Home Lab: Secure Pi-hole Recursive DNS with Unbound and HTTPS Admin Interface

Author: Felix Opoku

Date: December 2025

Overview

This home lab project demonstrates a secure, privacy-focused DNS setup using:

Pi-hole: Network-wide ad-blocking and DNS filtering

Unbound: Recursive caching DNS resolver for faster, private DNS

Let’s Encrypt: HTTPS-secured Pi-hole admin interface

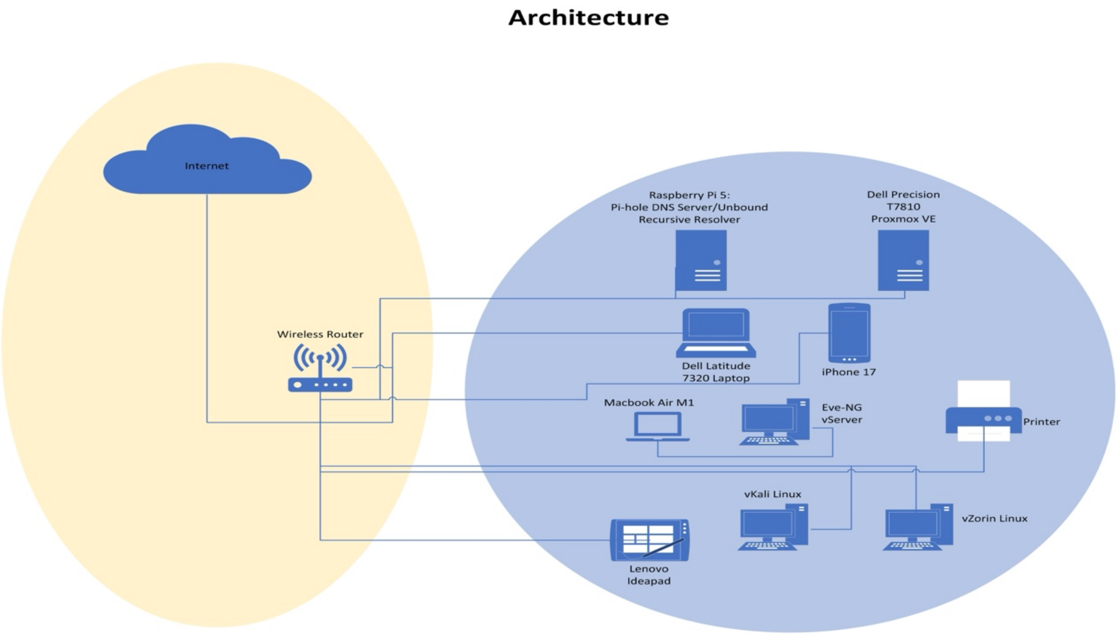
Namesilo DNS API: Automated wildcard certificate validation

The project highlights DNS security, TLS/SSL management, and home lab automation skills.

Hardware & Software

- Device: Raspberry Pi 5
- RAM: 16 GB
- Storage: 32 GB SD Card
- OS: Latest Raspberry Pi OS 13 64-bit (Trixie)
- Software Stack: Pi-hole, Unbound, Certbot, Namesilo DNS API plugin

Architecture



Implementation Steps:

Install Pi-hole & Unbound

```
sudo apt update && sudo apt install -y pi-hole unbound
```

Configure Unbound as a recursive resolver on 127.0.0.1:5335.

Set Pi-hole upstream DNS to Unbound.

Obtain Let's Encrypt Certificate

Set up Certbot in a Python virtual environment:

```
python3 -m venv ~/certbot-venv

source ~/certbot-venv/bin/activate

pip install certbot certbot-dns-<PROVIDER>
```

- Create credentials.ini with API token (masked).
- Issue wildcard certificate:

```
~/certbot-venv/bin/certbot certonly \

  --authenticator dns-<PROVIDER> \

  --dns-<PROVIDER>-credentials /etc/letsencrypt/credentials.ini \

  -d example.com -d *.example.com
```

Configure Pi-hole HTTPS

- Combine certificate and key for Pi-hole:

```
sudo mkdir -p /etc/pihole/ssl

sudo cat /etc/letsencrypt/live/example.com-0001/fullchain.pem \

         /etc/letsencrypt/live/example.com-0001/privkey.pem \

         > /etc/pihole/ssl/tls.pem

sudo chown pihole:pihole /etc/pihole/ssl/tls.pem

sudo chmod 600 /etc/pihole/ssl/tls.pem
```

- Update /etc/pihole/pihole.toml:

```
[webserver]
domain = "example.com"
port = "443s,[::]:443s"
tls = true
tls_cert = "/etc/pihole/ssl/tls.pem"
threads = 50
```

Restart Pi-hole FTL:

```
sudo systemctl restart pihole-FTL
```

Automate Renewal

- Add Certbot deploy hook:

```
sudo mkdir -p /etc/letsencrypt/renewal-hooks/deploy
sudo nano /etc/letsencrypt/renewal-hooks/deploy/pihole_tls.sh
```

```
#!/bin/bash
cat /etc/letsencrypt/live/example.com-0001/fullchain.pem \
    /etc/letsencrypt/live/example.com-0001/privkey.pem \
    > /etc/pihole/ssl/tls.pem
chown pihole:pihole /etc/pihole/ssl/tls.pem
chmod 600 /etc/pihole/ssl/tls.pem
systemctl restart pihole-FTL
```

Make executable:

```
sudo chmod +x /etc/letsencrypt/renewal-hooks/deploy/pihole_tls.sh
```

Usage

- Access Pi-hole dashboard: https://example.com/admin
- All home devices automatically benefit from ad-blocking and recursive DNS.

Security Considerations

- Admin interface is fully HTTPS-secured.
- Certificates are automatically renewed.

- Private key and PEM files have strict permissions (600).
- Recursive DNS prevents reliance on third-party resolvers, improving privacy and security.

Outcomes

Fully functional, privacy-respecting DNS server for home lab.

Network-wide ad-blocking with Pi-hole.

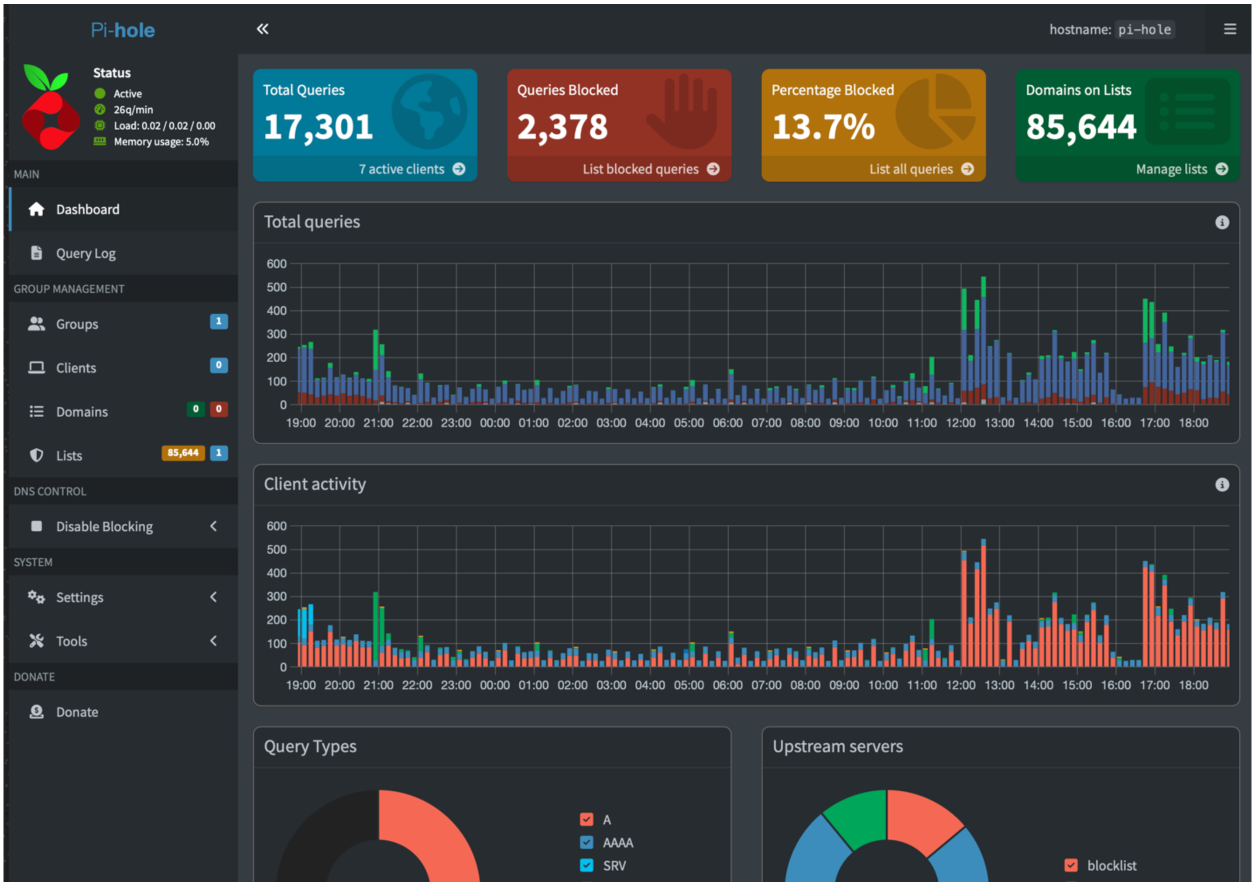
HTTPS-secured admin interface with automatic certificate renewal.

Demonstrates expertise in DNS infrastructure, TLS security, and home lab automation.

Screenshots

Screenshots of Pi-hole dashboard, query logs, and Unbound query results for visual demonstration.

Screenshot 1: Pi-hole Dashboard



hostname: pi-hole

Status
Active
26q/min
Load: 0.02 / 0.02 / 0.00
Memory usage: 5.0%

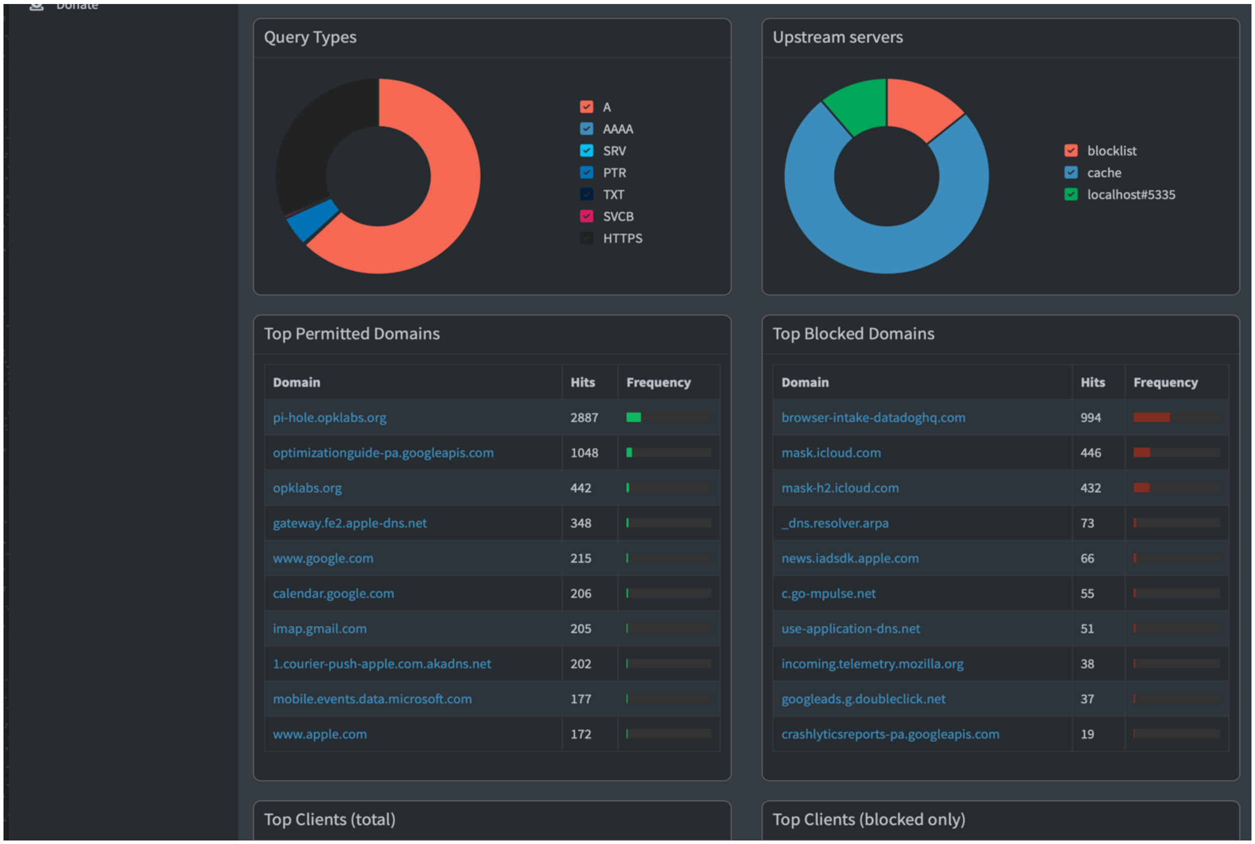
Total Queries 17,301 — 7 active clients

Queries Blocked 2,378 — List blocked queries

Percentage Blocked 13.7% — List all queries

Domains on Lists 85,644 — Manage lists

Screenshot 2: Pi-hole Dashboard



Query Types

Upstream servers

Top Permitted Domains

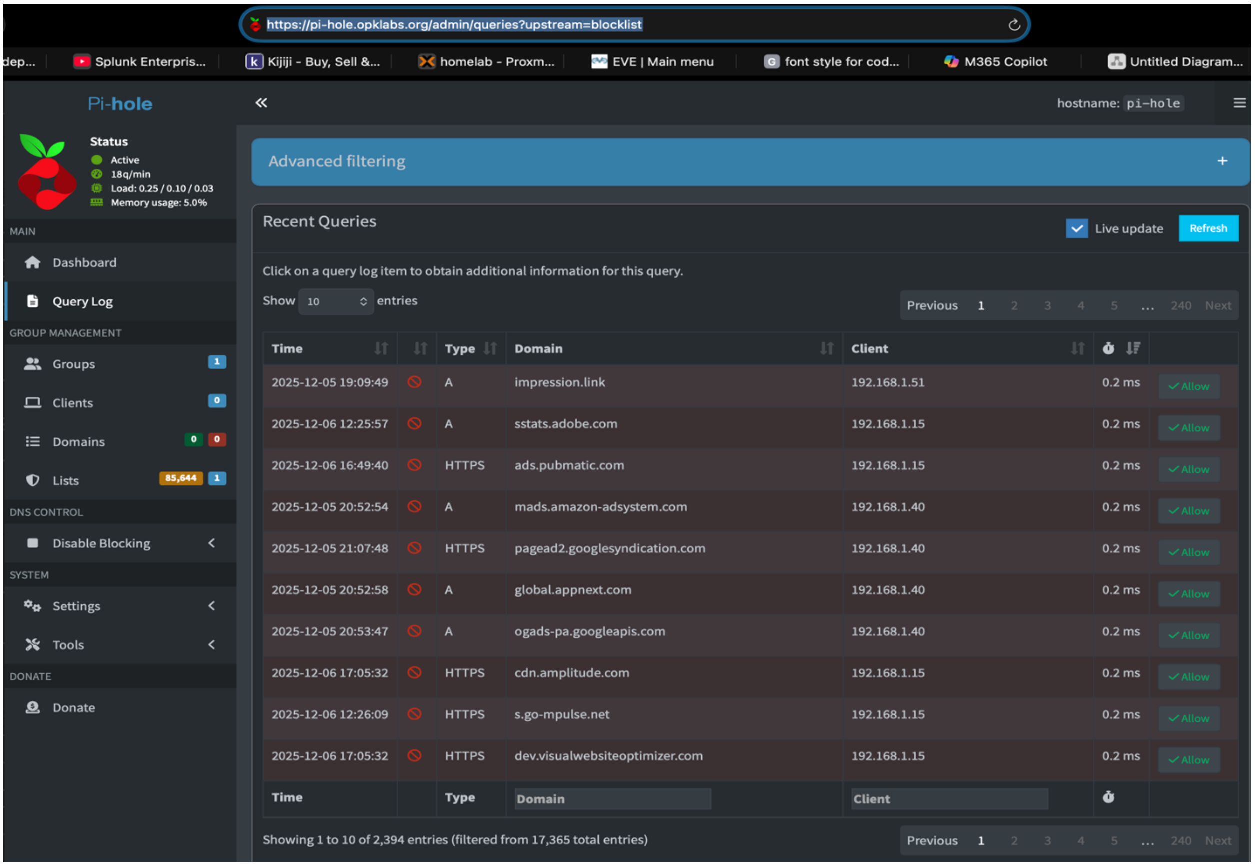
Domain	Hits	Frequency
pi-hole.opklabs.org	2887	
optimizationguide-pa.googleapis.com	1048	
opklabs.org	442	
gateway.fe2.apple-dns.net	348	
www.google.com	215	
calendar.google.com	206	
imap.gmail.com	205	
1.courier-push-apple.com.akadns.net	202	
mobile.events.data.microsoft.com	177	
www.apple.com	172	

Top Blocked Domains

Domain	Hits	Frequency
browser-intake-datadoghq.com	994	
mask.icloud.com	446	
mask-h2.icloud.com	432	
_dns.resolver.arpa	73	
news.iadsdk.apple.com	66	
c.go-mpulse.net	55	
use-application-dns.net	51	
incoming.telemetry.mozilla.org	38	
googleads.g.doubleclick.net	37	
crashlyticsreports-pa.googleapis.com	19	

Top Clients (total)

Top Clients (blocked only)



https://pi-hole.opklabs.org/admin/queries?upstream=blocklist

Status
- Active
- 18q/min
- Load: 0.25 / 0.10 / 0.03
- Memory usage: 5.0%

Recent Queries

☑ Live update

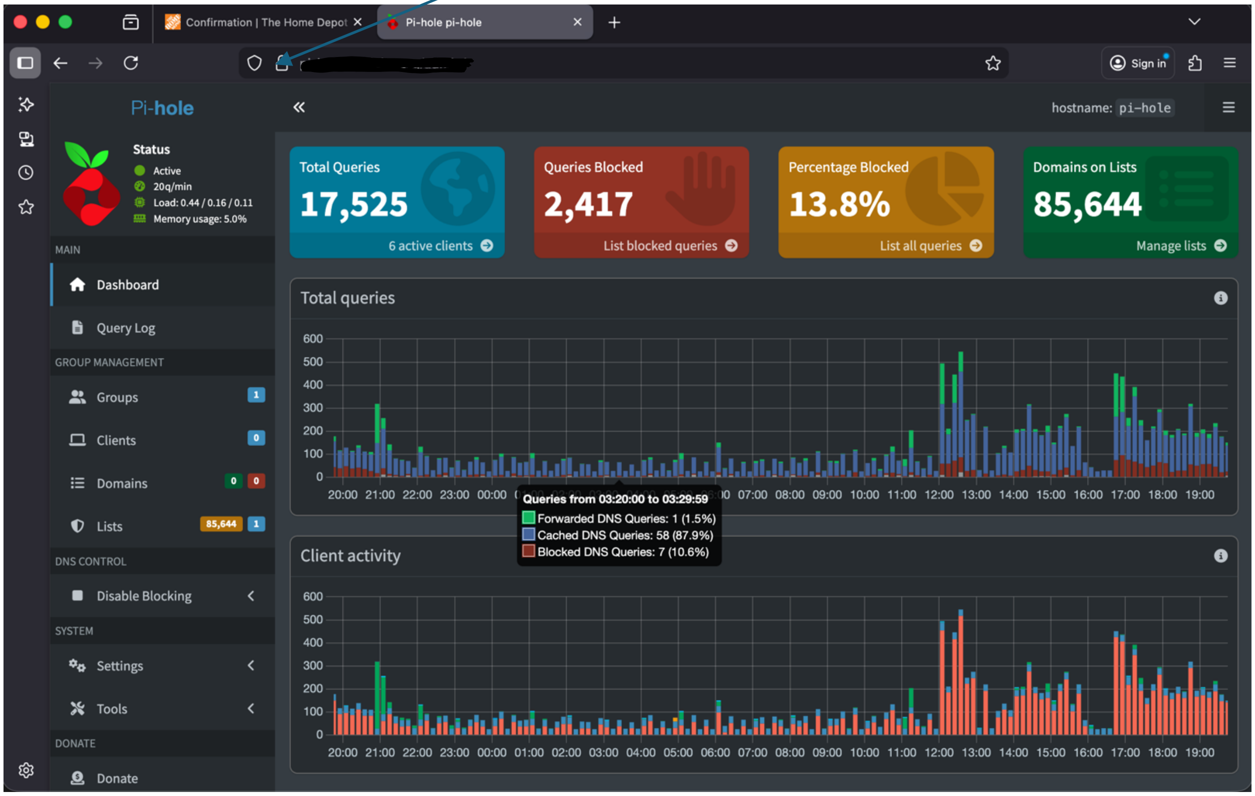
Click on a query log item to obtain additional information for this query.

Show 10 entries

Time		Type	Domain	Client		
2025-12-05 19:09:49	🛇	A	impression.link	192.168.1.51	0.2 ms	✓ Allow
2025-12-06 12:25:57	🛇	A	sstats.adobe.com	192.168.1.15	0.2 ms	✓ Allow
2025-12-06 16:49:40	🛇	HTTPS	ads.pubmatic.com	192.168.1.15	0.2 ms	✓ Allow
2025-12-05 20:52:54	🛇	A	mads.amazon-adsystem.com	192.168.1.40	0.2 ms	✓ Allow
2025-12-05 21:07:48	🛇	HTTPS	pagead2.googlesyndication.com	192.168.1.40	0.2 ms	✓ Allow
2025-12-05 20:52:58	🛇	A	global.appnext.com	192.168.1.40	0.2 ms	✓ Allow
2025-12-05 20:53:47	🛇	A	ogads-pa.googleapis.com	192.168.1.40	0.2 ms	✓ Allow
2025-12-06 17:05:32	🛇	HTTPS	cdn.amplitude.com	192.168.1.15	0.2 ms	✓ Allow
2025-12-06 12:26:09	🛇	HTTPS	s.go-mpulse.net	192.168.1.15	0.2 ms	✓ Allow
2025-12-06 17:05:32	🛇	HTTPS	dev.visualwebsiteoptimizer.com	192.168.1.15	0.2 ms	✓ Allow
Time		Type	Domain	Client		

Showing 1 to 10 of 2,394 entries (filtered from 17,365 total entries)

Https secured connection



[redacted]

Status

Active

20q/min

Load: 0.44 / 0.16 / 0.11

Memory usage: 5.0%

Total Queries 17,525 — 6 active clients

Queries Blocked 2,417 — List blocked queries

Percentage Blocked 13.8% — List all queries

Domains on Lists 85,644 — Manage lists

hostname: pi-hole

Queries from 03:20:00 to 03:29:59

🟩 Forwarded DNS Queries: 1 (1.5%)

🟦 Cached DNS Queries: 58 (87.9%)

🟥 Blocked DNS Queries: 7 (10.6%)