



CQX WAVE-PLUS 100 SERIES PQC TRANSLATION PROXY PRODUCT BROCHURE

© 2026 CeQureX Technology Limited. All rights reserved.

No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of CeQureX Technology Limited, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law.

PRESENTED BY
CeQureX Technology Limited

CQX Wave-Plus 100 Series PQC Translation Proxy Product Brochure

This official specification introduces the **Wave-Plus 100 Series Post-Quantum Cryptography (PQC) Translation Proxy** for enterprise systems. Designed to facilitate a seamless security migration, the series is delivered via **hardware appliance, virtual machine (VM), or containerized deployment** under a software subscription model.

The platform's unrivaled value is its "**Zero-code change**" capability, allowing organizations to migrate web services to PQC without modifying any application source code. By operating as a **reverse proxy**, Wave-Plus establishes quantum-resistant TLS encryption channels while ensuring total **backward compatibility** with traditional cryptographic standards. This is the ideal solution for bringing legacy systems into the post-quantum era seamlessly.

1. Product Overview

Product Positioning: Next-Generation Quantum-Safe Infrastructure – The Definitive Traffic Proxy Gateway. The **Wave-Plus 100 series** is a future-ready and intelligent traffic proxy gateway, architected specifically for the post-quantum era. By empowering with hardware-accelerated PQC, it serves as the essential security anchor for organizations transitioning to quantum-resistant standards without compromising infrastructure performance.

Core Values:

- 1. Seamless PQC Migration (Zero-Code Change)** We eliminate the complexity of cryptographic upgrades. Our solution enables organizations to adopt Post-Quantum Cryptography across their entire web service architecture with **zero modifications to application source code**. This "drop-in" readiness ensures a risk-free transition at a fraction of the traditional development cost.
- 2. Quantum-Resistant Hybrid Security** We provide the best of both worlds. By acting as a high-performance **reverse proxy**, Wave-Plus establishes robust, quantum-resistant TLS channels while maintaining **full backward compatibility** with classical cryptographic mechanisms. This ensures uninterrupted service for legacy systems while securing them against future quantum threats.
- 3. Performance-Driven Resilience** Security should never be a bottleneck. Optimized for high-load environments, Wave-Plus maintains ultra-low latency and high connection throughput. Our hardware-level acceleration ensures that as you adopt the mathematically heavy algorithms of the post-quantum era, your user experience remains fast, fluid, and responsive.

2. Solution Architecture

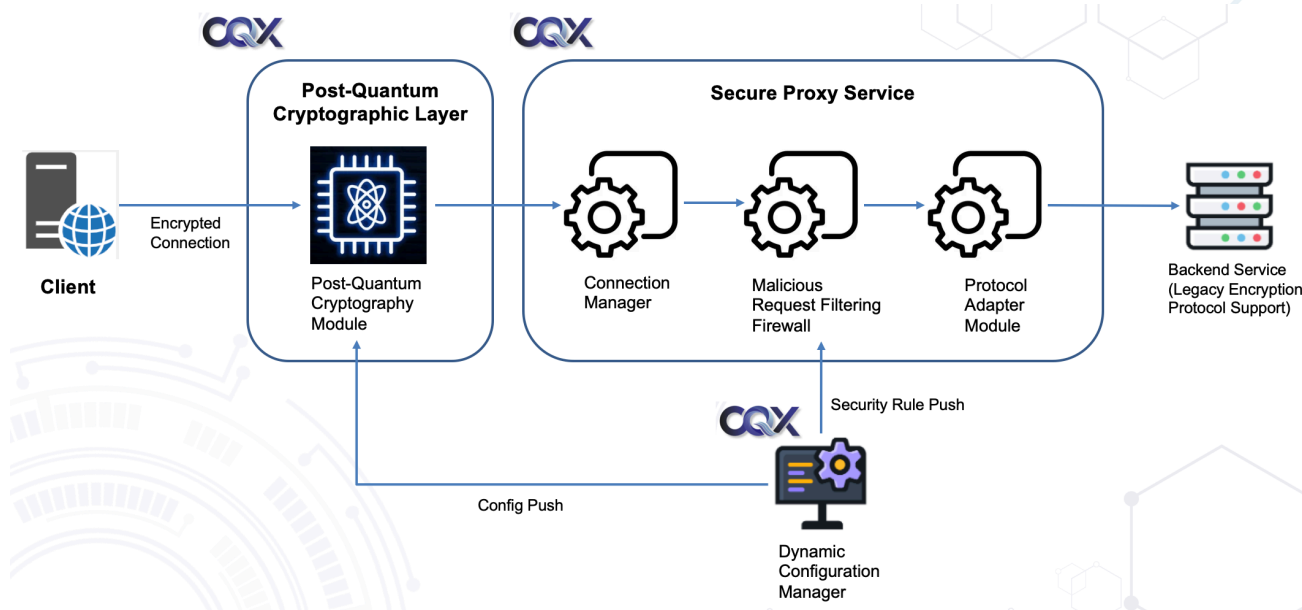


FIGURE 1 – SOLUTION ARCHITECTURAL DIAGRAM OF CEQUREX WAVE-PLUS 100 SERIES PQC TRANSLATION PROXY

The system adopts a **multi-layered secure proxy architecture** centered on **post-quantum cryptography**. Client requests are first encrypted by the Post-Quantum Cryptography Module, then sequentially processed within the Secure Proxy Service through a Connection Manager, a Malicious Request Filtering Firewall, and a Protocol Adapter Module before being forwarded to the backend service.

A centralized Dynamic Configuration Manager enables **real-time propagation of security policies and cryptographic parameters** at runtime, eliminating the need for service interruption during reconfiguration.

3. Technical Features

3.1. Hybrid PQC TLS Module: Advanced Cryptographic Orchestration

The Wave-Plus 100 series employs a sophisticated **Hybrid PQC TLS Module** designed to bridge the gap between classical infrastructure and quantum-safe standards. It ensures that every handshake is optimized for maximum security without compromising connectivity.

- **NIST FIPS 203 Compliance (ML-KEM/Kyber):** Our module offers native, full-stack support for the **NIST-standardized Kyber (ML-KEM)** algorithm. By implementing high-performance Key Encapsulation Mechanisms (KEM), we ensure that session key exchange is mathematically resistant to future Shor's algorithm-based quantum threats.
- **Defense-in-Depth: Hybrid Dual-Layer Encryption:** We utilize a "best-of-both-worlds" cryptographic approach. By **simultaneously combining classical Elliptic Curve (ECC, e.g., X25519) or RSA** with the Kyber algorithm, we create a multi-layered security wrapper. This prevents a single point of failure: even if a quantum breakthrough occurs or a new vulnerability is found in one algorithm, your data remains protected by the other.
- **Smart "Zero-Friction" Downgrade Fallback:** Designed for 99.999% service availability, our **intelligent handshake negotiation** engine ensures seamless user experiences across a diverse client landscape:

- **PQC-Native Discovery:** Automatically negotiates and establishes a **Quantum-Safe Channel** when the client demonstrates PQC capability.
- **Deterministic Fallback:** If the client is restricted to legacy protocols, the module executes an **instant, secure fallback** to classical ECC or RSA. This ensures universal service accessibility while maintaining the strongest possible encryption supported by the endpoint.

3.2. Backend Proxy & Legacy System Integration: The Cryptographic Bridge

The Wave-Plus 100 series acts as a high-performance intermediary, enabling modern, quantum-safe connectivity for backend infrastructures that are otherwise restricted by legacy limitations.

- **Seamless Architectural Offloading:** Our solution functions as a dedicated cryptographic front-end, **completely offloading PQC handshakes** and intensive cryptographic operations. By shifting the "mathematical tax" of post-quantum math to our specialized hardware, we significantly reduce the computational burden on backend servers, reclaiming their CPU cycles for application logic and improving overall system throughput.
- **Intelligent Legacy System Support:** We ensure that existing infrastructure remains functional and secure without requiring costly hardware or software overhauls.
 - **High-Velocity Plaintext Forwarding:** For legacy servers residing within secure, air-gapped, or internal trusted networks, the device executes high-speed decryption and forwards traffic as **Standard HTTP**. This allows the backend to remain simple and fast while the Wave-Plus handles the complex PQC-secured perimeter.
- **Legacy Encryption Bridging (TLS 1.2 Translation):** To resolve critical compliance gaps, the device supports bidirectional encryption translation. For internal systems restricted to older standards, the Wave-Plus can initiate secure **TLS 1.2 connections** to the backend. This resolves compliance and compatibility issues for legacy Operating Systems (OS) that are physically unable to support modern TLS versions, effectively future-proofing aging infrastructure.



THANK YOU

We are a team of dedicated Ph.D.-level cybersecurity experts and passionate pioneers in post-quantum cryptography and quantum-secure networking.

Our mission is to be the region's leading partner in building sovereign, quantum-resilient infrastructure, enables our partners/clients to agilely discover, plan and transform their security systems to quantum-grade protection across multi-cloud environments—including on-premise data centers, AWS, GCP, and Azure.”.

ADDRESS

8 F.-5, No. 19, Jingye 1st Rd., Zhongshan
Dist., Taipei City 104051, Taiwan (R.O.C.)

E-MAIL

sales@cequirex.com

WEBSITE

www.CeQureX.com