NQX™ Network Encryptor

The first practical step toward quantum-safe networks.

Protect sensitive data in transit with an easy to deploy, cost effective network encryption overlay as you advance your broader quantum-safe migration and build data sovereignty.

End harvest-now-decrypt-later exposure on critical links now.

Your secrets have long lives

Satellite imagery, classified data, program data, product designs, source code and test telemetry often need protection for 15–30 years. NSA treats anything needing 15+ years of protection as "long-life" data that needs quantum threat mitigation now.

Harvest now, decrypt later is already happening

Recording encrypted traffic is passive and undetectable. Adversaries don't need a quantum computer today, only storage and patience. Supply chains are attractive because they are often softer than the prime or ministry they serve.

Requirements are flowing down to you

The EU PQC roadmap wants high-risk use cases quantum-safe by 2030. Defense customers increasingly ask suppliers for a PQC plan and data sovereignty options.

Your estate can't move all at once

Engineering, production, OT and test environments run systems you can't patch or replace on a regulator's timeline. Migrating applications, PKI and embedded crypto takes most organizations 3–7 years.

Protecting the links with an overlay is phase one of your PQC migration

An NQX quantum-safe encryptor pair builds an overlay to remove harvest-now-decrypt-later exposure on a link immediately, regardless of the applications or protocols on top. It's easy to deploy, requires no rip-and-replace projects and is a quick win for protecting your mission-critical data without delay.

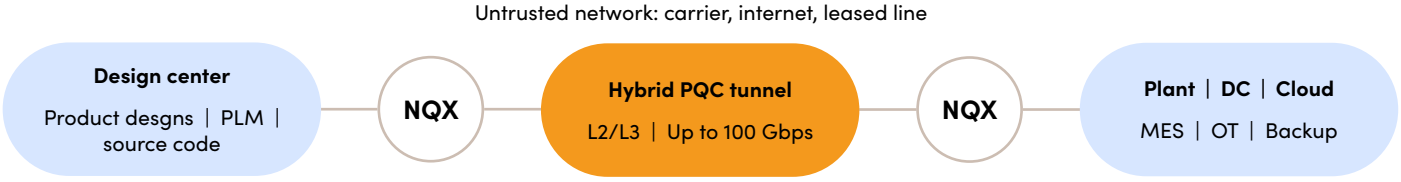
Now with NQX
Secure critical links with NQX and protect long-life data from day one.

2026-2030
Build your crypto inventory and migrate TLS, PKI, and applications by risk.

2030-2035
Migrate lower- risk systems and update NQX algorithms as standards evolve.

What NQX covers

- Ethernet (L2) and IP (L3) traffic between NQX nodes
- Site-to-site, data-center, backup and backbone links
- Network topologies, including hub & spoke and mesh
- Links into and between clouds and colocation sites
- Legacy, OT, and ICS traffic that can't be upgraded
- Hardware matching your needs or virtual appliance



ssh.com | info@ssh.com

Go quantum safe without changing apps or existing network infrastructure.

1 Hybrid post-quantum key agreement

Classical algorithms run alongside FrodoKEM and ML-KEM (FIPS 203), so a link stays secure even if one method is broken.

2 Crypto-agile by design

A software-based crypto engine runs classical, post-quantum and hybrid modes. New algorithms arrive as software updates, not hardware swaps.

3 Layer 2 and Layer 3 together

Encrypts Ethernet and IP traffic simultaneously, out of the box, without changes to the surrounding network.

4 Wire speed, low latency

Up to 100 Gbps from remote offices to data centers, so security doesn't throttle engineering or production traffic.

5 Built-in key management

Automated key generation, rotation and renewal inside your own NQX deployment, with perfect forward secrecy across all tunnels.

6 One console

Nodes, tunnels, configuration, software lifecycle, monitoring and audit logs from a single management interface, with role-based administration.

Use case examples

Engineering to production: Protect product designs and other IP moving between R&D centers and manufacturing plants.

Data center & backup: Encrypt DCI and replication links that carry complete copies of program data. Transmit at high throughputs.

Segregated programs: Separate 1) defense work from commercial business on shared carrier networks, 2) data for different customers, and 3) data at different classification levels.

OT & test sites: Protect traffic travelling from test ranges, labs, and plants whose systems can't run modern crypto themselves.

Cloud interconnect: Secure cloud and colocation links supporting engineering workloads.

Satellite data: Protect data travelling over satellite links or from ground stations to other destinations.

← NQX 5200 with 100 Gbps performance

European assurance

- Finnish national TL III (Confidential) certification by NCSA-FI (Traficom).
- IN PROGRESS: NATO Restricted and EU Restricted certification.
- SSH is a registered supplier to the NATO Communications and Information Agency (NCI Agency).
- Developed in Finland for data sovereignty by SSH, the company behind the Secure Shell protocol.

Why a dedicated encryptor, not firewall IPsec?

Independent layers: Layered, independent encryption follows the principle behind the NSA's CSfC programme. A flaw in one layer doesn't expose the other.

No throughput penalty: Enabling encryption can reduce a firewall's throughput from negligible (with hardware acceleration) to well over 50%.

Separate certification and keys: Each control can be certified, upgraded and audited independently.