Quantum-Safe Cloud Connectivity: Secure Data Transfers to AWS

Challenges

Quantum threats demand stronger encryption

Traditional VPNs can’t guarantee long-term data confidentiality in cloud environments

As quantum computing advances, existing encryption methods are increasingly vulnerable to "Harvest Now, Decrypt Later" attacks. Enterprises face rising regulatory pressure to protect sensitive data — especially when transferring it to public cloud environments. Traditional VPNs using public-key encryption may soon be inadequate for long-term confidentiality, making quantum-safe solutions a priority for forward-looking organizations.

Sparkle Solution

Advanced security with no impact on performance or existing infrastructure

Sparkle’s Quantum Safe over Internet (QSI) service enables secure, high-performance IPsec VPN connections with post-quantum symmetric encryption even over Internet connectivity. Leveraging Arqit’s SKA platform, Intel NetSec Accelerator cards, and zero-touch by Adtran, Sparkle allows customers to easily provisioning and establish quantum-safe VPN tunnels (NIST and FIPS 140-3) between their sites, data centers or Cloud and AWS regions — ensuring secure end-to-end data transmission without modifying existing infrastructure.

Benefits

Ensure quantum-safe, high-performance data transfers to AWS with simple deployment and zero changes to customer infrastructure

Future-Proof Security

Protect sensitive data in transit against both current and quantum-era threats with symmetric post-quantum encryption (compliant to NIST standards and FIPS 140-3 inside)

Seamless Integration

Deploy easily across existing infrastructure without hardware upgrades or changes to the customer's network environment

High Performance at Scale

Maintain optimal VPN throughput and reliability — even in high-traffic enterprise or multi-cloud scenarios — without performance loss

(Sparkle) Contact: Ettore Pulieri | Ettore.Pulieri@tisparkle.com

Sparkle on AWS

Sparkle's "Quantum Safe to Cloud" offering complements AWS's post-quantum cryptography roadmap by adding robust, future-proof transport layer encryption. Enterprises can confidently run sensitive workloads in the cloud and ensure secure data exchanges to and from AWS. Combined with AWS native security and encryption controls, Sparkle QSI adds another layer of protection for critical verticals like finance, healthcare, and government.

Backed by decades of experience in global connectivity, Sparkle operates an extensive fiber network and has deep expertise in secure cloud enablement. Its Network-as-a-Service model simplifies access to advanced quantum-safe technologies, helping AWS customers accelerate digital transformation with confidence and compliance

SPARKLE

Case Study:

Quantum-Safe Deployment for a Strategic Customer

Challenges

A Sparkle customer needed to ensure long-term confidentiality for sensitive data processed and stored in AWS. They required secure site-to-cloud connectivity that could withstand emerging quantum threats.

Solution

Sparkle deployed its QSI solution between the customer's location and the AWS region using Arqit quantum-safe keys and Intel-based acceleration at the Sparkle PoP.

Results

The customer achieved post-quantum secure VPN connectivity with zero impact on performance, strong key rotation, and compliance with emerging crypto-security standards.

Features

Post-Quantum Ipsec VPN Encryption

Sparkle QSI uses Arqit's symmetric key agreement (SKA) to deliver symmetric keys resistant to quantum attacks. These keys can be integrated with any network layers and injected into the IPsec VPN tunnel. This ensures that data in transit to AWS remains protected even if harvested for future decryption.

Zero-Touch Deployment

The solution runs on Intel's NetSec Accelerator cards, enabling efficient encryption and seamless deployment. Adtran's Ensemble MANO orchestrates the VNFs, allowing Sparkle to scale connectivity to AWS securely and efficiently without hardware reconfiguration..

Visit AWS Marketplace or Sparkle website to purchase or start a Free Trial.

Get started with Sparkle solutions on AWS

aws PARTNER Advanced Tier Services

- Solution Provider
- Public Sector Solution Provider
- Networking Consulting Competency

(Sparkle) Contact: Ettore Pulieri | Ettore.Pulieri@tisparkle.com