Case study

Telecommunications

Embracing Quantum-Safe Connectivity: The future of Secure Internet

Overview

Leading global service provider Telecom Italia Sparkle SpA (Sparkle) offers a comprehensive suite of services tailored to a diverse range of customers including OTTs, carriers, service providers, and enterprises. Their offerings span from secure global IP transit for accessing any internet content to high-performance international bandwidth. Additionally, Sparkle provides a unique array of infrastructure solutions and proprietary colocation services, ensuring top-tier connectivity and security for all their customers.

A leader in delivering advanced connectivity services, Sparkle excels in providing fast, reliable, and secure infrastructure for mission-critical IT systems. Their state-of-the-art solutions ensure top-tier performance and dependability. As such, Sparkle has expressed their ambition to be the world's first quantum-safe internet service provider. This commitment involves ensuring robust protection for the internet links deployed at customer branch offices and sites, setting a new standard for security in the face of emerging quantum computing threats.

Facing the challenge of ensuring secure communication between data centers over the open internet with the promise of forward-secrecy, Sparkle embraced the ambitious project to implement a quantum-safe IPsec solution.

To address the challenge, Sparkle collaborated with Arqit to deploy a sophisticated solution on Intel-based netsec accelerator cards, installed on Dell PowerEdge servers, renowned for their powerful performance and reliability. The project aimed to establish IPsec traffic between both servers such that the data remains quantum- safe from end-to-end, regardless of the route taken over the open internet.

At a glance

Telecom Italia Sparkle SpA - Sparkle

Athens Data Center 'Metamorphosis II', Greece

Global transmission of IP data

International routing infrastructure and global connectivity services for TIM Group

Challenges

Increased threat to customer's sensitive data through sophisticated cyber risk including from a quantum computer

Risk of store now, decrypt later attacks

Requirements

Secure communication between data centers in an open-source environment

Quantum-safe VPN for data in transit

Reliable and scalable solution available today

Fast key rotation over-the-air (OTA)

> **Our NaaS vision is rooted in the belief that connectivity should be seamless, ubiquitous, secure and adaptable. We envision a world where businesses can effortlessly scale their Wide Area Networks, adapting to changing demands with agility and precision. NaaS enables this by offering flexible, ondemand network services that are easily customizable to meet the unique needs of each customer. Whether it's expanding bandwidth during peak times, ensuring low latency for critical applications, or providing secure connections for sensitive data, Sparkle's NaaS solutions are designed to deliver unparalleled performance and reliability.**
>
> – Daniele Mancuso, Chief Marketing & Product Management Officer, Sparkle

Transitioning to Quantum-Safe Connectivity: Defending Against Store Now, Decrypt Later (SNDL) attacks.

As the threat of Store Now, Decrypt Later (SNDL) becomes increasingly significant, it is crucial for Sparkle's customers to transition to quantum-safe connectivity. To combat this evolving risk, telecom companies and internet service providers must upgrade their offerings, ensuring that their networks are equipped to meet the advanced security demands of the quantum era.

Expanding their partnership with Arqit, Sparkle is pioneering the exploration of quantum-safe IPsec connectivity between data centers. The focal point of this groundbreaking initiative is their most advanced data center in Europe, the Metamorphosis II site in Athens, Greece. This state-of-the-art facility was the perfect choice to host the world's first Proof of Concept (POC) quantum-safe internet links, utilizing Arqit's cutting-edge technology.

Metamorphosis II, an open datacenter facility, provides an unparalleled and advanced experience for the most sophisticated customers. It is designed to deliver a fast, open, and resilient configuration, tailored to the needs of carriers, OTTs, and enterprises. This facility ensures direct interconnection for corporate and institutional entities, enhancing their operational efficiency and security.

By leveraging this advanced infrastructure, Sparkle aims to lead the industry in implementing quantum-safe solutions, setting a new benchmark for data security and high-speed connectivity. This initiative underscores their commitment to innovation and excellence, paving the way for a more secure and reliable internet for all.

Pioneering Quantum-Safe Connectivity with Arqit, Intel and Adtran

Sparkle partnered with Arqit, Intel, and Adtran to deploy the quantum-safe VPN solution directly on Intel-based netsec accelerator cards. This collaboration marks a significant leap forward in the quest for robust and future-proof internet security.

Arqit's NetworkSecure Adaptor integrates seamlessly with strongSwan, a widely used open-source VPN library, to create an out-the-box quantum-safe VPN. Leveraging Arqit's SKA-Platform, this setup generates post-quantum, symmetric pre-shared keys (PPK), which are then passed into the strongSwan configuration.

Solving the problem

Solution

Arqit SKA-Platform™ – post-quantum symmetric cryptographic key generation.

Arqit NetworkSecure™ Adaptor – seamless integration of quantum-safe preshared keys with existing infrastructure.

Dell PowerEdge R530 Servers – VM-ready server powered by Intel® Xeon® processors.

Intel-based Netsec Accelerator Cards – offload cryptographic operations to improve throughput and reduce CPU load.

FD.io VPP (Vector Packet Processing) – accelerated network functions for fast, efficient data plane operations.

Adtran Ensemble MANO – management platform for virtualized services.

Adtran Ensemble Connector – high performance switching and virtualization for multi-vendor VNFs.

strongSwan IPsec VPN – secure VPN tunnel creation with encryption and authentication, supporting post-quantum pre-shared keys (PPK) for quantum safe IPsec connections.

Benefits

- Quantum-safe VPN with perfect forward secrecy.
- Zero-trust architecture.
- No loss of performance on the IPsec tunnel.
- Strong authentication.
- Zero downtime, continuous running of IPsec tunnel.
- Configurable re-keying frequency.
- Fast and frequent key rotation – every 3 minutes.

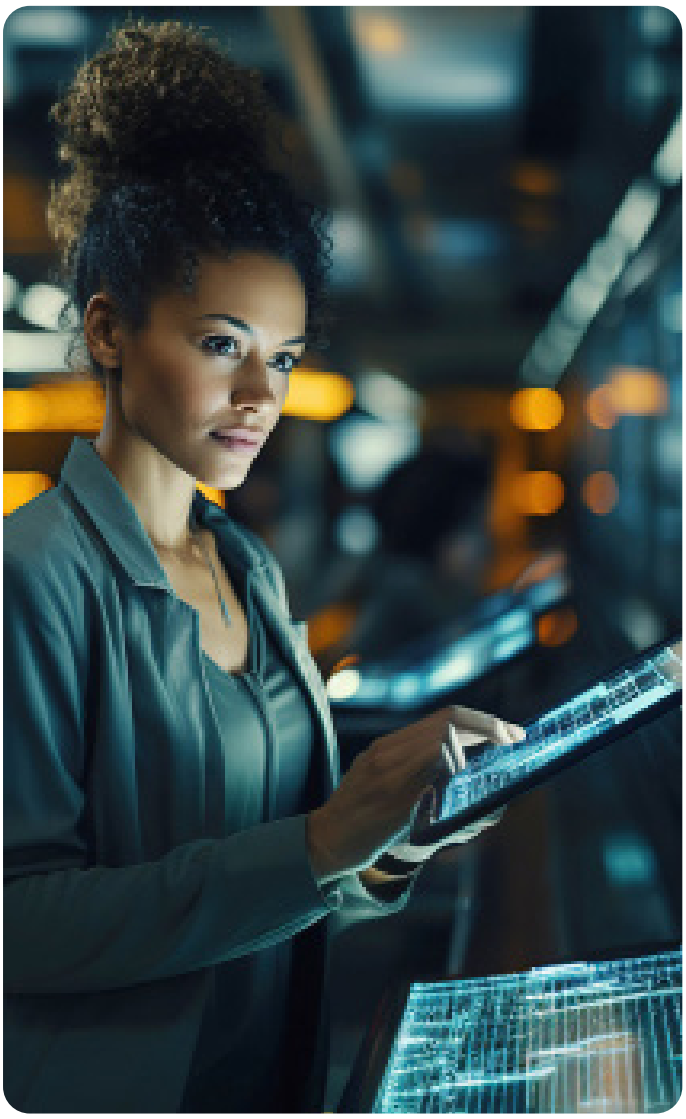
The Intel-based NetSec Accelerator (based on Intel® NetSec Accelerator Reference Design) is a high-performance server on a PCie form factor. This server on a card coupled with an Intel optimized Vector Packet Processing (VPP) strongSwan plugin creates a high-performance IPSec VPN solution that is ready to add Arqit's quantum safe solution. The underlying hardware and software coupled with Arqit's NetworkSecure Adapter enables a highly performant, scalable, and cost optimized solution for edge points of presence that are post quantum cryptography ready.

Adtran then enable zero-touch deployment of the solution through Ensemble MANO, a management platform for the creation and deployment of virtualized services, and the Ensemble Connector, a highperformance switching and virtualization platform that hosts multivendor VNFs. The entire solution can be templated and automatically deployed, allowing the infrastructure to be scaled without the overhead of manual deployment.

This architecture is ideally suited for a quantum-secure point of presence (PoP) server, delivering a high-throughput, quantum-safe VPN connection. For the POC, this advanced system is deployed at Sparkle's Metamorphosis II site – a strategic location serving as the central hub to receive secure connections from other locations, demonstrating the feasibility and efficiency of the solution.

In addition to the robust infrastructure at the PoP, the initiative also leverages universal customer premise equipment (uCPE). These lightweight and inexpensive hardware devices can be easily deployed at customer sites. With Arqit's software integrated, the uCPE can consume Arqit's encryption keys and connect back to the PoP, enabling a quantum-safe internet link directly at the customer premises.

The POC aims to validate the architecture before its rollout in a production environment. By demonstrating the effectiveness of this quantum-safe VPN solution, Sparkle, Arqit, Intel and Adtran are setting new standards in internet security, ensuring that businesses and consumers alike are protected against evolving quantum threats.



Quantum-safe VPN: revolutionizing secure data communication for Sparkle

Sparkle's implementation of a quantum-safe IPsec VPN solution marks a significant advancement in secure internet connectivity. By leveraging the combined strengths of Intel, Adtran, and Arqit, Sparkle has set a new benchmark for data security, paving the way for a secure and resilient network infrastructure capable of withstanding the evolving threats posed by quantum computing.

The primary objective of the project was to construct an architecture with a hub-and-spoke topology, validating it through a proof of concept before expanding the network. Exploratory test cases on key creation and policy options driven by strongSwan and Arqit SKA-Platform were conducted to ensure the solution's effectiveness.

The outcomes of the project were significant and multifaceted. Sparkle successfully established quantum-safe IPsec VPN tunnels, ensuring robust, secure communication between data centers. The team became well versed in Arqit's SKA-Platform and NetworkSecure solutions, gaining valuable hands-on-experience. The project demonstrated the effective deployment of strongSwan and VPP on Intel-based netsec accelerator cards, highlighting their compatibility and performance. High-frequency key rotation was enabled, providing forward secrecy without compromising the IPsec tunnel stability. Zero-touch deployment via the Adtran solution proved effective scalability.

The measurable results included secure encrypted tunnels configured between servers at the Athens site, validating the project's core objective. Additionally, the project evaluated Arqit's enhanced quantum-safe encryption alongside existing VPN products, ensuring comprehensive security integration. The successful deployment and configuration of the Arqit SKA-Platform for an open-source VPN scenario using strongSwan and VPP underscored the feasibility of the solution. Finally, the validation of strongSwan's ability to frequently rotate symmetric keys, facilitated by Arqit, demonstrated the project's effectiveness in maintaining continuous, secure communication.