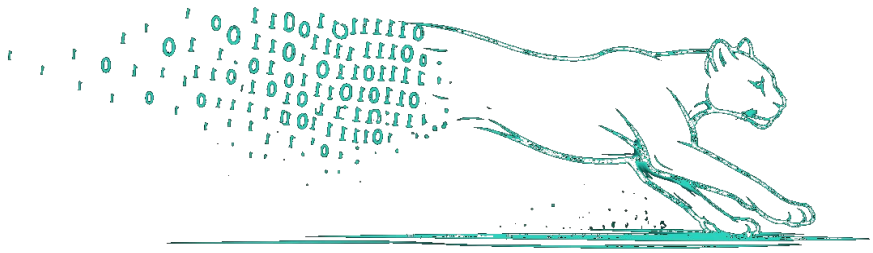
# PumaMesh Relay



*Software-Defined Secure Router. Zero Knowledge. Line-Rate Forwarding.*

A lightweight, STIG-hardened mesh router that forwards encrypted traffic between PumaMesh nodes across network boundaries — through NAT, firewalls, air-gapped enclaves, or WAN segments. **It sees routing metadata. It never sees file content.**

| ~50 MB | 25/29 | 10 sec | 0 bytes |
|---|---|---|---|
| Idle memory footprint | STIG controls implemented | HA failover time | File content stored |

## Zero-Knowledge Forwarding

| Relay Sees | Relay Cannot See | Relay Does Not Do |
|---|---|---|
| • Source & destination agent ID<br>• Transfer hash (routing key)<br>• Shard size & TTL<br>• Network addresses | • File names or content<br>• Classification markings<br>• PII/PHI data<br>• Encryption keys | • Store files<br>• Scan or classify content<br>• Decrypt payloads<br>• Run AI/LLM inference |

## Core Capabilities

✓ **Line-Rate Forwarding** — Two forwarding modes: stream relay (reliable QUIC uni-streams) and FEC datagram relay (unreliable QUIC datagrams). Both forward raw bytes unchanged — no decompression, no decryption, no re-encoding. Datagram relay patches only a single TTL byte in-place.

✓ **Multi-NIC Boundary Routing** — Up to 8 network interfaces with independent QUIC endpoints per NIC. Cross-NIC forwarding is zero-copy. Sit at the boundary between LAN segments, WAN links, VPC networks, or air-gapped enclaves and route traffic across all of them.

✓ **Automatic NAT Traversal** — Detects NAT'd peers by comparing self-reported vs observed QUIC source address. Announces relay_for=[nat-peer] via gossip so other nodes route through it. Behind-NAT nodes initiate outbound — no inbound ports required.

✓ **High Availability** — Primary/secondary pairing with 3-second heartbeat and 10-second failover. 8 HA slots support up to 16 relays (8 primary + 8 secondary). Optional DNS failover via RFC 2136 dynamic DNS with TSIG authentication.

✓ **BGP-E Route Integration** — Participates in PumaMesh Flow's dynamic routing. Advertises relay capacity (0–100) via gossip. Overloaded relays are automatically penalized in route scoring. Flap dampening suppresses unstable relays.

✓ **STIG Hardened** — 25 Application STIG controls implemented: 15-char passwords with complexity, bcrypt cost-12 hashing, 3-attempt lockout, TLS 1.3 only, mTLS, CSRF tokens, session timeouts, systemd sandboxing (ProtectSystem=strict, NoNewPrivileges=true).

## Architecture

| Port | Protocol | Purpose |
|---|---|---|
| **443** | HTTPS | Minimal web GUI (topology view + certificate management) |
| **8443** | HTTPS | REST API + Swagger UI (16 authenticated endpoints) |
| **9443** | QUIC | Control plane — gossip, peer discovery, key exchange, routing updates |
| **9444–9459** | QUIC | Data plane — forwarded transfers (Up to 16 ports per NIC, scales with NIC count) |

## Relay vs Hub

| Aspect | Relay | Hub |
|---|---|---|
| **Purpose** | **Route encrypted traffic** | Store, scan, classify, search files |
| **Binary size** | **~15 MB** | ~200 MB |
| **Memory (idle)** | **~50 MB** | ~500 MB |
| **Data stored** | **Routing state only** | Files + catalog + findings + audit |
| **QUIC data ports** | **Up to 16 per NIC** | 16 |
| **API endpoints** | **16** | 80+ |
| **ABAC** | **Pass-through** | Full pre-filter + post-filter |
| **Scanning** | **None (opaque data)** | 120+ patterns, 40+ parsers |
| **Search** | **None** | FTS5, Find, federated SQL |

### Bandwidth Management

✓ **Token bucket rate limiting** — per-NIC and global caps with 2-sec burst
✓ **Capacity signaling** — 0–100 advertised via gossip, scored in routing
✓ **Per-NIC bandwidth cap** — configurable Gbps limit per interface
✓ **Forwarding metrics** — FEC bytes, stream bytes, per-NIC, per-peer

### Security

✓ **TLS 1.3 only** — mTLS with FIPS 140-3 OpenSSL (#4282)
✓ **PQ key exchange** — X25519MLKEM768 on every connection
✓ **HMAC-SHA256 gossip** — every message authenticated
✓ **Loop prevention** — TTL field, self-loop check, 8-hop max

## Deployment

Single RPM install. Configure mesh role, TLS certs, and bootstrap peers. Start with systemd. Relay immediately discovers peers from its peer cache — no gossip wait required on restart. Peer state persists across reboots for instant convergence.

**Deploy at Every Network Boundary. Route Everything. Store Nothing.**

**sales@pumamesh.com** | **pumamesh.com**

PumaMesh Inc. | April 2026 | Written in Rust. Built on Open Standards.