QUNU

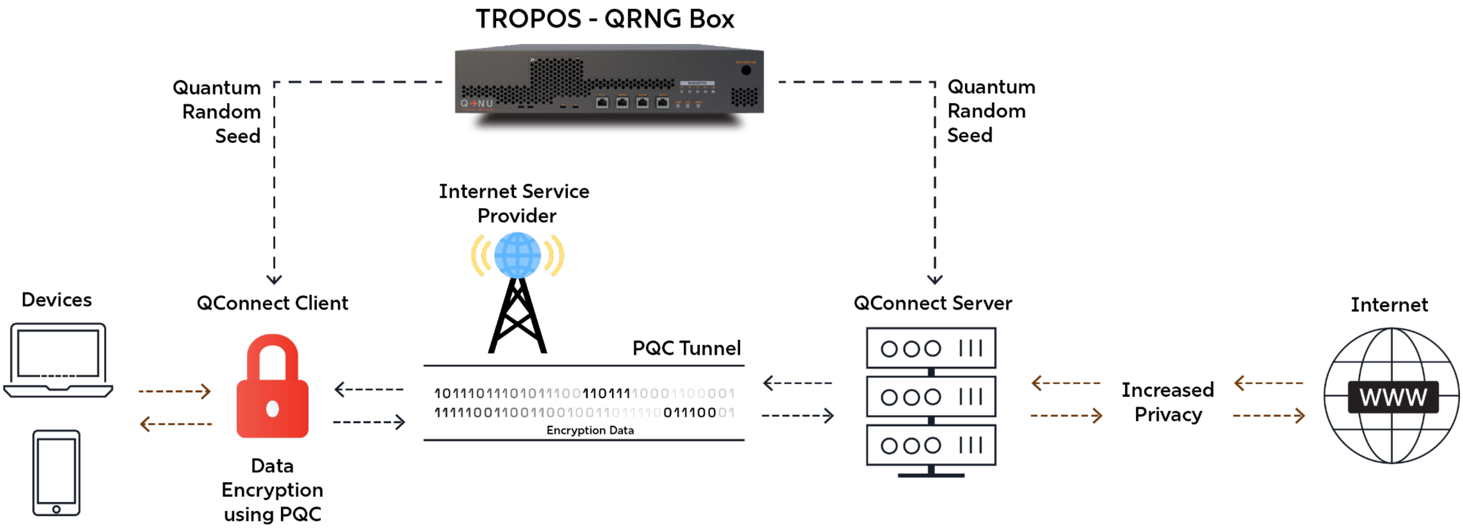
Secure Your Data Journey with QShield™ QConnect: Advanced Encryption for Tomorrow's Security Challenges.

Introduction

Safeguard your data exchanges in transit with QShield QConnect, a future-oriented encryption system of link security enhanced with quantum-resistant, unpredictable keys.

QShield™ QConnect uses **Crystals-Kyber 1024** for key exchange and **AES-256-GCM** for authenticated encryption, ensuring robust security against classical and quantum attacks. Utilizing **TLS 1.3** with post-quantum cryptography, QShield™ QConnect creates a secure tunnel for complete data protection.

QShield™ QConnect Architecture



Key Elements of QShield™ QConnect

- **QShield™ Platform: -** Central Provisioning and Management server.
- **QShield™ QConnect: Server -** Hosts a single peer node acting as a server, establishing a secure tunnel and awaiting connections from multiple clients.
- **QShield™ QConnect: Client -** Includes a single peer node acting as a client, responsible for establishing a secure tunnel connection with the QShield™ Connect server.

Features

QShield™ Platform	
Server and Server Instance Management	Easily add and manage servers and their instances. Configure and customize server settings as needed.
Dashboard Display	Display server and server instance information prominently on the dashboard. Real-time updates on server status and performance.
Server Tunnel Control	Start and stop server tunnels effortlessly through intuitive controls. Ensure efficient resource allocation and management.
Secure Client Management	Add and manage clients/users securely. Associate clients/users with specific server instances for streamlined access.
Secure Tunnel Establishment	Utilize cutting-edge PQC-based authentication for robust security. Clients and servers authenticate themselves securely before establishing connections.
Certificate and Configuration Distribution	Automatically provide clients/servers with respective certificates and configurations post-authentication. Simplify setup and ensure secure communication channels.
Monitoring Dashboard	Monitor server tunnel usage effectively with comprehensive dashboard analytics.

QShield™ QConnect: Client	
Client Authentication	Seamlessly authenticate clients through Platform to obtain necessary credentials for secure connections. Ensure a streamlined and secure authentication process for clients.
TLS 1.3 Based Secure Connection	Utilize the latest TLS 1.3 protocol for establishing secure connections between clients and servers. Enhance security and performance with robust encryption and authentication standards.
Dynamic QConnect Server IP Access	Dynamically retrieve QConnect server IP addresses from configuration files provided by Platform.
Quantum-Safe Channel Establishment	Establish secure, quantum-safe channels between clients and servers for enhanced security against quantum threats.
Data Encryption and Authentication	Encrypt and authenticate all application data using AEAD (Authenticated Encryption with Associated Data) algorithms.

QShield™ QConnect: Server	
Platform Authentication	Seamlessly authenticate servers through Platform to obtain necessary credentials for secure connections. Ensure a streamlined and secure authentication process for clients.
TLS 1.3 Based Secure Connection	Initiate server tunnels using the TLS 1.3 protocol to await client connections. Enhance security and performance with the latest in encryption and authentication standards.
Re-keying Provision with Configurability	Offer configurable re-keying options to generate new sets of handshake keys (PQC-based), encryption, and decryption keys. Enhance security and adaptability by allowing periodic key updates as per user-defined configurations.
Quantum-Safe Channel Establishment	Establish quantum-safe secure channels upon client connection using TLS 1.3 protocol. Mitigate potential quantum threats by ensuring secure communication channels.
Dynamic AES-256-GCM Key Generation	Generate AES-256-GCM encryption/decryption keys upon secure channel establishment. Provide robust encryption for all application data transmitted over the secure channel.