Quantum Bridge

Product Data Sheet

Quantum Fabric

A double-encrypted, compliance-ready overlay
No MPLS lock-in, no third-party hold on your cryptography.

Platform

Quantum Fabric is a high-assurance VPN platform designed for organizations that need secure, policy-driven connectivity across sites, cloud networks, and remote users. It combines a modern overlay architecture with layered encryption and distributed key trust to reduce single points of failure while keeping operations manageable at scale.

The platform supports day-to-day VPN access and true site-to-site connectivity with stronger cryptographic posture, stronger key governance, and better control of traffic paths between nodes and routed networks.

Architecture

The design is inspired by the operational principles behind NSA CSfC-style layered protection: independent security controls, clear separation of duties, and resilient cryptographic workflows. In practical terms, Quantum Fabric uses an inner encrypted transport for workload traffic and an outer encrypted transport for network transit, then continuously rotates shared secrets through a distributed key exchange model backed by multiple security hubs.

What is DSKE?

Distributed Symmetric Key Establishment (DSKE) is a key establishment protocol uniquely based on symmetric cryptography. Multiple Security Hubs independently distribute cryptographic material (PSRD) to clients. Clients can then use the Security Hubs as brokers to negotiate symmetric keys which can be used to authenticate and encrypt further communication. As Security Hubs are independent of each other, the final DSKE keys are only known to the clients, leveraging a secret-sharing scheme, which also provides reliability against Hub failure or compromise.

Key Features

- Quantum Safe Security
- Easy setup and management
- Minimal configuration
- Protected by DSKE
- No firewall configuration needed
- Authentication with SSO
- Intuitive policy management
- Configure and manage DNS
- Site-to-Site Connectivity

Security

- Independent Cryptographic Tunnels
  - ChaChaPoly1305 + PQC PSK
  - AES-256-GCM + DSKE PSK
- Designed for CSFC Multi Site Connectivity for Top Secret Data over the Public Internet
- Defense-in-depth encryption
- Multi-hub trust model

Management

- Centralized policy control
- Unified peer onboarding
- Dynamic route orchestration
- Automation-ready RPCs
- Secure-by-default posture
- Rich runtime visibility
- Dual-range network planning

Contact Us

+1-249-225-5099

contact@qubridge.io

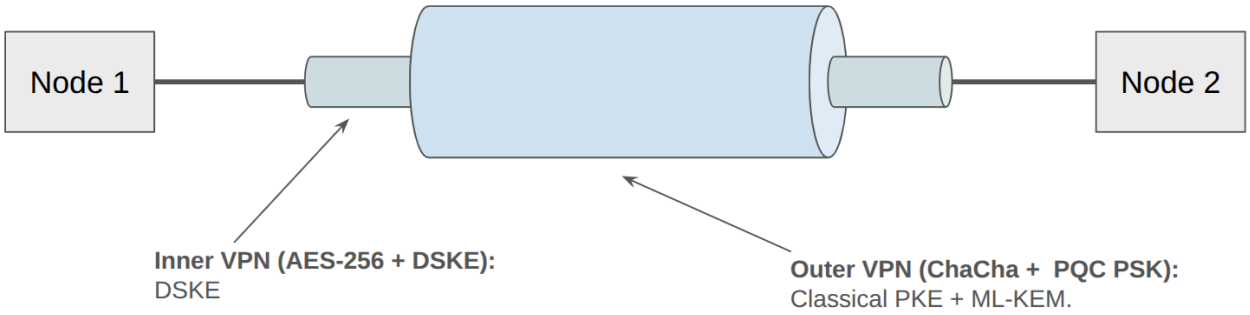
How it works

Step 1 - Authenticate

Every node authenticates to a central management service first. That service defines identity, discovers approved peers, and distributes network rules and policy.

Step 2 - Connect

Distributed STUN/TURN and relay servers enable NAT traversal even behind the toughest firewall rules - creating a trusted baseline VPN for all participating nodes under centralized control.



Step 3 - Secure Mesh

Security hubs and workload nodes coordinate DSKE-based key workflows to establish an additional encrypted mesh layer - keeping onboarding simple while strengthening cryptographic posture.

Step 4 - Route and Scale

Routing nodes advertise and forward site networks, interconnecting branch offices, datacenters, and cloud segments through policy-controlled paths.