# LATTICE NETWORK

## REFERTO DI AUDIT TECNICO · v7.9.0

Questo foglio non contiene dichiarazioni di intenti. Contiene misure prese sul sistema in funzione il giorno indicato, con il metodo scritto in fondo: chiunque puo' rifarle e smentirle. Dove un numero non e' stato misurato, qui c'e' scritto che non lo e' stato.

### IDENTITA' DEL REFERTO

| | |
|---|---|
| Generato (UTC) | **2026-09-25T09:20:02Z** |
| Versione della rete | **7.9.0** |
| Catena · altezza del blocco | **54** |
| Catena · validatori annunciati | **9** |

`impronta del binario in esecuzione (SHA3-256)`
`11ae8847ad28792f86344cd55c1491223bc34d0fb766a542a7e2e41079b94fdd`

### VELOCITA' MISURATA ORA (mediana e 95° percentile)

| | |
|---|---|
| Messaggio: invio accettato dal nodo | **10 ms (p95 88 ms · su 12 giri)** |
| Messaggio: arrivo sul filo del destinatario | **10 ms (p95 88 ms · su 12 giri)** |
| Apertura di una chat (ultimi 12 messaggi) | **6 ms (p95 12 ms · su 12 giri)** |
| Elenco delle conversazioni | **7 ms (p95 19 ms · su 12 giri)** |
| Biglietto del relay (emissione firmata) | **9 ms (p95 10 ms · su 12 giri)** |
| Canale aperto sul relay IT (UDP 3478) | **2 ms (p95 6 ms · su 5 giri)** |
| Canale aperto sul relay DE (UDP 3478) | **8 ms (p95 11 ms · su 5 giri)** |
| Canale aperto sul relay FI (UDP 3478) | **51 ms (p95 54 ms · su 5 giri)** |
| Canale aperto su TLS (IT, porta 5349) | **10 ms (p95 10 ms · su 3 giri)** |
| Canale aperto su TLS (IT, porta 443) | **9 ms (p95 12 ms · su 3 giri)** |
| Canale aperto su TLS (DE, porta 5349) | **210 ms (p95 353 ms · su 3 giri)** |
| Canale aperto su TLS (DE, porta 443) | **197 ms (p95 213 ms · su 3 giri)** |
| Canale aperto su TLS (FI, porta 443) | **non misurato** |

Nota onesta sulla cifra dei «26 ms» che circolava nei materiali: non era una misura verificata e l'audit precedente l'aveva gia' smentita. I numeri qui sopra sono quelli veri, presi su rete pubblica con TLS e firma post-quantistica attive. Il tempo che conta per una chiamata e' la somma di biglietto piu' canale sul relay: sul nodo italiano si sta sotto i 20 millesimi di secondo.

### INTEGRITA' DEL RELAY (credenziali a tempo)

| | |
|---|---|
| Validita' di un biglietto | **600 secondi** |
| Credenziale = HMAC-SHA1 del segreto condiviso | **VERIFICATA** |
| Indirizzo dell'identita' dentro la credenziale | **ASSENTE (impronta SHA3)** |
| Vecchia coppia fissa (fino alla 7.6.0) | **RIFIUTATA (401)** |
| Biglietto scaduto, con firma perfetta | **RIFIUTATO (401)** |
| Credenziale manomessa | **RIFIUTATA (401)** |
| Richiesta del biglietto senza sessione | **RIFIUTATA (401)** |

## COPERTURA DEI RELAY (la voce non passa da nessun terzo)

| | |
|---|---|
| Italia · turn.lattice-network.it | **3478 UDP/TCP · 5349 TLS · 443 TLS** |
| Germania · 2-28-43-117.nip.io | **3478 UDP/TCP · 5349 TLS · 443 TLS** |
| Finlandia · 204-168-137-30.nip.io | **3478 UDP/TCP · 5349 TLS · 443 TLS** |

Tre relay in tre paesi, un solo segreto: un biglietto emesso da qualunque nodo apre qualunque relay, cosi' la voce prende la strada piu' corta e se un relay cade gli altri due restano come riserva. Ogni nodo annuncia PRIMA il proprio.
Sul nodo finlandese le porte del relay risultavano chiuse e si era scritto che fosse il fornitore a filtrarle. Non era lui: era il firewall del nodo di uscita, che lasciava passare soltanto SSH e le porte travestite da HTTPS. Dalla 7.8.1 sono aperte anche quelle del relay, e solo quelle; la 443 resta disponibile dietro lo smistatore per nome (SNI) che la condivide con il travestimento del tunnel.
La 443 dei nodi italiano e tedesco e' condivisa con il sito: nginx legge il nome richiesto (SNI) senza aprire la connessione e la passa al relay o al sito. Per chi guarda la rete, una chiamata dietro un firewall aziendale e' traffico TLS sulla 443, indistinguibile da una pagina web.

## RELE' SUL DOMINIO UFFICIALE (novita' della 7.9.0)

| | |
|---|---|
| Nome annunciato dal nodo italiano | **turn.lattice-network.it** |
| Certificato del relay | **lo stesso del sito, con turn.lattice-network.it nel** |
| Nome vecchio (app gia' installate) | **167-233-85-189.nip.io, ancora instradato sulla 44** |
| Cruscotto pubblico /rete-rele | **HTTP 200 · API 200 in 123 ms** |
| Impronte esposte in pubblico | **0** |
| Porte di inoltro del relay finlandese | **49160-50999 (prima 41 porte in tutto)** |

## CRUSCOTTO DEI RELAY (dalla 7.9.0 anche in pubblico: /rete-rele)

| | |
|---|---|
| Foglio dei tre relay a sessione valida | **HTTP 200** |
| Senza sessione | **RIFIUTATO (401)** |
| Relay che rispondono alle proprie misure | **3 su 3** |
| Tempo di composizione del foglio | **208 ms** |

Il cruscotto mostra canali aperti, biglietti emessi e le dieci impronte piu' attive per fermare chi munge il relay. L'impronta e' SHA3-256 dell'indirizzo troncata: nel registro l'indirizzo non entra affatto, quindi nemmeno il cruscotto puo' dire chi stava chiamando. Oltre la soglia l'abuso finisce nel registro a catena e la striscia del Canarino diventa rossa.

## ZERO GOOGLE (verificato sul binario, non sulla parola)

| | |
|---|---|
| Esito del referto di rete | **ASSOLUTO** |
| Indirizzi dei servizi Google nel binario | **0** |
| Credenziali Google sul server | **NESSUNA** |
| Token Google nella base dati | **0** |
| Reti di Google vietate nel kernel | **77** |
| Nodi della rete allineati alla stessa versione | **SI** |

## REGRESSIONE: TUTTE LE SUITE STORICHE, RILANCIATE

| | |
|---|---|
| test_v790 (dominio ufficiale e cruscotto pubblico) | **49 superati · 0 falliti** |
| test_v781 (tre relay e cruscotto) | **52 superati · 0 falliti** |
| test_v770 (relay a tempo) | **36 superati · 0 falliti** |
| test_v744 (rete e attestato) | **57 superati · 0 falliti** |
| test_v743 (nodi allineati) | **45 superati · 0 falliti** |
| test_v740 (nodo puro) | **43 superati · 0 falliti** |