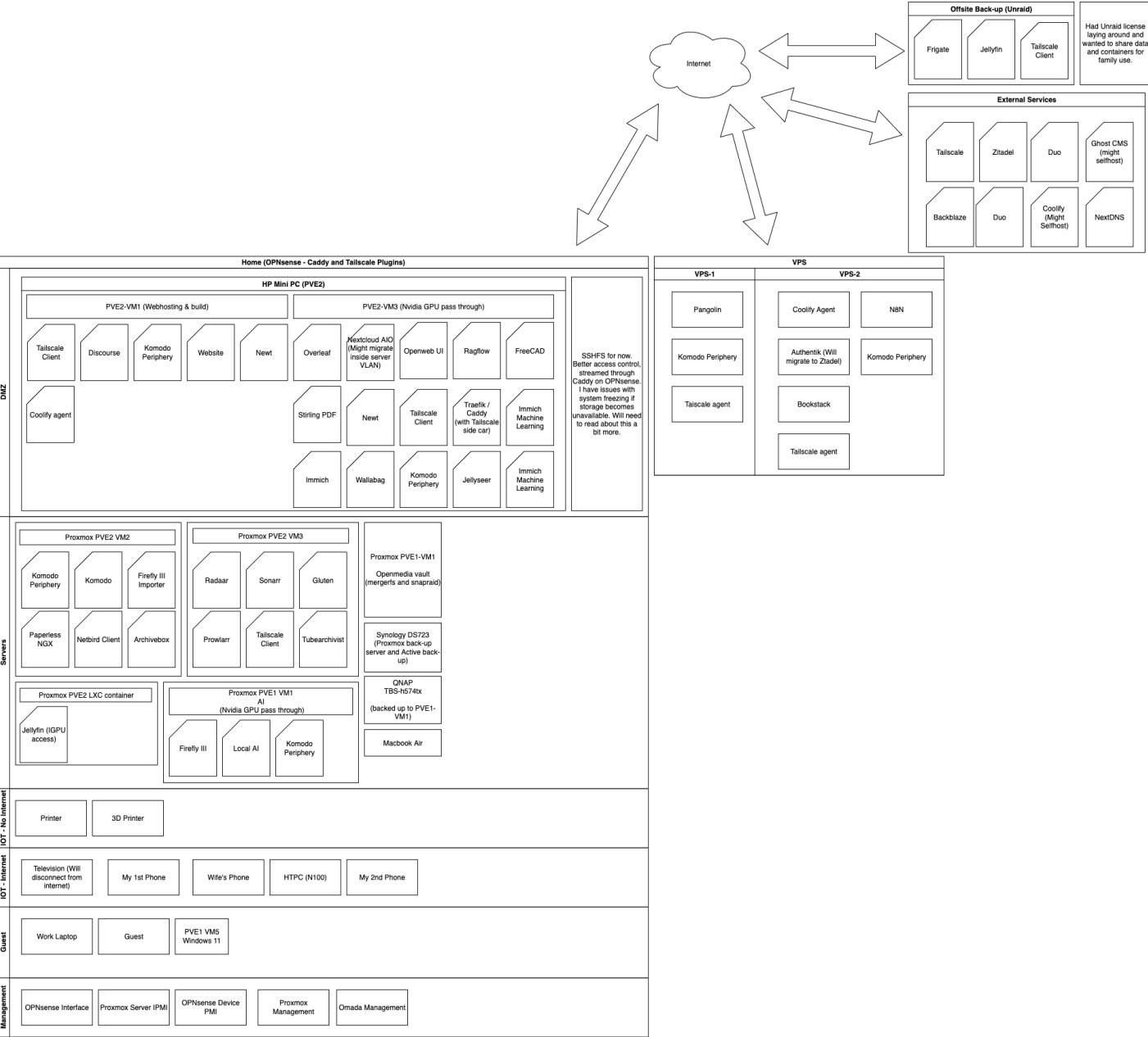


Network Layout

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

Revision #41

Created 1 July 2025 15:02:50 by Alen Alex Ninan

Updated 4 July 2025 10:36:14 by Alen Alex Ninan