OPNsense as a 44Net router/firewall

Mark Phillips, NI2O 07/2024 V1.1

Contents

Abstract

The aim of this document is to walk the reader through the steps necessary to connect their OPNsense router/firewall to the 44Net Wireguard VPN service.

Assumptions

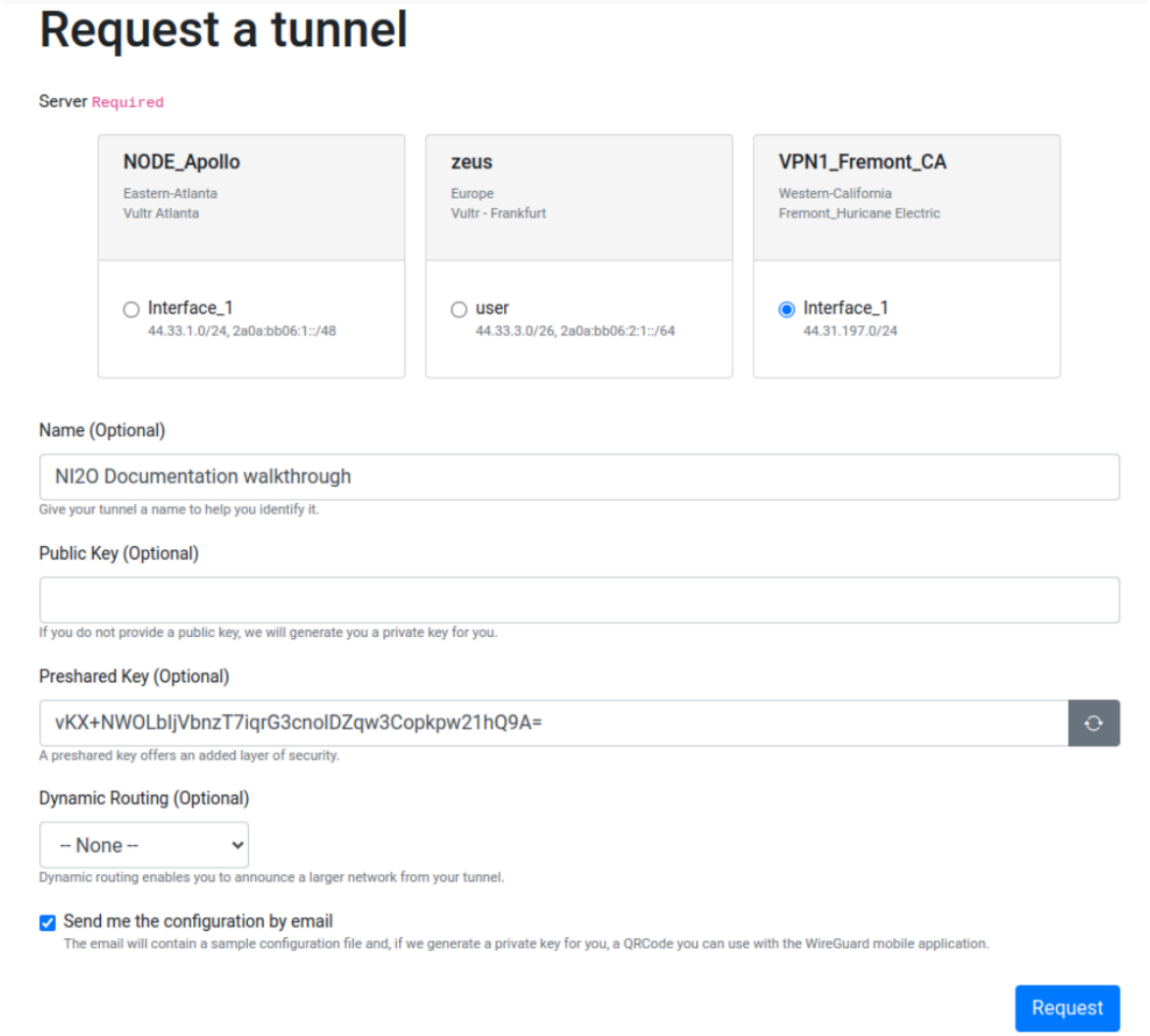
A functioning OPNsense firewall with all the current patches and updates with at least 2 network ports is already installed. Familiarity with the OPNsense user interface.

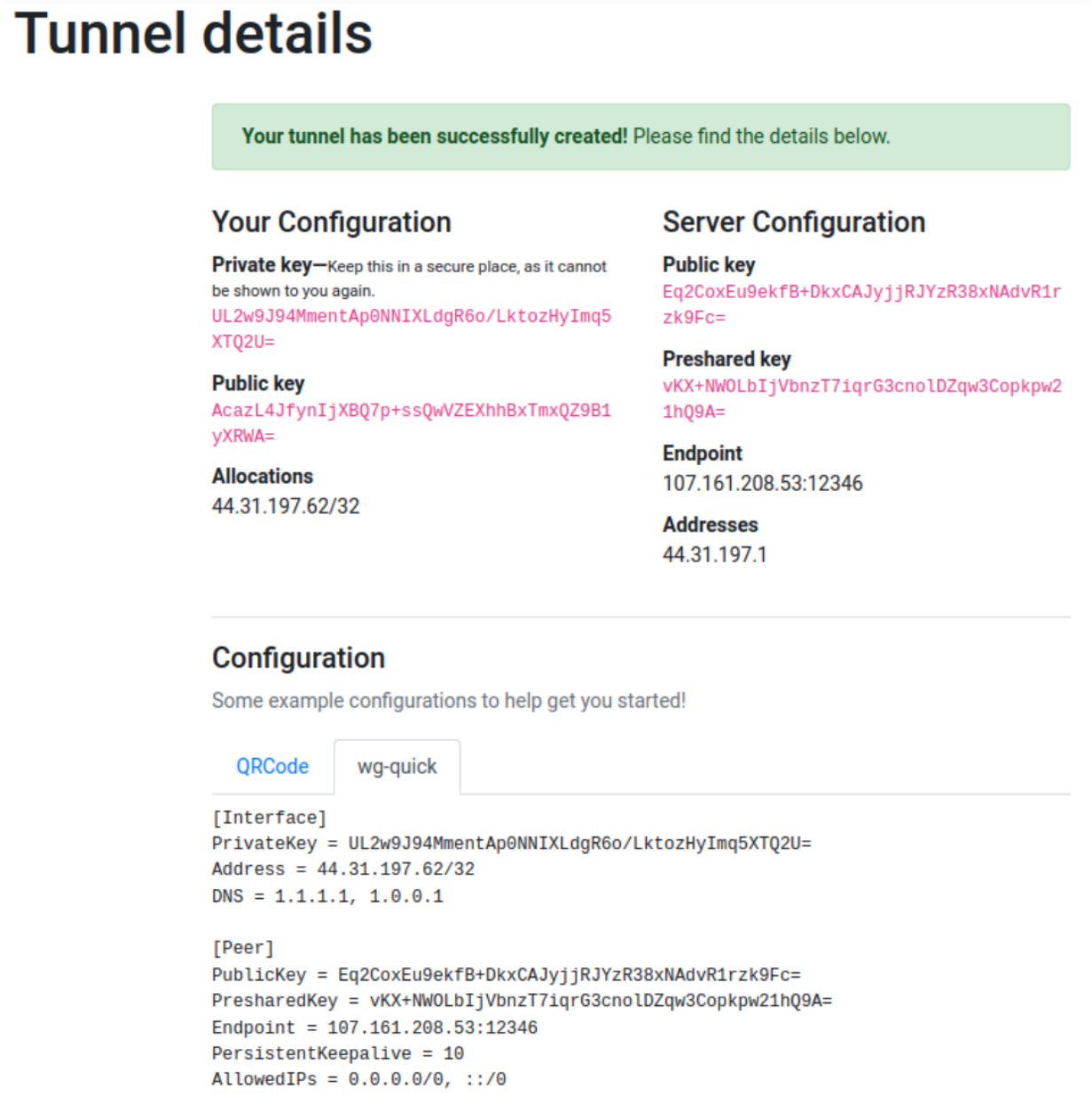
Requirements

44Net Wireguard VPN credentials
44Net subnet allocation (optional)

Obtain a POP account

Create a POP access account at https://pop.44net.cloud. Then request a tunnel. Ensure to click the refresh button at the end of the “Preshared Key (optional)” box. A Preshared Key will ensure even greater security (Wireguard is very secure in itself).

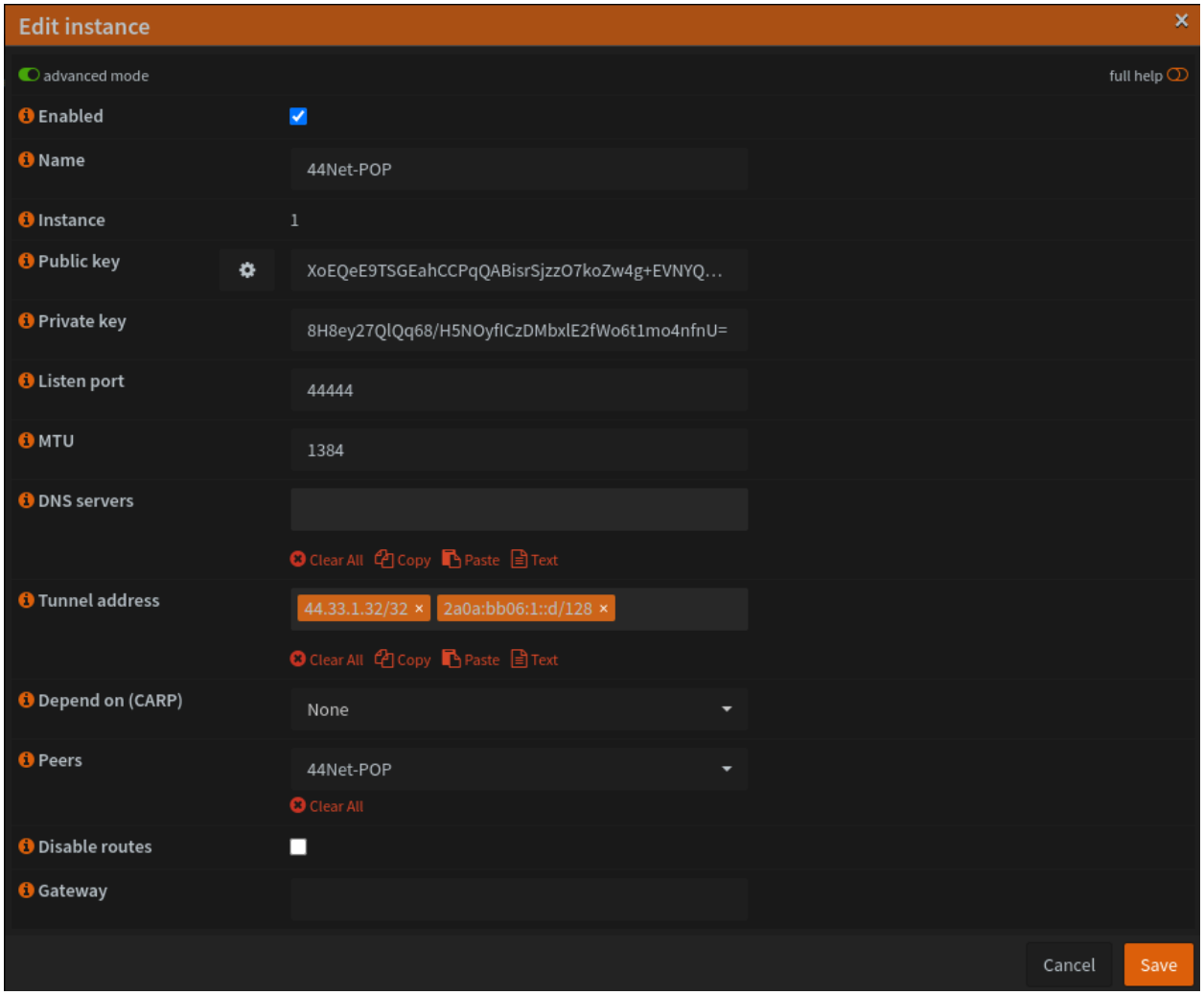




Screenshot this webpage. It contains your keys. Ensure to copy the “wg-quick” information to a text file. In a separate file record your Public and Private keys from under the “Your Configuration” heading. This information will NEVER be shown again. Keep these files for later use.

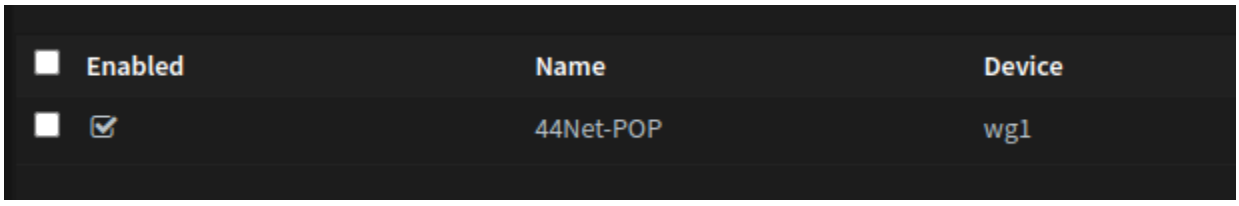
Set up the VPN

Using the left side menu system navigate to VPN > Wireguard > Instances. Click the + sign on the right side of the screen to add a new VPN Instance. Populate all the fields on this form with the information you saved from your POP account files. Ensure to populate the IPv6 information as well as the traditional IPv4



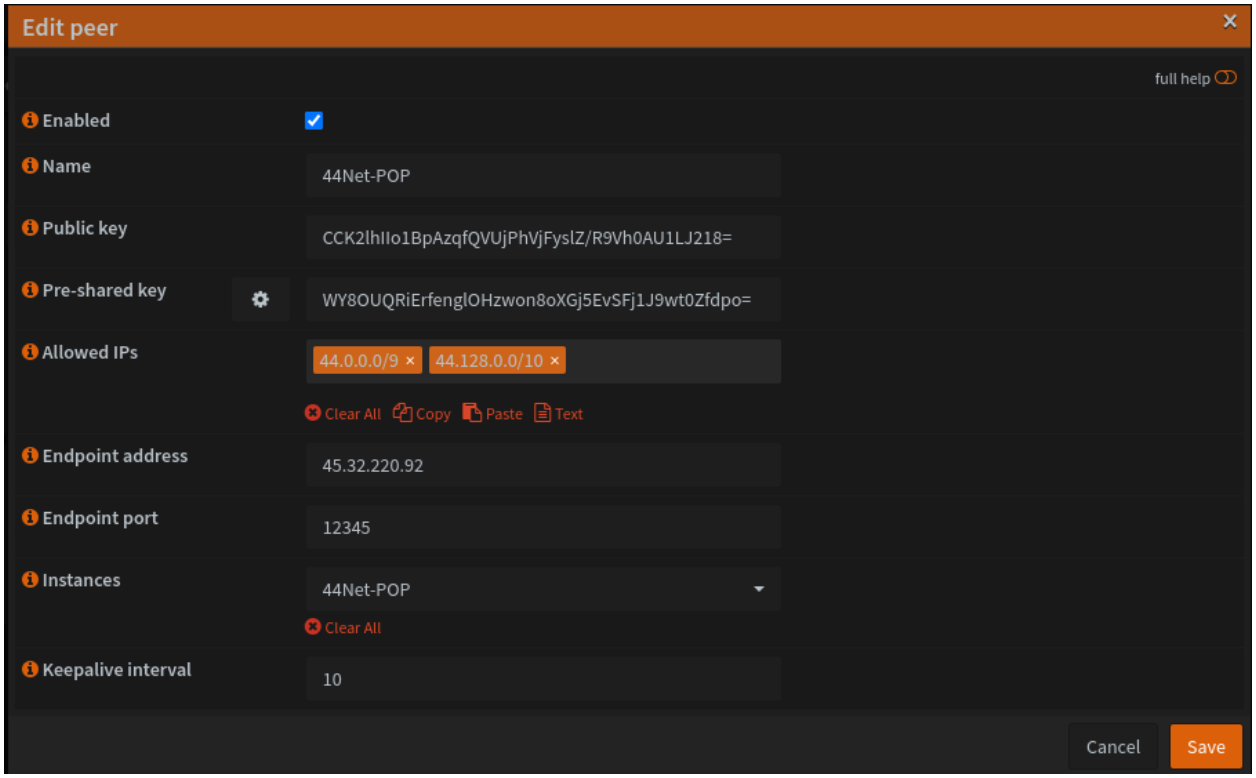
Be sure to populate the MTU field with a value of 1384. This will give you the best packet transfer over the VPN.

Click “Save” and then “enable” the instance



Move on to the “Peers” tab and click the + button over on the right.

Populate the fields with the data you saved earlier then click “Save”

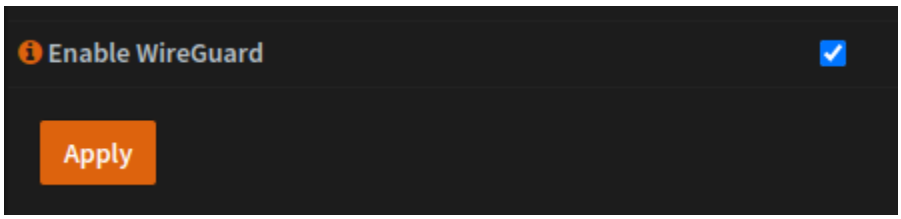


Note that in the example above the “Allowed IP’s” differ from your settings file. In this instance the VPN is only allowed to carry traffic going to and from the 44Net. If you need full Internet access (e.g. for your Echolink node) then set this field to 0.0.0.0/0 for IPv4 and ::/0 for IPv6.

Select the Instance you created just a few moments ago.

The “Keepalive Interval” setting is also important here. If you are behind a cable company router or any ISP that uses CGNAT (most cellphone and many Cable co’s) your incoming VPN session will be interrupted after a very short time. Setting the “Keepalive" does exactly what it suggests; it keeps the VPN session alive. In the example above it is set for 10 seconds. You may experiment with this setting. The longer interval you set the Keepalive for the more secure your system will be (see the Wireguard documentation for an explanation of how traffic passes for this VPN method).

Finally, click the “Enable WireGuard” box and click “Apply”.

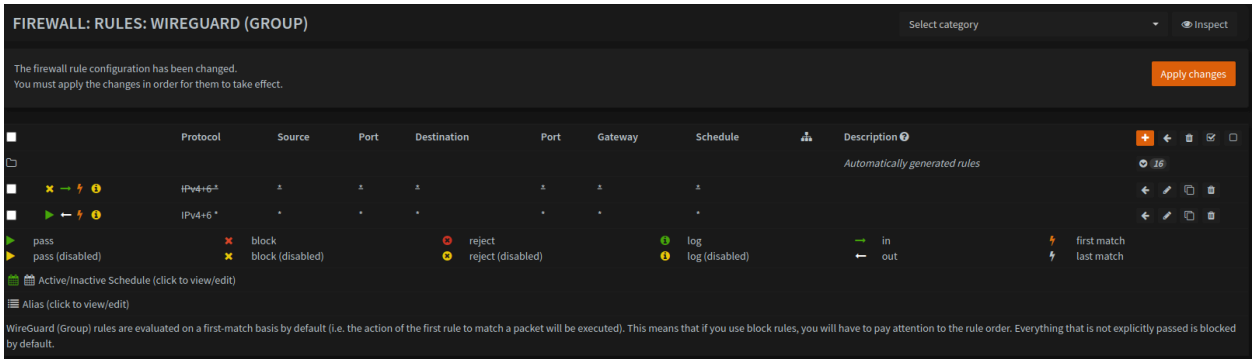


Firewall rules

We need firewall rules so as to allow our traffic to flow out to the 44Net and prevent bad traffic coming in from the 44Net (its an Internet network so safe sex rules apply!).

If you are simply connecting to the 44Net to access its services then your firewall rules will be simple: “deny” incoming and “allow” outgoing.

From the left side menu select Firewall > Rules > Wireguard (group) and then click the + button on the right to enter a new rule



In the above example we have created a “deny” rule for incoming traffic and an “allow” rule for outgoing traffic. The deny rule is set to “block” incoming traffic rather than reject it. Again, this is a security feature. By “rejecting” traffic we confirm that there is in fact a server/service available to the incoming hacker. “Blocking” the traffic means that we quietly drop the data we don’t want without responding to the sender. They will never know if there is in fact a service to connect to or not.

Finally “Apply” the changes.

Test the VPN

A simple test would be to ping a 44net address from your connected workstation. Try 44.1.1.17 (portal.ampr.org). To check that you are in fact going out over the VPN, perform a traceroute or MTR to any 44Net IP address (44.1.1.17 again?). Note that your first few hops should be 44Net addresses.