ARQIT

Product Sheet

NetworkSecure

NetworkSecure™

Arqit and strongSwan

Integrated Post Quantum Cryptography (PQC) for IPsec VPN communications

Arqit NetworkSecure is a lightweight software application that integrates seamlessly with strongSwan, a widely deployed open-source VPN technology, to protect IPsec VPN network communications against Store Now, Decrypt Later[1] quantum attacks and traditional PKI-based cybersecurity threats. Session keys and authentication credentials are actively rotated on a frequent basis to implement a zero-trust, defense-in-depth approach enabling organisations to easily and cost-effectively 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.

Challenges

1. Protect VPN data-in-transit and identities against cyber attacks
2. Time, skills and effort to migrate to post quantum-safe cryptography
3. High cost and management burden of VPN solutions
4. Compliance with industry standards and regulations

Solution

Arqit's NetworkSecure is an easy to deploy and manage application that seamlessly integrates with strongSwan to protect network communications within IPsec VPN tunnels. 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 data-in-transit traffic against the quantum threat. Symmetric session and authentication keys are actively rotated for each live VPN session to enhance and simplify identity and data security. The combined solution upgrades classical cryptography to future-proof the security of sensitive data transmitted over public networks.

Benefits

- Ensures data confidentiality, preventing devastating SNDL attacks that carry significant financial, compliance, and reputational risk
- Supports multiple VPN topologies: hub & spoke, point-to-point and mesh to secure a wide range of use cases
- Simple, small-footprint overlay to existing infrastructure, avoiding rip-and-replace by integrating seamlessly with IKE and IPsec VPN protocols
- Active online authentication aligned to zero-trust principles with auth keys rotated every VPN session
- Improved security, cost and operational efficiency - data keys actively rotated for each live VPN session
- 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 Adaptor configuration and policy management
- Negligible performance and latency impact

Deployment

The Arqit NetworkSecure software is a lightweight Kotlin (Java) application that runs in a Linux VM which can be deployed within the same VM or alongside a VM hosting the strongSwan VPN software. NetworkSecure 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 NetworkSecure to generate quantum-safe keys locally, as well as allowing 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 – requires less than 1GB 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)

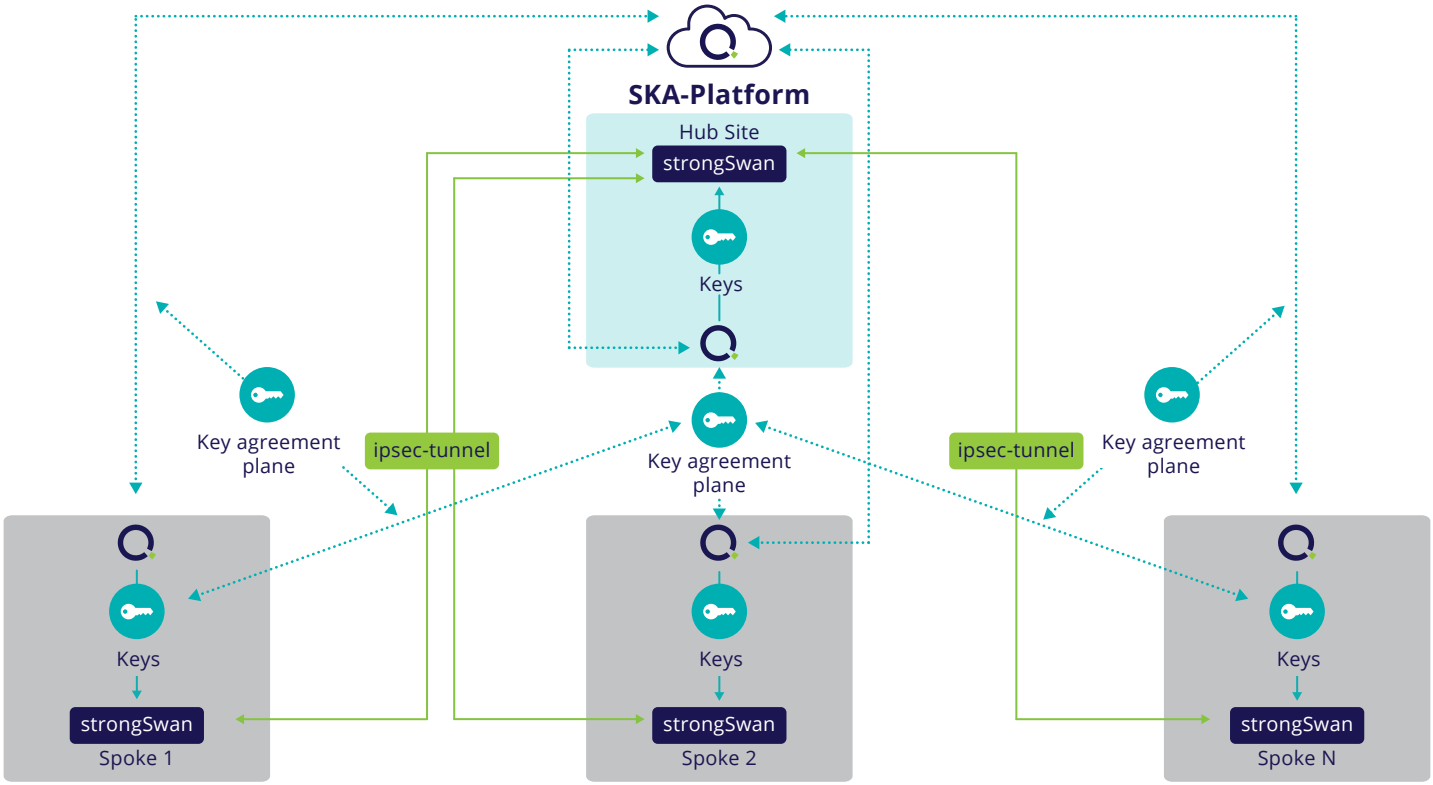
Other Resources

- Ordering Guide
- SKA-Platform Product Sheet

Case study - Hub and Spoke Post Quantum Cryptography (PQC) strongSwan IPSec VPN

Arqit integrates with strongSwan to enhance the security of IPsec VPN Hub and Spoke connections.

Figure 1. Quantum-secure IPsec hub and spoke architecture using NetworkSecure and strongSwan deployed in a virtual machine (VM) on OEM hardware



The NetworkSecure software interoperates with strongSwan through the strongSwan vici interface 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 generates PPKs, brokered by SKA-Platform, on-demand and at scale. PPKs are additionally used to derive dynamic authentication keys that are used by strongSwan for mutual endpoint authentication, enhancing identity security and avoiding scalability and security challenges associated with PKI.

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.

The hub site support hundreds of concurrent spoke connections providing a scalable architecture to cost-effectively secure connectivity from IoT edge, branch sites or private 5G base stations to cloud or on-premises data centers. Additionally, NetworkSecure for strongSwan supports other topologies such as high-speed point-to-point VPN links and mesh networks, enabling multiple network communication use cases.