

---

## Bypassing a CGNAT with Wireguard

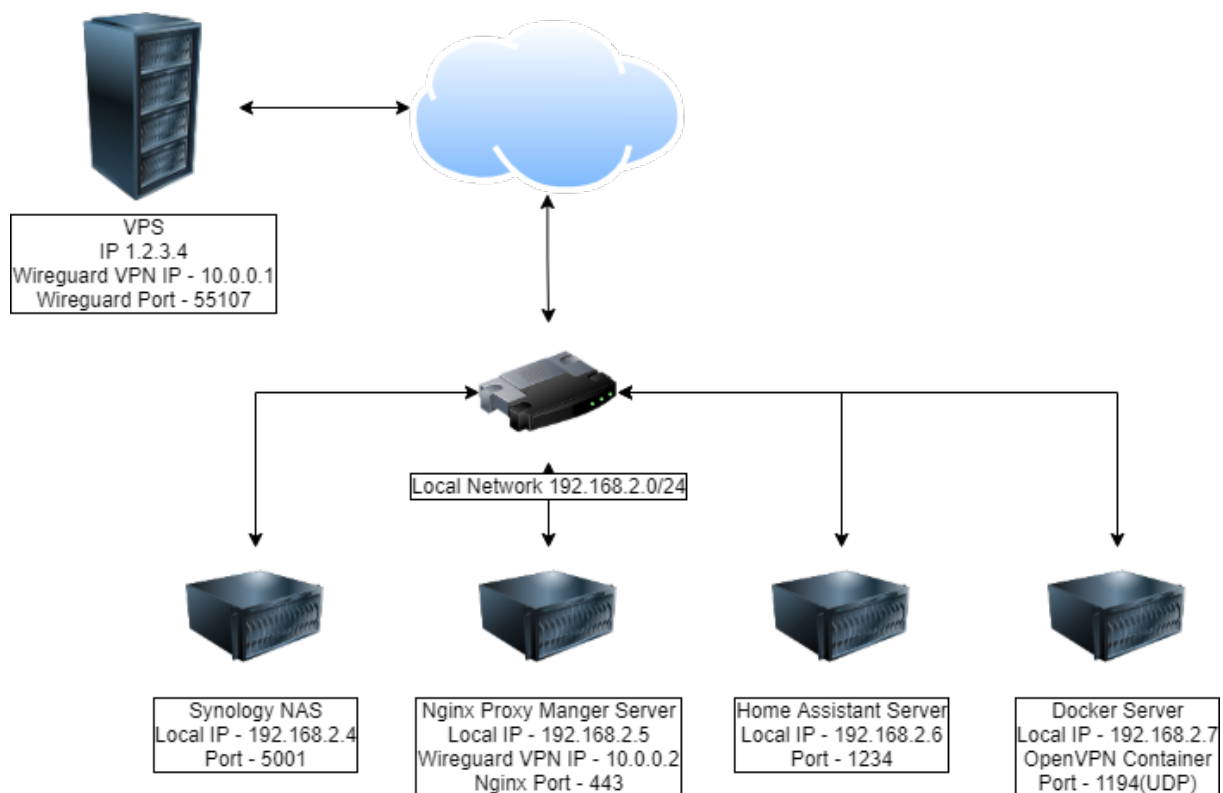
### Overview

Before switching ISPs, I had a public IP that allowed me to use port forwarding on my router to pass traffic to services hosted on my internal network. My new ISP uses a CGNAT, so I had to find a workaround. I chose this path, because it keeps pretty much everything the same for my services. The main things I wanted to do with my setup were: \* Forward only specific traffic from the internet to my services \* Provide my NPM (Nginx Proxy Manager) Server with clients real IPs (for fail2ban blocking purposes) \* Allow for traffic to flow to internal services that NPM doesn't manage

I went through a couple configurations and VPS providers before I created this solution. Prior to attempting this, I had little to no knowledge about VPS providers, wireguard, ufw, and iptables. Getting it to work the way I wanted took a few days of research, trial, and error. This will hopefully be a useful tutorial for people who are in a similar situation.

This tutorial assumes you have some basic knowledge about how to use Ubuntu from the command line.

Here is a basic diagram of my configuration. The IPs and ports will need to be changed by you to meet your requirements.



---

### Tested with:

- Digital Ocean ([link](#))
- Oracle Cloud ([link](#))
- AWS Lightsail ([link](#))

**If this is something you would like to try out, please go to the wiki section to start the tutorial.**

### Other ways to bypass a CGNAT

Wireguard Installer for Gaming - Can be used to bypass a CGNAT so you can have a **Full Clone NAT**

Cloudflared Tunnels

BoringProxy

ZeroTier ([u/RedKyet's Tutorial](#))

Awesome-Tunnel - List of many open/closed source tunneling solutions.