Build your Home Network with OPNsense

A Step-by-Step Guide

1. Introduction

This guide will walk you through setting up your home network using OPNsense as your firewall/router. We will cover everything from initial installation to configuring essential network services, providing a solid foundation for a secure and efficient home network. This guide assumes that you will be installing OPNsense on a physical machine. If you are planning to virtualize OPNsense please refer to the document **HOME Router.**

Table of Contents

Figures

Tables

2. Planning Your Network

System Overview

Before diving into the technical aspects, it's important to understand the basic structure of your desired network. Here is a breakdown of the key components and their roles:

- **Internet Connection:** Your internet service provider's (ISP) modem will provide the incoming internet connection.
- **OPNsense Router/Firewall:** This will be your central device, responsible for routing traffic, enforcing security policies, and acting as your primary gateway.
- **Managed Network Switch:** A smart switch allows you to manage traffic through VLANs (Virtual Local Area Networks), segmenting your network into separate logical networks.
- **Wireless Access Point (AP):** This device will provide wireless access to your network.
- **Trusted Network (LAN):** This network will host your trusted devices such as PCs, laptops, and NAS devices.
- **Untrusted Network (VLAN):** This network will host less secure devices like IoT devices and guest devices.

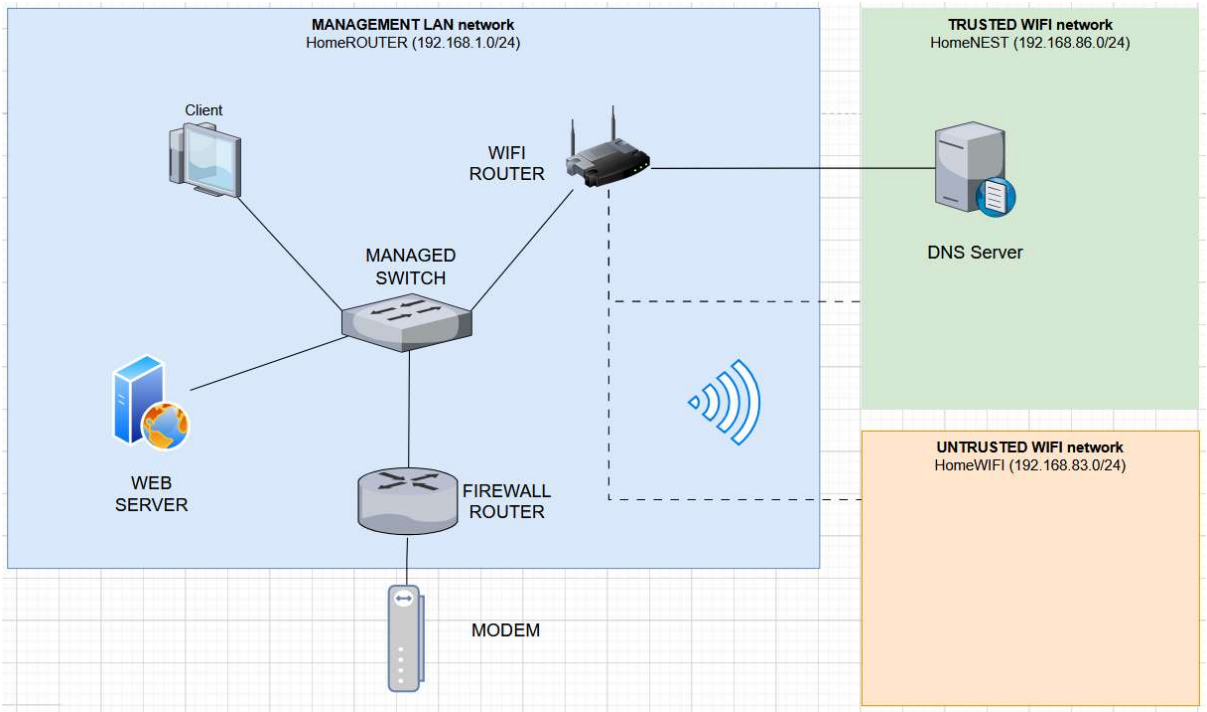


Figure 1 - **Logical Diagram**

A diagram showing the basic network layout, with the internet connection to the modem, which then connects to the OPNsense router. From the router a connection goes to a managed switch. The switch divides into two lines, one to LAN and other to untrusted devices.

Components

The following hardware components will be used:

Table 1: Components

COMPONENT	DESCRIPTION	LINK TO SOURCE
CPU	Intel Alder Lake N100 (4 cores, 6MB Cache, 3.40 GHz)	Aliexpress
RAM	Minimum: 8 GB PC5-38400 DDR5 4800MTs 262 Pin	Webuy
OS STORAGE	WD Black WD5000LPLX 500GB 2.5" SATA III	Not provided
OPNSENSE	OPNsense for firewall and routing	OPNsense Download

- **NOTE: Computer for management** A second computer is required to manage OPNsense via web interfaces.

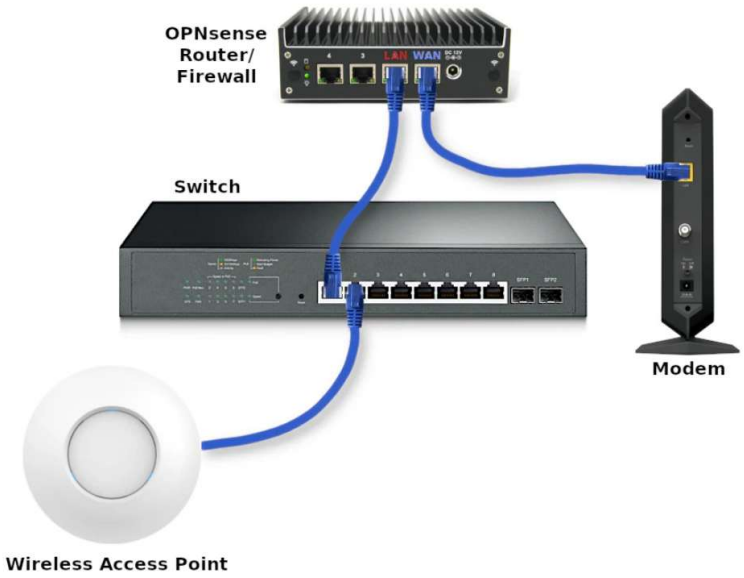


Figure 2 - **Physical Diagram**

A diagram showing a more realistic layout. The internet connection coming into the modem, from there the OPNsense router (connected through ethernet port). Then, from the OPNsense router to the managed switch (connected to port 1). On the managed switch you will find connections to devices including a wireless access point (connected to port 2), a PC, a NAS, and a TV.

3. Initial Setup: Installing OPNsense

The first step is to install OPNsense on your dedicated hardware.

Prerequisites:

- A computer that meets OPNsense hardware requirements
- A USB drive for creating an installation media
- A computer connected to your local network.

Installation steps:

1. **Download the OPNsense Installer:** Visit the OPNsense download page and download the **"VGA"** installer.
2. **Create Bootable USB:** Use a tool like Etcher to flash the downloaded image to your USB drive. You don't need to extract the image.
3. **Boot from USB:** Plug the USB into your target computer, start the computer, and configure the BIOS to boot from the USB drive.
4. **Follow the On-Screen Prompts:**
    i. Do not press any keys when prompted for configuration importer.
    ii. Press a key for manual interface assignment.
    iii. Press “n” to skip LAGG configuration.
    iv. Press “n” to skip VLAN creation.
    v. Enter [igc0] for the WAN interface name.
        - This is the port that will connect to your ISP.
        - Note: Your interface names may be different, use the correct names for your hardware.
    vi. Enter [igc1] for the LAN interface.
        - This will connect to your network switch.
    vii. When prompted for an optional interface name press “Enter” to skip configuration.
    viii. Press “y” and "Enter" to continue.
    ix. Log in with the username [installer] and the password [opnsense].
    x. Press “Enter” to select the default keymap (UK keyboard).
    xi. Select “Install (ZFS)” to use ZFS file system.
    xii. Select the disk “SPACE BAR” and then “Enter” where you want to install OPNsense.
    xiii. Select "Yes" to continue with the recommended swap partition.
    xiv. Select "Yes" to destroy the current contents of the disk.

xv. Select “Change root password” and enter a strong password. This password will be used to access the web interface and console.

xvi. Select “Complete Install” to finish the installation.

After the installation the system will reboot. You will see a login screen which lists all the IP addresses of your interfaces.

Don’t forget to remove the BOOTABLE USB drive before restarting.

4. Basic OPNsense Configuration

Now, let's configure basic OPNsense settings.

Accessing the Web Interface

1. Make sure your computer is connected to the LAN interface of OPNsense.
2. Open a browser and go to https://192.168.1.1.
    - If page shows on load- Warning: Potential Security Risk Ahead
        i. Click “Advanced”
        ii. Click “Accept the Risk and Continue”
    - You can also use the default hostname opnsense.local.
3. Login with the user “root” and the password you set during the installation.
4. Skip the Configuration Wizard by clicking on the OPNsense logo in the upper left-hand corner of the page.

System Settings

Go to **System > Settings > General** and configure these settings:

Table 2 – System Settings: General

OPTION	DESCRIPTION	VALUE
HOSTNAME	a hostname of your choice	router
DOMAIN	your domain name	HomeNETWORK.local
TIME ZONE	Your time zone	Europe/London
DNS SERVERS	Leave blank	
DNS SERVER OPTIONS	Check "Allow DNS server list to be overridden by DHCP/PPP on WAN"	Enable

- Click “save” for changes to be applied

Administration

Go to **System > Settings > Administration** and configure these settings:

Table 3 – System Settings: Administration

OPTION	VALUE
PROTOCOL	HTTPS (default value)
HTTP STRICT TRANSPORT SECURITY	Check “Enable HTTP Strict Transport Security”
TCP PORT	443
HTTP REDIRECT	Leave unchecked
DNS REBIND CHECK	Leave unchecked (may interfere with name resolution)
HTTP COMPRESSION	Low (for slow systems)
LISTEN INTERFACES	All (recommended)

- Click “save” for changes to be applied

Miscellaneous

Go to **System > Settings > Miscellaneous** and adjust these settings:

Table 4 – System Settings: Miscellaneous

OPTION	VALUE
THERMAL SENSORS HARDWARE	Intel Core CPU (or AMD equivalent if applicable)
PERIODIC RRD BACKUP	24 hours (optional)
PERIODIC DHCP LEASES BACKUP	24 hours (optional)
PERIODIC NETFLOW BACKUP	24 hours (optional)
USE POWERD	Checked (if power saving is enabled in BIOS)
POWER MODE	Hiadaptive (balance performance with power saving)

- Click “save” for changes to be applied

5. Interface Configuration

Next, configure your network interfaces:

Interface Settings

Go to **Interfaces > Settings**. You may want to check the following to disable hardware offloading options. This can sometimes cause problems.

Table 5 – Interfaces Settings

OPTION	VALUE
HARDWARE CRC	Check "Disable hardware checksum offload"
HARDWARE TSO	Check "Disable hardware TCP segmentation offload"
HARDWARE LRO	Check "Disable hardware large receive offload"
VLAN HARDWARE FILTERING	Choose the "Disable VLAN Hardware Filtering"

- Click “save” for changes to be applied

Create VLAN

1. Navigate to **Interfaces > Other Types > VLAN.**
2. Create a new VLAN with the following settings:

Table 6 – Interfaces Other Types: VLAN

OPTION	VALUE
DEVICE	Leave empty (auto-generate a name)
PARENT	igc1 (your LAN interface)
VLAN TAG	10
VLAN PRIORITY	Default, or select priorities if required
DESCRIPTION	UNTRUSTED

- Click “apply” for changes to be applied

Interface Assignments

1. Go to **Interfaces > Assignments**.
2. Click the "+" button in the New interface section.
3. Assign the UNTRUSTED VLAN, which should be in the dropdown menu.
4. Enter the description UNTRUSTED.
5. Click "Add".

Interface Pages

Now, let's adjust the specific interface settings by going to **Interfaces > [WAN]**, **Interfaces > [LAN]** and **Interfaces > [UNTRUSTED]**:

WAN Interface

Table 7 – Interfaces: WAN

OPTION	VALUE
ENABLE	Checked by default
LOCK	Checked
DESCRIPTION	WAN (default)
BLOCK PRIVATE NETWORKS	Checked (if connected directly to internet; uncheck otherwise)
BLOCK BOGON NETWORKS	Checked (if connected directly to internet; uncheck otherwise)
IPV4 CONFIGURATION TYPE	DHCP (if applicable)
IPV6 CONFIGURATION TYPE	None

- Click “save” for changes to be applied
- Click “Apply changes” for changes to take effect

LAN and UNTRUSTED Interface Settings

Table 8 – Interfaces: LAN and UNTRUSTED

OPTION	VALUE	IPV4 ADDRESS
ENABLE	Checked	
LOCK	Checked	
BLOCK PRIVATE NETWORKS	Unchecked	
BLOCK BOGON NETWORKS	Unchecked	
IPV4 CONFIGURATION TYPE	Static IPv4	
IPV4 UPSTREAM GATEWAY	Auto-detect	
IPV6 CONFIGURATION TYPE	None	
INTERFACE	LAN	192.168.1.1/24
INTERFACE	UNTRUSTED	192.168.10.1/24

- Click “save” for changes to be applied
- Click “Apply changes” for changes to take effect

6. DHCP Configuration

Go to **Services > DHCPv4** and configure DHCP for both interfaces:

Table 9 – Services: DHCPv4

INTERFACE	RANGE FROM	RANGE TO
[LAN]	192.168.1.100	192.168.1.200
[UNTRUSTED]	192.168.10.100	192.168.10.200

- Ensure the check box “Enable” is ticked for- Enable DHCP server on the UNTRUSTED interface
- Click “save” for changes to be applied

7. DNS Configuration

You will be using your ISP's DNS servers for this guide. You may want to consider creating your own DNS servers using Unbound DNS in future.

System Settings

Go to **System > Settings > General**, and make sure that the DNS servers are blank, and the option "Allow DNS server list to be overridden by DHCP/PPP on WAN" is checked.

Unbound DNS

Navigate to **Services > Unbound DNS > General** and set the following values:

Table 10 – Services: Unbound DNS

OPTION	VALUE
ENABLE	Check "Enable Unbound" (If not enabled already)
LISTEN PORT	Leave as default 53
NETWORK INTERFACES	All (recommended)
DNSSEC	Check "Enable DNSSEC Support" (If upstream DNS servers support)
DHCP REGISTRATION	Check "Register ISC DHCP4 leases"
DHCP STATIC MAPPINGS	Check "Register DHCP static mappings"
DNS CACHE	Check "Flush DNS cache during reload"
LOCAL ZONE TYPE	transparent

- Click “Apply” for changes to be applied

8. Firewall Configuration

Firewall rules are essential for securing your network.

Firewall Aliases

1. Go to **Firewall > Aliases**.
2. Click on the "+" button to create a new alias with the following settings:

Table 11 – Firewall: Aliases

OPTION	VALUE
ENABLED	Checked
NAME	PrivateNetworks
TYPE	Network(s)
CONTENT	10.0.0.0/8,172.16.0.0/12,192.168.0.0/16
DESCRIPTION	All local IPv4 networks

- Click “save” for changes to be applied
- Click “Apply” for changes to take effect

Firewall Rules: LAN

Go to **Firewall > Rules > LAN** and add the following rules:

- You may remove the two “allow all IPv4/IPv6 rules
- Do not click “Apply” until you have added the rules below!!!
- Click “+” to add each rule below
- For each new rule: Click “save” rule to be added
- Make sure to have “destination invert” option checked on the 3rd rule!

Table 12 – Firewall: Rules LAN

ACTION	TCP/IP PROTOCOL	SOURCE	DEST/INVERT	DESTINATION	DEST PORT	DESCRIPTION
PASS	IPv4 TCP/UDP	LAN net	unchecked	LAN address	53	Allow DNS to LAN interface
PASS	IPv4 ICMP	LAN net	unchecked	any	any	Allow ICMPv4 from LAN
PASS	IPv4 any	LAN net	checked	PrivateNetworks	any	Block access to other networks but allow access to the internet

- Click “Apply changes” for changes to be take effect

If you want to allow the LAN to reach anything specific in your UNTRUSTED network, you simply just need to add a firewall rule above the bottom rule.

Firewall Rules: UNTRUSTED

Go to **Firewall > Rules > UNTRUSTED** and add these rules:

Table 13 – Firewall: Rules UNTRUSTED

ACTION	TCP/IP PROTOCOL	SOURCE	DEST/INVERT	DESTINATION	DEST PORT	DESCRIPTION
PASS	IPv4 TCP/UDP	UNTRUSTED net	unchecked	UNTRUSTED address	53	Allow access to DNS on the UNTRUSTED interface
PASS	IPv4 any	UNTRUSTED net	checked	PrivateNetworks	any	Block access to other networks but allow access to the internet

- Click “save” for each new rule created
- Click “Apply changes” for changes to take effect

If you need access to (for example) your NAS from two different networks, for instance, you may make use of “multi-homing” if your NAS has more than one network interface. Essentially you can connect the NAS to both networks so the traffic to/from the NAS does not have to pass through the firewall. Multi-homing can minimize wasteful network usage since less bandwidth intensive traffic needs to route through your firewall.

9. Configure Network Switch

Now, configure your managed network switch. For this guide, a Netgear GS305E – 5-Port Gigabit Ethernet Smart Managed Plus Switch will be used as an example. Please adjust the steps accordingly based on your switch's model.

Access the Switch

1. Connect your computer directly to the switch.
2. Set your computer's IP address to be on the same subnet as the switch.
3. Open a browser and go to your switch's default address.
4. Login with the default username and password.
5. Change the password after the initial login.

Change the Switch's IP Address

1. Go to the "System" tab, and select "System IP".
2. Set the IP address to 192.168.1.2.
3. Set the subnet mask 255.255.255.0.
4. Set the default gateway 192.168.1.1.
5. Click Apply. You will need to change the IP address on your computer to be on the same subnet again to connect to the switch.

VLAN Configuration

1. Go to "VLAN > 802.1Q VLAN"
2. Click the "Add" button and create a new VLAN for the untrusted network using these settings:

Option	Value
VLAN ID	10
VLAN Name	UNTRUSTED

3. Set port 5 as untagged, all other ports (1 and 2) as tagged.

Figure showing a dialog box with VLAN settings. The name and ID for the VLAN are specified, in addition there are settings for tagged and untagged ports.

4. In the "Port Config" section, set the PVID for port 5 to 10.
   Figure showing a table with the network ports, including a VLAN ID settings for the port.

10. Configure Wireless Access Point (AP)

Finally, you need to configure your wireless access point. This will be a general guide as interfaces vary between different devices, using a Grandstream wireless AP as an example.

Access the Wireless AP:

1. Connect your computer to the same network as the wireless AP.
2. Check your OPNsense lease list to get the IP address of your AP.
3. Open a browser and go to https://<AP_IP_Address>.
4. Login with the default username and password for your AP.

Configure the LAN Network SSID

1. Navigate through the initial configuration wizard.
2. Configure the first SSID, which will be used for the LAN network, with the following settings:

   Option Value

   SSID Your_LAN_SSID

   Pre-Shared Key Your_LAN_Password

   Security Mode WPA2 or WPA2/WPA3

3. *Figure of a basic configuration page for a wireless SSID. A Name, password, security mode, and encryption type will be shown.*
4. Click "Complete" to finish.

Configure the UNTRUSTED Network SSID:

1. Go to the “SSIDs” page and click the “Add” button to add a new SSID.
   Figure showing the SSID configuration page.
2. Set the "VLAN" option and enter the "VLAN ID" with the value 10.
3. Configure the following settings:

Table 14 – UNTRUSTED Network SSID

OPTION	VALUE
SSID	Your_Untrusted_SSID
PRE-SHARED KEY	Your_Untrusted_Password
SECURITY MODE	WPA2 or WPA2/WPA3

4. *Figure of the basic configuration page for a wireless SSID, with a VLAN ID setting in addition.*
5. Optionally enable “Client Isolation” in the Advanced section.
6. Optionally set the "DTIM period" to 3 to reduce battery drain.
   Figure of the Advanced tab for the wireless SSID configuration, showing the Client Isolation and DTIM period settings.

7. Go to the "Device Membership" tab and assign the AP to the current SSID.
   Figure of the device membership tab for the wireless SSID configuration, showing the available and member devices.

8. Click "Save" and then "Apply".

11. Connect to Internet and beyond

Congratulations! If you have followed the above instructions your network should be set up. You should now have a fully functioning home network with a trusted LAN and an untrusted VLAN. This will help to improve the security of your network.

Configure Internet Service Provider (ISP) connection

Navigate to **Interfaces > Point-to-Point > Devices** and set the following values:

Table 15 – Interfaces: ISP connection

OPTION	VALUE
LINK TYPE	PPPoE
LINK INTERFACE(S)	Igc0 (WAN)
DESCRIPTION	Plusnet ISP
USERNAME	kalvinsimon@plusdsl.net
PASSWORD	<broadband password>

- Click “save” for changes to be applied

Next steps

Here are some areas to explore:

- **Additional Security Features:** Explore various security measures to further enhance your network's protection.
- **Full Network Build:** Refer to the original full network guide for more advanced network configurations.
- **Multi-Homing Devices:** Explore multi-homing devices for more efficient routing, especially for services such as a NAS.
- **Remote Access:** Set up remote access using VPNs such as IPSec, OpenVPN, WireGuard, or Zerotier.

This guide should provide a solid foundation for your home network. Let me know if you have further questions.

Annex A - Replace the OPNsense Web UI Self-Signed Certificate

1. Introduction

This how-to describes the process of creating **self-signed certificate chains** with OPNsense as PKI (Public Key Infrastructure). For up-to-date instructions go here: https://docs.opnsense.org/manual/how-tos/self-signed-chain.html

Table of Contents

8. A Potential Gotcha

2. Creating a Certificate Chain

We will create a certificate chain using the following components:

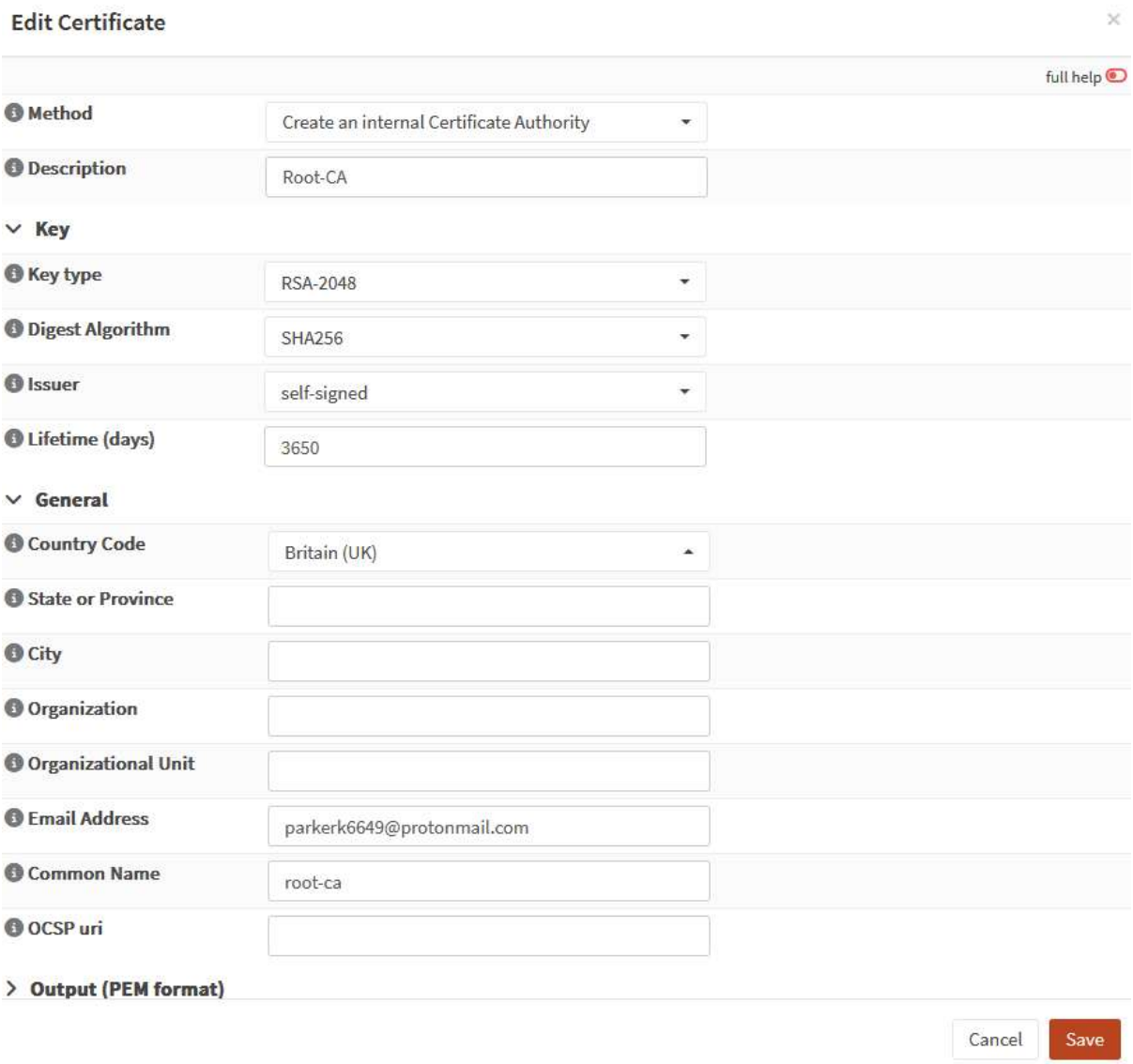
- **Root CA**: Self-signed → Signs intermediate certificates
- **Intermediate CA**: Signed by the Root CA → Signs leaf certificates
- **Leaf Certificate**: Signed by the Intermediate CA → Server or user certificate

Important: Ensure all data is backed up before proceeding.

2.1. Creating the Root CA

Go to System ‣ Trust ‣ Authorities

Press **+** to create a new authority, it will become your root certificate authority.

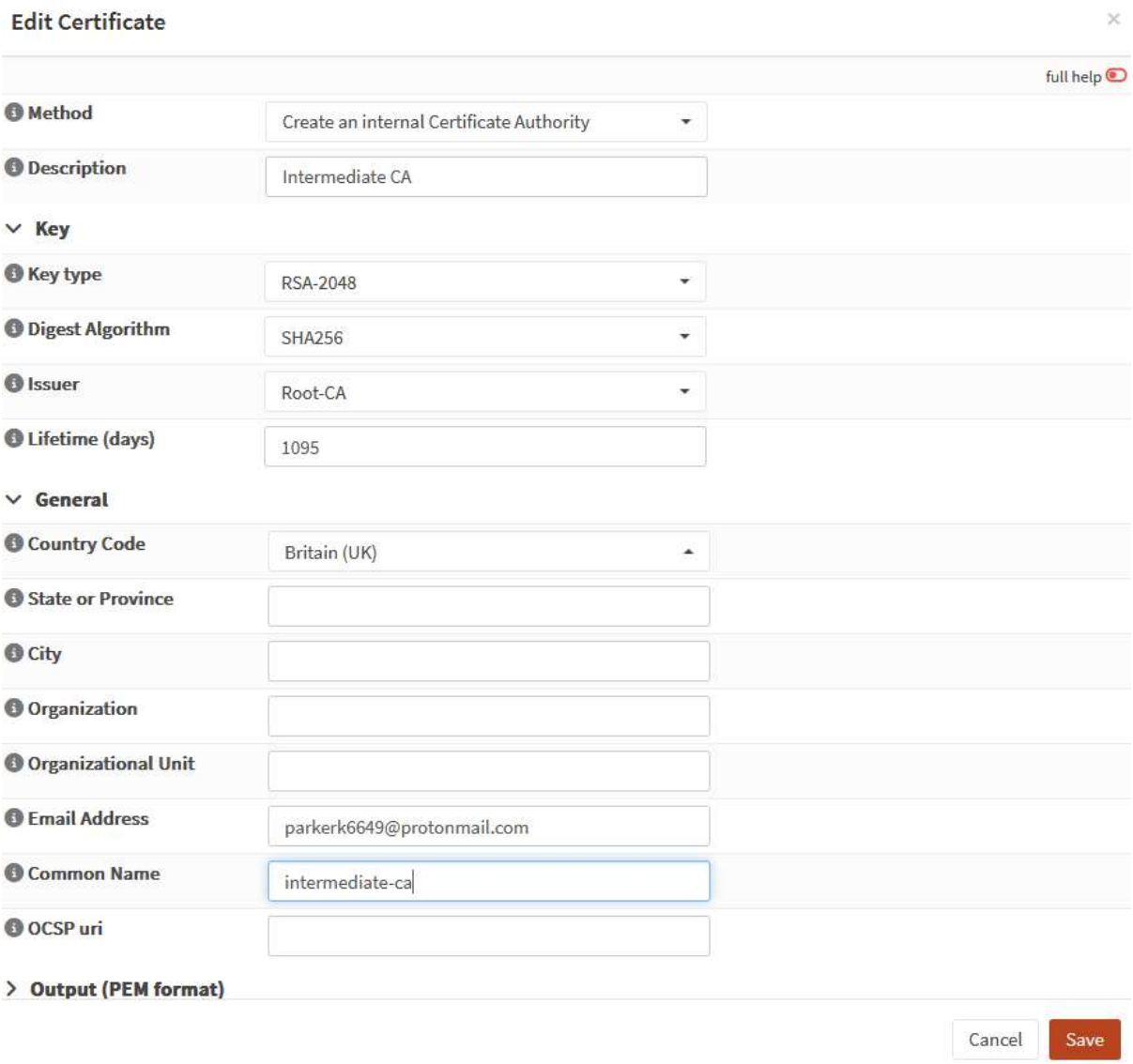


Press **Save** and the root CA has been created. The private and public key are saved on the OPNsense.

2.2. Issuing the Intermediate CA

Go to System ‣ Trust ‣ Authorities

Press **+** to create a new authority, it will become your intermediate certificate authority.

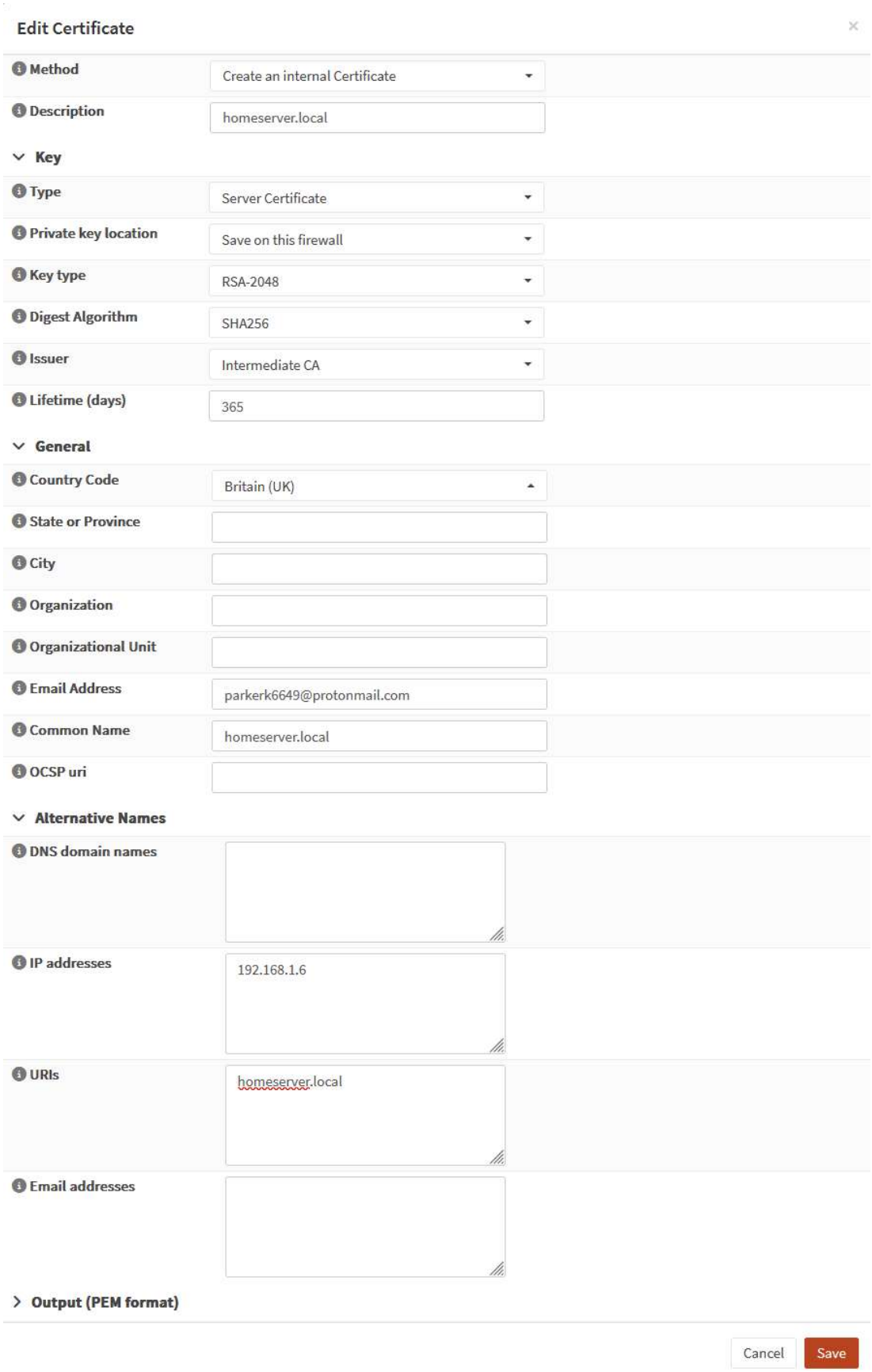


Press **Save** and the intermediate CA has been created. The private and public key are saved on the OPNsense.

2.3. Issuing a Leaf Certificate

Go to System ‣ Trust ‣ Certificates

Press **+** to create a new authority, it will become your leaf certificate (end-entity certificate). It can be used on a server, user, or both; depending on the type.



Press **Save** and the leaf certificate has been created. The private and public key are saved on the OPNsense.

2.4. Exporting the Certificate Chain

Now that we have the whole certificate chain, we create a certificate bundle for a generic linux apache/nginx web server.

For that, we need two files:

- A certificate bundle populated in the correct order in PEM format:
    1. Root CA
    2. Intermediate CA
    3. Leaf Certificate

- The private key of the leaf certificate

1. Export Root CA public key:
    - Go to System ‣ Trust ‣ Authorities
    - Press the download button in the *Commands* column of the `Root CA` row
    - Choose *File type: Certificate* and press *Download*

2. Export Intermediate CA public key:
    - Go to System ‣ Trust ‣ Authorities
    - Press the download button in the *Commands* column of the `Intermediate CA` row
    - Choose *File type: Certificate* and press *Download*

3. Export Leaf Certificate public key:
    - Go to System ‣ Trust ‣ Certificates
    - Press the download button in the *Commands* column of the `Leaf Certificate` row
    - Choose *File type: Certificate* and press *Download*

4. Export Leaf Certificate private key:
    - Go to System ‣ Trust ‣ Certificates
    - Press the download button in the *Commands* column of the `Leaf Certificate` row
    - Choose *File type: Private Key* and press *Download*

Open a text editor and create a file with all 3 public keys:

1. `certificate-bundle.pem`

```
-----BEGIN CERTIFICATE-----
Root CA public key data
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Intermediate CA public key data
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Leaf Certificate public key data
-----END CERTIFICATE-----
```

The key of the certificate bundle is only the leaf certificate's private key. Private keys of root and intermediate CAs are **not** required.

2. `certificate-bundle.key`

```
-----BEGIN PRIVATE KEY-----
Leaf Certificate private key data
-----END PRIVATE KEY-----
```

Implement these into your webserver, and the website will be secured with this certificate bundle. For automatic trust, you must install the intermediate and/or root CA certificate public keys into any client that connects to the webserver. Since the webserver offers a full certificate chain to the connecting client, manual trust can be established if a user decides to install the public key themselves.

3. Apply certificates to Server

For this step, the 2 x certificate-bundle files you just generated will need to be transfered to My Downloads of the HomeSERVER. Moving certificate files from your Downloads folder to `/etc/ssl/homeserver.local/` involves using command-line tools, primarily the `mv` (move) command.

3.1. Open a Terminal:

- You'll need to use a terminal application.

3.2. Use the mv Command:

- The `mv` command is used to move files. You'll need to use `sudo` because `/etc/ssl/homeserver.local/` is a system directory that requires administrator privileges.

    - `sudo mv ~/Downloads/certificate-bundle.pem /etc/ssl/homeserver.local/`
    - `sudo mv ~/Downloads/certificate-bundle.key /etc/ssl/homeserver.local/`

3.3. Permissions:

- After moving the files, it's crucial to set the correct permissions. Private keys, in particular, should be very strictly protected.
    - To set permissions for the private key:
        - `sudo chmod 600 /etc/ssl/homeserver.local/certificate-bundle.key`
        - (This restricts access to only the owner.)
    - To set permissions for the certificate:
        - `sudo chmod 644 /etc/ssl/homeserver.local/certificate-bundle.pem`
        - (This allows the owner to read and write, and others to read.)
    - It is also good practice to ensure the files are owned by root.
        - `sudo chown root:root /etc/ssl/homeserver.local/certificate-bundle.pem`
        - `sudo chown root:root /etc/ssl/homeserver.local/certificate-bundle.key`

3.4. Important Notes:

- **Directory Existence:**
    - Ensure that the `/etc/ssl/homeserver.local/` directory exists. If it doesn't, you'll need to create it using `sudo mkdir -p /etc/ssl/homeserver.local/`.
- **Security:**
    - Private keys are highly sensitive. Handle them with extreme care. Never share them or store them in publicly accessible locations.
- **Backups:**
    - Always back up your certificate and key files before making any changes.
- **File names:**
    - Double check that the names of the files in the download directory, match the names used in the commands.

By following these steps, you should be able to successfully move your certificate files and set the appropriate permissions.

3.5. Troubleshooting

Local Certificate Generation: Try generating a self-signed certificate directly on the Ubuntu server to rule out any OPNsense-related issues.

- `sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/homeserver.local/local.key -out /etc/ssl/homeserver.local/local.crt`

- Modify your Nginx configuration to use `/etc/ssl/homeserver.local/local.crt` and `/etc/ssl/homeserver.local/local.key`.
    - sudo nano /etc/nginx/sites-available/homeserver.local
    - Replace <.pem> or <.crt> and <.key> files with above.

- Test Nginx again. If it works, the problem is definitely with the OPNsense-generated certificates.
    - sudo nginx -t

Annex B - Add/Remove repositories manually

1. Enable SSH

To enable or disable SSH in OPNsense, you can do the following:

Navigate to System > Settings > Administration

In the Secure Shell pane, check or uncheck the Enable Secure Shell option

To install packages on OPNsense, you must be root.

2. Add a repository

3. Remove a repository

1. To remove a repository from OPNsense, you can use the command rm /usr/local/etc/pkg/repos/repository.conf. For example, to remove the repo-mihak repository, you would use the command rm /usr/local/etc/pkg/repos/repo-mihak.conf.

2. Removing a repository will not remove any packages that were previously installed from that repository.

3. You can use the pkg search command to see what is available in an installed repo, and the pkg query command to see what you have installed from a repo.

Annex C – Setting up a WireGuard VPN Server in OPNsense

Introduction

This guide will walk you through setting up a WireGuard VPN server within your OPNsense firewall/router. WireGuard is a modern, lightweight, and secure VPN protocol that offers a significant performance boost over older protocols like OpenVPN. It's designed to be easy to configure once you understand its underlying principles. This guide focuses on how to enable remote access to your home network, not connecting your OPNsense router to an external VPN.

Understanding WireGuard Concepts

- **Peers:** WireGuard uses the concept of "peers" instead of "clients" and "servers." Every device is a peer and can act as both a client and a server. In our case, OPNsense will be acting as a central peer, accepting connections from your devices.
- **Keys:** WireGuard operates on public/private key cryptography. Each peer has a public key (which it shares) and a private key (which it keeps secret).
- **Endpoints:** An "endpoint" is a peer's publicly reachable IP address and port.
- **Tunnels:** WireGuard creates encrypted "tunnels" between peers, ensuring secure communication.

Prerequisites

- An OPNsense firewall/router is set up and functional.
- You have a public IP address that is accessible on the internet. (If your ISP uses CGNAT, you will need a VPS or a service like Cloudflare Tunnel)

Step-by-Step Configuration

I. Configure the WireGuard Server Instance

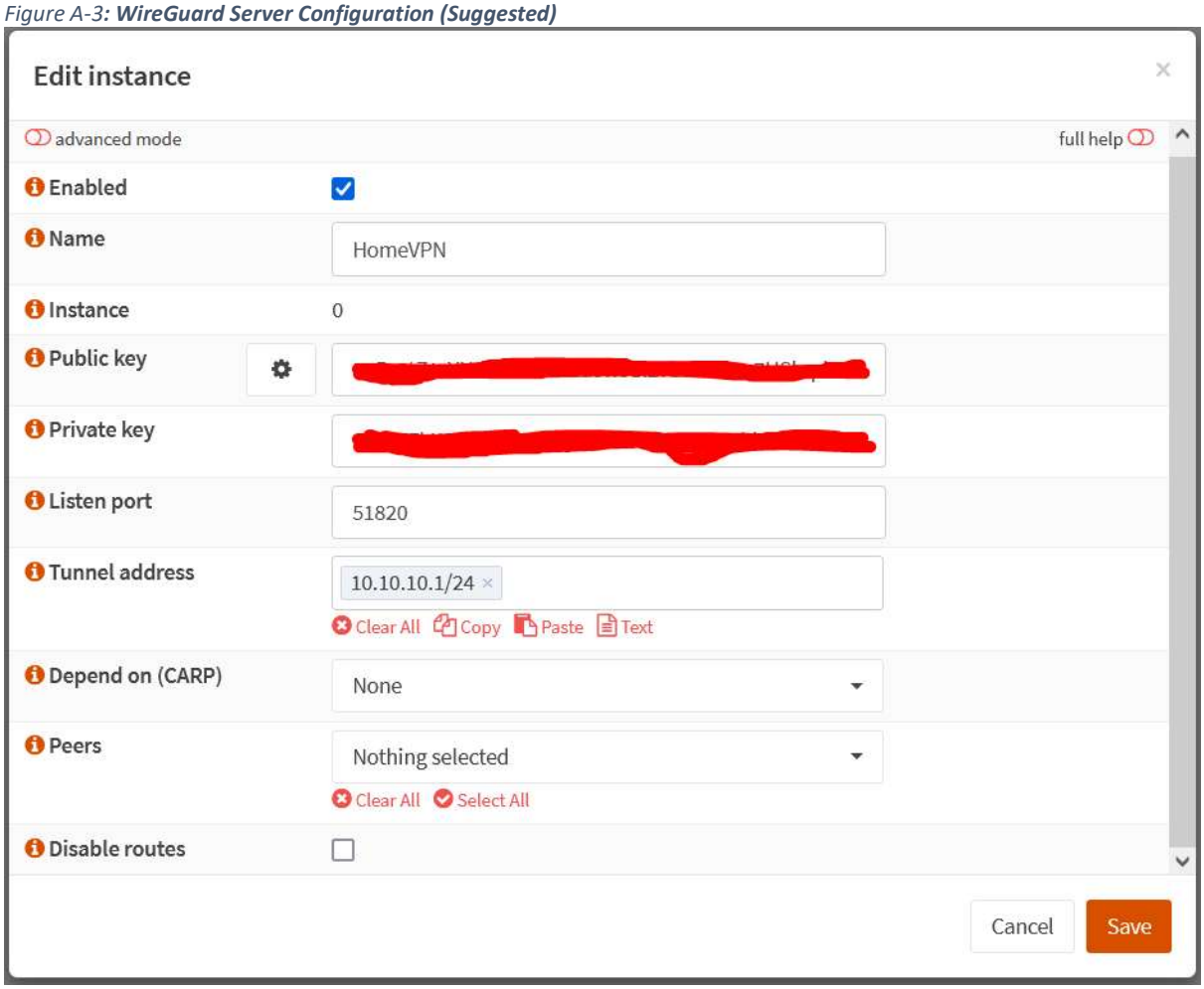
1. **Access the WireGuard Menu:** Navigate to "VPN > WireGuard" in the OPNsense web UI.
2. **Go to Local Tab:** Click on the "Interfaces" tab.
3. **Add New Instance:** Click the "+" button to create a new WireGuard server instance.
4. **Enable the server** Ensure that the "Enabled" checkbox is checked.
5. **Name the Server:** Enter a descriptive "Name" for your WireGuard server instance (e.g., "HomeVPN").
6. **Generate Keys:** Click the gear icon next to the "Public key" field to automatically generate a public/private key pair for the server.
7. **Set Listen Port:** Enter "51820" into the "Listen Port" field. *It's necessary to specify even if you are using the default.*
8. ***Set MTU:*** *1420 (default) or 1412 if you use PPPoE; it's 80 bytes less than your WAN MTU*
9. **Set Tunnel Address:** Enter a private network address for the WireGuard tunnel interface (e.g., 10.10.10.1/24).

Note: Leave the DNS Server field blank to avoid interfering with OPNsense DNS settings. The Peers field blank as we will come back to this later.

Warning: This address range must not conflict with other networks used on your home network or any network you might connect from. For example, if your home network is 192.168.1.0/24, and your remote network is 10.0.0.0/24 your WireGuard network should be something different such as 10.10.10.0/24.

10. **Leave Peers field blank:** For initial setup, you must leave this blank as no peers have been created. It is **critical** to return and select peer(s) once created.
11. **Save the Settings:** Click the "Save" button.

*Figure A-3: **WireGuard Server Configuration (Suggested)***



II. Generate the Configuration for a New Peer (Client)

1. **Go to Peer Generator:** Click on the "Peer generator" tab within the "VPN > WireGuard" page.
2. **Select Instance:** Select the proper “Instance” for this peer. This will default to the instance you created earlier.
3. **Set Endpoint:** In the “Endpoint” field enter your external DNS FQDN followed by the port you specified in step 7, for example wg.homenetworkguy.com:51820.

Note: If you do not enter an endpoint, the configuration will not work.

4. **Name the Peer:** Enter a “Name” for the peer (e.g., User1).

5. **Peer IP address:** You can use the IP provided by the generator or a different IP within your subnet.
6. **Allowed IPs:** You may leave this with the default value of 0.0.0.0/0,::/0. *This will tunnel all traffic over the VPN*.
7. **DNS Servers:** Set the “DNS Servers” option to the IP address of the WireGuard interface you setup earlier, in this example 10.10.10.1.
8. **Copy/Scan the Peer Configuration:**
    - **For mobile clients:** Use the QR code (it's located below the generated config) to easily set up the connection on mobile devices.
    - **For other clients:** Copy the text-based configuration into the appropriate client's configuration file.

III. Configure the WireGuard Client (iOS Example)

This example demonstrates setting up WireGuard on iOS but will be similar for Android and other systems

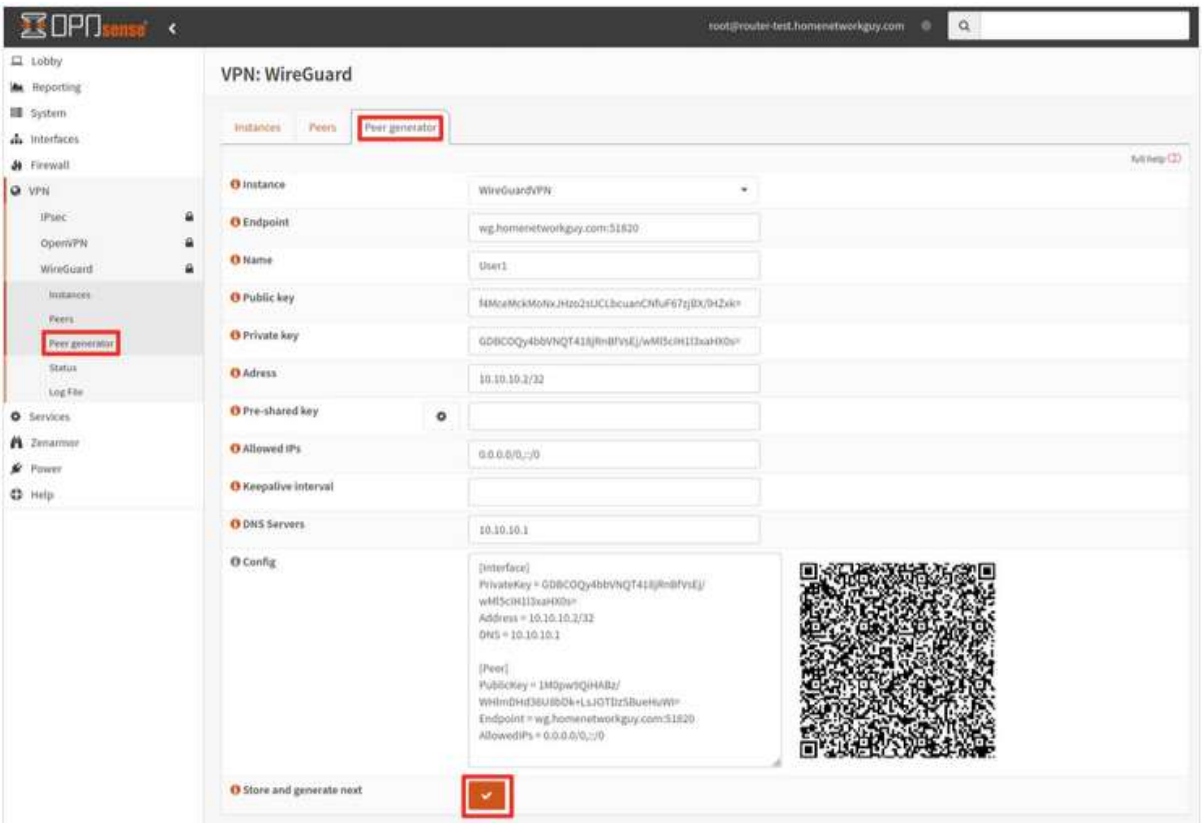
1. **Install WireGuard App:** Download the official WireGuard app from the app store.
2. **Add New Tunnel:** Open the WireGuard app, and press the "Add a tunnel" (+) button.

Figure 4: Adding a new tunnel on iOS (Suggested)
[Insert a screenshot from the wireguard iOS app showing the add tunnel button highlighted.]

3. **Create From QR Code:** Choose "Create from QR code".
4. **Scan QR Code:** Scan the QR code generated in the OPNsense interface.
5. **Name the Tunnel:** Enter a name for the connection and click “Save” (e.g., "Home VPN").

IV. Save the Peer Configuration (OPNsense)

1. **Save Peer:** After configuring your first client device, click the checkmark icon next to the peer settings to save the changes.



ADD FIGURE

V. Enable the WireGuard Server

1. **Go back to Instances:** Go to the “VPN > WireGuard > Instances” page.
2. **Enable Server:** Enable the WireGuard Server instance by clicking the “Enable WireGuard” checkbox and click "Apply" to save the changes.

VI. Assign the WireGuard Interface (Recommended)

1. **Go to Interfaces:** Navigate to "Interfaces > Assignments."
2. **Assign Interface:** In the 'Device' dropdown menu, select the wg0 interface.
3. **Add Description:** Enter a "Description" for the interface (e.g., "WG").
4. **Click Add:** Click the "Add" button to add the interface.
5. **Go to Interface Settings:** Go to "Interfaces > [Your WG Interface Name]" (e.g., Interfaces > WG).
6. **Enable Interface:** Check "Enable Interface" and "Prevent Interface Removal" checkboxes.
7. **Save Changes:** Click the "Save" button.

VII. Add the WAN Firewall Rule

1. **Go to WAN Rules:** Navigate to "Firewall > Rules > WAN" page.
2. **Add New Rule:** Click the "+" button to add a new rule.
3. **Set Action and Protocol:**

- Action: "Pass"
- Protocol: "UDP"

4. **Set Source**: “any”
5. **Set Destination:** “WAN address”
6. **Set Destination Port:** Enter “other” and specify the same listen port you setup in step 7. (51820 if using default)
7. **Description:** Add a descriptive "Description" (e.g., "Allow WireGuard access").
8. **Save Rule:** Click the "Save" button.

VIII. Add the Outbound NAT Rule (If Not Creating WireGuard Interface)

*This step is required only if you choose not to create a WireGuard Interface, which is **not recommended**.*

1. **Go to Outbound NAT:** Navigate to "Firewall > NAT > Outbound NAT."
2. **Change Mode** Set the mode to "Hybrid outbound NAT rule generation” or “Manual outbound NAT rule generation”.
3. **Add New Rule:** Click "+" in the "Manual rules" section to add a new NAT rule.
4. **Set Interface:** Set the "Interface" to "WAN".
5. **Set Protocol:** Set the protocol to “any”.
6. **Set Source Address:** Set “Source address” to “WireGuard (Group) net”.
7. **Set Translation/Target:** Set “Translation/target” to “interface address”.
8. **Save Rule:** Click "Save".

IX. Firewall Rules to Access Internal Network(s)/Internet

1. **Go to WG Interface Rules:** Navigate to "Firewall > Rules > [Your WireGuard Interface Name]" (e.g., "Firewall > Rules > WG").
2. **Add a Rule for DNS Access:**

- Action: “Pass”
  * Interface: "WG"
  * Protocol: "TCP/UDP"
  * Source: "WG net"
  * Destination: "WG address"
  * Destination Port: "DNS (53)"
- Description: Allow access to the WG DNS Server

1. **Add a rule blocking Private networks.**
   - Action: “Pass”
   - Interface: "WG"
   - Protocol: “any”

- Source: "WG net"
- Destination / Invert: Checked
- Destination: “PrivateNetworks” Alias.

Note: You must create an alias that includes 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16 to include all private networks.

- Description: Allow access to the Internet and block access to all local networks.

*Table C-16: **Firewall Rules for WireGuard Interface***

OPTION	VALUE
ACTION	Pass
INTERFACE	WG
TCP/IP VERSION	IPv4
PROTOCOL	TCP/UDP
SOURCE	WG net
SOURCE PORT	any
DESTINATION	WG address
DESTINATION PORT	DNS (53)
DESCRIPTION	Allow access to the WG DNS server
OPTION	Value
ACTION	Pass
INTERFACE	WG
TCP/IP VERSION	IPv4
PROTOCOL	any
SOURCE	WG net
SOURCE PORT	any
DESTINATION / INVERT	checked
DESTINATION	PrivateNetworks
DESCRIPTION	Allow access to Internet and block access to all local networks

X. Connect to the WireGuard VPN

1. **Activate Connection:** On your mobile device, activate the WireGuard connection you created.
2. **Monitor Status:** In OPNsense, go to "VPN > WireGuard > Status." You should see an active connection with information about the connected peer.

Figure 11: Status Page of the WireGuard Server (Suggested)
[Insert a screenshot of the status page with connected peers showing, and other key details.]

XI. (Optional) Add ACL for Unbound DNS

If you are using Unbound DNS in OPNsense as the primary DNS resolver for your WireGuard clients, and are experiencing issues try this step.

1. **Go to Unbound DNS Settings:** Navigate to "Services > Unbound DNS > Access Lists".
2. **Add New Network:** Click “Add” and add the wireguard network you created earlier such as 10.10.10.1/24.

3. **Restart Unbound DNS** Go to the "Services > Unbound DNS > General" page and click "restart."

Conclusion

Congratulations! You have successfully set up a WireGuard VPN server on OPNsense, allowing you to securely access your home network remotely. Remember to tailor the firewall rules based on your specific network needs. WireGuard simplifies the setup experience for high performance VPN connectivity.