

Readiness report — Pi-hole Network DNS Filter Appliance

Checked 2026-09-03 02:14 · 7 searches, 7 pages fetched

Readiness: Pi-hole Network DNS Filter Appliance

Verdict: Ready · 2026-09-03 · est. parts cost \$78-\$95 **Cybersecurity — software & network: Review before networking**

All four items on this lab's bill of materials are current, plentiful commodity products, available today from several independent sellers at ordinary prices — a Raspberry Pi 4 Model B 2GB at \$55.00, a 32 GB Class 10 microSD card from \$11.74, an official 5.1 V 3 A USB-C supply from \$7.99, and a Cat6 patch cable from \$3.14. The snapshot also grants wide latitude on every line (any 32/64-bit host with at least 512 MB of RAM and a supported Linux, any Class 10 or better card, any well-regulated 5 V supply, any Cat5e/Cat6 cable or Wi-Fi instead), so no single part can hold the lab up. This is the cold check for this lab — there is no previous report, so the prices and sellers below establish the baseline against which the next check measures drift. The lab's real exposure is not in its parts list: it is the network posture and the entirely unpinned software stack described in the Cybersecurity section.

Action required

None — all checked parts are sourceable.

Cybersecurity — software & network

Review before networking — The stack installs cleanly with no default credentials, but it is entirely unpinned, its dashboard ships a Bootstrap release with two unfixed XSS advisories, and its DNS/DHCP and plain-HTTP admin services need an isolated network segment before students attach one to a campus LAN.

Component	Version	How known	Support status
Pi-hole core (pi-hole/pi-hole)	v6.4.3	inferred (installer runs <code>git reset --hard \$(git describe --abbrev=0 --tags)</code> (fetched/05-basic-install.sh); GitHub releases/latest for pi-hole/pi-hole returns tag v6.4.3 (fetched/01-latest))	—
pihole-FTL daemon (DNS, DHCP, embedded web server)	v6.7	inferred (installer downloads <code>github.com/pi-hole/ftl/releases/latest/download</code> (fetched/05-basic-install.sh); GitHub releases/latest for pi-hole/FTL returns tag v6.7 (fetched/03-latest))	—

Component	Version	How known	Support status
Pi-hole web dashboard (pi-hole/web)	v6.6	inferred (installer resets the clone to the newest tag; GitHub releases/latest for pi-hole/web returns tag v6.6 (fetched/02-latest), whose package.json was fetched and checked)	—
Bootstrap (dashboard front-end library)	3.4.1	read from project (pinned in fetched/04-package.json (pi-hole/web v6.6 package.json))	—
pihole-meta, Debian/Ubuntu meta-package	0.7	read from project (PIHOLE_META_VERSION_APT=0.7 in fetched/05-basic-install.sh)	—
pihole-meta, Alpine apk virtual package	0.3	read from project (PIHOLE_META_VERSION_APK=0.3 in fetched/05-basic-install.sh)	—
pihole-meta, RPM/Fedora spec package	0.4	inferred (snapshot records Version 0.4 Release 1 in the installer's RPM control block; the extraction from fetched/05-basic-install.sh surfaced only the APT and APK version variables)	—
Debian (base OS named by the snapshot)	12	inferred (the lab pins no OS; the snapshot's check plan names Debian 12 as the representative base)	extended/LTS support only until 2028-06-30
Raspberry Pi OS Bookworm (base OS named by the snapshot)	bookworm	inferred (snapshot names Raspberry Pi OS Bookworm; Bookworm is the Debian 12 base, so Debian's cycle was looked up)	extended/LTS support only until 2028-06-30
Fedora (base OS option named by the snapshot)	40	inferred (the lab pins no OS; the snapshot's check plan names Fedora 40)	unsupported since 2025-05-13
Alpine Linux (base OS option named by the snapshot)	3.20	inferred (the lab pins no OS; the snapshot's check plan names Alpine Linux 3.20)	unsupported since 2026-04-01
StevenBlack Unified Hosts List (default adlist)	not determined	unpinned (installer fetches the master branch head of the hosts file (snapshot))	—
macvendor.db (IEEE MAC vendor database)	not determined	not determined (binary database downloaded from ftl.pi-hole.net with no published version identifier)	—

Component	Finding	Severity	Fix available?
Bootstrap 3.4.1 (dashboard front-end)	The admin dashboard ships Bootstrap 3.4.1, which carries two cross-site-scripting flaws with no fixed release in the 3.x line, so text that reaches a dashboard page could run script in the browser of whoever is signed in to the appliance. — GHSA-VXMC-5X29-H64V , CVE-2024-6485 , GHSA-Q58R-HWC8-RM9J , CVE-2025-1647	moderate	No - the project pins bootstrap 3.4.1 and OSV lists no fixed version; mitigate by keeping the admin interface off untrusted networks and signing out when finished.
Base operating system	The lab pins no operating-system version, and the releases the snapshot names as representative are already out of standard support: Fedora 40 ended 2025-05-13 and Alpine Linux 3.20 ended 2026-04-01, while Debian 12 Bookworm left standard support on 2026-07-11 and now depends on extended/LTS updates until 2028-06-30.	posture	Mitigation only - build the appliance on a release that is still in support at lab time (check endoflife.date for whichever distribution you choose) rather than the versions the snapshot names.
DNS and DHCP services on the local network	The appliance answers DNS on port 53 for any client that can reach it and can be switched into serving DHCPv4 on port 67 and DHCPv6 on port 547, so a lab device plugged into a shared campus LAN can start handing out addresses and redirecting name resolution for machines that have nothing to do with the lab.	posture	Mitigation only - keep the appliance on an isolated lab segment or VLAN, and never enable its DHCP server on a shared network without clearing it with campus IT first.
HTTP admin interface and REST API	The dashboard and API are reachable over plain HTTP on port 80 at http://pi.hole/admin/ , so the admin password and the query log it displays - every domain each client on the network looked up - cross the LAN unencrypted unless the HTTPS interface on port 443 is used instead.	posture	Mitigation only - use the HTTPS interface, keep the device on an isolated segment, and set a strong password with 'pihole setpassword'.
Pi-hole core, FTL and web dashboard (version pinning)	Nothing in the lab pins a Pi-hole version: the installer clones the repositories and resets each to whatever the newest git tag happens to be, and pulls the newest FTL binary, so two students installing a fortnight apart get different code and this check goes stale the moment upstream publishes a release.	posture	Mitigation only - record the installed version with 'pihole -v' at lab time and re-run this check before each term rather than trusting an earlier report.

What this means for your lab

This appliance is meant to sit on your network and answer DNS for every device on it, so treat it as a piece of network infrastructure rather than a desk gadget. Two things deserve attention before students plug one in. First, if the DHCP feature is switched on while the device is attached to a shared campus network, it will start handing out addresses to machines outside

the lab and pointing them at itself for name resolution - that is the kind of incident campus IT notices, so agree an isolated segment or VLAN with them in advance and leave DHCP off on any shared network. Second, anyone who can reach the device on the network sees the admin dashboard on plain HTTP, and that dashboard lists every domain every client looked up; that is a privacy question about your students as much as a security one, so use the HTTPS interface and keep the device off open networks. The good news is that there are no default passwords to worry about: the installer generates a random admin password on a fresh install and tells you to change it with 'pihole setpassword'. The dashboard's Bootstrap library has two unpatched cross-site-scripting flaws that upstream cannot fix in that version line, which is another reason not to expose the admin page beyond the lab. Finally, nothing here is version-pinned - the installer always takes the newest Pi-hole release - so record what version each student actually installed, and re-check before you run the lab again.

Not checked

- pihole-FTL C daemon and its vendored libraries: the binary is downloaded at whatever version is newest and the FTL repository carries no runtime dependency manifest (CMakeLists.txt and git submodules only; its package.json is openapi test tooling), so there is no registry to check its bundled C code against
- Pi-hole core shell scripts (gravity.sh, piholeDebug.sh, the installer): no vulnerability database covers a source-only shell project; the snapshot's planned 'pi-hole / github / v6.0' lookup has no OSV ecosystem behind it
- 22 apt, 20 rpm and 25 apk packages pulled in by the pihole-meta packages: unpinned by design - each distribution supplies whatever version its release carries, so there is no version to look up
- pi-hole/web devDependencies (autoprefixer, eslint, eslint-plugin-compat, globals, postcss, postcss-cli, prettier, xo): version ranges rather than pins, and they are build tooling the installer never puts on the appliance
- StevenBlack Unified Hosts List: a rolling list fetched from a master branch, with no version identifier to check
- macvendor.db: a binary database with no published version identifier
- Host SSH access (port 22) and the base OS image's own accounts: not installed or configured by the Pi-hole installer - they come from whichever OS image the instructor writes to the card, which this check cannot see
- install.pi-hole.net, docs.pi-hole.net and ftl.pi-hole.net: the GitHub repositories and the raw installer script were reached this run, but these three hosts were not fetched directly

Parts

Bill of materials

Part	Spec/Package	Status	Stock	Price	Source
Host single-board computer / appliance platform	Raspberry Pi 4 Model B 2GB (representative); any x86-64/ARM host, RAM $\geq$ 512 MB, 5.0–5.1 V at 2.5–3.0 A	Readily available	Retail, not published	\$55.00	PiShop USA (also \$55.00 Electromaker, \$61.05 Vilros)
MicroSD flash storage card / boot drive	32 GB Class 10 UHS-I microSDHC, 11.0 × 15.0 × 1.0 mm; $\geq$ 4 GB usable	Readily available	Retail, not published	\$11.74	Walmart, PNY 32GB Elite (also \$14.95 SanDisk Extreme, Adorama)
Host AC/DC power supply adapter	100–240 VAC in; 5.1 V DC 3 A out, USB-C captive plug	Readily available	Retail, not published	\$7.99	Micro Center (also \$9.84 DigiKey, \$12.95 Jameco, 5.1 V 3 A exact)
Ethernet network patch cable	Cat5e/Cat6 UTP, RJ-45 (8P8C) both ends, 1–2 m	Readily available	Retail, not published	\$3.14	My Cable Mart (also \$4.99 3 ft Micro Connectors)

Two notes on reading the table. Retail sellers do not publish stock counts the way an authorised distributor does, so "readily available" here means several independent sellers listed the item at a normal price on 2026-09-03, not a warehouse quantity. And the shopping results carry near-matches that are **not** this BOM: a Raspberry Pi Compute Module 4 2GB at \$90.00 and a Raspberry Pi 4 Desktop Kit at \$105.81 are different products from the Model B board, and the "Official Raspberry Pi 5 USB-C PD Power Supply 27W" at \$12.00 is the Pi 5 unit, not the 5.1 V 3 A Pi 4 supply.

Substitutes

None needed. No part on this list is out of stock, obsolete, or overpriced, so no substitute was proposed or verified this run. If you do swap something, the snapshot's own latitude is your guide: any supported Linux host with at least 512 MB of RAM, any Class 10 or faster card of at least 4 GB, any regulated 5 V supply that holds above 4.8 V under load at the current your board draws, and any Cat5e or better patch cable.

Verify any substitute against its datasheet or product page before ordering.

Other dependencies

- **Fabrication: none.** The snapshot states explicitly that no PCB is designed, fabricated, or assembled — the appliance is entirely commercial off-the-shelf hardware. Nothing to check, nothing to order.
- **Project repositories reached this run.** The `pi-hole/pi-hole`, `pi-hole/web`, and `pi-hole/FTL` repositories on GitHub, and the raw installer script the lab's instructions run, all responded normally on 2026-09-03 — the download paths the lab depends on are live.
- **Installer endpoint** `https://install.pi-hole.net`, **the documentation portal** `https://docs.pi-hole.net/main/prerequisites/`, **the post-install guide, and the** `ftl.pi-hole.net` **host: not checked.** No fetch was dispatched against these three hosts this run, so treat their availability as unverified until the next check.
- **Upstream preset DNS resolvers** referenced in the setup dialogue (Google 8.8.8.8/8.8.4.4, OpenDNS, Level3, Comodo, Quad9 9.9.9.9, Cloudflare 1.1.1.1): not checked — no lookup was dispatched against them.

Watch list

- **Raspberry Pi 4 Model B 2GB pricing and availability.** The 2 GB Pi 4 is a maturing board in a family that has moved on to the Pi 5; the \$55.00 price point held across sellers this run, but board-by-board price and stock swings are the most likely thing to move by the next check. The snapshot's high substitution latitude (Pi 3 Model B+, Pi Zero 2 W, or an x86-64 mini PC all qualify) means this is a budget risk, not a blocker.
- **Power supply variants.** Official Raspberry Pi supplies come in a 5.1 V 3 A USB-C unit for the Pi 4 and a 27 W PD unit for the Pi 5, and they turn up side by side in the same search results. Order against the board you actually buy.
- **microSD card endurance, not sourcing.** Cards are cheap and everywhere; the failure mode for a DNS appliance that logs continuously is write wear, so treat the high-endurance wording in the snapshot as a real requirement rather than a price-shopping opportunity.
- **The software stack, not the parts.** Nothing in this lab pins a Pi-hole version, and the base OS releases the snapshot names have already passed their support dates. That is where this lab will drift first — see the Cybersecurity section above.