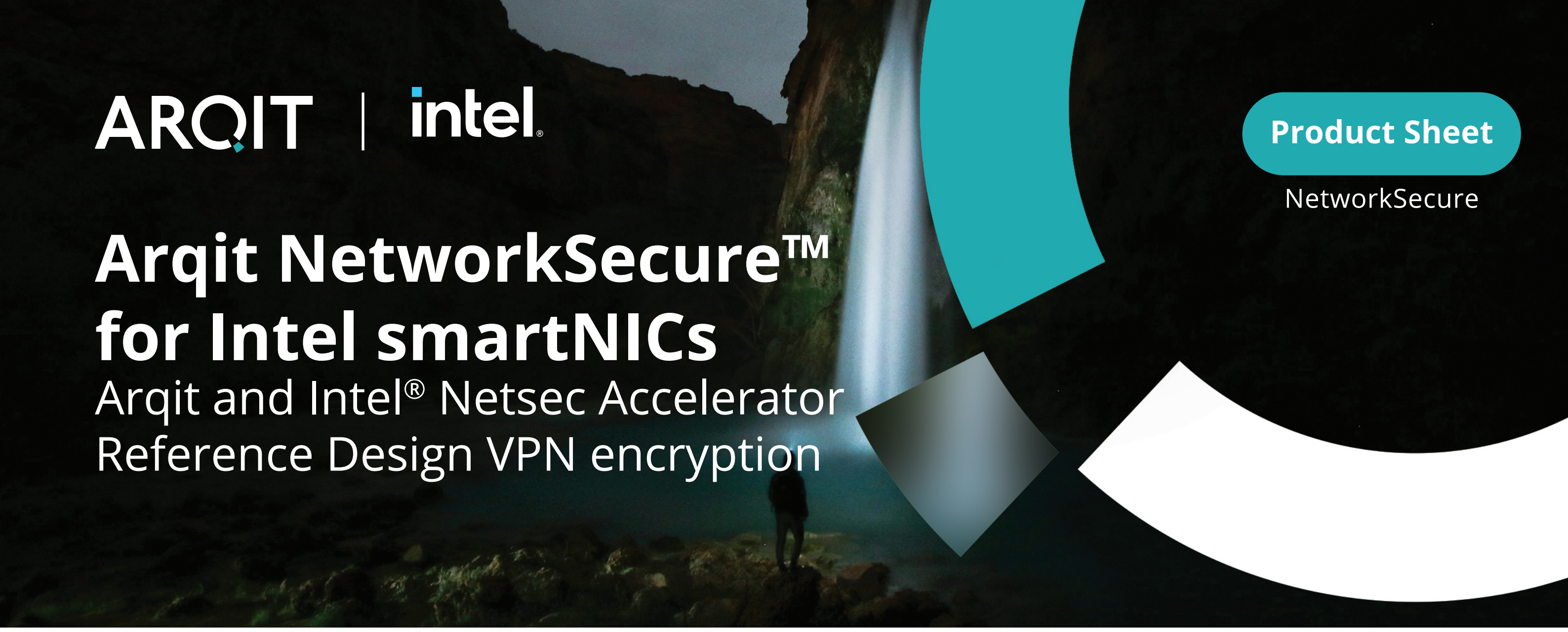


Product Sheet

NetworkSecure

Arqit NetworkSecure™ for Intel smartNICs

Arqit and Intel® Netsec Accelerator Reference Design VPN encryption

High performance, Integrated Post Quantum Cryptography (PQC) IPsec VPN communications

Arqit NetworkSecure is a lightweight software application that integrates seamlessly with Intel's NetSec Accelerator cards to provide high throughput IPsec VPN network communications and protection against Store Now, Decrypt Later[1] quantum attacks. Through a simple integration with Intel's technology that offloads and accelerates network and security workloads, NetworkSecure allows organisations to easily and cost-effectively implement a defencein-depth approach to achieve quantum-resilient encryption and comply with industry standards and government recommendations.

[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.

Solution

Arqit's NetworkSecure is an easy to deploy and manage application that seamlessly integrates with Intel's NetSec Accelerator Cards to enhance the security of high throughput IPsec tunnels created by Intel's FD.io VPP IPsec technology to deliver fast, reliable and quantum-safe communications. NetworkSecure provides on-demand Post Quantum Pre-shared Keys (PPKs) brokered by SKA-Platform™, Arqit's symmetric key agreement platform, which are mixed in with keys generated by the IKE VPN protocol, protecting datain-transit traffic against the quantum threat. The combined solution upgrades classical cryptography to future-proof the security of sensitive data transmitted over public networks. This preserves the benefits of network performance and resource efficiency that Intel smartNICs provide through workload offloading and hardware acceleration.

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

Benefits

- Immediately hardens high-speed communications and keeps data confidential, 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 IPsec and IKE VPN protocols
- Strong, active authentication to mitigate spoofing attacks and frequent rotation of session data keys
- Minimal management overhead, with data easily exportable to existing SIEMs/XDR 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
- Easy-to-use Arqit cloud console for advanced configuration and policy management
- Negligible performance and latency impact

Deployment

The Arqit NetworkSecure Adaptor is a lightweight Kotlin (Java) application that runs in a Linux VM or directly on the Intel Netsec Accelerator Reference Design. The Adaptor is deployed using a simple configuration and setup process where it registers with an instance of SKA-Platform, hosted on-premise or offered as a service.

The SKA-Platform provides the source of key material used by Ne to generate quantum-safe keys locally, as well as allows management of the Adaptors through a central, 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)

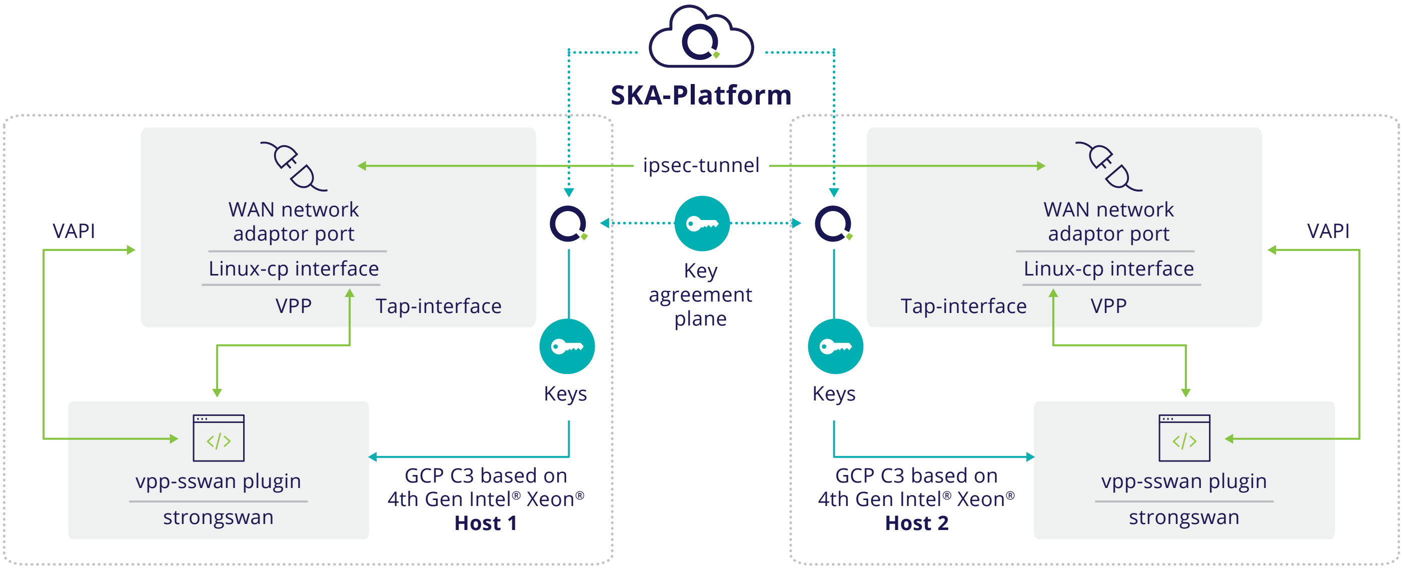
Other Resources

- Solution Brief
- Ordering Guide
- SKA-Platform Product Sheet

Case study - Site-to-Site Post Quantum Cryptography (PQC) IPSec - SKA-Platform and Intel

Arqit has partnered with Intel, a market leader in processor technology, to enhance the security of high performance IPsec VPN site-to-site connections between data centers.

Figure 1. Quantum-secure IPsec architecture using SKA-Platform and VPP-SSwan on two Intel Netsec Accelerator Reference Designs



The solution builds upon the integration by Intel of strongSwan (widely deployed IPsec/IKE standard) with their FD.io VPP-SSwan and Linux-CP technologies to deliver accelerated IPsec packet processing on Intel Xeon Scalable platforms. NetworkSecure Adaptor interoperates with strongSwan and Intel VPP to upgrade the security of IPsec tunnels to provide quantum attack resistance. StrongSwan implements RFC 8784 which allows a PPK to be ‘mixed’ with a IKEv2 negotiated key, resulting in IPsec security associations (SAs) that protect data-in-transit traffic from SNDL and future quantum attacks.

Arqit NetworkSecure Adaptors generate PPKs, brokered by SKA-Platform, on-demand and at scale.

Furthermore, these keys are automatically rotated during the tunnel re-keying process, improving security unlike typical manually provisioned preshared keys which are difficult and costly to change.

Additionally, Intel smartNICs support ‘Full or Partial Appliance Offload’ deployment model whereby 3rd party virtual security appliances e.g. next generation firewalls (NGFW) provide gateway services to directly connected or networked hosts. In these scenarios, NetworkSecure Adaptor can be used to enable quantum safe IPSec tunnels created by NGFWs installed on Intel Netsec Accelerator Reference Design hardware.