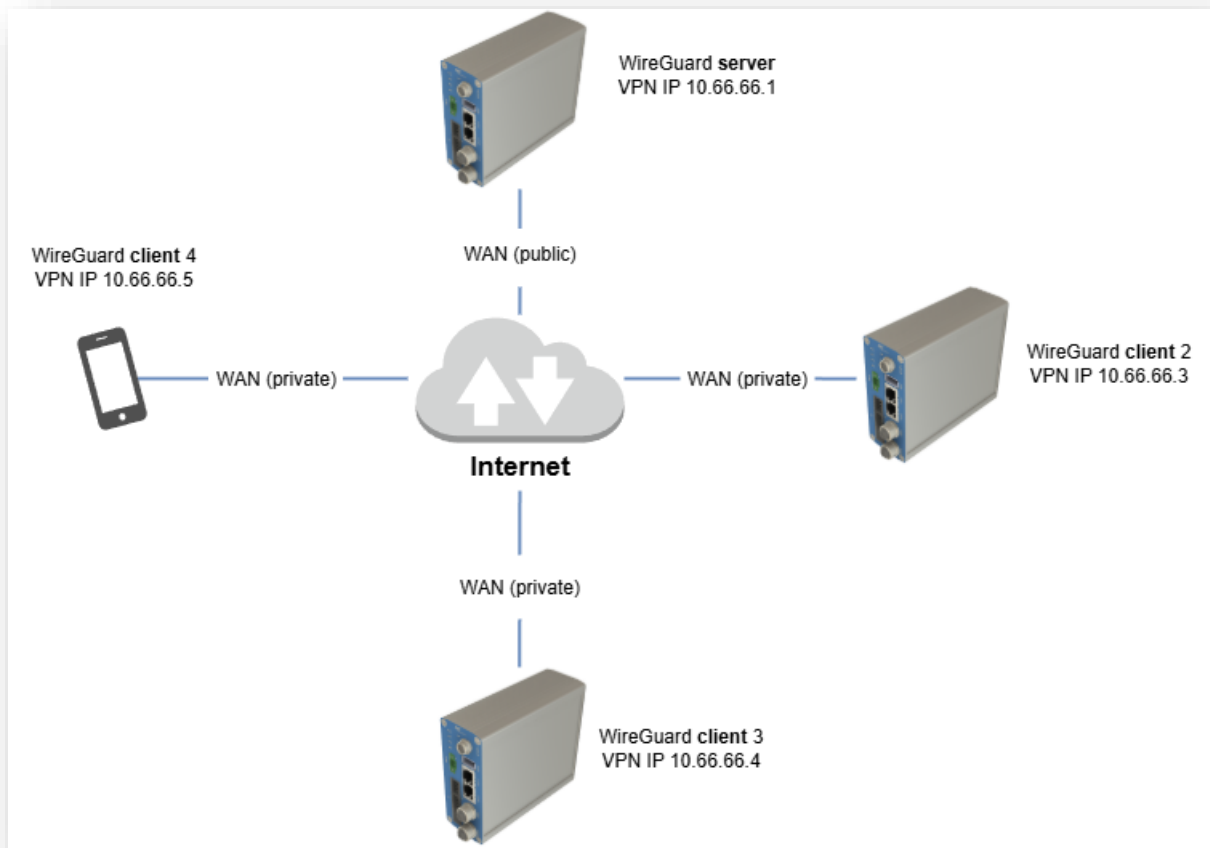
Table of Contents

Inhalt

Revision History	2
Table of Contents.....	3
Introduction	4
Prerequisites	5
Creating a WireGuard Client Configuration	5
Method 1: Use a Provided Config File.....	5
Method 2: Generate Client Keys on Your Router	5
Installing Required Packages.....	6
Configuring WireGuard on your Router.....	6
Creating a WireGuard Interface.....	6
Adding a Firewall Zone.....	9
Configuring DNS.....	10
Final Steps	11

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 client 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

- MC router running OpenWRT 24 or higher
- The following packages installed:
 - wireguard-tools
 - luci-proto-wireguard
- Administrative (root) access to the router

Creating a WireGuard Client Configuration

You can generate a WireGuard configuration file using one of the following methods:

Method 1: Use a Provided Config File

1. Extract the archive containing the config files.
2. Open the config file with any text editor.
3. Copy its contents for use.

Method 2: Generate Client Keys on Your Router

1. Log in to your router via SSH (e.g. with PuTTY or terminal).
2. Run the following command to generate client keys:

```
genkey | tee /etc/wireguard/client1_privatekey | wg pubkey > /etc/wireguard/client1_publickey
```

3. The keys will be stored in /etc/wireguard/:
 - Private key: /etc/wireguard/client1_privatekey (Keep this file secure and do not share it).
 - Public key: /etc/wireguard/client1_publickey

4. Use This client.conf Template:

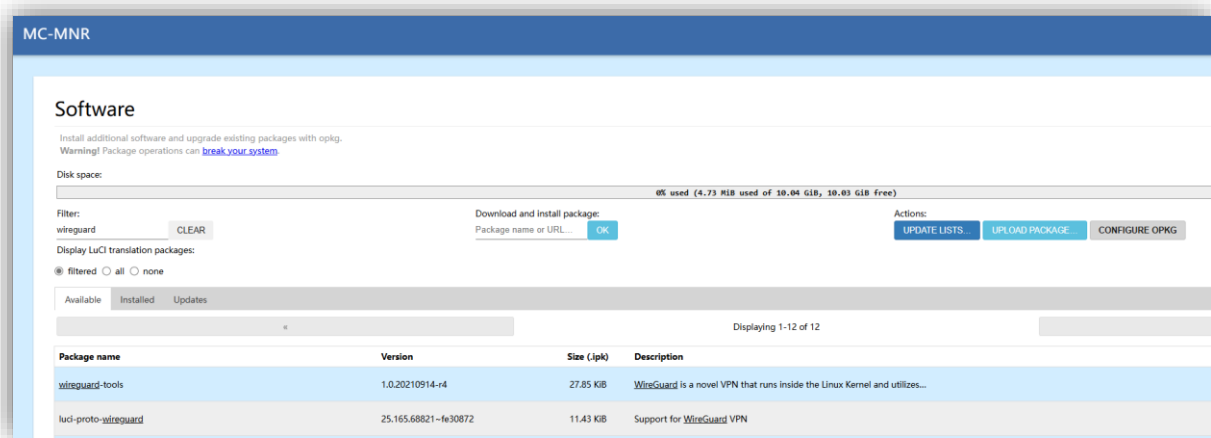
```
[Interface]
PrivateKey = [contents of client1_privatekey]
Address = [e.g., 10.66.66.3/32, fd42:42:42::3/128]
DNS = [e.g., 10.66.66.1, 10.66.66.1]
```

```
[Peer]
PublicKey = [server public key]
Endpoint = [server public IP]:[port]
AllowedIPs = 0.0.0.0/0, ::/0
PersistentKeepalive = 25
```

Replace the placeholders ([...]) with actual values from your setup.

Installing Required Packages

1. To begin open your browser and connect to LuCi (<https://192.168.2.1>)
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



Configuring WireGuard on your Router

To begin open your browser and connect to LuCi (<https://192.168.2.1>)

Creating a WireGuard Interface

On your router:

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.

Add new interface...

Name	MNR_Wireguard
Protocol	WireGuard VPN ▼

Under General Settings:

1. Click Load configuration...
2. Paste the copied WireGuard config and click Import settings.

Interfaces » MNR_Wireguard

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

Status **Device:** wireguard-MNR_Wireguard
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**

Under Advanced Settings, Set MTU to 1420:

Interfaces » MNR_Wireguard

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

Force link
Set interface properties regardless of the link carrier (If set, carrier sense even

MTU 1420
Optional. Maximum Transmission Unit of tunnel interface.

Under the Peers tab:

1. Click Edit next to the imported peer.
2. Enable Route Allowed IPs.
3. Set Persistent Keep Alive to 25.
4. Click Save.
5. Click Save & Apply.

Interfaces » MNR_Wireguard » Edit peer

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

Description: wg0-client-MNR.conf
Optional. Description of peer.

Public Key: yfYtsuqWeBRbT...Efg/QhbTbY...Yx+0H0=
Required. Public key of the WireGuard peer.

Private Key: *
Optional. Private key of the WireGuard peer. The key is not required for establishing a connection but allows generating a peer configuration.

Preshared Key:
Optional. Base64-encoded preshared key. Adds in an additional layer of symmetric-key cryptography for post-quantum resistance.

Allowed IPs: 0.0.0.0/0 [x]
::/0 [x]
[+]
Optional. IP addresses and prefixes that this peer is allowed to use inside the tunnel. Usually the peer's tunnel IP addresses and the network.

Route Allowed IPs
Optional. Create routes for Allowed IPs for this peer.

Endpoint Host: 212...
Optional. Host of peer. Names are resolved prior to bringing up the interface.

Endpoint Port: 59053
Optional. Port of peer.

Persistent Keep Alive: 25
Optional. Seconds between keep alive messages. Default is 0 (disabled). Recommended value if this device is behind a NAT is 25.

Configuration Export:
Generates a configuration suitable for import on a WireGuard peer.

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
Conntrack 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"/>
	<small>Enable network address and port translation IPv4 (NAT4 or NAPT4) for outbound traffic</small>
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 on the destination zone, while *source zones* cover forwarded traffic on the source zone.

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

DISMISS
SAVE

Configuring DNS

1. Go to Network → Interfaces.
2. Click Edit next to the WAN interface.
3. Under Advanced Settings:
 - Uncheck Use DNS servers advertised by peer.
 - Enter the WireGuard DNS server (e.g., 10.66.66.1).
4. Click Save.
5. Click Save & Apply.

Interfaces » m2

General Settings	Advanced Settings	Firewall Settings	DHCP Server
	Force link	<input type="checkbox"/>	Set interface properties regardless of the link carrier (If set, carrier sense events do not invoke hotplug handlers).
	Operator Code	<input type="text"/>	If omitted, operator selection is set to automatic
	Enable IPv6 negotiation	<input type="checkbox"/>	
	Use DHCP	Automatic	▼
	Use DHCPv6	Automatic	▼
	Modem init timeout	10	Maximum amount of seconds to wait for the modem to become ready
	Override MTU	1500	
	Use DNS servers advertised by peer	<input type="checkbox"/>	If unchecked, the advertised DNS server addresses are ignored
	Use default gateway	<input checked="" type="checkbox"/>	If unchecked, no default route is configured
	Use custom DNS servers	10.66.66.1	✖ +
	DNS search domains		+
	DNS weight	0	The DNS server entries in the local resolv.conf are primarily sorted by the weight specified here
	Use gateway metric	0	Metric is an ordinal, where a gateway with 1 is chosen 1st, 2 is chosen 2nd, 3 is chosen 3rd, etc

If you also have a WAN6 (IPv6) interface, repeat the above steps for it.

Step 6: Test Connection

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

```
ping <Server_VPN_IP>
```

Done!

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

Final Steps

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