SOLUTION BRIEF

Fortinet and QuintessenceLabs Quantum-Enhanced Security

VPN/DCI Data Encryption Augmented by Quantum Technologies for Quantum-Safe Protection of Data in Transit

Executive Summary

Fortinet and QuintessenceLabs have partnered to help you build a quantum-resilient future for your organization. This gives you the opportunity to use today's technologies to prepare for tomorrow's quantum impacts.

The Challenge

Quantum computing will disrupt the way all industries currently do business. Quantum cyberattacks have the potential to completely disrupt all commonly secured data, information systems, and infrastructure, and, by extension, to impact the privacy and security we enjoy today significantly. This presents identity and security issues for various websites, applications, and transactions. Furthermore, in Harvest Now, Decrypt Later (HNDL) attacks, cyber spies steal encrypted data that they believe holds long-term value, anticipating that the data can be decrypted later. Securing keys has never been more urgent, and this issue is one of the biggest challenges in data security.

Joint Solution

QuintessenceLabs and Fortinet have collaborated to fortify your defenses and step confidently into the quantum era. QuintessenceLabs products harness quantum science and seamlessly integrate with existing Fortinet FortiGate NGFWs in your security infrastructure to quickly and cost-effectively strengthen your data in transit protection.

FORTINET FABRIC-READY

Solution Components

- Fortinet FortiGate Next-Generation Firewall (NGFW)
- QuintessenceLabs Trusted Security Foundation (TSF) Enterprise Key and Policy Manager
- QuintessenceLabs qStream Quantum Random Number Generator (QRNG)
- QuintessenceLabs qOptica 100 Quantum Key Distribution (CV-QKD)

Bringing the Fortinet FortiGate and QuintessenceLabs TSF and qOptica products together in an integrated solution delivers advanced quantum-safe protection for data in transit in your organization.

Solution Components

QuintessenceLabs' quantum-enabled solutions integrate with today's encryption technologies to offer quantum resilience now and seamlessly transition to a post-quantum world.

qStream - Quantum Random Number Generator (QRNG)

Perfectly unpredictable true random numbers form a foundational layer for quantum security. They instantly strengthen all cryptosystems and represent the new norm in random number generation. They are also available as-a-service.

Trusted Security Foundation (TSF) - Enterprise Key and Policy Manager (KMS)

A centralized and vendor-neutral encryption key management solution tackles the toughest key management challenges. It provides crypto agility and is adaptable to quantum-resistant algorithms.

qOptica 100 - Quantum Key Distribution (QKD)

Our CV-QKD technology is the most secure means of distributing keys, protected by the laws of physics. It can be easily integrated into legacy infrastructure through various APIs and represents a significant step toward providing a proven quantum-safe crypto environment.

Fortinet FortiGate NGFW

FortiGate NGFWs protect data, assets, and users across today's hybrid environments. Built on patented Fortinet security processors, they accelerate security and networking performance to effectively secure the growing volume of data-rich traffic and cloud-based applications. FortiGate NGFWs, backed by FortiGuard AI-Powered Security Services, help prevent cyberattacks and mitigate security risks with consistent, real-time protection.

Use Cases

Use case #1:

Enhance security by providing additional key material for VPNs. This addresses the issue that most VPN equipment uses asymmetric crypto to exchange AES keys, which has been proven not to be quantum-safe.

QuintessenceLabs TSF is a secure platform for generating, distributing, storing, managing, and controlling cryptographic objects, including quantum-resistant keys and other cryptographic material. It allows flexible deployment of classical, QRA, and hybrid crypto algorithms.

In this first integrated solution use case, TSF delivers separate encryption AES-256 key into local and remote encryption and VPN FortiGate devices. It is achieved using a single centrally located TSF instance powered by QuintessenceLabs high-speed QRNG. The standardized ETSI GS QKD 014 API provides the key delivery process. This additional key material is then mixed with the existing SA key material into the FortiGate devices, creating, in that manner, "super session" keys (per RFC8784). This instantly increases your security posture over the WAN. The AES-256 keys are short-lived and automatically removed from the TSF after being retrieved by the FortiGate NGFW.

Solution Benefits

- Instantly increases your security posture over the WAN by delivering additional key material generated out of a QRNG into local and remote FortiGate devices
- Uses the laws of physics to secure key distribution between FortiGate DCI devices, ensuring long-term confidentiality, regardless of any future advances in computer sciences and mathematics
- Prepares your organization for tomorrow's quantum threat
- Unparalleled protection using the Fortinet FortiGate NGFW and the Fortinet Security Fabric

Furthermore, the TSF key and policy manager integrates the qStream QRNG, which provides access to the highest quality random numbers for generating keys or other cryptographic objects.

Finally, FortiOS IPsec SA keys can also be retrieved from the TSF server using KMIP. Here, keys are persistent and stored on the TSF platform. This feature allows the FortiGate to offload the task of generating IPsec SA keys to a TSF server, regardless of specific IPsec VPN topologies with a FortiGate, when the administrator requires centralizing cryptographic key management in a KMS server.

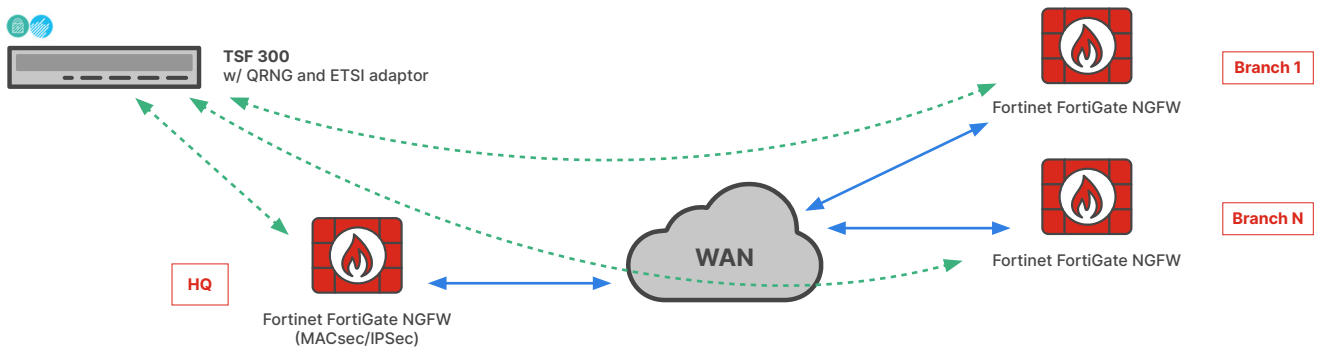

Figure 1: Additional key material for VPNs

Use Case #2:

Prevent HNDL attacks through QKD for ultra-secure Data Center Interconnect and Metropolitan Area Networks.

Your business continuity and security plan must address the acknowledged risk of HNDL attacks. In this scenario, cybercriminals, often state-sponsored, quietly download large amounts of mission-critical data that will still hold value in a decade or longer.

Ultra-secure DCI and MAN

QKD ensures the secrecy of the encryption keys through the laws of quantum physics. No advancements in computing power or crypto-analysis will be able to break the QKD protocols, including quantum computers. QKD secures data against advanced attacks using specialized hardware to enable the fast exchange of secure keys. Keys are sent point-to-point using an optical link and are known only to the shared parties.

QuintessenceLabs qOptica 100 CV-QKD system can be coupled with FortiGate equipment to distribute secret keys into a pair of AES symmetrical encryptors. These keys are usually mixed with the original FortiOS exchanged keys (dual key agreement), resulting in "super AES session keys," offering quantum-safe encryption to the data in transit at high speed.

QuintessenceLabs delivers CV-QKD technology, which offers built-in advantages in terms of cost, form factor, and performance compared to other QKD approaches.

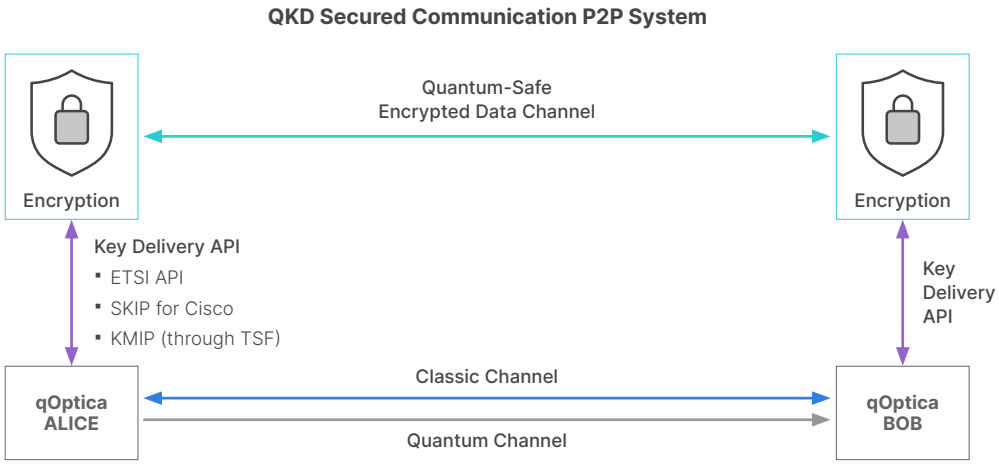

Figure 2: Ultra-secure DCI

About QuintessenceLabs

QuintessenceLabs is at the forefront of quantum cybersecurity, providing the strongest data protection to protect your information against today's and tomorrow's threats. Our capabilities extend from quantum key generation and crypto-agile key management to quantum key distribution, helping you build a quantum-safe future for your organization.

Learn more at quintessencelabs.com

December 26, 2024 1:35 PM / MKTG-557-0-0-EN