enQase

CASE STUDY

Global Top 10 Naval Power

Quantum-safe security solution enhances fleet readiness and reduces operational costs.

> ENQASE.COM

Challenge

Naval ships docked in port leverage a variety of communication methods – including wired connections – to maintain secure and reliable communications with shore facilities and other vessels.

The Navy faced significant challenges with traditional undersea port cables, or tethered cables, including limited mobility for ships and vulnerability to physical damage. These cables are also difficult and expensive to maintain, requiring specialized equipment and personnel for maintenance and repairs. To address these issues, the Navy sought to implement data exchange without physical tethers. This approach aimed to provide unparalleled defense against current and future threats. By moving away from physical cables, the Navy could enhance operational flexibility and reduce vulnerabilities associated with physical infrastructure and improve operational readiness.

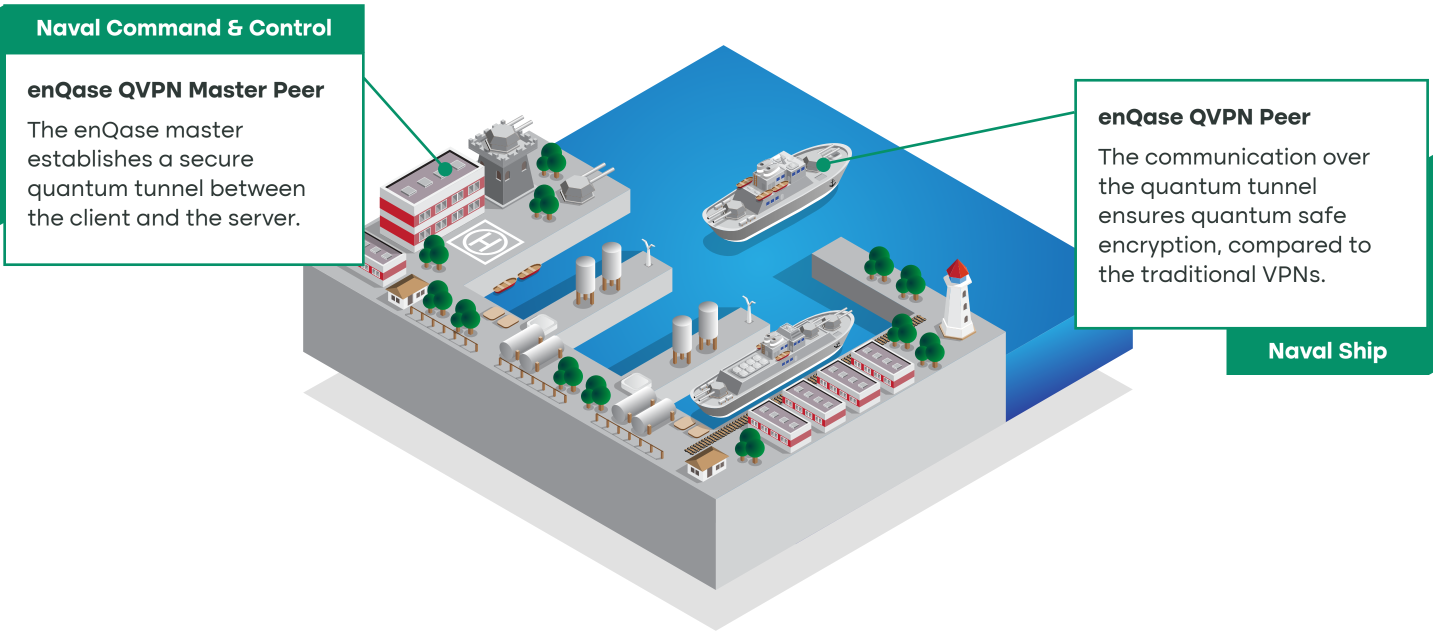
Post-quantum cryptography (PQC) was a consideration to possibly solve this problem. However, PQC faces potential unexpected vulnerabilities as its cryptography standards are based on mathematical assumptions and deterministic algorithms which may be challenged by future advancements in quantum computing or AI driven mathematical breakthroughs. Additionally, the use of Pseudo-Random Number Generators for key generation and other random values in PQC solutions could expose them to sophisticated quantum or AI-driven hacking attempts in the future.

These factors led the Navy to explore more robust quantum-safe solutions that could provide comprehensive protection against the evolving landscape of cybersecurity threats and free naval vessels from physical secure communication tethers.

Solution

enQase QVPN (Quantum Virtual Private Network) offered cutting-edge quantum-safe protection through a multi-layered approach. enQase bolsters mathematical based PQC encryption with the power of quantum mechanics-based unpredictability – providing a more robust future-proof quantum safe solution.

This powerful combination ensures quantum safe communication through a wireless channel. In this implementation at a naval base, a Quantum Virtual Private Network (QVPN) server was placed onshore in the secure naval communications office. The QVPN peer machine was also placed on a Naval ship. The QVPN establishes a quantum-secured tunnel between the ship and the shore, and ship to ship over wireless channels, enabling the exchange of confidential data.



Naval Command & Control

enQase QVPN Master Peer

The enQase master establishes a secure quantum tunnel between the client and the server.

enQase QVPN Peer

The communication over the quantum tunnel ensures quantum safe encryption, compared to the traditional VPNs.

Naval Ship

Outcome

The enQase Quantum Virtual Private Network (QVPN) system, once deployed and activated on the host machine, established a secure tunnel between the client and server. This quantum tunnel interface facilitates the encrypted transfer of data, ensuring quantum-safe communications that surpass the security levels of traditional VPNs.

The implementation of enQase QVPN addresses a critical limitation in current naval ship-to-shore communications. It eliminates the need for manual data transfer via ethernet cables, which previously required ships to be docked, or tethered to each other for secure information exchange. This advancement enables multiple vessels to communicate simultaneously with each other and the naval base, significantly enhancing operational readiness.

Advantages of enQase Quantum-Safe QVPN

Advanced Quantum-Safe Security

enQase Quantum-safe VPN combines post-quantum cryptographic (PQC) algorithms with Quantum Random Number Generators (QRNG). This hybrid approach provides superior protection against both classical and quantum computer attacks, offering enhanced security for sensitive military communications compared to solutions using PQC alone.

Enhanced Operational Readiness & Improved Defense Response

By enabling secure wireless communications, enQase allows naval forces to "cut the cord" all the while maintaining robust security. This capability significantly improves operational readiness and reduces response times for defense operations, enabling more agile and effective military responses.

Secure Today & Future-Proof

Harvest Now Decrypt Later (HNDL) attacks against defense communications can have devastating consequences when quantum computers are able to crack conventional cryptography. enQase secures communications today, and in the future, with quantum-safe QVPNs ensuring long-term data security.

Rapid Deployment and Scalability

enQase QVPN solutions are designed for quick implementation and can be easily scaled across multiple vessels without requiring significant changes to existing physical infrastructure. This allows for efficient expansion of secure communication networks across fleet.

Cost-Effectiveness

enQase quantum-safe QVPNs eliminates the need for expensive undersea or tethered cable installations and ongoing maintenance. Over time, this results in substantial cost savings and a more sustainable approach to secure naval communications.

> "The enQase team understood the challenges we were trying to overcome and were able to quickly develop a recommendation and deploy a hardware and software solution to implement an innovative solution for Quantum Secure ship-to-ship and ship-to-shore secure wireless communications."
>
> Commander, Top ten Global Naval Power