

LAN Layout & Gateway

LAN Layout & Gateway

☐☐ Internet Edge

- **ISP:** AT&T Fiber (1Gbps Up/Down)
- **Gateway/ONT:** HUMAX BGW320-500 (Located in Sunroom)
- **Mode:** Bridge/Pass-through mode enabled (February 2026 upgrade)

☐☐ Core Routing (Server Closet)

- **Device:** Protectli FW2B (Pluto)
- **OS:** Ubuntu 24.04 LTS (ZFS on Root)
- **Role:** Primary Gateway & Firewall (Replacing opnSense architecture)
- **Internal LAN:** 192.168.13.0/24 (Native), 10.13.x.y (VLANs - Deploying)

Core Services

- **Firewall:** nftables (v2 production Ruleset active)
- **DHCP:** Technitium DHCP (192.168.13.0/24 scope active)
- **DNS:** Technitium DNS (DNS-over-TLS enabled via Cloudflare/Google)
- **Identity:** JumpCloud (Fully configured on Pluto for identity management)
- **Monitoring:** Beszel-agent + Vector (Shipping to ClickHouse)
- **Backup:** Syncoïd/Sanoid (OS snapshots and replication to Luna)
- **VPN:** WireGuard (Pluto Gateway + MacBook Client - Deployed March 18, 2026)

☐☐ Physical Switching & Wireless

- **Switch:** 24-port Gigabit Managed Switch with 12x PoE+ ports.

- **AP:** 2x Grandstream Mesh Access Points (PoE powered).
- **Update (Feb 26, 2026):** Backbone migration to the new Ubuntu-based routing on Pluto is complete. Network is stable on 192.168.13.x.

☐ Security Updates (March 19, 2026)

- **WireGuard:** Tunnel configured for `pluto` and Macbook client; nftables updated for tunnel traffic.
- **Fail2Ban:**
 - Refined `default` and `SSH` jail configs.
 - Added **Recidive** jail (repeat offenders).
 - Added **Portscan** detection jail.
- **Edge Hardening:**
 - **Port Closures:** Removed Minecraft Bedrock (19132) and Bittorrent (52341) forwards.
 - **Rate Limiting:** Enabled `nftables` rate-limiting for Minecraft Java (25565), Voice Chat (24454), and CoTurn (3478).
 - **Geo-blocking:** Implemented automated `nftables` blocklist (CN, KP, RU, IR) via `systemd` timer + lookup sets.

Revision #6

Created 2026-02-09 14:40:42 UTC by Chris

Updated 2026-03-19 02:16:54 UTC by Flobot