QSphere™

VPN Data Sheet

Quantum Resistant Solution

Proprietary Hybrid Protocol

Advanced Networking Features

QuantumGate™

Features

QSphere VPN is a next-generation Virtual Private Network solution that provides quantum-resistant encryption for enterprise communications. Designed to secure data against both classical and emerging quantum threats, QSphere VPN utilizes advanced cryptographic algorithms—including hybrid modes that combine classical and quantum-safe methods. This ensures long-term confidentiality and robust protection for your organization's sensitive information.

Quantum-Safe Cryptography	Utilizes cryptographic algorithms resistant to quantum computing threats, including algorithms hardened with sovereign-national cryptography.
Strong Symmetric Ciphers	Provides robust encryption for secure data transmission, ensuring data integrity and confidentiality.
Hybrid Mode Cryptography	Combines classical and quantum-resistant cryptography for enhanced security and future-proofing against emerging threats.
Full Forward Secrecy	Ensures session keys remain secure even if long-term keys are compromised, providing robust protection for encrypted communications.
Custom Protocol	Proprietary lightweight protocol based on WireGuard, optimized for security and performance with classical, quantum-resistant, and national cryptography.
Per-Application VPN	Enforces VPN use on a per-application basis for granular control, enhancing security by isolating app traffic.

Features

Split Tunneling	Allows users to route specific traffic through the VPN while other traffic accesses the internet directly, optimizing bandwidth and performance.
Lock-Down Mode	Restricts all traffic outside the VPN tunnel, preventing unauthorized data transmission and enhancing security.
Always-On VPN	Ensures a continuous and secure connection, reducing the risk of accidental exposure.
Kill Switch	Automatically disconnects the device from the internet if the VPN connection drops, preventing data leaks and maintaining security.
IPv4 and IPv6 Support	Compatible with both IPv4 and IPv6 networks, ensuring broad compatibility and future readiness.
Site-to-Site VPN Tunnel	Supports secure connections between different network locations, facilitating secure inter-office communication.
Simple CLI-Based Configuration	Offers an easy-to-use command-line interface for quick and efficient configuration and management.
Monitoring, Logging, and Metrics	Provides straightforward tools for monitoring VPN performance and status, aiding in administration and troubleshooting.
Enterprise Readiness	Modular server architecture allows easy deployment and integration into various existing systems such as mobile device management (MDM), identity and access management (IAM), multi-factor authentication and single sign-on as well as SOC integration

Capabilities

Quantum-Resistant Encryption

Employs quantum-safe algorithms built to resist quantum computing threats, combining classical and quantum-resistant methods to protect session keys and data integrity.

Proprietary Hybrid Protocol

Features a custom protocol optimized for superior security and performance, integrating classical, quantum-resistant, and national cryptographic techniques.

Advanced Networking Features

Offers per-application VPN control, split tunnelling, always-on VPN, kill switch, and lock-down mode to provide granular control and enhanced security over network traffic.

Centralized Administration

Provides simple CLI-based configuration along with monitoring, logging, and metrics tools for efficient administration and oversight.

Requirements

Technical

VPN Server Environment	✓ Deployable Options: Docker image or Kubernetes (K8s) in privileged container mode. ✓ Container 1: VPN Server Includes Node Exporter (Prometheus system agent) and VPN Exporter (Prometheus VPN agent). ✓ Container 2: Prometheus Server For data aggregation and monitoring. ✓ Container 3: Grafana Server Provides visualized metrics and monitoring dashboards.
VPN Client Applications	Deployment: Deployable on iOS, Android, Windows devices through Corporate Mobile Device Management (MDM) systems.
Deployment Options	Supports flexible deployment models, including on-premises, cloud-based, or hybrid environments. The Key Directory Server can be deployed in data centers or cloud infrastructures, and client applications can be distributed via standard software deployment tools.

System

Operating System	✓ Desktop: macOS 13 or later, Windows 10 or later ✓ Mobile: iOS 17 or later ✓ Linux: Debian-based and Red Hat-based distributions; supports Docker and K8s
Storage Space	Minimum of 500 MB
RAM	✓ Windows/macOS: 4 GB ✓ Linux: 1 GB
Additional Requirements	All necessary frameworks and dependencies are bundled within the application for seamless installation and operation.

Networking Configuration

	Incoming Rules	Outgoing Rules
Container 1: VPN Server	✓ Configurable VPN UDP port exposed through the DMZ for VPN tunnel access. ✓ SSH management access from the management VLAN.	✓ Configurable according to enterprise requirements for remote VPN clients.