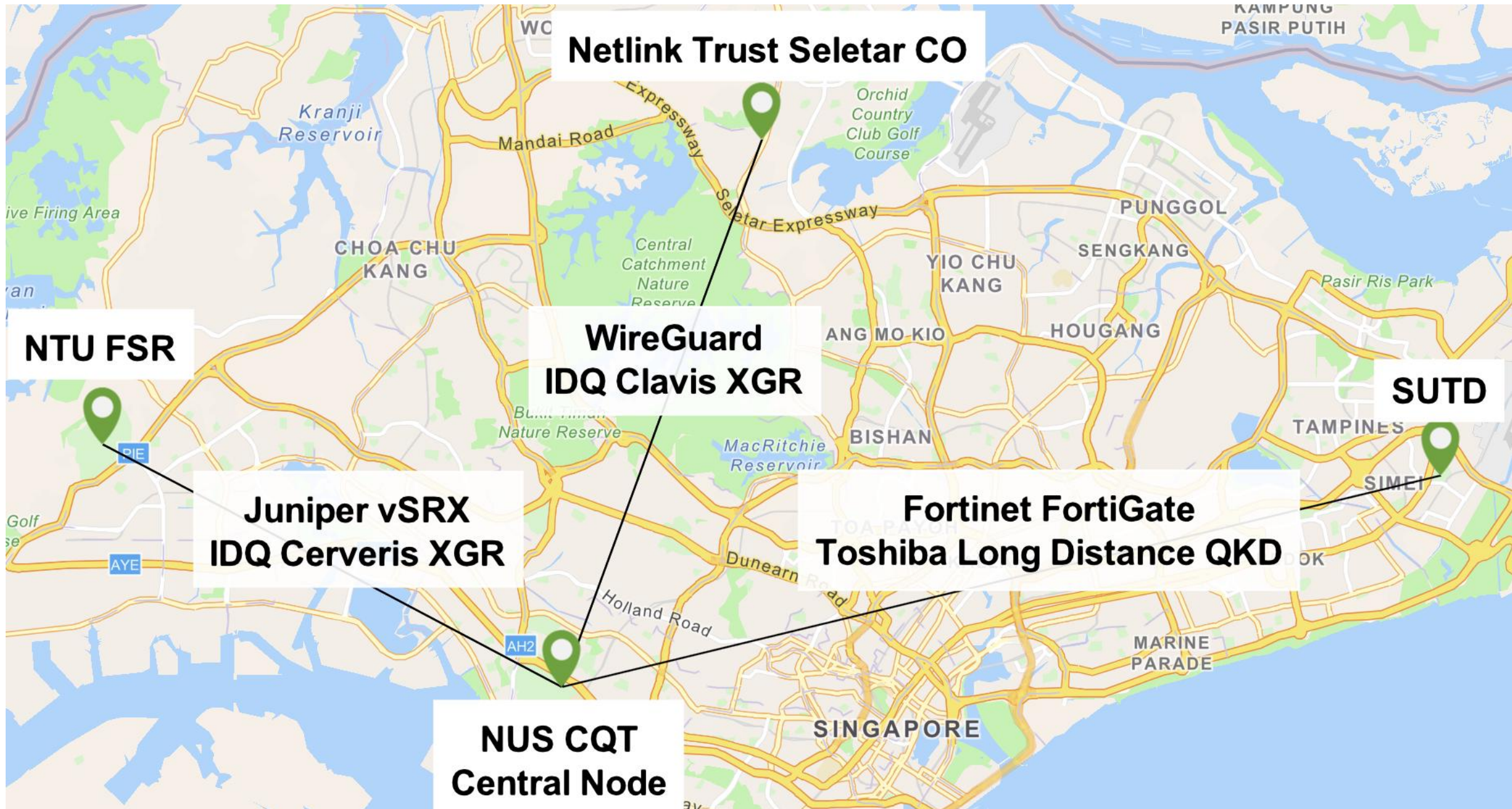


Summary

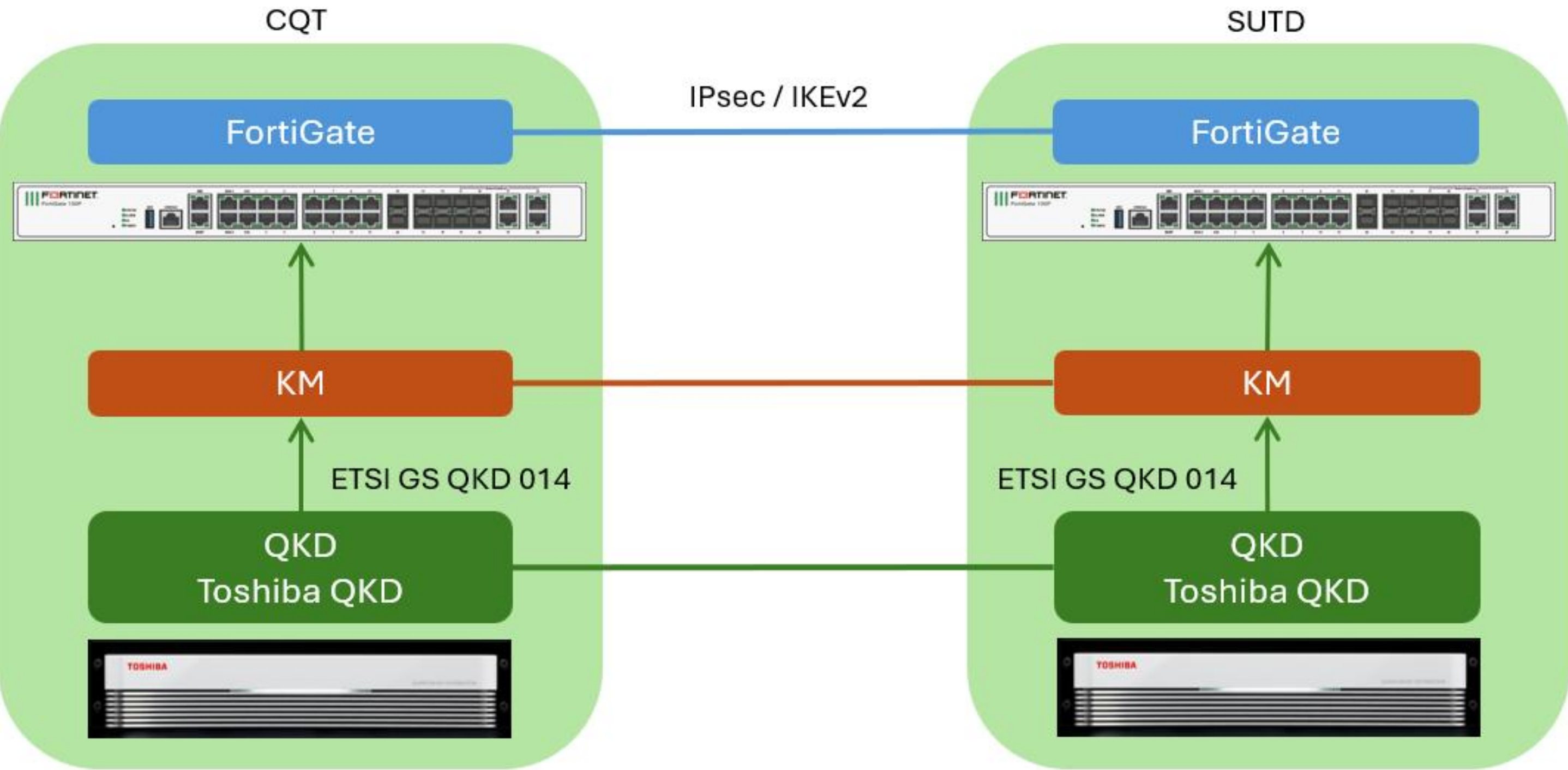
Data today is exposed to harvest-now-decrypt-later threats. This work presents a defence-in-depth approach that integrates Quantum Key Distribution (QKD) and Post Quantum Cryptography (PQC) with network-layer VPN technologies. The project spans 4 nodes across Singapore and 3 different QKD systems, as shown in the node diagrams on the right. The NQSN Key Management System (KMS) retrieves QKD-generated keys and supplies them to cryptographic applications.



	CQT-FSR	CQT-NLT CO	CQT-SUTD
QKD System	IDQ Cerberis XGR	IDQ Clavis XGR	Toshiba Long Distance QKD
QKD Protocol	Coherent One-Way	BB84	BB84
Distance	32.48 km	29.58 km	46.66 km
Loss	12.25 dB	8.94 dB	19.38 dB
SKR	2.93 kb/s	10.1 kb/s	133 kb/s
QBER	1.7%	0.718%	3.03%
VPN	Juniper vSRX (IPsec)	WireGuard	Fortinet FortiGate (IPsec)

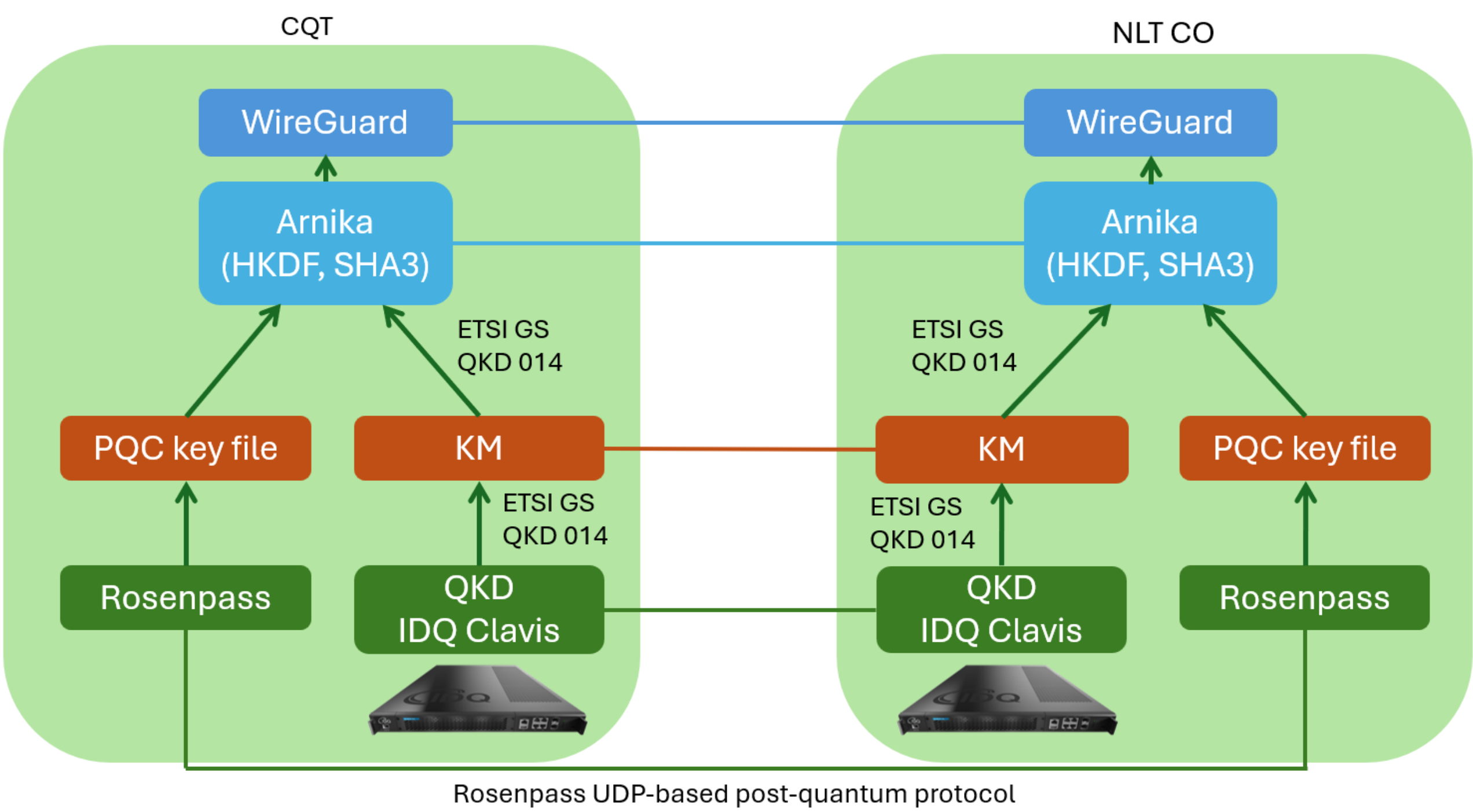
Fortinet FortiGate

IPsec VPN is a technology that operates on Layer 3 (network-layer) of the Open Systems Interconnection (OSI) model. An IPsec VPN tunnel is established using the Internet Key Exchange version 2 (IKEv2) protocol, which sets up the connection in two phases. Once both phases are completed, the real data traffic flows securely through the IPsec VPN tunnel. The FortiGate devices establish the site-to-site IPsec VPN tunnel between the CQT and SUTD sites. Each FortiGate connects to its local Key Manager (KM) to retrieve QKD-derived key material and, where enabled, combines it with key material from PQC algorithms (provided by FortiGate). This combined material is then incorporated into the key-establishment and re-keying process that secures the IPsec tunnel.



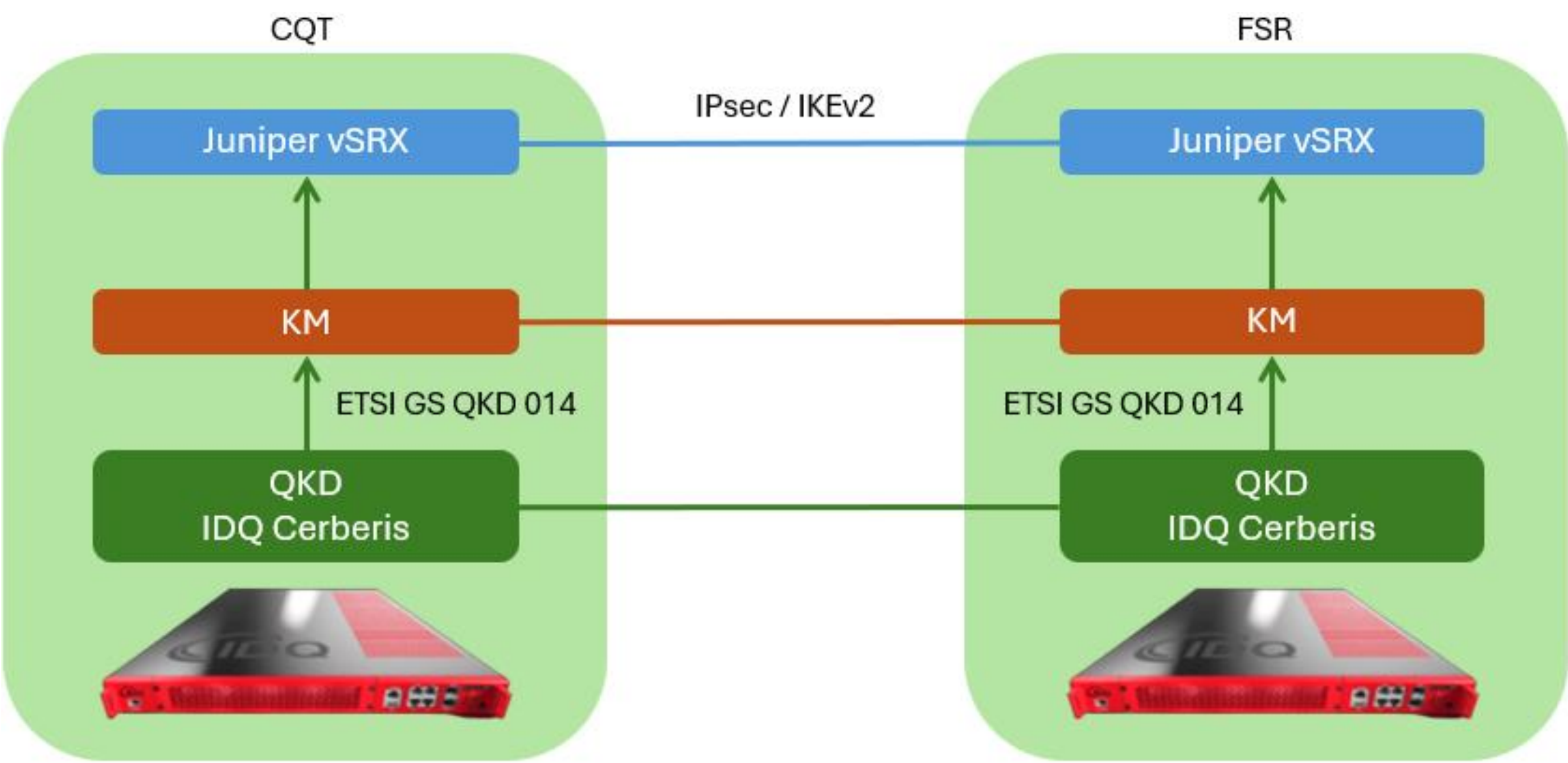
WireGuard

This setup combines three open-source tools to achieve quantum-safe connectivity. WireGuard provides the base OSI Layer 3 VPN tunnel, while Rosenpass performs post-quantum key exchange to protect against quantum adversaries. Arnika retrieves QKD-generated keys from the KMS and combines them with the WireGuard and Rosenpass key material. These three key sources are combined to derive a single symmetric key for the WireGuard tunnel, ensuring that an attacker would need to compromise all three sources to recover the final encryption key and decrypt the protected traffic. This hybrid design maintains compatibility with standard WireGuard while enhancing its resistance to quantum attacks.



Juniper vSRX

This setup used a Juniper vSRX, a software-based VPN, to establish an IPsec tunnel using the IKEv2 protocol for peer authentication and key negotiation. Only QKD keys were drawn from the KM for this configuration (no PQC algorithm involved). The QKD keys were injected as post-quantum pre-shared keys and mixed into IKEv2's key derivation alongside the classical key exchange, allowing the VPN connection to become quantum-safe.



OSI Layer 3 VPNs Comparison

Layer 3 VPN Comparison			
	WireGuard (CQT-NLT CO)	Juniper vSRX (CQT-FSR)	Fortinet FortiGate (CQT-SUTD)
Hardware/Software	Software	Software	Hardware
Encryption Algorithm	ChaCha20	AES256-GCM	AES128
Authentication Algorithm	Poly1305	AES256-GCM	SHA256
Key Exchange	Curve25519	Diffie-Hellman group 14	Diffie-Hellman group 5
Key Combination Algorithm	BLAKE2s	HMAC-SHA384	SHA256
Key Source(s)	QKD, PQC	QKD	QKD, PQC

To verify a successful connection and test the tunnel performance we conducted an iperf test (a command-line tool to measure network throughput, packet loss, latency, and jitter between two endpoints) on each setup with and without the quantum-safe technologies. We observed that the technologies had no significant impact on the bandwidth, indicating that enhanced security can be achieved without compromising network throughput performance.

Performance Test Results for Classical only Setup

	WireGuard (CQT-NLT CO)	Juniper vSRX (CQT-FSR)	Fortinet FortiGate (CQT-SUTD)
Average Upload rate (Mbits/sec)	897	898	902
Average Download rate (Mbits/sec)	890	720	903

Performance Test Results for Classical + QKD + PQC Setup (Juniper: Classical + QKD only)

	WireGuard (CQT-NLT CO)	Juniper vSRX (CQT-FSR)	Fortinet FortiGate (CQT-SUTD)
Average Upload rate (Mbits/sec)	897	895	903
Average Download rate (Mbits/sec)	888	719	903

Future Work

- **Stress Testing:** Evaluate performance under heavy traffic.
- **Cross-Operation via Relaying:** Test interoperability across different VPN systems.
- **Simulated Failure Testing:** Evaluate resilience against disruptions and failures.

