NQX™

Secure Your Critical Data in Transit

Datasheet

NQX in a nutshell

SSH NQX™ is a quantum-resilient encryption solution for transporting Ethernet and IP traffic across any network, private or public. It provides state-of-art cryptographic protection for data leaks, breaches, misuse, and interference.

NQX provides quantum-resilient protection and government-grade security for highly-classified information in transit.

About NQX:

- **High-speed encryptor that provides a transparent security channel for your sensitive data.**
- **Quantum-resilient network encryptor to secure your data-in-transit now and in future.**
- **Comprehensive network management for nodes and services that minimizes operational costs.**
- **L2 and L3 support makes NQX easy to deploy in various network infrastructures.**

The Critical Role of Network Encryption in Securing Data During Transit

In today's digital landscape, data in transit is one of the most vulnerable assets, as it moves across networks, devices, and systems. Network encryption plays an essential role in safeguarding this data, acting as a robust defense against interception, eavesdropping, and unauthorized access. By encrypting data at the network level, organizations can ensure that sensitive information remains protected from malicious actors who seek to exploit vulnerabilities in communication channels.

Unlike data stored at rest, which can be protected by physical and logical controls, data in transit is exposed to greater risks. As sensitive information – ranging from personal details and financial transactions to confidential business communications – travels across public or private networks, it becomes a prime target for interception. Network encryption mitigates this risk by transforming readable data (plaintext) into an unreadable format (ciphertext), ensuring that even if intercepted, the data cannot be deciphered without the appropriate decryption key.

Network encryption is not just a defensive measure, it is also a legal and regulatory necessity. Frameworks like GDPR, HIPAA, and PCI-DSS mandate the protection of data during transmission, holding organizations accountable for securing personal, financial, and medical information. Failure to implement effective encryption strategies can lead to severe consequences, including data breaches, financial losses, and reputational damage.

Modern encryption solutions, such as secure tunneling protocols and advanced quantum resistant cryptographic algorithms, offer robust protection for data as it moves between endpoints. These technologies ensure the confidentiality and integrity of transmitted information, preventing unauthorized alterations and maintaining trust in the communication process.

By prioritizing network encryption, organizations can build a secure foundation for their operations, safeguarding sensitive data, maintaining compliance with regulatory standards, and defending against evolving cyber threats. In an era where data breaches are increasingly sophisticated and frequent, network encryption is not just an option – it is an absolute necessity for protecting the lifeblood of modern digital interactions.

SSH

Purpose of Network Encryptors

Secure Critical Data in Transit

NQX is a purpose-built network encryption solution designed to safeguard critical data against eavesdropping and manipulation. By delivering top-notch end-to-end encryption, NQX ensures that sensitive information remains secure during transmission, even across public networks.

With its versatile deployment options, NQX can function as either an Ethernet-level (Layer 2) or IP-level (Layer 3) encryptor. This flexibility allows organizations to seamlessly extend their networks—whether connecting datacenters or building dedicated secure networks over public IP infrastructures.

The automated key management system is the core of NQX's effectiveness. This mechanism ensures key exchange procedures are made appropriately during data transfer. The procedure also maintains the lifecycle of the keys in the encryption network. This comprehensive approach is critical for service availability.

Key Features of NQX

Security Strength: Leverages superior key lengths and post-quantum cryptography (PQC) algorithms to deliver unmatched protection against current and future threats.

Security Lifecycle Management: Ensures long-term protection and system integrity.

High-Speed Encryption: Supports rapid data transfer without compromising security.

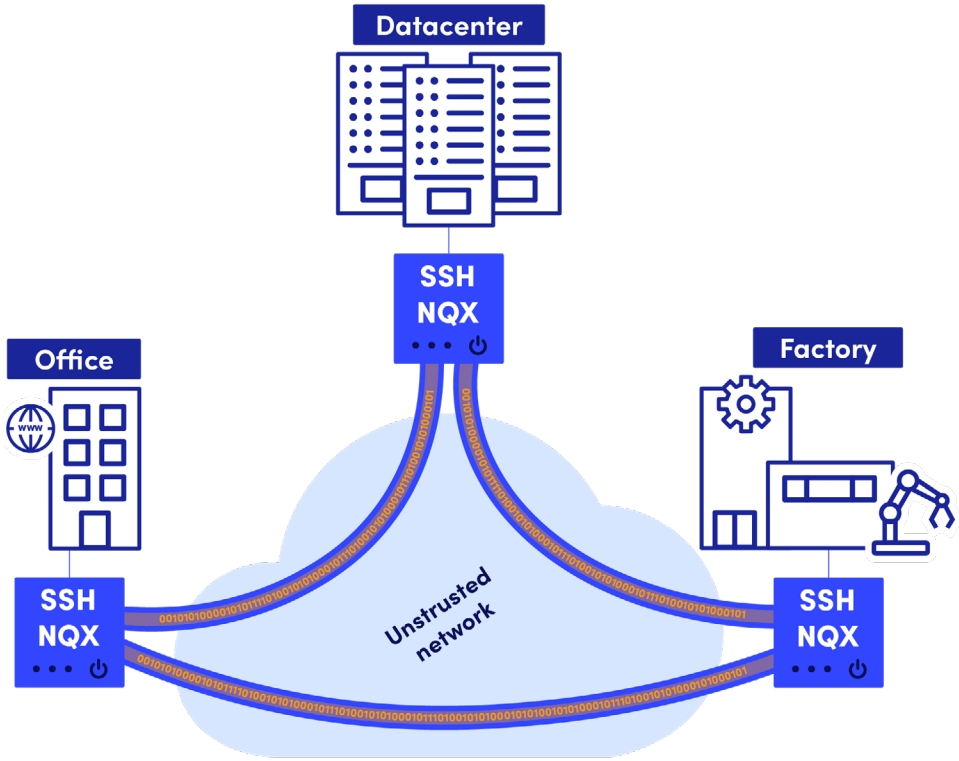
Crypto Agility: Adaptable to evolving cryptographic standards and requirements.

Flexibility: Accommodates diverse network architectures and use cases.

Operational Efficiency: Simplifies deployment and maintenance while reducing overhead.

NQX is the ideal solution for organizations seeking a secure, scalable, and future-ready approach to protecting their critical data in transit.

SSH



NQX nodes are deployed on the edge of organizations sites. All the critical data transferred between sites (like business, IPRs, customers data, etc.) is encrypted by utilizing quantum-resilient means. NQX provides high-speed encryption and makes it possible to deploy network encryption layer to secure all data transmitted over various transport technologies, such as xWDM, MPLS, Ethernet, or even over the Internet. The built-in security and automated key management functions ensure data is always secured and the availability of services is ensured.

Key Features

High Security Strength

NQX ensures robust security with advanced features like L2/L3 IPSec tunnel modes, anti-replay protection, dynamic session re-keying, and strong encryption standards (AES-256-GCM, ASE-256-CBC with HMAC-SHA2). Enhanced with Perfect Forward Secrecy, Post-Quantum Pre-Shared Keys, and resilient key exchange mechanisms, it provides future-proof data protection against evolving threats.

NQX Built-In Key Management

Key management is the cornerstone of security in a Public Key Infrastructure (PKI) system. It ensures the protection of data integrity, authentication, and confidentiality, forming the backbone of trust in a PKI framework. Without effective key management, the entire infrastructure becomes susceptible to attacks, undermining its security and reliability.

The key management system in NQX is purpose-built to address these challenges by implementing robust controls and safeguards. Keys are

generated for specific, dedicated purposes, ensuring they are used in alignment with security best practices. Lifecycle management and key rotation are executed in a controlled and secure manner to mitigate risks associated with key reuse or compromise.

A critical aspect of NQX's key management is its non-exportable key design. Keys are securely contained within the system, preventing unauthorized access or leakage outside the protected environment. Furthermore, NQX integrates with a centralized management system to streamline key renewal processes automatically. This approach minimizes the risk of manual errors and prevents service outages, ensuring the continuous availability and integrity of encrypted communications.

By combining advanced lifecycle management, secure storage, and automated renewal mechanisms, NQX delivers a comprehensive and reliable key management solution to protect sensitive data and uphold the integrity of the PKI framework.

Crypto Agility

NQX demonstrates exceptional crypto agility in two key aspects, ensuring adaptability and resilience against evolving cryptographic needs.

Firstly, NQX leverages standards-based key exchange and encryption algorithms by default, providing robust and widely recognized security. Its flexible configuration allows the use of various authenticated encryption methods and key exchange mechanisms. Additionally, customers can customize their cryptographic parameters by utilizing the NQX crypto module, tailoring the solution to specific security requirements.

Secondly, the NQX platform’s software-based architecture enables swift support for new cryptographic algorithms without requiring changes to existing hardware. This capability ensures that NQX is a future-proof solution, ready to adapt to the quantum era while safeguarding organizations' prior investments in infrastructure.

High-Speed Encryption with Resiliency

The NQX portfolio caters to a wide range of network needs, from remote site solutions to connecting data centers. It supports network connections from 10 Mbps up to 100 Gbps, ensuring scalability and high performance across diverse environments. The scalability leverage the transparency to end users due the encryption to have minimal impact on data transfer and latency.

The resiliency can be implemented at port level, which allows sophisticated network solutions while maintaining cost efficiency. The high availability solution can be made utilizing up to four appliances, which can be different models, e.g. backup line may be lower performance node.

Flexibility

NQX can operate on both, Ethernet (L2) and IP (L3) simultaneously. L2 operates as protocol agnostic mode, which gives robust operation mode to encrypt all traffic between sites. At IP layer NQX supports various network topologies from point-to-point. Hub'n spoke as well MESH networks.

The routing capabilities enable operators to use NQX in large networks.

IP mode gives sophisticated tools to control traffic at transport layer (L4) as well means to implement network segmentations and rules based tunneling.

Operational Efficiency

The Central Manager (CM) tool of NQX provides a set of functions to manage nodes and tunnels lifecycle. Managing the configurations of large amount of nodes may be laborious. CM node management tools help administrators to maintain node configurations and changes, software versions as well as the keys and certifications. The predefined configurations help to mitigate errors and via that way increase the security posture. The system provides standard based interfaces for network operation centers (NOC) and Security operation centers (SOC) to collect situational information about network statistics.

Looking for more information?

Interested in seeing NQX in action?

CONTACT US

Specifications

	NQX APPLIANCE MODEL				
PERFORMANCE	**120**	**1160**	**1170**	**5170**	**5200**
Throughput [Gbps][1]	1	10	40	60	100
IPSEC tunnels	15	50	100	400	400
Encryption [Gbps] with PQC ML-KEM[2]	1	6	15	30	60
Latency, average [ms]	0.6	0.6	0.5	0.5	0.4
INTERFACES Fixed/Max	**120**	**1160**	**1170**	**5170**	**5200**
Module slots	-	-	-	2	4
Gigabit Ethernet RJ45	3	6	8	8/24	0/16
10 Gigabit Ethernet SFP+	-	2	4	4/12	4/12
100 Gigabit Ethernet QSFP+	-	-	-	-	2/4
OPERATIONAL MODE	**120**	**1160**	**1170**	**5170**	**5200**
Ethernet (L2)	yes	yes	yes	yes	yes
IP (L3)	yes	yes	yes	yes	yes
MANAGEMENT	**120**	**1160**	**1170**	**5170**	**5200**
Console/LAN/inband	yes/yes/yes	yes/yes/yes	yes/yes/yes	yes/yes/yes	yes/yes/yes
USB	2	1	3	2	2
PHYSICAL	**120**	**1160**	**1170**	**5170**	**5200**
Dimensions (W x H x D) mm	147 x 40 x 110	240 x 44 x 220	340 x 44 x 250	438 x 43 x 480	438 x 44 x 511
Weight [kg]	1	1.9	3.4	8	10
Power supply	2 x 12V-48V TB[3]	100-240 VAC adapter		Redundant 100-240 VAC	
Operating temperature	-40 - 65°C	0 - 40°C			
Relative humidity (non-condensing)	5 - 95%	10 - 90%			
APPROVALS	**120**	**1160**	**1170**	**5170**	**5200**
NCSA-FI CAA		Confidential			
Safety		CE/EMC, FCC class A			

[1] IPv4 UDP 1500 byte packet, 4x/8x 10G port configurations
[2] L2/L3 AES-256-GCM 1500 byte frame/packet
[3] Terminal block connector

NQX Features

Security Feature Highlights

- Transparent L2-Ethernet encryption and L3-IP VPNs
- IPSec and IKEv2: Support for PSK Key lists and x.509 certicates (PKI)
- Adjustable IKEv2 and IPSec parameters to meet security requirements
- Key exchange using NIST P521, or Diffie Hellman fixed groups 18 and 1336
- Quantum-safe key encapsulation methods FrodoKEM and ML-KEM (FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard)
- Automatic Post-Quantum Pre-Shared Keys (PPK) support
- Crypto module enables customer to implement own key settings.
- Peer identity options: FQDN, email, IPv4/IPv6 address, or certificate
- Adaptive WRED with upper bound on IKEv2 open tunnel negotiation for DoS protection
- DDoS reciliency up to 2 million flows/second without impact to services availability
- Emergency security features to purge the connections immediately and disable the appliance
- Remote Attestation to secure and control the appliance lifecycle.
- Secure Boot verify the system integrity at firmware and software level.

Networking Feature Highlights

- Native dualstack architecture supporting concurrent IPv4 and IPv6 traffic flows
- Simultaneous VPN support (IPSec) for both L2 and L3, all frames and protocols
- Flexible L3-operations with IPv4 and IPv6 capabilities
- BGP4 support for IGP/EGP dynamic routing
- DHCP, NAT, and NAT-T support for mobile and broadband access
- Editable MAC address table
- Rule-based forwarding for granular flow management
- Jumbo Frames support (9k bytes)
- Link aggregation Control Protocol (LACP)
- Automatic Path MTU to optimize performance

Central Management Highlights

- Browser based user interface
- Inventory management for nodes, configurations and node software releases
- VPN wizards for easy service provisioning
- Configuration revision management
- Automatic NQX node back-up for rapid restoration
- Lifecycle management of NQX node certifications
- PSK-ID management for tunnels
- Security policies with version management
- Role and domain based user policy
- Inband management utilizing quantum-resilient authentication keys