Project Overview

The goal was to create a secure VPN tunnel that allows a remote Windows laptop and a mobile device to access a local server while maintaining the ability to browse the internet.

Network Architecture

- **Public Internet** ⟶ **MTN Router (Public Internet)**
- **MTN Router (**LAN: 192.168.0.1) ⟶ **pfSense WAN** (192.168.0.143)
- **VPN Tunnel** (10.0..8.0/24) ⟶ **Local Resources** (CasaOS/Internet)

Configuration Steps

1. **External Access (MTN Router)**
   To allow the VPN traffic into my house, a **port forward** was required on the primary MTN Router:
   - **Protocol:** UDP
   - **External/Internal Port:** 1194
   - **Destination IP:** 192.168.0.143 (pfSesne WAN IP)

2. **pfSense Interface Adjustments**
   Since pfSense sits behind another router, the default “Private Network” block had to be disabled:
   - **Path:** Interfaces > WAN
   - **Settings:** Uncheck “Block private networks and loopback addresses”

3. **OpenVPN Server Settings**
   The server was configured with the following critical to ensure compatibility with mobile and Windows clients
   - **Protocol:** UDP on IPv4 only
   - **Tunnel network:** 10.0.8.0/24

- **Redirect Gateway:** Enabled (forces all traffic through VPN for secure browsing)
- **DNS Servers:** 8.8.8.8 and 1.1.1.1

4. **Firewall and Traffic Routing (NAT)**
   To enable internet browsing (outbound traffic), two specific "gates" were opened:
   - **Firewall Rule:** A "Pass" rule was added to the OpenVPN tab allowing Any protocol from Any source to Any destination
   - **Outbound NAT:** changed to Hybrid Outbound NAT mode
   - **Manual Mapping:** a rule was created to translate the 10.0.8.0/24 subnet to the WAN address

5. **Dynamic DNS Configuration (Duck DNS)**
   - **Create your DuckDNS Domain**
     - Go to DuckDNS.org and login
     - Create a unique subdomain (eg. Myhomevpn2026)
     - Note down your Token (the long string of letters/numbers on your account page)
   - **Configure pfSense to Update DuckDNs**
     This tells pfSense to "call" DUckDNS every few minutes and reports its current public IP address.
     - In pfSense, go to **Services > Dynamic DNS > Clients**
     - Click **Add**
     - **Service Type:** select Custom or DuckDNS (if available in your version)
     - **Interface to Monitor:** WAN
     - **Username:** (Leave blank for DuckDNS)
     - **Password:** paste your DuckDNS token here
     - **Hostname:** Enter your full domain (eg. Myhomevpn2026.duckdns.org)

- **Update URL:** if using ‘Custom’ enter: https://www,duckdns.org/update?domains=YOURDOMAIN&token=YOURTOKENS&io=%IP%
- **Save and click force update:** the “Cached IP” should turn green and match your public IP

6. **Updating the VPN to use the Domain**
   Now that the domain is live, you need to tell your VPN clients to look for the name instead of the number.
   - Go to VPN > OpenVPN > Client export
   - Find the Host Name Resolution setting
   - Change it to Other
   - In the text box that appears, type your DuckDNS address: myhomevpn2026.duckdns.org
   - Download the Inline Config for your phone and the Windows installer for your PC
     Benefit: You will never have to change these files again, even if MTN changes your home IP address

Client Implementation

Windows Laptop

- **Tool:** OpenVPN GUI
- **Export Type:** Windows Installer (64-bit)
- **Key fix:** Re-downloading the config after changing the server protocol from TCP to UDP (In my testing, I mistakenly placed the protocol on TCP. (So I changed it to UDP and redownloaded the config)

Mobile Phone

- **App:** OpenVPN Connect

- **Export Type:** Inline Config (.opvpn file)
- **Critical Fix:** Setting Host Name Resolution in the Client Export tool to ypur public IP or DuckDNS hostname so the phone can find the router from outside the house

Troubleshooting Summary

- **Connection but no Internet:** fixed by enabling **Redirect IPv4 Gateway** and creating **Outbound NAT**
- **Protocol Mismatch:** Resolved by ensuring the MTN Port Forward (UDP), pfSense Server (UDP), and client Config (UDP) all matched.
- **Phone Connection Issues:** Resolved by ensuring the exported config points to the public IP rather than the internal 192.168 IP

Maintenance and Security Tips

- **VirtualBox Autostart:** Ensure your pfSense VM is set to start automatically when your PC boots up so the VPN is always available.
- **Firewall Logs:** Periodically check **Status > System Logs > Firewall** to see if any unauthorized IPs are trying to “knock” on your VPN port
- **Backup:** Go to **Diagnostics > Backup and Restore** and download your current config. If your VM crashes, you can restore everything in seconds.