HONEY MESH | CORE BETA TECHNICAL PROOF

RC4 evidence update · 2 November 2026 · Vendor-run isolated AWS validation

Verified scope

The signed HoneyMesh Core candidate detected a controlled TCP trap interaction and applied an exact-source XDP block without a manual ban. Separate tests demonstrated bounded automatic expiry, reboot recovery, operator release, and ordinary reference API request handling. Results apply to the stated builds and environments.

Capability	Reviewed observation
Automatic detection	A controlled TCP trap created a local enforcement grant; selected-source traffic stopped while independent control traffic remained reachable. Earlier signed build: 16 XDP exact-ban packets per family at the tested snapshot. The IPv6 final controller check timed out, although its detection, enforcement, and release subtests passed.
Automatic expiry	Latest signed build: a 120-second trap-generated local grant expired naturally in IPv4 and IPv6 VM tests. Source connectivity returned without an operator release.
Reboot recovery	A separate 600-second automatic grant survived reboot as pending in TEST. An authorized ENFORCE transition reapplied it; operator release restored connectivity.
Ordinary Node.js traffic	12,000 expected HTTP responses across baseline, TEST, and ENFORCE IPv4/IPv6 runs, zero unexpected responses, and no local grants. All 12 preregistered p95 checks were under 250 ms.
Multi-owner logic	48 four-owner removal-order component cases passed across IPv4 and IPv6. Live four-producer packet qualification remains open.

Release boundary

This is vendor-run controlled evidence, not independent certification or general production qualification. Core Beta package access requires a paid HoneyMesh subscription and is for Ubuntu 24.04 AMD64 generic-XDP evaluation on noncritical hosts. Node Guard, Exchange-driven enforcement, native-XDP line-rate performance, and customer false-positive rates are not qualified by these tests.

Exact builds and measurements

Latest signed Core candidate

Source **b47095a81d0b09d9084b4c961ddad49c50afa3d1**; Debian SHA-256 **fbd192d23acbe1f02c68934c34aeadf06cb40adac3da0096c7789b1a65c6ebf5**. The publisher-signed manifest and public key are distributed with the beta. The automatic TTL setting defaults to 900 seconds, with accepted bounds of 30–86,400 seconds. VM tests used explicit 120- and 600-second settings; the 900-second default has source-level evidence only.

Latest candidate	IPv4	IPv6
Controlled TCP trap in TEST	Event; no grant	Event; no grant
Trap in ENFORCE	Local grant; XDP applied	Local grant; XDP applied
First grant	120 seconds; natural expiry; restored	120 seconds; natural expiry; restored
Second grant	600 seconds; pending after reboot in TEST	600 seconds; pending after reboot in TEST
Authorized ENFORCE re-entry	Selected source blocked; control reachable	Selected source blocked; control reachable
Controller / cleanup	58/58; restored and deleted	58/58; restored and deleted

Reference API workload

Each independent client sent 1,000 seeded HTTP requests at a target 25 requests/second per condition: 750 expected 200, 150 expected 401, and 100 expected 404. Clients ran sequentially. The Node.js fixture did not include Node Guard.

Family / mode	Test p95	Control p95	Unexpected
IPv4 baseline	4.697 ms	1.780 ms	0
IPv4 TEST	1.627 ms	1.479 ms	0
IPv4 ENFORCE	2.096 ms	1.635 ms	0
IPv6 baseline	2.331 ms	2.013 ms	0
IPv6 TEST	1.483 ms	2.211 ms	0
IPv6 ENFORCE	1.844 ms	1.991 ms	0

Evidence and limitations

Earlier signed packet campaign

The earlier signed Core package (Debian SHA-256 **099973404bce64ae7b46f2c349439849a96167596ea309f367d7307f0f19c535**) passed a separate controlled manual-ban packet campaign. Its source/control captures, UEE state, and XDP exact-ban counter supported selective IPv4/IPv6 blocking; 7 XDP drops were counted per family. Those measurements are historical evidence for that package and are not silently transferred to the newer automatic-TTL build.

Open product gates

Area	Still required
Core pilot	Representative workload, management recovery, protected allowlist, repeatable CPU/memory and latency tests, failure injection, monitored soak, and named rollback owner.
Pro	Live four-producer XDP behavior, Node Guard two-app lifecycle, Exchange propagation/retraction/outage/poisoning, portal authorization, backup restore, and full release review.
Claim limits	No line-rate, broad detection accuracy, sustained throughput, customer false-positive, or independent-certification claim. Local-only sharing is configured off, not code-locked.

Evidence register

RC4_CORE_AUTOMATIC_TTL_2026-11-01.md; RC4_CORE_REFERENCE_NODE_WORKLOAD_2026-11-01.md; RC4_CORE_AUTOMATIC_DETECTION_2026-11-01.md; RC4_CURRENT_PACKET_ATTRIBUTION_2026-11-01.md; RC4_QUALIFICATION_CHECKPOINT_2026-11-01.md. Reports and sanitized machine results are in the HoneyMesh-Validation repository. Raw PCAPs, source addresses, operational logs, and credentials remain private for internal audit.