HOMELAB PROJECT / 2026

Pi-hole Network DNS Filtering Lab

Network-wide DNS filtering, query visibility, and privacy controls

Project overview

This project deployed Pi-hole as a centralized DNS filtering service for devices on a home network. The lab explored how DNS-level controls can block known advertising and tracking domains before a connection is completed, while also providing a single dashboard for reviewing DNS activity across connected clients.

OBJECTIVE	CONTROL	EVIDENCE
Reduce unwanted advertising and tracking requests	Blocklist-based DNS filtering	Pi-hole dashboard and query metrics

Architecture

Network clients use Pi-hole as their DNS resolution point. Pi-hole evaluates requested domains against configured lists. Requests that do not match a blocking rule continue to an upstream DNS resolver; matched domains are blocked and recorded for review.

CLIENT DEVICES	PI-HOLE DNS	ALLOW / BLOCK
Laptop Mobile Smart devices	Query logging Blocklist evaluation Central policy	Forward permitted requests Block unwanted domains Record results

01 / IMPLEMENTATION

Centralizing DNS control

The lab was configured so participating network devices submitted DNS requests through Pi-hole. This created one control point for applying domain lists and one interface for observing which clients were making requests.

1	**DNS service** Established Pi-hole as the DNS filtering layer for the lab network.
2	**Domain lists** Applied configured lists containing advertising, tracking, and other unwanted domains.
3	**Upstream resolution** Permitted requests continued to an upstream resolver; the dashboard identifies one.one.one.one#53 among observed upstream activity.
4	**Monitoring** Reviewed total queries, blocked requests, client activity, query types, and upstream results in the Pi-hole dashboard.

What the control provides

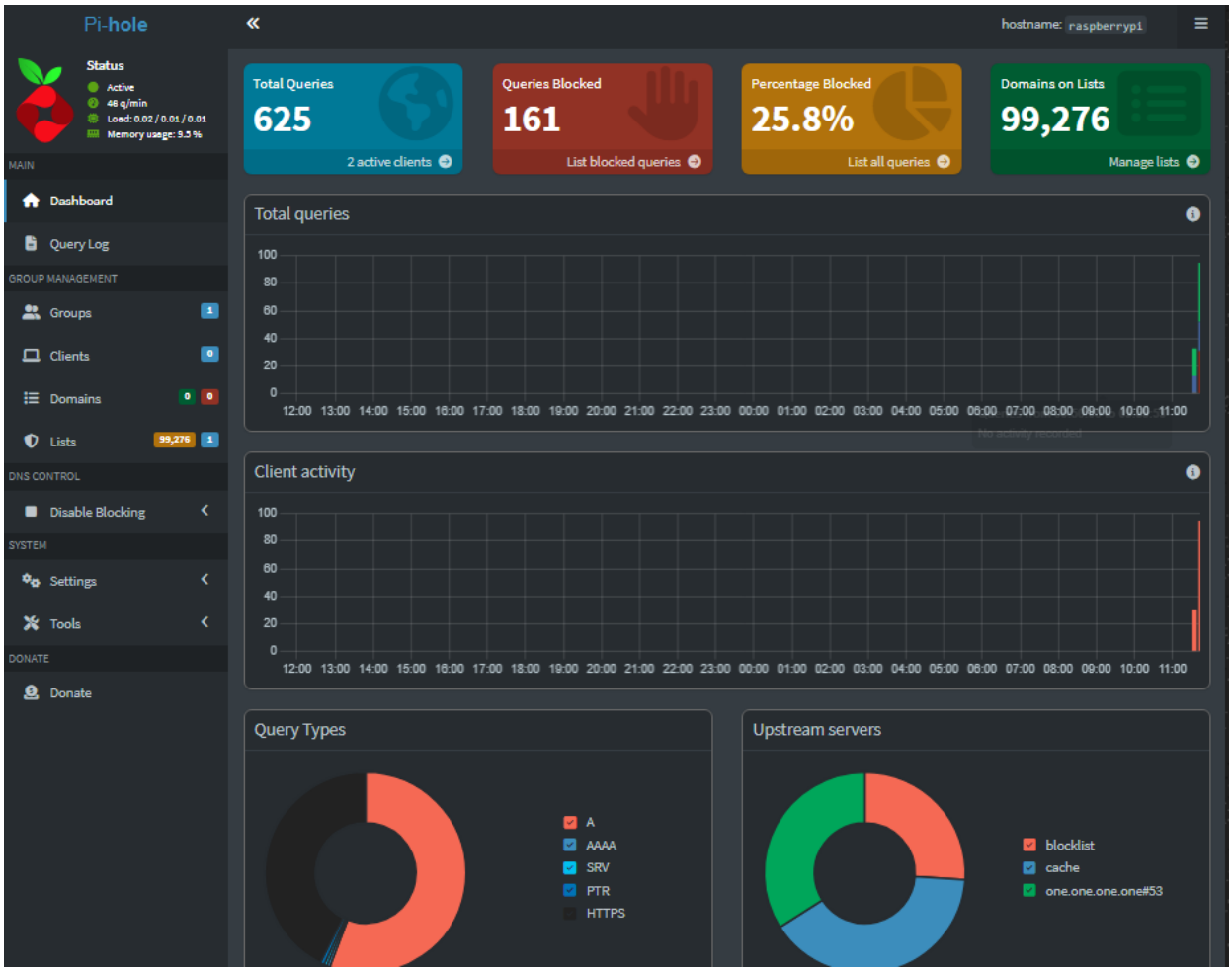
- Network-level filtering that does not depend on a browser extension for each device.
- Centralized visibility into DNS activity across participating clients.
- A repeatable place to review allowed and blocked requests.
- Practical experience connecting DNS behavior to privacy and network-security outcomes.

Scope note

This write-up documents the configuration and evidence visible in the provided dashboard. It does not claim a particular Raspberry Pi model, operating system build, router platform, or named blocklist because those details were not captured in the project evidence.

02 / DASHBOARD EVIDENCE

Reviewing the DNS activity snapshot



625	161	25.8%	99,276
TOTAL QUERIES	QUERIES BLOCKED	PERCENTAGE BLOCKED	DOMAINS ON LISTS

The captured dashboard shows Pi-hole active with two clients. The query-type panel includes A and AAAA activity, and the upstream panel shows a mix of blocked results, cached responses, and requests sent to one.one.one.one#53. These values represent one point-in-time snapshot rather than permanent performance totals.

03 / OUTCOME

Security value and lessons learned

The project demonstrated how a foundational service such as DNS can become a practical security and privacy control. Instead of installing separate filtering tools on every device, the network can apply a consistent rule set at a shared resolution layer.

VISIBILITY	The dashboard makes client requests, query types, block activity, and upstream behavior easier to review from one place.
CONTROL	Domain lists allow unwanted destinations to be filtered consistently for participating devices.
PRIVACY	Blocking advertising and tracking domains can reduce unnecessary third-party connections.
OPERATIONS	Pi-hole requires ongoing list review, exception handling, and validation to avoid disrupting legitimate services.

Skills demonstrated

DNS fundamentals	Network security	Privacy controls
Query analysis	Blocklist management	Operational troubleshooting

Potential next steps

- Document the underlying host, operating system, and network path.
- Establish a repeatable allowlisting and false-positive review process.
- Compare query and blocking trends over a longer observation window.
- Add authenticated administrative access and routine configuration backups.
- Export or forward DNS telemetry for correlation with other homelab security data.

Project conclusion

The Pi-hole lab created a functional network-wide DNS filtering layer and provided evidence of active query processing, blocklist enforcement, and client visibility. It strengthened hands-on understanding of DNS, centralized network controls, privacy protection, and the operational tradeoffs involved in filtering shared infrastructure.