Network Analysis Report

Host 172.16.0.4 · Historical Session · Feb 20, 2026 10:13 – 14:00

Executive Summary

This report analyses historical network flow data for host **172.16.0.4** (lucky.lbasense.com) captured over a **~3 hour 47 minute** window from 10:13 to 14:00 on February 20, 2026. A total of **108 flows** were recorded, transferring **542 KB** of data across six application types.

The device operated within its expected profile for the majority of the session — maintaining a persistent encrypted tunnel (OpenVPN to the Czech Republic), active SSH management sessions to South Korea, and high-frequency TLS status reporting to LBASense infrastructure. **One significant anomaly was detected: two HTTP flows scored 400/100 and triggered a "Possible Exploit" alert. These warrant immediate review.**

✔ NORMAL	TLS status reporting, OpenVPN tunnel, and DNS lookups are all operating within expected parameters.
⚠ REVIEW	SSH generated 2 large burst flows (45 KB and 20 KB) at 13:56 and 13:58 — unusual volume compared to baseline keep-alive traffic.
✖ ALERT	Two unencrypted HTTP flows to Canonical (Ubuntu) servers scored 400/100 with a "Possible Exploit" alert. No action has been taken automatically.

1. Detailed Activity & Performance Analysis

This section summarises all six applications detected during the session, including data volumes, destinations, and peak throughput.

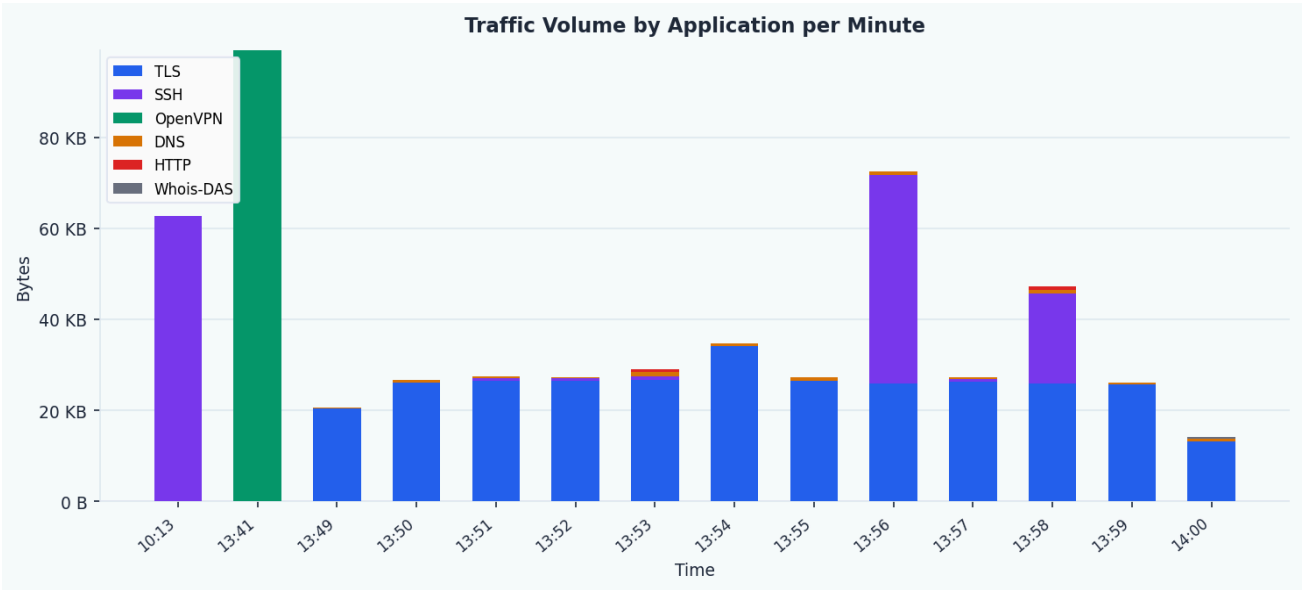
Application	Protocol	Destination	Total Data(Session)	Peak Speed	Why This Matters
TLS	TCP	South Korea · Canada · US(LG DACOM, Amazon, Fastly)	**~297 KB**	**11.6 kbps**	Encrypted status reporting to api.status.lbasense.com. High frequency (69 flows). Normal.

SSH	TCP	South Korea(Amazon AWS — 15.164.1.120 & 3.34.242.51)	**~128 KB**	**1.6 kbps**	Remote management sessions. One long-running background session + burst activity at 13:56 and 13:58 requires review.
OpenVPN	TCP	Czech Republic(Quantcom, a.s. — 212.24.158.212)	**~97 KB**	**0.47 kbps**	Single persistent encrypted management tunnel. Active for ~19 minutes. Normal configuration.
DNS	UDP	United States(Google — 8.8.8.8)	**~6.6 KB**	**< 0.1 kbps**	Standard name resolution queries. 28 flows, all to Google Public DNS. Score: 0. Benign.
HTTP	TCP	United Kingdom & US(Canonical — 91.189.91.48, 185.125.190.97)	**~1.5 KB**	**0.06 kbps**	⚠ Score: 400 — "Possible Exploit" alert. Unencrypted HTTP to Canonical Ubuntu update servers. Review recommended.
Whois-DAS	TCP	United States (Team Cymru — 216.31.12.17)	**~0.4 KB**	**< 0.1 kbps**	Single WHOIS lookup. Standard network diagnostic query. Score: 0. Benign.

2. Traffic Analysis Charts

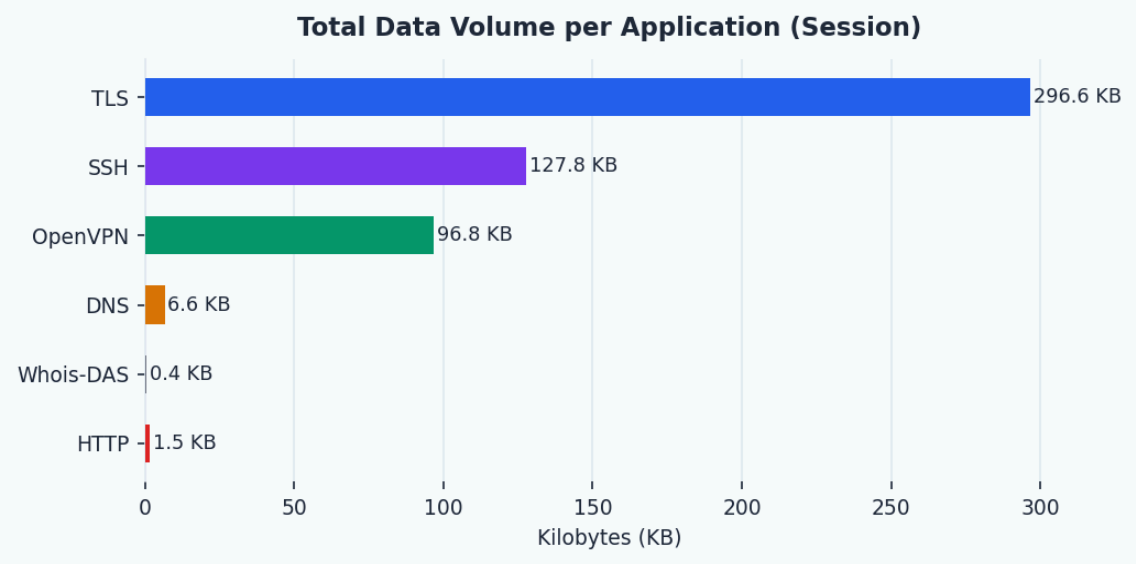
Traffic Volume Over Time

The chart below shows bytes transferred per minute, broken down by application. Note the large OpenVPN burst at 13:41 and the SSH activity spikes at 13:56 and 13:58.



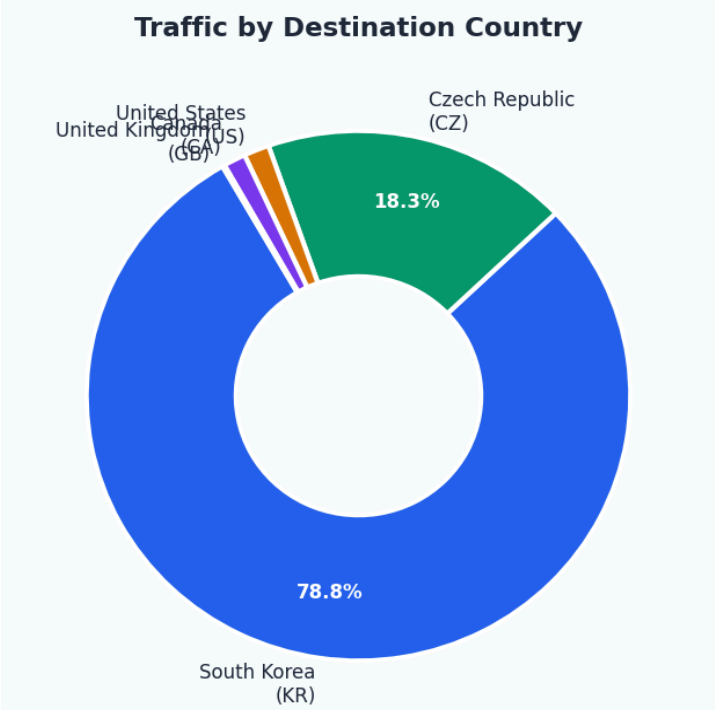
Total Data Volume by Application

TLS dominates overall volume due to its high frequency of status reporting flows. SSH is second despite fewer flows, indicating larger individual data transfers.



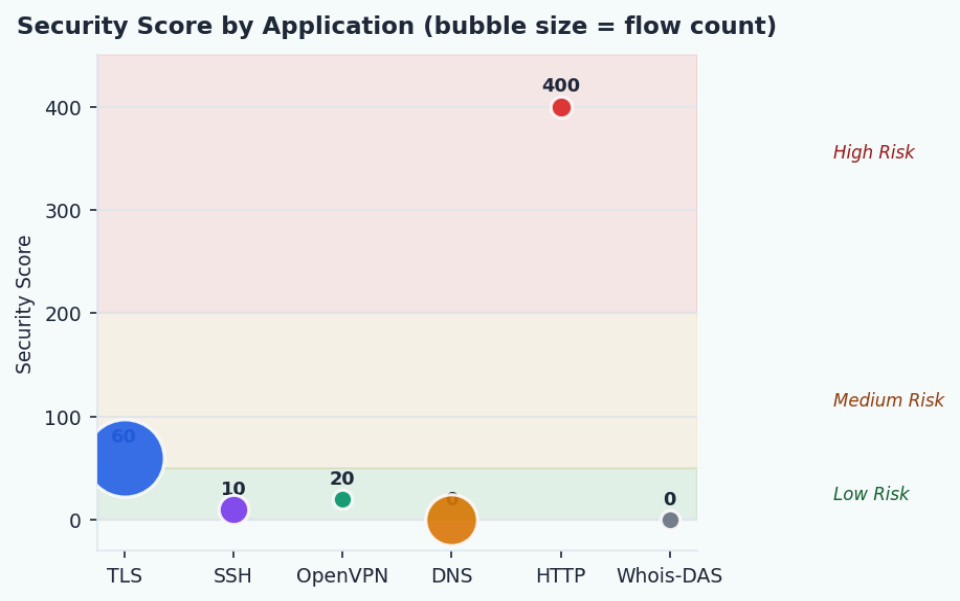
Traffic by Destination Country

South Korea accounts for 78% of all traffic, driven by TLS reporting to LG DACOM and SSH sessions to Amazon AWS Seoul. The Czech Republic represents the OpenVPN management tunnel.



Security Score by Application

Bubble size represents the number of flows. HTTP is the critical outlier with a score of 400. TLS flows score 60 (medium) due to non-standard port usage (38443 instead of 443), which is expected for this device.



3. Security Score & Alert Analysis

Score Scale Reference

Score Range	Risk Level	Meaning
0 – 49	Low	Normal traffic. No action required.
50 – 199	Medium	Flagged for review. May be expected device behaviour on non-standard configurations.
200+	High	Significant anomaly. Manual investigation required.

Alert Details

Alert 1 — Known Proto on Non-Std Port (TLS, Score: 60)

- Affects 69 TLS flows to South Korea on port 38443 (standard HTTPS uses port 443).
- This is a deliberate configuration for lucky.lbasense.com status reporting. The "side door" is expected and approved.
- **Status:** No action required. This is documented device behaviour.

Alert 2 — Remote Access (SSH & OpenVPN, Score: 10–20)

- SSH sessions to 15.164.1.120 and 3.34.242.51 (Amazon AWS Seoul) are standard administrative connections.
- OpenVPN to Quantcom, a.s. in the Czech Republic is a persistent management tunnel — consistent with the 172.16.0.16 report.
- Two SSH burst flows at 13:56 (~45 KB) and 13:58 (~20 KB) are larger than typical keep-alive traffic and should be verified.
- **Status:** Routine sessions confirmed. Investigate burst volumes.

Alert 3 — Possible Exploit (HTTP, Score: 400) ⚠ ACTION REQUIRED

- Two unencrypted HTTP (port 80) flows to Canonical Group Limited servers (Ubuntu update infrastructure).
- Server IPs: 91.189.91.48 (GB) and 185.125.190.97 (US). Path: / (root).
- While Canonical servers are legitimate, unencrypted HTTP to update endpoints is a security concern — traffic can be intercepted or modified in transit (MITM risk).
- The score of 400 is the highest recorded in this session.
- **Recommendation:** Verify whether the device's package manager is configured to use HTTPS. If plain HTTP is intentional, whitelist with documented justification. If not, update apt/package configuration to enforce HTTPS.

4. Location Analysis: Where Is Your Data Going?

Traffic from 172.16.0.4 flows to five countries. The two primary destinations align with known DFRC / LBASense infrastructure.

Country	Provider / ASN	Traffic	Application	Assessment
🇰🇷 **South Korea**	LG DACOM Corp · Amazon AWS	417 KB (77%)	TLS, SSH	Expected — DFRC HQ infrastructure
🇨🇿 **Czech Republic**	Quantcom, a.s.	97 KB (18%)	OpenVPN	Expected — EU management tunnel
🇺🇸 **United States**	Google LLC · Team Cymru	8 KB (1.5%)	DNS, Whois	Expected — standard utilities
🇨🇦 **Canada**	Fastly, Inc.	7 KB (1.3%)	TLS	Expected — CDN edge node
🇬🇧 **United Kingdom**	Canonical Group Ltd	0.7 KB (<1%)	HTTP ⚠	Review — unencrypted HTTP alert

5. Conclusion & Recommendations

Over the 3 hour 47 minute observation window, host 172.16.0.4 operated largely within its expected profile. The device consistently reported health status to LBASense infrastructure via TLS, maintained its management tunnel to the Czech Republic via OpenVPN, and performed regular DNS resolution via Google Public DNS.

Priority	Finding	Recommendation
🔴 **High**	HTTP Exploit Alert	Investigate and remediate unencrypted HTTP to Canonical servers. Enforce HTTPS for package management.
🟡 **Medium**	SSH Burst Traffic	Review the 45 KB and 20 KB SSH sessions at 13:56 and 13:58. Confirm these were authorised admin operations.
🟢 **Low**	TLS Port 38443	Already documented. No action needed. Consider adding to allowlist to suppress recurring alerts.
🟢 **Low**	All Other Traffic	OpenVPN, DNS, and Whois-DAS all normal. No new or unexpected destination IPs detected.

No additional action is required beyond the items listed above. The device is performing its intended duties securely.