3. VPN Setup (Wireguard)

Source: Home Network Guy

In this tutorial we will setup a wireguard VPN connection on top of the OPNsense home network that we just created. This is most often what I do straight away after an installation. Since, this makes sure you can connect to the network remotely. It is extremely simple, since OPNsense already comes with three different VPN integrations that can be used straight away. Note here! You can only use a VPN if you have a public facing IP address. If you do not have this (behind CGNAT) then have a look at Mesh VPN's! Do know that if you don't have a public facing IP address you cannot host any public available services. Therefore, always try to get a public IP address from your ISP.

- 1. Wireguard Instance Creation
- 2. Peer Generator
- 3. Enable VPN Interface
- 4. Setup VPN Firewall Rules

1. Wireguard Instance Creation



In this tutorial we will setup a Wireguard VPN Instance which will allow you to connect to your local network remotely. That means you can connect to it from any place in this world as if you were at home. This is extremely secure as well since it will use public private key cryptography. The mathematics does not matter here now, but the point is that you can only access your home network if you have a key that nobody else has. This is different if you would expose your home network or services to the public internet since then anyone could access your public facing services (at least the login screens, which is a security vulnerability)

1. First we will create a new Wireguard instance. Go to your OPNsense Dashboard and go to VPN > Wireguard > Instances > + Add

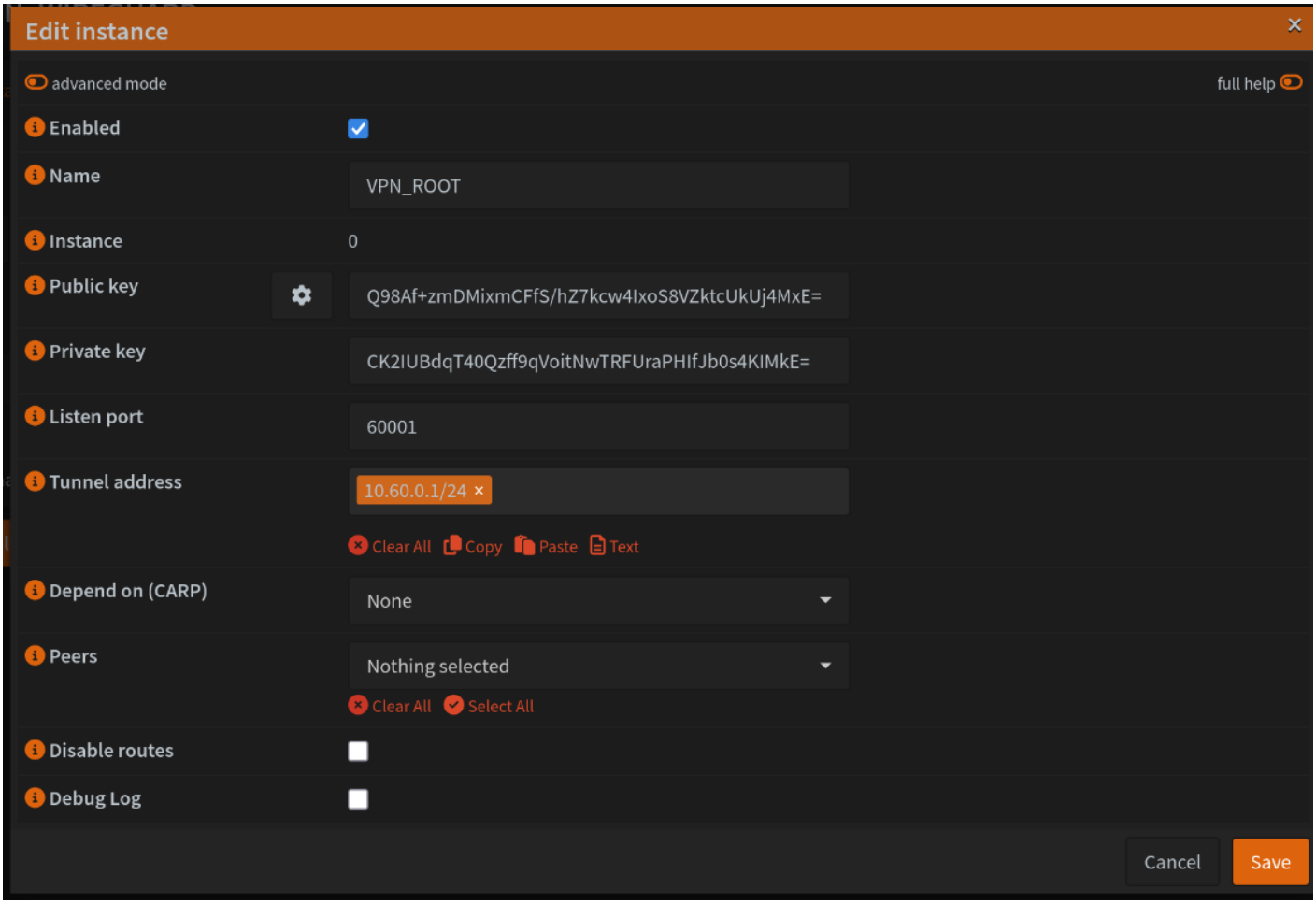
2. Provide it a name that is related to the VLAN you want to connect your Wireguard. In the case of root access I would leave it to VPN_ROOT.

3. Generate a Public and Private key by hitting the wheel button

4. Choose a listen port: Make sure you give each instance a different listening port. I would recommend to choose a port different from the default port 51820 since this port is often blocked by other networks you connect to.

5. Tunnel address: This will be a virtual network address given to your Wireguard instance. Its function exist for encryption, authentication and routing purposes. You and other peers will connect to this network. Hence, this is not the VLAN you want to connect to. We will do that later. I would recommend to choose the same 4 numbers that are in the port number. For instance if the port is 45891 then you could choose the IP address 10.45.89.1/24.

6. Then leave the other options untouched. This results then in something looking like this



7. Sweet! Then hit save and your instance is setup ;)

8. Then the most important step !! Don't forget to enable the Wireguard instance when you are done by hitting apply !! Check the box

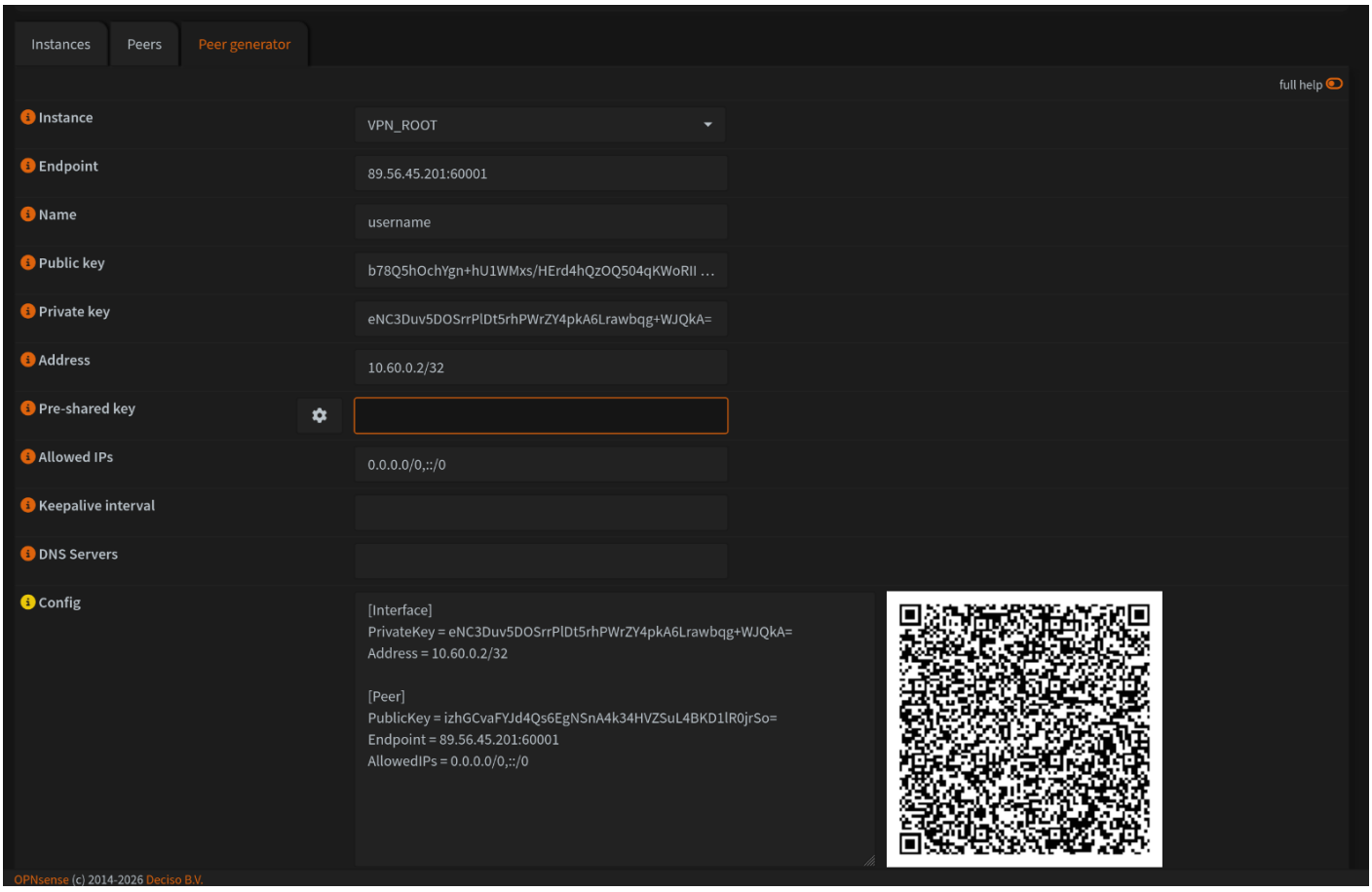
☑ Enable Wireguard

2. Peer Generator

Okey now you have setup your Wireguard Instance. Then now it is time to create a peer that can connect to the created instance. OPNSense makes this extremely simple.

1. Just go to VPN > Wireguard > Peer Generator

2. Endpoint: This is the public IP address of your network. In the case of a static Subnet you can choose any of the IPv4 addresses in your subnet. However, if you have not configured all of them yet then I would recommend to use the first IP address hat defines your subnet. Finally, you make sure the Endpoint includes the listening port defined in your WIreguard Instance.



3. Now, what I would recommend if everything is correct before saving is to make a screenshot of the QR code s.t you can easily use it with the Wireguard app on your phone for instance. Next, also copy the config file details into a text document and save it as *name_location.conf*. I specify here **name_location** s.t you can distinguish between multiple VPN's.

4. Perfect, if that is all done you can hit Save and your peer is saved !

5. Now, we are not done yet! Your instance and peer might be created but we still need to setup the VPN interface and configure the firewall rules to make this all work. This is what we will do in

the next pages ;)

3. Enable VPN Interface

Now, that you have setup your Wireguard instance and peer it is time to enable the VPN interface.

1. Go to Interfaces > Assignments > Device drop down menu > Select wgo (Wireguard - VPN_ROOT) and add it as a new interface

2. Then click on the newly created VPN interface and simply check the box

   ☑ Enable Interface

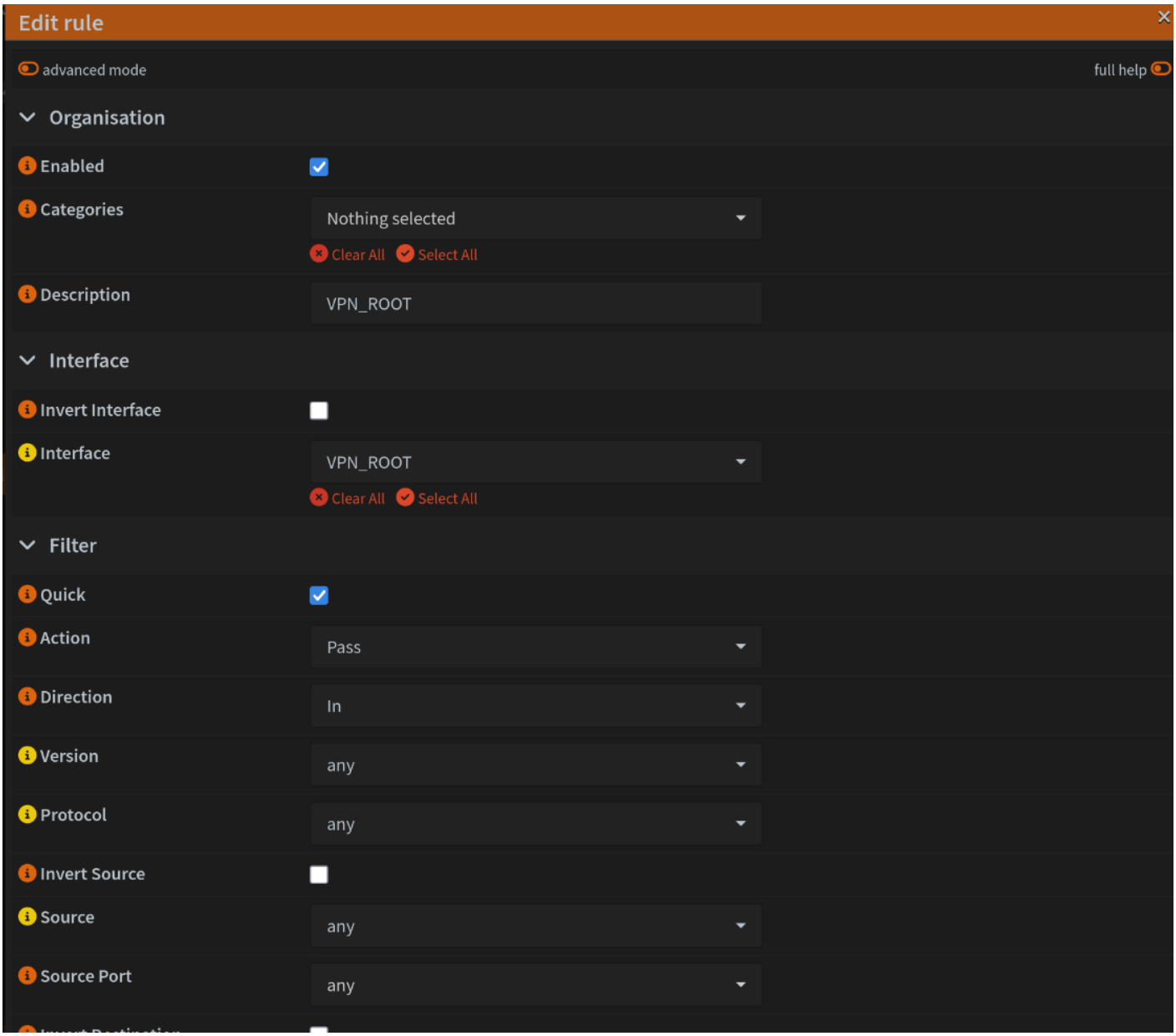
3. Then Hit Save and Apply changes at the right top corner !

4. Let's go almost there. Now we still need to setup the firewall rules for this VPN connection

4. Setup VPN Firewall Rules

We are almost there! The last thing we need to do is setup the correct firewall rules. Now, since you will create a root VPN you want this user to have access to all the different networks. Hence, the rules will be pretty simple.

1. Go to Firewall > Rules [New] > +Add
2. Then make sure you give it a proper Description name such as VPN_ROOT
3. Finally check that all passing rules are set to "any"

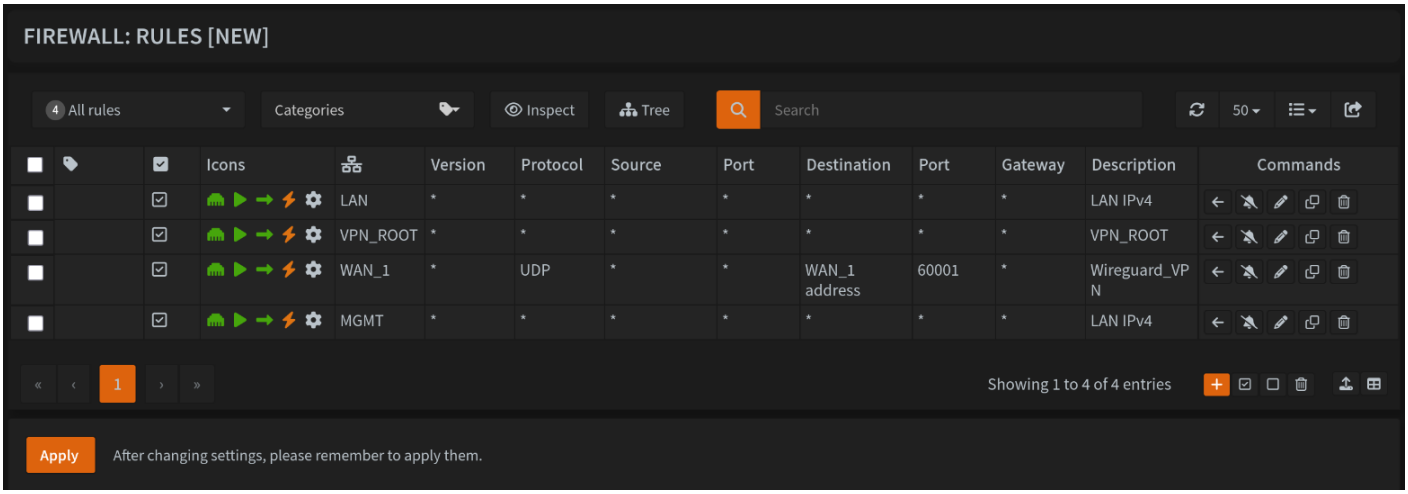


4. Perfect then save your configuration and apply the changes.

5. Now after setting up the allow all access to the VPN_ROOT the final rule that you need to apply is to allow your WAN_1 port to be accessible over the Wireguard PORT you have set in the Wireguard Instance creation. Wireguard only needs UPD access and hence in Protocols you can choose UDP instead of any.

6. For the destination you will choose the WAN_1 address and not the WAN_1 network since that would provide permissions that are not necessary in this simple case.

7. If all done right the firewall rules should look something like this



8. Now, your VPN should be working for your peer. Test it out by using the Wireguard app on your phone and or in Linux there is a VPN option where you can upload the name_location.conf file saved in the Peer generation step.

9. If for some reasons it does not work yet try to enable and disable Wireguard!

10. Congratzzz you made it to the end and hopefully you can now access your home network from any place in the world like you would be home.