

# My Gear

- [The Hardware List](#)
- [The Software Stack](#)
- [Network Layout](#)

# The Hardware List

The main tools I have available for my Home lab are listed below:

1. A Prebuilt Desktop (Keep)
2. HP mini PC (Keep) - DMZ services and Media streaming.
3. Qnap SSD Nas (Keep)
4. Synology DS723 (Keep - for Now)
5. Synology J223 (Sell)
6. Terramaster Nas (Keep) - Back-up - Move to parents house for offsite back-up
7. N100 Mini PC (Keep for media TV)
8. Thinclient (OPNsense) (Keep)
9. Omada Switch (Sell 1 and Keep 1)
10. Alogic Monitor (Keep)
11. Logitech Keyboard (keep)
12. Sit stand Desk (Keep)
13. 2 UPS (Keep)
14. Multiple other keyboards - Sell

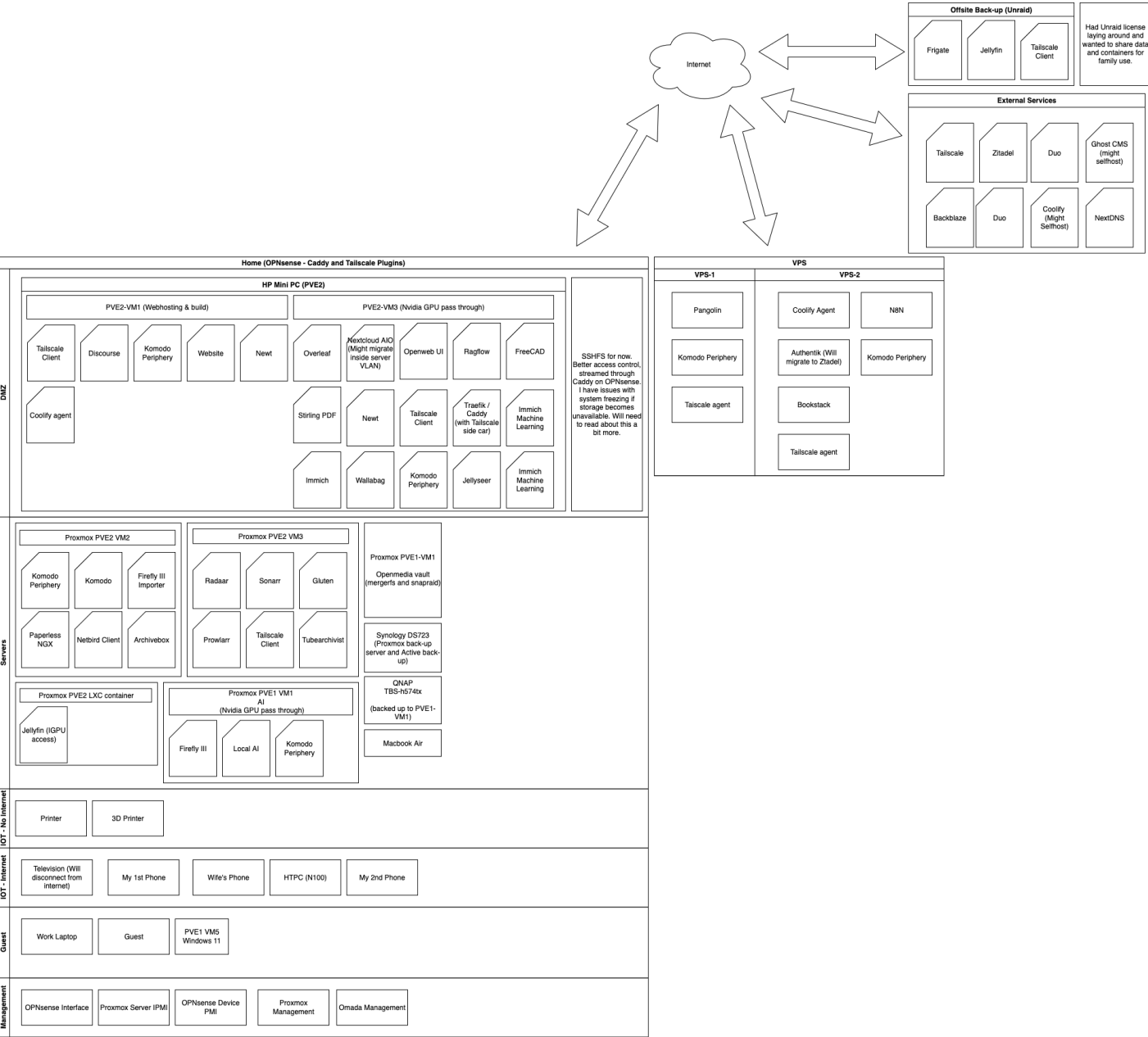
I think I have too many random devices that I don't use. I will be selling some of my stuff to streamline everything. I think of my VPS servers as an extension of my home lab. I have 2 Hetzner that VPS that I use for Pangolin, Coolify and Discord.

# The Software Stack

1. Promox (ZFS) for primary NAS
2. QNAS SSD Nas - QutsHero (might swap out for Truenas)
3. Synology DSM (was great, but they are acting like entitled pricks nowadays. Planning to sell one of my synology device. Will keep one for active back-up) - Don't recommend anyone buying this unless you need something specific from Synology.
4. Davinci Resolve for Video Editing
5. Plasticity and FreeCad for CAD drawing
6. Sublime text and VScode for Text editor and programming. (Used Emacs a lot. Keeping it on hold temporarily until I get my head around other topics I want to learn. This seems to be eating up my time),
7. Unraid - Archival and back-up (Tailscale integration appears to be really good).
8. Pangolin
9. Authentik
10. Netbird
11. ntfy
12. Ghost CMS
13. Discourse
14. Regflow
15. n8n
16. Bookstack
- 17.

# Network Layout

This is an article discussing my network configuration and services I run in my home. I have also attempted to show the network segmentation and the services I run in my homelab. I need to figure out routing of storage to the servers in DMZ. Jellyfin and Media stack is only accessible using Tailscale outside. The access controls for media stack is managed using Tailscale ACLs. This helps with difficulty in configuring SSO in Jellyfin, and also secure access outside my LAN for my family. Jellyfin and Other media tools are available inside my Lan network using Caddy module in OPNsense. All the containers hosted inside the DMZ is also accessible using OPNsense Caddy. This results in insecure traffic in DMZ. I need to decide if I need the VMS isolated using firewalls from each other in the DMZ and if I want independent Caddy/Traefik instances inside all the DMZ VMs.



I use my Qnap TBS-h574tx thunderbolt connection to have a fast network storage available on my Macbook (I have been having some issues with thunderbolt connection. Might migrate to connecting using RJ45). I also use it to share internet with the device. The data on the Qnap is backed up using rsync to the Open Media Vault server. The open media vault server is then backed up to the offsite Unraid server for archival. Some important documents/items are backed up using Duplicacy to Backblaze B2.

Plan:

- ☐ Learn Docker
- ☐ Learn IPTables
- ☐ Learn Traefik
- ☐ Learn Nginx
- ☐ Learn Docker Swarm
- ☐ Learn Ansible
- ☐ Learn OpenTofu