

SOLUTION BRIEF

Fortinet and Arqit VPN Encryption Solution

Integrated, Automated Solution Provides On-Demand Quantum-Safe Encryption for Enhanced Protection of VPN Data Communications

Executive Summary

Fortinet and Arqit have partnered to deliver an industry-leading security solution by integrating FortiGate Next-Generation Firewalls with the QuantumCloud™ Symmetric Key Agreement Platform. The solution provides quantum-safe symmetric keys that can be created and rotated on-demand to encrypt and protect sensitive data between point-to-point VPN links. It also delivers enhanced security against today's human-in-the-middle attacks and the future quantum threat, reducing the administrative burden and inefficiencies of current symmetric encryption solutions.

Challenge

Encryption is an essential security and compliance control for safeguarding sensitive data against an increasingly sophisticated threat landscape. Symmetric keys are universally used to encrypt internet traffic; however, current approaches for generating shared symmetric keys between two endpoints are vulnerable to attack and difficult to set up and administer. These approaches include:

- **PKI systems.** These are often complex, and if not correctly configured, organizations increase their risk of attacks and data breaches, in addition to potential risks in the future posed by adversaries using quantum technology for decryption.
- Physical delivery of cryptographic keys. This can be inefficient and restricts the ability to achieve the high-frequency, rapid, and on-demand symmetric key rotation associated with the highest level of security.

Arqit and Fortinet have established a technology partnership to provide organizations with an additional layer of security to protect IPsec VPN traffic against current attacks and the quantum threat, both of which exploit weaknesses in asymmetric (public) key cryptography. The joint solution also improves efficiency, flexibility, and scalability at a lower cost.

Joint Solution

The integration of Fortinet FortiGate Next-Generation Firewalls with the Arqit QuantumCloud SKA Platform provides quantum-secure symmetric keys that can be used to enhance the security and manageability of IPsec VPN connections between customer locations.

Each FortiGate (physical or virtual) securely connects to its designated Arqit QuantumCloud network adaptor over the local network, using mutually authenticated and encrypted TLS sessions. When point-to-point IPsec VPN sessions are initiated by FortiGate firewalls or re-keying of existing tunnels is

Solution Components

- Fortinet FortiGate
 Next-Generation Firewall
- Arqit QuantumCloud Symmetric Key Agreement (SKA) Platform
- Arqit QuantumCloud Network Adaptor (NA)

Solution Benefits

- Creates quantum-secure data links and supports a quantumsecure deployment
- Mitigates risks and complexities associated with PKI for data in transit
- Usable with existing and proven data encryption standards, such as AES256
- Provides enhanced security, operational efficiency, and cost reduction through on-demand key rotation
- Scalable creation of symmetric keys between any connected FortiGate firewalls, no distribution of keys





required, each participating firewall requests a shared quantum-safe key from its respective local network adaptor server, using the standardized ETSI 014 network protocol. The Arqit network adaptors agree to a shared symmetric key with each other, using the QuantumCloud SKA Platform as the key broker. The keys are delivered in near real time to the requesting firewalls over the ETSI interface. The FortiGate firewalls use the keys in constructing the IPsec VPN tunnel to provide enhanced data protection.

The QuantumCloud Cloud Console can define and enforce organizational security policies that govern FortiGate firewall registration and permissions, symmetric key strength, and key usage. It also enables centralized configuration management, audit tracking, and health visibility of deployed QuantumCloud network adaptors.

Solution Benefits (cont.)

- Easy-to-use Arqit console for device management and policy enforcement, e.g., for device permissions, grouping, and key rotation rate
- Supports zero trust: quantumsecure session keys are known only to FortiGate firewalls and never sent across the network

Solution Components

Arqit QuantumCloud Symmetric Key Agreement Platform

QuantumCloud is a cloud-based software solution that replaces or layers on top of existing PKI asymmetric key agreement technologies to deliver an entirely new way to create high entropy and unbreakable shared symmetric keys as often as required. Keys can be used with standard encryption algorithms like AES, enabling easy integration. QuantumCloud can either be consumed as a Platform-as-a-Service (PaaS) or deployed on-premises to meet data sovereignty and compliance requirements.

Argit QuantumCloud Network Adaptor

QuantumCloud network adaptor is an Arqit software application deployed in the customer's local network and serves as an intermediary to deliver quantum-safe symmetric keys to FortiGate firewalls using the ETSI 014 API interface.

MQTT Broker

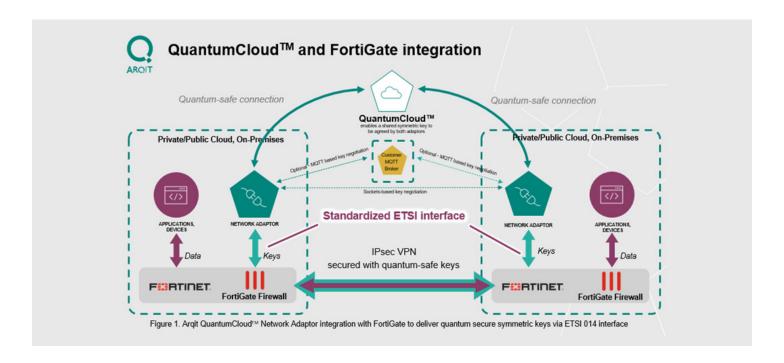
An optional customer-provided MQTT server deployed in the customer's network facilitates secure messaging between QuantumCloud network adaptors across a network. The use of a centralized MQTT broker avoids the need for opening inbound firewall ports to support network adaptor key peering communications.

Fortinet FortiGate

Fortinet FortiGate Next-Generation Firewalls (NGFWs) deliver industry-leading enterprise security for any edge at any scale with full visibility and threat protection. Organizations can weave security deep into the hybrid IT architecture and build security-driven networks to deliver ultra-fast security end to end, enable consistent real-time defense with Al/ML-powered FortiGuard Services, achieve seamless user experience with security processing units, and improve operational efficiency and automate workflows.



Symmetric keys are created and consumed by FortiGate NGFWs (physical or virtual) during the formation of secure IPsec tunnels.



In summary, the Fortinet FortiGate integration with QuantumCloud enables enhanced security of VPN tunnels between FortiGate (physical or virtual) site locations and cloud infrastructure, for the site-to-site IPsec VPN use case.

About Argit

Arqit supplies a unique quantum-safe encryption Platform-as-a-Service that makes the communications links or data at the rest of any networked device or cloud machine secure against current and future forms of attack – even from a quantum computer. Arqit's product, QuantumCloud™, enables any device to download a lightweight software agent, which can create encryption keys in partnership with any number of other devices. The keys are computationally secure, optionally for one-time use, and have zero trust. QuantumCloud™ can create limitless volumes of keys in limitless group sizes and regulate the secure entrance and exit of a device in a group. Arqit believes it is the only company in the market to have achieved an Independent Assurance Review of its Security Proof demonstrating that the software can produce encryption keys that are zero trust and provably secure, i.e., permanently safe against attack from even a full-scale quantum computer. The GCHQ Accredited Centre of Excellence in Cyber Security at the University of Surrey conducted this review. The addressable market for QuantumCloud™ is every connected device. Arqit was recently awarded the Innovation in Cyber award at the UK National Cyber Awards and the Cyber Security Software Company of the Year Award at the UK Cyber Security Awards.



www.fortinet.com