AegisWire

ARCHITECTURE, TRUST MODEL, AND EVIDENCE BUNDLE

Post-Quantum Secure Transport for Regulated Industries

A technical whitepaper on the AegisWire platform — for CISOs, security architects, network engineering, GRC teams, and procurement.

Version 1.0 · Published April 2026 · Distribution Evaluation · NDA

AegisWire is operated by ITLOX LTD, registered in England & Wales.

sales@aegiswire.com · compliance@aegiswire.com

Executive Summary

Critical-infrastructure operators, banks, healthcare systems, regulated professional-services firms, and public-sector agencies face the same structural problem in private connectivity: the VPN and zero-trust-access products in production today were designed before the post-quantum threat was a scheduled regulatory event. As a consequence, nearly every bit of encrypted traffic moving through the enterprise perimeter is fit for **"harvest now, decrypt later"** — capture today, decrypt once a cryptographically-relevant quantum computer arrives, retrospectively read everything.

AegisWire is a purpose-built secure-transport and enterprise-VPN platform designed to be the exception. **Every connection through AegisWire, on every customer, in every deployment model, uses hybrid post-quantum encryption as the default and only mode.** There is no commercial-grade downgrade path, no per-tenant weaker cipher, no classical-only lane. Data captured today remains captured — not read.

Around that cryptographic foundation, AegisWire adds four further enterprise-grade properties that distinguish a governed enterprise VPN from a repackaged commodity tunnel:

- **Automatic breach containment** — continuous per-session rekeying so that compromise of one session key cannot spread to other sessions or expose past or future traffic.
- **Centrally-enforced signed policy** — policy authored in the management platform is cryptographically verified at every gateway, eliminating drift, tampering, and silent override.
- **Privacy-preserving monitoring** — full operational visibility without content inspection.
- **Verifiable software supply chain** — every release ships with a Software Bill of Materials (SBOM), reproducible-build attestations, signed release manifests, and an audit-evidence bundle.

AegisWire is delivered as managed SaaS, dedicated single-tenant cloud, self-hosted / sovereign, or customer-controlled hardware appliance. The cryptographic posture, trust model, and policy enforcement are identical in every delivery mode. Only the operational boundary changes.

1. The Threat Picture

1.1 Harvest-now, decrypt-later

"Harvest now, decrypt later" (HNDL) is the current operational assumption of any adversary with access to fibre taps, cloud transit, or compromised intermediate network equipment: **capture encrypted traffic at scale today, store it, and decrypt it when the tooling arrives.** Three factors have converted this from a speculative concern into an operational one:

1. **Hardware inevitability.** Cryptanalytically-relevant quantum computing (CRQC) is no longer a question of mathematical possibility. Milestones have moved from open research into public industry roadmaps with target windows in the early-to-mid 2030s.
2. **Storage has become free.** Multi-year storage of bulk encrypted traffic at state or criminal-enterprise scale is now economically trivial.
3. **Statute-of-limitations thinking is obsolete.** Banking, healthcare, legal, defence, and regulated-professional-services communications carry an expected confidentiality horizon of 7–30+ years. Any session encrypted today using pre-post-quantum algorithms will, with high probability, be readable by adversaries within that horizon.

1.2 The regulatory response

The regulatory environment has moved to match the threat:

YEAR	EVENT
2024	NIST finalises the post-quantum cryptographic standards.
2025	UK NCSC publishes post-quantum migration guidance.
2027	New US national-security systems **must** support CNSA 2.0.
2030	CNSA 2.0 is **exclusive** for new commissioning.
2031	Full enforcement begins.

CNSA 2.0 — the US NSA's Commercial National Security Algorithm Suite 2.0 — is the procurement-ready form of this regulation. UK NCSC PQ-migration guidance tracks the same parameter-set strengths. European DORA, NIS2, and the UK Telecommunications Security Act push the same direction from a different angle.

1.3 What this means operationally

An organisation procuring a new VPN, ZTNA, or secure-transport platform in 2026 has a narrow window to avoid two predictable failures:

- **Failure A — HNDL exposure.** Every session established on a classical-only platform contributes to an adversary's harvest.
- **Failure B — Forced 2030 retrofit.** Every classical-only system deployed now will need a disruptive cryptographic retrofit on a hard regulatory deadline, during a window in which every other regulated organisation is attempting the same migration.

AegisWire is designed so customers can move past both failures in a single procurement.

2. Design Goals

AegisWire was designed with five binding goals:

1. **Post-quantum by default, everywhere.** Every session, every customer, every packet, every deployment — one cryptographic posture. No cipher negotiation to a weaker suite. No classical-only lane for low-tier customers.
2. **Cryptographic agility as a first-class operational property.** The long-term risk to a single-suite deployment is that a specific suite is later weakened by cryptanalysis. AegisWire mitigates this by maintaining a pre-registered emergency replacement suite drawn from a fundamentally different mathematical family — compiled, continuously validated, and ready for cutover under a pre-documented operational procedure.
3. **Integrated, not assembled.** Encryption, policy, identity, gateway selection, and operational governance are one coherent system — not separate products loosely connected under a shared dashboard. Security failures most commonly appear at the boundaries between subsystems; AegisWire eliminates those boundaries by design.
4. **Evidence-backed, not claim-based.** Every procurement cycle ends with a security-review committee asking "how do we know?" AegisWire is designed so the answer is always a file — SBOM, reproducible build attestation, signed release manifest, audit evidence bundle, architecture documentation, threat model, incident response runbook.
5. **Deployable where the customer needs it.** The same cryptographic posture, trust model, and policy enforcement runs in managed SaaS, dedicated cloud, self-hosted sovereign, and hardware-appliance modes. Customers choose the operational boundary that fits their data residency, classification, and compliance model.

3. Architecture Overview

AegisWire is organised into three logical layers.

3.1 The client

A native client runs on every end-user device — macOS, Windows, Linux, iOS, and Android. The client implements operating-system-level kill-switch enforcement, secure in-tunnel DNS resolution, policy-driven traffic routing (full-tunnel or split-tunnel based on administrative intent, not user preference), and seamless roaming across wired, Wi-Fi, and cellular networks without session interruption.

Every client uses the same cryptographic posture. Mobile clients do not receive a weaker build. Linux clients are not missing enforcement features. The client consumes signed policy and signed trust-chain artefacts from the management platform and verifies them on receipt.

3.2 The global gateway network

AegisWire operates a global regional gateway network with pools in multiple regions. Gateway pools are the cryptographic and policy enforcement layer of the platform. Every session terminates at a gateway that:

- Verifies the client's cryptographic presence against the signed trust chain.
- Verifies the published policy applicable to the client's tenant, user, and device.
- Enforces default-deny — connectivity requires explicit authorisation, not the absence of an explicit denial.
- Applies privacy-preserving monitoring for operational visibility without ever inspecting content.
- Participates in DDoS-resistant connection setup — connection establishment requires proof of origin before resource commitment.

Gateway pools support controlled draining, capacity-aware scaling, and deterministic failover. Connection-affinity routing keeps established sessions stable during pool membership changes.

3.3 The management platform

The management platform is the customer's authoritative control surface. It authors and publishes signed policy, manages identity and certificate lifecycles, operates the enterprise admin console, and issues the evidence bundle. Three properties are worth emphasising:

1. **Policy is signed end-to-end.** Policy authored in the management platform is cryptographically signed. Gateways verify the signature before applying. There is no silent publication path, no stale cache that survives policy change, no way for a gateway to enforce a policy that was never authored.
2. **Certificate management is automated.** Certificate issuance, rotation, and revocation are integrated platform operations. Revocation propagates through the trust chain, not just the directory.
3. **Tenant isolation is structural.** Each customer tenant operates with dedicated management-platform resources, isolated database, and separate key material. Cross-tenant data leakage is prevented by structure, not by policy gating.

3.4 The evidence layer

Running alongside the architecture is an evidence pipeline that emits, for every release and every operationally-significant action, verifiable artefacts: SBOM, reproducible-build attestations, signed release manifests, policy-publication audit trail, incident response runbook, and the bundle used in formal security review.

4. Trust Model

The trust model is the answer to five questions a security-review committee will ask about AegisWire. Each answer is concrete and available in the evaluation bundle.

4.1 Confidentiality — "Can the adversary read our traffic?"

Every session is protected with hybrid post-quantum encryption. Both the classical component and the post-quantum component must succeed for key agreement to complete. An adversary must break both to read a session. Data captured today for future decryption is protected against an adversary who later holds a cryptographically-relevant quantum computer and who has broken the classical component.

4.2 Integrity — "Can the adversary modify or replay our traffic?"

Every packet is authenticated and replay-resistant. Tampered, duplicated, delayed, or injected packets are rejected. The wire format is deterministic and supports byte-level verification, which removes malleability as a vector.

4.3 Authenticity — "Can the adversary impersonate a client or a gateway?"

Both client and gateway identity are established by signed trust chains, not shared secrets or static credentials. Device enrolment binds device identity to user and policy relationships at onboarding; connectivity requires verified enrolment, not just valid credentials. Credential refresh and revocation are managed platform operations; revocation propagates through the trust chain, not just the directory.

4.4 Forward and post-compromise security — "If a session key is ever stolen, what is the blast radius?"

Forward secrecy is structural: past traffic is not recoverable from a stolen session key. Automatic breach containment — continuous in-session rekeying — bounds the window during which a stolen session key is useful and prevents compromise from spreading to other sessions.

4.5 Observability without surveillance — "How do we operate this without turning it into a monitoring tool?"

Privacy-preserving monitoring is the production default. Operational visibility — gateway health, session counts, policy enforcement outcomes — is available without content inspection, payload logging, or cross-tenant aggregation. The platform is designed so that an operator cannot, even with full administrative access, read a customer's traffic.

5. Operations and Evidence

The value of any security platform is determined, in procurement and audit, by the evidence the vendor can produce on the first call. AegisWire ships a standard evaluation bundle which is available under NDA:

- **Software Bill of Materials (SBOM)** — per release, in industry-standard CycloneDX or SPDX format.
- **Reproducible-build attestations** — independent parties can rebuild the exact release artefacts byte-for-byte from source.
- **Signed release manifests** — every binary, every container image, every client release signed; signing provenance documented.
- **Architecture documentation** — the internal version of this paper, with full component detail.
- **Threat model** — the adversary model, assumed capabilities, mitigations, and residual risk.
- **Incident-response runbook** — escalation paths, named on-call roles, customer-notification SLAs, forensic-preservation procedure.
- **Sub-processor list** — the current, versioned list of every third party that processes any part of customer-adjacent data, with purpose and region.
- **Data Processing Addendum (DPA)** — published, with UK IDTA and EU SCCs attached.
- **Service Level Agreement (SLA)** — availability, response-time, and resolution-time commitments with service-credit terms.
- **Vulnerability disclosure policy** — published, with a security@aegiswire.com contact and a clear safe-harbour commitment.
- **Source-code escrow** — available on request through a third-party escrow agent for regulated customers who require it.

Evaluation customers typically receive this bundle in week one of engagement, sufficient to pass their internal security-review committee.

6. Deployment Models

AegisWire delivers the same cryptographic posture, trust model, and policy-enforcement surface across four deployment models. Customers choose based on residency, isolation, and operational-control requirements — not based on security capability.

6.1 Managed SaaS

AegisWire operates the management platform and gateway network for the customer. The customer retains full policy authorship, administrative control, and certificate ownership. This is the fastest path to production and the operational default for customers whose compliance regime permits vendor-operated infrastructure.

6.2 Dedicated single-tenant

AegisWire operates a dedicated, isolated management-platform instance and dedicated gateway infrastructure for the customer. Custom update schedules and tenant-specific operational controls are available. This is the standard option for regulated customers who require stronger isolation than a shared-fleet managed service but do not want to operate the platform themselves.

6.3 Self-hosted / sovereign

The customer operates AegisWire inside their own cloud account, data centre, or sovereign enclave. The customer controls every component — infrastructure, update cadence, network boundaries, and data residency — with AegisWire providing the software, trust anchors, signed releases, and operational support. This is the model for customers with strict sovereignty, classification, or air-gap requirements.

6.4 Hardware appliance

AegisWire ships a rack-mount hardware appliance for customer-controlled edge enforcement. The appliance runs the same AegisWire trust model, policy enforcement, and cryptographic posture as the cloud deployment. This is the model for branch, field, and enclave use cases where a local enforcement point is required.

All four models share the same evidence bundle, SLA structure, DPA, and sub-processor list — adjusted only for who operates each boundary.

07 Security and Compliance Posture

AegisWire ships one cryptographic standard. Every customer, every session, every packet — aligned to the US NSA's CNSA 2.0 mandate, UK NCSC post-quantum migration guidance, and the NIST post-quantum standards that underpin both. This posture is built into the engineering; it is not retrofitted at procurement.

Standards implemented today

Every standard below is live in the platform as shipped. These are public standards, verifiable by technical inspection under NDA. The engineering posture is uniform across every deployment model — managed, dedicated, self-hosted, and hardware appliance.

STANDARD	AEGISWIRE POSTURE
US NSA CNSA 2.0 (2027–2031 mandate)	Every session uses the CNSA 2.0 parameter sets. Uniform across tenants. No downgrade path, no negotiation to a weaker cipher. This is the posture the mandate will require of new national-security systems from 2027 — AegisWire ships it today.
UK NCSC post-quantum migration guidance (2025)	The same cryptographic stack satisfies both CNSA 2.0 and UK NCSC's published migration guidance. One implementation answers both regimes.
NIST post-quantum standards (ML-KEM, ML-DSA family)	Hybrid post-quantum key agreement built on the NIST-finalised parameter sets. Classical and post-quantum components must both succeed for key agreement to complete; an adversary must break both to read a session.
NIST FIPS 140-3 (engineering posture)	The cryptographic module is engineered to FIPS 140-3 Level 2 / Level 3 design patterns — approved algorithms, boundary-enforced key lifecycle, tamper-evident build chain. Formal CMVP validation is tracked on the certification roadmap below.
UK GDPR · EU GDPR	Privacy-preserving architecture by design — no content inspection, no payload logging, no cross-tenant aggregation. A Data Processing Addendum (including UK IDTA and EU SCCs) and a published sub-processor list are bundled with every commercial engagement.
Software-supply-chain integrity (SLSA, SSDF-aligned)	SBOM (CycloneDX / SPDX), reproducible-build attestations, signed release manifests, and a per-release audit evidence bundle are published today. Every binary that runs is byte-for-byte verifiable against the source that was reviewed.

Certification roadmap

AegisWire's certification posture is deliberate: each third-party attestation is commissioned alongside the commercial engagement that scopes it, rather than collected as marketing inventory ahead of customer demand. The architecture below is built to carry every one of these certifications; the audit schedule is driven by customer commercial contracts, not by a blanket programme.

ATTESTATION	ENGAGEMENT MODEL
SOC 2 Type II	Commissioned on customer scope. Architecture and evidence bundle pre-built against the Trust Service Criteria.
ISO 27001	Commissioned on customer scope. ISMS practices documented and followed internally; formal certification timed to the first customer whose procurement requires it.
NIST FIPS 140-3 (CMVP validation)	Commissioned at Federal L5 engagement. The cryptographic module is already built to the Level 2 / Level 3 design patterns; the NVLAP-lab submission ($500k+) is triggered by the first national-security customer contract.
NIS2 (EU) formal attestation	Commissioned alongside EU critical-infrastructure engagements. Incident-response, SLA, and evidence artefacts are structured to drop into NIS2 operator-of-essential-services scope.
HIPAA Business Associate Agreement	Available under commercial engagement. Healthcare customers receive a negotiated BAA alongside the MSA.
PCI DSS Attestation of Compliance	Commissioned on customer scope for card-data environments. Not required for AegisWire's default deployment surfaces.
FedRAMP (US)	Commissioned with sponsoring agency. The sovereign deployment model is the carrier; the 3PAO engagement is scoped with the customer.
NCSC Foundation Grade / CAPS (UK)	Commissioned on UK MoD supply-chain engagement. Cryptographic-module validation work already aligns with the submission requirements.

If your procurement requires a specific attestation as a contract condition, raise it in the commercial conversation — the audit is scoped alongside the engagement.

8. Engagement Model

AegisWire engagements are engineering-led, not sales-led. The first conversation is a working session between your architects and ours, not a capabilities slide deck. A typical engagement follows five steps:

1. **Discovery call** — 30 to 45 minutes. Your environment, your compliance posture, your identity provider, your constraints.
2. **Architecture briefing** — a deep technical session against your reference architecture, under NDA. Nothing is out of scope.
3. **Proof of concept** — time-boxed, in your environment, with your identity provider and policy set. Jointly-agreed acceptance criteria. No charge for a scoped POC on the path to a commercial engagement.
4. **Commercial** — MSA, DPA, SOW, and SLA. Invoice-based annual terms. Procurement-standard paperwork. Customer-paper MSAs accepted for larger accounts.
5. **Delivery** — named Solutions Engineer, named Customer Success contact, named incident hotline, and a documented escalation path.

Purchase orders, NET 30 / 60 / 90, multi-year locks, and marketplace transactions (AWS and Azure) are all supported. Source-code escrow and dedicated-instance options are available for customers whose compliance model requires them.

Contact

Sales & commercial: sales@aegiswire.com

Compliance & procurement: compliance@aegiswire.com

Security disclosure: security@aegiswire.com · policy

Trust Center: aegiswire.com/trust

Architecture briefing: aegiswire.com/contact