AI-01794 Home Assistant DuckDNS Setup

Owner	Ⓡ Rigel Arcayan
Tags	
Created time	@July 5, 2025 9:54 AM

Setting up DuckDNS with Home Assistant

This guide will walk you through the process of setting up DuckDNS for your Home Assistant instance, allowing you to access it securely from outside your home network using a custom domain name.

Prerequisites

Before you begin, ensure you have the following:

- **Home Assistant Installation:** A running Home Assistant instance (e.g., Home Assistant OS, Supervised, Container).
- **Router Access:** Administrative access to your home router to configure port forwarding.
- **DuckDNS Account:** An account created on DuckDNS.org.

Step 1: Create a DuckDNS Account and Domain

1. Go to https://www.duckdns.org/.
2. Sign in using one of the provided authentication methods (e.g., Google, GitHub, Twitter).
3. Once logged in, you will see a section to add domains.
4. In the "Domain" field, enter your desired subdomain (e.g., `myhomeassistant`).

5. Click the "add domain" button. Your full domain will be `myhomeassistant.duckdns.org`.
6. **Important:** Note down your **token** (a long string of characters) displayed at the top of the page. You will need this for the Home Assistant add-on configuration.

Step 2: Install the DuckDNS Add-on in Home Assistant

1. Open your Home Assistant interface.
2. Navigate to **Settings** > **Add-ons**.
3. Click on the **Add-on Store** button in the bottom right corner.
4. In the search bar, type `DuckDNS` and select the "Duck DNS" add-on.
5. Click the **INSTALL** button and wait for the installation to complete.

Step 3: Configure the DuckDNS Add-on

Once the add-on is installed:

1. Go to the **Configuration** tab of the Duck DNS add-on.
2. You will see a YAML configuration section. Fill it out as follows:

```
# Example configuration
domains:
  - your_chosen_subdomain.duckdns.org  # Replace with your actual Duck DNS domain
token: your_duckdns_token_here         # Replace with the token from Duck DNS.org
aliases: []
seconds: 300
log_level: info
accept_terms: true
```

- `domains`: Enter the full DuckDNS domain you created (e.g., `myhomeassistant.duckdns.org`).

- `token`: Paste the token you noted down from DuckDNS.org.
- `accept_terms`: Change this to `true`.
- `log_level`: You can leave this as `info` or change it to `debug` for more detailed logging if troubleshooting.
- `aliases` and `seconds` can usually be left as default.

3. Click **SAVE**.
4. Go back to the **Info** tab of the add-on.
5. Enable **Start on boot** and **Watchdog** (recommended for automatic restart if the add-on crashes).
6. Click **START** to run the add-on.
7. Check the **Logs** tab of the add-on to ensure it started successfully and updated your IP address with DuckDNS without errors. You should see messages indicating a successful update.

Step 4: Configure Router Port Forwarding

This is a critical step that tells your router to direct incoming traffic on specific ports to your Home Assistant device.

Important Notes:

- **Internal IP Address:** You need the internal IP address of your Home Assistant device (e.g., `192.168.1.100`). You can find this in your Home Assistant settings (Settings > System > Network) or by checking your router's connected devices list. It's highly recommended to set a **static IP address** for your Home Assistant device to prevent it from changing.
- **Router Interface:** The exact steps and terminology may vary slightly depending on your router's brand and model. Refer to your router's manual if you have trouble finding the settings.

General Steps:

1. **Access your Router's Admin Interface:**
    - Open a web browser on a device connected to your home network.

- Type your router's IP address into the address bar (common defaults are `192.168.1.1`, `192.168.0.1`, `10.0.0.1`).
- Enter your router's username and password (often found on a sticker on the router itself, or in its manual).

2. **Locate Port Forwarding Settings:**
   - Look for sections like "Port Forwarding," "NAT," "Virtual Servers," or "Firewall." These are usually found under "Advanced Settings" or "Security."
3. **Create New Port Forwarding Rules:**
   - You need to forward two standard HTTPS ports: **80 (HTTP)** and **443 (HTTPS)**. These are used for SSL certificate generation and secure web access.
   - **Rule 1: For Port 80**
     - **Service Name/Description:** `Home Assistant HTTP` or `DuckDNS HTTP`
     - **External/Public Port:** `80`
     - **Internal/Private Port:** `80`
     - **Protocol:** `TCP` (or `Both` / `TCP/UDP` if `TCP` is not an option)
     - **Internal/LAN IP Address:** Enter the **internal IP address of your Home Assistant device** (e.g., `192.168.1.100`).
     - **Enable/Save:** Make sure to enable the rule and save the settings.
   - **Rule 2: For Port 443**
     - **Service Name/Description:** `Home Assistant HTTPS` or `DuckDNS HTTPS`
     - **External/Public Port:** `443`
     - **Internal/Private Port:** `443`
     - **Protocol:** `TCP` (or `Both` / `TCP/UDP` if `TCP` is not an option)
     - **Internal/LAN IP Address:** Enter the **internal IP address of your Home Assistant device** (e.g., `192.168.1.100`).
     - **Enable/Save:** Make sure to enable the rule and save the settings.

4. **Apply/Save Changes:** After creating both rules, ensure you apply or save the changes on your router. Your router might restart.

Step 5: Update Home Assistant `configuration.yaml`

Now you need to tell Home Assistant to use SSL and your DuckDNS domain.

1. In Home Assistant, go to **Settings** > **Add-ons**.
2. Find and open the **File editor** add-on. If you don't have it, install it from the Add-on Store.
3. In the File editor, open the `configuration.yaml` file.
4. Add or modify the `http:` section as follows. Ensure your `external_url` matches your DuckDNS domain.

```
http:
  ssl_certificate: /ssl/fullchain.pem
  ssl_key: /ssl/privkey.pem
  # Replace with your actual DuckDNS domain
  external_url: https://your_chosen_subdomain.duckdns.org:8123
  # Optionally, if you want to allow local access without SSL, you can add:
  # use_x_forwarded_for: true
  # trusted_proxies:
  #   - 127.0.0.1  # Example if using Nginx Proxy Manager or similar
```

   - `ssl_certificate` and `ssl_key`: These paths are standard for the DuckDNS add-on, which handles the certificate generation using Let's Encrypt.
   - `external_url`: **Crucially**, replace `your_chosen_subdomain.duckdns.org` with your actual DuckDNS domain. The `:8123` is the default Home Assistant port.
5. Click the **SAVE** icon (floppy disk) in the File editor.

Step 6: Restart Home Assistant

For all changes to take effect, you must restart Home Assistant.

1. Go to **Settings** > **System** > **Restart**.

2. Click **RESTART HOME ASSISTANT**.

Step 7: Verification

After Home Assistant has restarted:

1. **Test from outside your network:** Try accessing your Home Assistant instance from a device *not* connected to your home Wi-Fi (e.g., using mobile data on your phone).
    - Open a web browser and type your full DuckDNS domain: `https://your_chosen_subdomain.duckdns.org:8123`
2. **Check for HTTPS:** You should see a padlock icon in your browser's address bar, indicating a secure HTTPS connection.

Troubleshooting Tips

- **Check DuckDNS Add-on Logs:** The first place to look for issues. Go to the add-on's "Logs" tab. Errors related to token, domain, or IP updates will appear here.
- **Verify Port Forwarding:** Use an online port checker tool (e.g., canyouseeme.org) to see if ports 80 and 443 are open from the internet to your public IP. If they are not, your router configuration is likely incorrect or your ISP is blocking ports.
- **Double-Check IP Address:** Ensure the internal IP address used in port forwarding is indeed your Home Assistant device's IP.
- **Firewall on Home Assistant Host:** If Home Assistant is running on a generic Linux server, ensure its local firewall (e.g., `ufw`) is not blocking ports 80 and 443.
- **ISP Restrictions:** Some ISPs block incoming connections on common ports like 80 and 443. If port forwarding is correctly configured on your router but `canyouseeme.org` shows them as closed, contact your ISP.
- **Internal Access Issues:** If you can access it externally but not internally using the DuckDNS domain, it might be a "NAT Loopback" or "Hairpinning" issue with your router. Some routers don't support this. You might need to access

Home Assistant via its internal IP address when on your home network, or set up a DNS rewrite on your router if it supports it.

By following these steps, you should have DuckDNS successfully set up for your Home Assistant, allowing secure remote access!

Troubleshoot Home Assistant DuckDNS not connecting from outside

Troubleshooting Home Assistant DuckDNS External Access
If you're still unable to connect to your Home Assistant instance from outside your network using your DuckDNS domain, let's go through a systematic troubleshooting process. This covers the most common reasons for external access failure.

1. Verify Public IP Address and DuckDNS Update
   Even with the DuckDNS add-on, it's crucial to ensure your public IP is correctly registered.

- Find Your Current Public IP:
  - From a device inside your home network, open a web browser and go to https://whatismyip.com/ or https://ipinfo.io/. Note down the IP address displayed. This is your public IP.
- Check DuckDNS Recorded IP:
  - Go to https://www.duckdns.org/ and log in.
  - Look at the "current ip" listed next to your domain.
- Compare: Do the two IP addresses match?
  - If they do NOT match: Your DuckDNS add-on is not correctly updating your IP.
    - Go to Home Assistant > Settings > Add-ons > Duck DNS.
    - Check the Logs tab thoroughly. Look for errors related to token or domain. Ensure your token and domains in the add-on configuration are exactly as they appear on the DuckDNS website.
    - Restart the DuckDNS add-on.
    - Ensure "Start on boot" and "Watchdog" are enabled for the DuckDNS add-on.

    - If they DO match: Your DuckDNS setup is working correctly, and the issue lies elsewhere, most likely with port forwarding or a firewall.

1. Re-Verify Port Forwarding (Most Common Issue)
   This is the most critical step. Even a small misconfiguration will prevent external access.

- Confirm Home Assistant's Internal IP:
    - In Home Assistant, go to Settings > System > Network. Note the "IPv4 address" of your Home Assistant instance.
    - Recommendation: If your router supports it, set a static IP reservation for your Home Assistant device based on its MAC address. This prevents its internal IP from changing, which would break port forwarding.
- Access Router Settings: Log into your router's administration page (e.g., 192.168.1.1).
- Navigate to Port Forwarding: Find the "Port Forwarding," "NAT," "Virtual Servers," or "Firewall" section.
- Verify Both Rules:
    - Rule for Port 80:
        - External/Public Port: 80
        - Internal/Private Port: 80
        - Protocol: TCP (or Both/TCP/UDP)
        - Internal IP Address: MUST be the exact internal IP of your Home Assistant device.
    - Rule for Port 443:
        - External/Public Port: 443
        - Internal/Private Port: 443
        - Protocol: TCP (or Both/TCP/UDP)
        - Internal IP Address: MUST be the exact internal IP of your Home Assistant device.

- Enable/Save: Ensure both rules are enabled and you've saved/applied the changes on your router. A router reboot might be necessary.
- Use an External Port Checker:
    - From a device outside your home network (e.g., phone on mobile data, or a friend's computer), go to https://www.canyouseeme.org/.
    - Enter 80 in the "Port to Check" field and click "Check Port."
    - Then, enter 443 and click "Check Port."
    - Expected Result: Both should show "Success" or "Open."
    - If it shows "Connection Refused" or "Timeout": Your port forwarding is not working. This is the most common reason for failure.
        - Possible causes:
            - Incorrect internal IP address in the router rule.
            - Typo in port numbers.
            - Rule not enabled/saved on the router.
            - Another device on your network is using those ports.
            - Your ISP is blocking these ports (less common, but possible).

1. Check for Double NAT
   This is a common issue if you have multiple routers or a modem/router combo from your ISP.

- What is Double NAT? It means your router is behind another router (e.g., your ISP's modem/router is acting as a router, and then your personal Wi-Fi router is also acting as a router). Each router performs Network Address Translation (NAT), which can break port forwarding.
- How to Check:
    - Log into your main router (the one directly connected to your internet line/modem).
    - Find its WAN IP address (or Internet IP address).

    - Compare this WAN IP with the public IP you found in Step 1 (whatismyip.com).
      <!-- end list →
    - If they are DIFFERENT, and the router's WAN IP is a private IP range (e.g., 192.168.x.x, 10.x.x.x, 172.16.x.x to 172.31.x.x): You likely have Double NAT.
- Solution for Double NAT:
    - Option A (Preferred): Put your ISP's modem/router into "Bridge Mode" (if it supports it). This turns it into a simple modem, and your personal router handles all routing. You'll need to consult your ISP or modem manual for this.
    - Option B: Forward the ports on both routers. First, forward ports 80 and 443 from the ISP router to the WAN IP of your personal router. Then, forward ports 80 and 443 from your personal router to the internal IP of your Home Assistant. This can be complex.

1. Home Assistant configuration.yaml Settings
   Ensure your external_url is correct and SSL settings are pointing to the right place.

- In Home Assistant, open the File editor add-on.
- Open configuration.yaml.
- Verify the http: section:
  http:
  ssl_certificate: /ssl/fullchain.pem
  ssl_key: /ssl/privkey.pem
  external_url: https://your_chosen_subdomain.duckdns.org:8123 # ← IMPORTANT!

If you're using a reverse proxy like Nginx Proxy Manager, you might have:

use_x_forwarded_for: true

trusted_proxies:

172.30.33.0/24 # Example for NPM's internal network

- external_url: Ensure this exactly matches your DuckDNS domain, including https:// and :8123. A common mistake is a typo here.
- ssl_certificate and ssl_key: These paths are standard for the DuckDNS add-on and should typically not be changed unless you're using a different SSL method.
- Save any changes and Restart Home Assistant (Settings > System > Restart).

1. Local Network Access (Hairpinning/NAT Loopback)
   If you can access Home Assistant from outside your network but not from inside your network using the DuckDNS domain, this is a "hairpinning" or "NAT loopback" issue.

- Problem: Your router doesn't correctly loop traffic back to an internal device when you try to access it using its external (public) IP or domain name from within the same network.
- Solution:
  - Option A (Simple): When on your home network, use Home Assistant's internal IP address (e.g., http://192.168.1.100:8123) or homeassistant.local:8123 to access it.
  - Option B (Advanced): If your router supports "DNS Rebinding Protection" or "DNS Host Override," you can configure it to resolve your DuckDNS domain to Home Assistant's internal IP address when queried from within your network. This is router-specific.
  - Option C (Advanced): Set up a local DNS server (e.g., AdGuard Home, Pi-Hole) on your network and configure it to resolve your DuckDNS domain to your Home Assistant's internal IP.

1. Check Home Assistant Logs Again
   After attempting any of these fixes, always check the Home Assistant logs for

new errors.

- Go to Settings > System > Logs.
- Look for any errors related to http, ssl, or network.
  By methodically going through these steps, you should be able to pinpoint where the connection is failing. The vast majority of external access issues are resolved by correctly configuring port forwarding and ensuring your public IP is updated with DuckDNS.

PLDT Fibr Port Forwarding Not Working

It sounds like you're facing a common challenge with PLDT Fibr when it comes to port forwarding. The search results confirm that the primary reason for port forwarding not working on PLDT Fibr residential plans is often Carrier-Grade NAT (CGNAT).
Here's a breakdown of the issue and the most effective solutions, building upon the existing troubleshooting guide:
Understanding CGNAT and Why it Affects Port Forwarding

- What is CGNAT? PLDT, like many ISPs, uses CGNAT to conserve IPv4 addresses. This means multiple customers share a single public IPv4 address. When you try to port forward, your router's public IP isn't truly unique to your home; it's shared. Therefore, incoming connections on a specific port cannot be reliably directed to your specific device because many users are behind the same public IP.
- Impact on Port Forwarding: If you are behind CGNAT, even if you configure port forwarding correctly on your PLDT router, it won't work for external access because the traffic never reaches your router from the internet. The deploy_challenge error you saw earlier is a strong indicator of this, as Let's Encrypt can't reach your Home Assistant to verify the domain.
  Solutions for PLDT Fibr Port Forwarding Issues
  Based on the search results, here are the main approaches to resolve this:

1. Request CGNAT Removal / Public IP from PLDT (Most Direct Solution)
   This is often the most straightforward and recommended solution.

- How to do it: Contact PLDT customer support (e.g., via their hotline, social media, or their messenger service).

- What to ask for: Request to be removed from CGNAT and be assigned a Dynamic Public IP address. Some users report that PLDT might try to push for a "Static IP" which usually comes with an additional monthly fee. A dynamic public IP is often sufficient for Home Assistant and typically comes at no extra cost for residential users, though policies can vary.
- Verification: After they confirm the change, check your router's WAN IP address (as described in "Check for Double NAT" in the troubleshooting guide). If it now matches your public IP from whatismyip.com and is not in a private IP range (like 100.64.x.x to 100.127.x.x), then you are no longer behind CGNAT.

1. Bridge Mode (If you have your own router)
   If you have your own router that you prefer to use, you can ask PLDT to put their modem/router into "Bridge Mode."

- What it does: Bridge mode turns the PLDT device into a simple modem, passing the public IP directly to your personal router. Your personal router then handles all the routing, including port forwarding.
- Considerations:
  - You'll need a capable personal router.
  - You'll still need to ensure you're not behind CGNAT (see point 1). Bridge mode alone doesn't bypass CGNAT if the public IP assigned to the bridged modem is still a CGNAT IP.
  - Some PLDT routers might require specific "superadmin" access or a call to PLDT to enable bridge mode. The search results show some complex DIY methods, but it's generally safer to ask PLDT to do it.

1. Alternative Remote Access Solutions (Workarounds for CGNAT)
   If getting a public IP from PLDT proves difficult or impossible, there are services that can bypass CGNAT:

- VPNs with Port Forwarding Add-ons: Services like PureVPN (mentioned in the search results) offer dedicated IP addresses and port forwarding features. This routes your traffic through their server, bypassing CGNAT.
- Cloudflare Tunnels: (Advanced) Cloudflare Tunnels create a secure, outbound-only connection from your Home Assistant to Cloudflare's network,

allowing you to expose services without opening ports on your router. This is a very robust and secure solution.

- Tailscale: (Recommended for personal access) Tailscale creates a secure mesh VPN network between your devices. You install Tailscale on your Home Assistant and on the devices you want to access it from. It works even behind CGNAT and doesn't require port forwarding. This is excellent for accessing your Home Assistant from your phone, laptop, etc., but not for sharing with others who don't have Tailscale installed.
  Action Plan for You:
- Confirm CGNAT:
  - Go to https://whatismyip.com/ and note your public IP.
  - Log into your PLDT router and find its WAN IP address.
  - If these two IPs are different, and your router's WAN IP is in the 100.64.x.x to 100.127.x.x range, you are almost certainly behind CGNAT.
- Contact PLDT: Call or message PLDT customer support and explicitly request to be removed from CGNAT and assigned a Dynamic Public IP address. Explain that you need to host a service (Home Assistant) that requires incoming connections.
- Re-test Port Forwarding: Once PLDT confirms the change (and after your router potentially reboots), re-run the canyouseeme.org test for ports 80 and 443.
- Consider Alternatives: If PLDT cannot or will not provide a public IP, explore Tailscale (for personal access) or Cloudflare Tunnels (for more general access) as robust workarounds.
  The "Troubleshooting Home Assistant DuckDNS External Access" guide (the immersive artifact you provided) remains highly relevant for all other checks (DuckDNS add-on logs, configuration.yaml settings, etc.) once the CGNAT hurdle is overcome. The key is confirming whether you have a truly public IP address.

How to bypass pldt fibr cgnat?

How to Bypass PLDT Fibr CGNAT for Port Forwarding

If you're trying to set up services like Home Assistant, game servers, or remote

access on your PLDT Fibr connection and find that port forwarding isn't working, it's highly likely you're behind
Carrier-Grade NAT (CGNAT). This guide outlines the most effective methods to bypass CGNAT and enable proper port forwarding.
Understanding CGNAT and Its Impact

CGNAT (Carrier-Grade Network Address Translation) is a technique used by Internet Service Providers (ISPs) to conserve IPv4 addresses. Instead of giving each customer a unique public IP address, they assign a single public IP to a large group of customers. Your home router then gets a private IP address from this shared public IP pool.

Why it breaks port forwarding: When an external device tries to connect to your public IP on a specific port, the ISP's CGNAT router doesn't know which of its many customers the connection is intended for. It cannot forward the traffic to your specific router, thus preventing your port forwarding rules from working.

How to confirm if you're under CGNAT:
1.
Check your Public IP: Go to `https://whatismyip.com/` from any device connected to your PLDT Fibr network. Note this IP address.
2.
Check your Router's WAN IP: Log in to your PLDT Fibr modem/router's administration page (usually `192.168.1.1` or `192.168.0.1`). Look for a "WAN Status," "Internet Connection," or "Network Status" section. Find the IP address listed as the "WAN IP" or "Internet IP."
3.
Compare:
    - If your router's WAN IP is
different from the public IP you found on `whatismyip.com`, AND your router's WAN IP falls within these private ranges:
        - `100.64.0.0` to `100.127.255.255` (most common for CGNAT)
        - `10.0.0.0` to `10.255.255.255`

    - `172.16.0.0` to `172.31.255.255`
    - `192.168.0.0` to `192.168.255.255`
  - ...then you are almost certainly behind CGNAT.

Method 1: Request CGNAT Removal / Public IP from PLDT (Recommended First Step)

This is the most direct and often the simplest solution, as it resolves the root cause.

1. **Contact PLDT Customer Support:**
   - **Hotline:** Call 171 (PLDT's customer service hotline).
   - **Social Media:** Message PLDT Home on Facebook (often more responsive for technical requests).
2. **State Your Request Clearly:**
   - Explain that you need to set up port forwarding for a home server (e.g., for security cameras, smart home, or a personal server) and that you suspect you are behind CGNAT.
   - **Explicitly request to be removed from CGNAT and to be assigned a "Dynamic Public IP address."**
   - **Important Note:** They might try to offer a "Static IP" plan, which usually incurs an additional monthly fee. For most home users, a **dynamic public IP** is sufficient and should ideally be provided at no extra cost for residential plans if you push for it. Emphasize that you only need a public IP, not necessarily a static one.
3. **Follow Up:** PLDT's process for this can sometimes take a few days or require follow-ups. Be persistent. Some users report that a Level 2 technician might need to remotely configure your router or even visit your location.
4.

Verify Removal: After PLDT confirms the change, repeat the "How to confirm if you're under CGNAT" steps above. If your router's WAN IP now matches your public IP from `whatismyip.com` and is not in a private range, you have successfully bypassed CGNAT. You can then proceed with standard port forwarding on your PLDT router.

Method 2: Request Bridge Mode (If you have your own router)

If you have a more capable personal router that you prefer to use for your network management, you can ask PLDT to put their modem/router into "Bridge Mode."

- **What it does:** In bridge mode, the PLDT device acts purely as a modem, passing your internet connection (including the public IP address) directly to your personal router's WAN port. Your personal router then handles all the routing, Wi-Fi, and critically, port forwarding.
- **Steps:**
  1. **Acquire a Capable Router:** Ensure you have a good quality personal router that supports port forwarding and other features you need.
  2. **Contact PLDT:** Similar to CGNAT removal, contact PLDT customer support and request that your modem/router be set to "Bridge Mode."
  3. **Connect Your Router:** Once PLDT confirms it's in bridge mode, connect the WAN/Internet port of your personal router to one of the LAN ports on the PLDT device.
  4. **Configure Your Router:** All your network configuration, including port forwarding, will now be done on your personal router.
- **Important Considerations:**
  - **CGNAT Still Applies:** Bridge mode *alone* does not bypass CGNAT. If PLDT still assigns you a CGNAT IP, even in bridge mode, you will still face the same port forwarding issues. **You will likely need to request CGNAT removal (Method 1) in conjunction with bridge mode.** Some users report that requesting bridge mode

first, then CGNAT removal, works for them.

- **Superadmin Access:** Some PLDT modem models might require "superadmin" access to enable bridge mode or modify advanced settings. While there are online guides for this (often involving specific URLs like `192.168.1.1/fh` and default superadmin credentials), it's generally safer to have PLDT perform this configuration remotely.
- **Loss of PLDT Wi-Fi/VoIP:** If your PLDT device handles Wi-Fi or VoIP (landline phone service), these might be affected or cease to function when in bridge mode, as your personal router takes over.

Method 3: Alternative Tunneling/VPN Solutions (Workarounds for CGNAT)

If PLDT is unwilling or unable to provide you with a public IP address, these solutions create a "tunnel" through CGNAT, allowing external access without traditional port forwarding. These are excellent workarounds.

1. **Tailscale (Highly Recommended for Personal Access):**
   - **Concept:** Tailscale builds a secure mesh VPN network between your devices, regardless of their location or network configuration (including CGNAT). It's like having all your devices on the same local network, even if they're physically miles apart.
   - **How it works:** You install the Tailscale client on your Home Assistant device and on any device you want to access it from (phone, laptop, other computers). Tailscale handles the routing and NAT traversal automatically.
   - **Pros:** Extremely easy to set up, highly secure (WireGuard-based), works perfectly behind CGNAT, free for personal use (up to 100 devices).
   - **Cons:** Only devices with the Tailscale client installed can access your Home Assistant. Not suitable for public-facing services (like a website for everyone to see).
   - **Setup:** Install the Tailscale add-on in Home Assistant, follow the instructions to

authenticate, and install Tailscale on your client devices.

2. **Cloudflare Tunnels (More Advanced, for Public-Facing Services):**
    - **Concept:** Cloudflare Tunnels create a secure, outbound-only connection from your Home Assistant (or any server) to Cloudflare's global network. This means you don't need to open any incoming ports on your router. Cloudflare then exposes your service to the internet via their network.
    - **How it works:** You install a `cloudflared` daemon on your Home Assistant machine. This daemon establishes an outbound tunnel to Cloudflare. When someone accesses your domain (e.g., `myhomeassistant.yourdomain.com`), Cloudflare routes the traffic through this tunnel to your Home Assistant.
    - **Pros:** Bypasses CGNAT entirely, no port forwarding needed, adds Cloudflare's security and DDoS protection, can be used for public-facing services.
    - **Cons:** More complex to set up than Tailscale, requires owning a domain name (though Cloudflare offers free DNS), might have some learning curve.
3. **VPN Services with Port Forwarding / Dedicated IP:**
    - **Concept:** Some commercial VPN providers offer a "dedicated IP address" and/or "port forwarding" as add-ons. You connect your router (or Home Assistant) to this VPN, and the VPN provider's server then acts as the public endpoint, forwarding traffic to your device.
    - **Pros:** Bypasses CGNAT, can provide a static public IP.
    - **Cons:** Requires a paid VPN subscription, performance might be impacted, not all VPNs offer this feature or do it reliably. PureVPN was mentioned in search results as one that offers this.
4. **Reverse SSH Tunnel / VPS (Advanced):**
    - **Concept:** You rent a small, inexpensive Virtual Private Server (VPS) with a public

IP address. You then establish an SSH tunnel from your Home Assistant (or a device on your home network) to the VPS. This tunnel creates a pathway for traffic to flow from the VPS back to your Home Assistant.

-

Pros: Full control, highly flexible, bypasses CGNAT.

-

Cons: Requires technical expertise to set up and maintain a VPS, ongoing cost for the VPS.

Recommendation

1.

Start with Method 1 (Request CGNAT Removal): This is the cleanest solution if PLDT cooperates. It gives you a true public IP and allows standard port forwarding.

2.

If Method 1 Fails, Consider Tailscale: For personal remote access to Home Assistant, Tailscale is incredibly simple, secure, and effective at bypassing CGNAT without any router configuration.

3.

For Public-Facing Services or if Tailscale isn't enough, explore Cloudflare Tunnels or a VPN with dedicated IP/port forwarding.

By understanding CGNAT and utilizing these methods, you should be able to achieve external access to your Home Assistant instance, even with PLDT Fibr.