SOLUTION BRIEF

Fortinet and Quantum Xchange Team to Deliver Quantum-Safe SD-WAN

Immediate Quantum-Safe Security to the Fortinet Network's Edge

Executive Summary

Fortinet and Quantum Xchange have partnered to offer powerful crypto-diverse and quantum-safe security capabilities to Fortinet Secure SD-WAN environments. Phio TX from Quantum Xchange works with the Fortinet FortiGate Next-Generation Firewall (NGFW), to transmit a secondary-symmetric key down a quantu m-protected tunnel and mesh network, making data transmitted between sites within a Fortinet SD-WAN or virtual private network (VPN), immediately more secure and impervious to many cryptographic threats, including quantum attacks.

Challenge

Shor's algorithm proves quantum computers are capable of breaking modern public key cryptography. Because encryption is so embedded at the endpoint, changing encryption is hard, disruptive, and resource intensive. It can require modifying or replacing libraries, validation tools, hardware, operating systems, application code, device protocols, and user/administrative procedures–on every network node. This leads to disruptions, downtime, and lost productivity. And it's unclear if the transition to NIST-backed Post-Quantum Cryptographic (PQC) algorithms will be a one-time change or an iterative process requiring the continuous swapping of cryptography for decades to come.

The quantum threat aside, encryption suffers from risks and vulnerabilities other than advanced mathematics or increased computing power. Weak entropy sources leading to key and certificate collisions; programming and implementation errors; reliance on a single trusted user responsible for key input and management–all contribute to cryptography shortcomings and potential points of failure within most enterprise environments.

Security-focused government entities and commercial enterprises understand these everyday crypto challenges and are looking for next-generation solutions that bypass brute-force attacks, overcome everyday programming and key management errors, protect long-duration data, and easily future-proof their network environment for the quantum era. Fortinet and Quantum Xchange have partnered to deliver this solution simply, affordably, and with no network interruptions or downtime.

Joint Solution

The crypto-agile and crypto-diverse capabilities of Phio TX, coupled with its unique out-of-band key technology and adherence to the ETSI QKD protocol and data format for open standards-based key delivery makes it ideally suited for the Fortinet Security Fabric. No other key delivery system supports all forms of quantum-safe

Solution Components

- Fortinet FortiGate Next-Generation Firewall
- Fortinet Secure SD-WAN
- Phio TX from Quantum Xchange
- Solution Benefits

Solution Benefits

- Instantly upgrade all FortiGate VPN and Fortinet Secure SD-WAN connections to be quantum-safe.
- Gain immediate NSM-8 and NSM-10 compliance with a crypto-diverse approach that is FIPS 140-2 validated.
- Deploy NIST-backed PQCs with zero downtime on upgrade and rekeying, zero-latency, zero-packet loss.
- Overcome inherent vulnerabilities of public key encryption using out-of-band, quantum-safe key delivery.

FORTINET FABRIC-READY

encryption including all NIST-supported, post-quantum cryptographic (PQC) algorithms, Quantum Random Number Generated (QRNG) keys, or Quantum Key Distribution (QKD) where Layer 1 security is critical. The vendor-agnostic and platform-independent key delivery system allows customers to select the level of quantum-safe security needed based on their data inventory requirements and risk tolerance levels delivered through the ETSI-compliant FortiGate NGFW.

Solution Components

Phio Trusted Xchange (TX) by Quantum Xchange

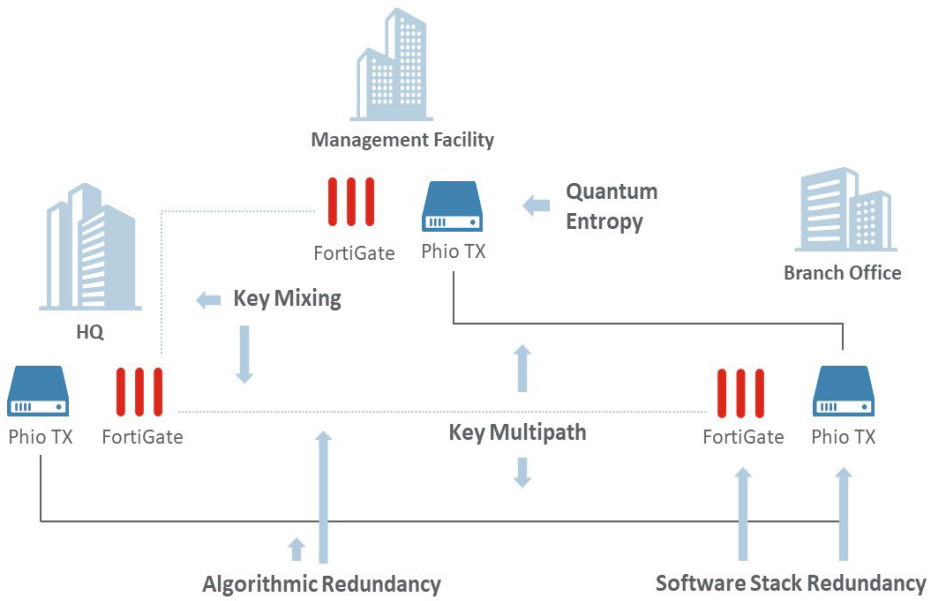
Phio TX is a first-of-its-kind, crypto-diverse key delivery system that supports encryption keys generated by any source, protected by any method (PQC, QKD, or a combination), to update any connection (existing routing, VPN, and SD-WAN infrastructures) to quantum-safety without adding a hop in the wire. The FIPS-validated solution and technology overlay effortlessly plugs into the existing crypto infrastructure to generate on-demand ephemeral key pairs that replace static pre-shared keys, sent out-of-band down a separate quantum protected tunnel and mesh network.

By completely decoupling the cryptographic key generation and delivery from the existing infrastructure, users achieve significant security benefits while gaining flexibility. The platform incorporates point-to-multipoint intelligent key routing and can operate over any TCP/IP connection and network media type to deliver quantum-generated keys anywhere on the planet. With Phio TX, users can switch or upgrade cryptographic algorithms without incurring packet drops or added latency.

FortiGate NGFWs utilize purpose-built security processors and threat-intelligence security services from artificial intelligence (AI)-powered FortiGuard labs to deliver top-rated protection and high-performance inspection of clear-texted and encrypted traffic. FortiGate NGFWs reduce cost and complexity with full visibility into applications, users, and networks and provide best-of-breed security. Other products that complement the FortiGate security profile include FortiGate Secure Web Gateway and FortiWeb.

Joint Solution Integration

Multisite environments that leverage FortiGate Wide Area Network (WAN) connections, such as SD-WAN and VPN tunnels, are instantly upgraded to next-generation cryptography by deploying Phio TX alongside the main FortiGate appliance. Each time the FortiGate gateway establishes a tunnel connection to a remote site or data center, an additional quantum-safe symmetric key is supplied and delivered to both sides in an out-of-band manner. This ensures the connection is NSM-8 and NSM-10 compliant and makes use of the latest NIST-approved PQC algorithms without incurring packet loss or latency. The end-user can simply configure each FortiGate appliance to request cryptographic keys from one of the Phio TX virtual or physical instances to upgrade the connection to quantum-safe encryption.



Multisite deployment deployment of Phio TX and FortiGate integration for quantum-secure SD-WAN

Joint Use Cases

Use Case #1: Avoid Premature System Obsolescence with Crypto-Diverse Infrastructure
Organizations with current or planned network infrastructure projects should embrace crypto-diversification and make quantum safety part of the approach—or risk premature system obsolescence. The FortiGate NGFW and Phio TX combination ensures your data and communications links are protected with the strongest encryption available and can be switched or swapped without a packet dropped as technology evolves and new cryptographic methods are introduced.

Use Case #2: Bring Quantum-Level Security to the New Disparate Workforce
Data in transit between two computers happens more in the Covid-era than ever before, as employees, and in some cases entire organizations, have moved to a remote-work format. Add to this the acceleration of digital transformation–moving resources to the cloud, deploying functionality at the edge, and connecting branches and remote workers to the digital enterprise–and the need for secure remote access means future-proofing networks is essential. With FortiGate, the Phio TX edge device, Phio TX-D, makes quantum-safe VPN possible.

Use Case #3: Meet Federal Quantum-Resistant Mandates with Ease
For government clients who must meet strict quantum-resistant mandates outlined in National Security Memorandum (NSM) 8, NSM 10, and The Quantum Computing Preparedness Cybersecurity Act, the FortiGate and Phio TX integration is especially attractive because it allows government agencies to avoid replacing their current cryptosystems or embarking on an expensive multiyear, even iterative, crypto-migration project to be quantum-safe and compliant.

About Quantum Xchange

Quantum Xchange gives commercial enterprises and government agencies the ultimate solution for protecting data today and in the quantum future. Its award-winning, crypto-diverse key delivery system, Phio Trusted Xchange (TX), mixes asymmetric, symmetric, and quantum-based encryption methods, i.e., post-quantum crypto (PQC), Quantum Random Number Generated (QRNG) keys, and Quantum Key Distribution (QKD) sent out-of-band down a separate quantum-protected tunnel and mesh network. Decoupling key generation and delivery from data transmissions allows organizations to practice crypto-agility with no network interruptions while experiencing the cost-benefits of making their existing crypto environment immediately quantum-safe. To learn more about future-proofing your data from whatever threat awaits, visit QuantumXC.com.

FORTINET

www.fortinet.com

September 6, 2022 2:52 PM | 1680740-0-0-EN