ARQIT

Product Sheet

NetworkSecure

NetworkSecure™

Integrated, automated, on-demand quantum-safe protection of VPN data communications

Arqit NetworkSecure is a lightweight software application that hardens traditional VPN communications against both traditional man-in-the-middle attacks and Store Now, ecrypt Later[1] quantum attacks. Through a simple integration with existing network infrastructure, NetworkSecure allows organisations to easily and costeffectively adopt a defense-in-depth approach, complying with the latest cybersecurity recommendations from standards bodies like NIST and protecting themselves from devastating future breaches.

[1]SNDL attacks – Encrypted data is harvested today and stored by adversaries with the intent to decrypt it in the future when quantum computers reach sufficient maturity.

Challenges

1. Quantum threat to data-in-transit
2. Time, skills and effort to migrate to post quantum-safe cryptography
3. High cost and management burden of many solutions
4. Compliance with industry standards and regulations

Solution

Arqit's NetworkSecure is an easy to deploy and manage application that seamlessly integrates with a customer's network infrastructure to provide on-demand quantum-safe shared symmetric keys brokered by Arqit SKA-Platform™, Arqit's symmetric key agreement platform. The keys are requested in realtime using the standard-based ETSI-014 API interface and consumed by network devices to provide an additional layer of encryption security, protecting data-in-transit traffic against PKI related attacks and the quantum threat, both of which exploit weaknesses in public key cryptography. The solution improves efficiency, flexibility, and scalability at a lower cost compared to alternative solutions relying on Quantum Key Distribution (QKD) or Post Quantum Algorithms (PQA) alone.

Integrates with:

FORTINET | JUNIPER NETWORKS

Benefits

- Immediately hardens network communications and keeps data secure, preventing devastating SNDL attacks that carry significant financial, compliance, and reputational risk
- Simple, small-footprint overlay to existing infrastructure, avoiding rip-and-replace by integrating seamlessly with PKI and IPsec
- Minimal management overhead, with data easily exportable to existing SIEMs/XRD solutions
- Enables compliance with National Security Memorandum NSM-10 and NSA CSfC Symmetric Key Management Requirements Annex 2.1
- Conforms to NIST standards for cryptography e.g. AES-256, as well as NSA's recommended use of preshared keys to protect against the quantum threat
- Easy-to-use Arqit cloud console for advanced configuration management e.g. endpoint logical grouping and endpoint policies
- Negligible performance and latency impact

Deployment

Arqit NetworkSecure is a small footprint Kotlin (Java) application that is deployed in a customer provided and maintained Linux Virtual Machine (VM) on COTS server hardware within the customer's network. An Adaptor is required per physical or virtual firewall and can support High Availability (HA) active-passive firewall configurations. The Adaptor is installed using a simple provisioning process in a secure logical subnetwork adjacent to network and security devices.

NetworkSecure registers with an instance of SKA-Platform hosted in a selected data centre which provides the source of random material used to generate quantumsafe keys, as well as allows management of the Adaptors through a single, easy to use console.

VM Specifications

- x86 64-bit
- CPU - single Core 2.8GHz / minimum 1 vCPU
- Memory – minimum 2GB RAM
- Disk – minimum 4GB
- Guest Operating System: Ubuntu 22.04 LTS, Oracle Enterprise Linux 8.7, Red Hat Enterprise Linux 8.2, 8.4 and 8.6
- Java Virtual Machine (JVM) (version 17.x)

Other Resources

- NetworkSecure Juniper Product Sheet
- NetworkSecure Fortinet Product Sheet
- NetworkSecure strongSwan Product Sheet
- SKA-Platform Product Sheet