Redefining Security

Use Case: Financial Services

Securing Network for Disaster Recovery

10G Ethernet Encryption with Quantum Key Distribution

Customer Profile: Private asset and wealth management company

Industry: Banking

Country: Switzerland

Business need	Solution	Results
Protect sensitive business and customer data for the long term.	Layer 2 Ethernet encryption combined with Quantum Key Distribution (QKD).	The QKD server provides forward-secrecy for the most sensitive long term data.

Business need

A world-leading private asset and wealth management company is committed to protecting the confidentiality of its data and the trust of its global customer base. The move to a new headquarters provided the security team the opportunity to re-assess the firm's long-term data protection procedures and architecture, and to rationalise and update their communications network for leading-edge performance, as well as to ensure legal and regulatory compliance.

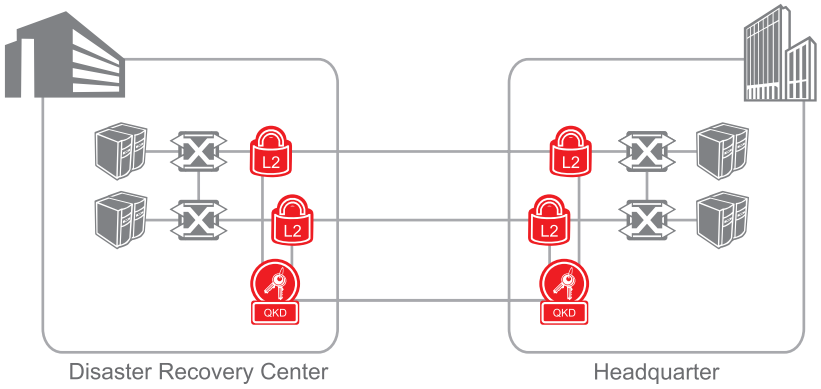
The company had to deal with multiple protocols for network and storage, and required a Fibre channel-over-Ethernet protocol for the link between the headquarters and the Data Recovery Center (DRC)

Solution

The company chose IDQ's hybrid encryption solution, incorporating state-of-the-art layer 2 encryption with Quantum Key Distribution (QKD). IDQ's 10 Gigabit Ethernet encryptors were chosen to secure the bank's extended backbone between the headquarters and the DRC nearly 100 kilometers away, with an additional layer of security provided by the Cerberis QKD server.

The primary criteria for the client was performance of the system – both in terms of throughput and the quality and robustness of the encryption. During the assessment phase multiple systems were tested at 100% capacity to simulate the flow of data to a back-up center. IDQ's products were the only devices which combined crucial Link Loss Forwarding capability with 100% throughput on the network without packet loss.

ID QUANTIQUE SA
Chemin de la Marbrerie 3
1227 Carouge/Geneva
Switzerland
T +41 22 301 83 71
F +41 22 301 89 79
info@idquantique.com
www.idquantique.com



The Centauris encryptors use the state of the art AES-256 encryption, and are certified to the highest commercial standards- Common Criteria EAL4+ & FIPS PUB 140-2 level 3.

IDQ's Cerberis QKD server was installed to ensure forward-secrecy for the most sensitive information. QKD works on the intrinsic and proven principles of quantum physics – ie. that the generation of the quantum key is truly random, and that any interruption or eavesdropping of the data will perturb the system and can thus be detected.

Unlike classical encryption based on mathematical algorithms, QKD will not be compromised by mathematical progress or the continual increase in computing power and it is not vulnerable to passive attacks. Such passive attacks are potentially the most dangerous for the financial industries, made worse by the fact that they are most often not even detected. Typically, important data is recorded and stored offline for future decryption – either through brute force attacks or when current Public Key algorithms are broken by upcoming quantum computers. Data such as customers' financial, credit card or personal details have long-term relevance for identity theft or fraud, and so longer-term protection is essential.

Thanks to the structure of the QKD key generation and detection, eavesdropping is impossible and the key is never recorded (only detected during the decryption process) so such offline attacks are not possible.

In addition, thanks to IDQ's Dual-Key agreement where the AES-256 encryption key used by the encryptor is combined with the quantum key and changed up to 60 times per hour in both directions, two-fold key security is provided and renewed in real-time.

The final factor in the company's decision making was the usability of the system, and specifically the CypherManager graphic user interface. This allowed the users to monitor the network, encryption keys and the encryptor in real time and to manage remote updates through a secure SMNP v3 connection.

Results

The company uses four 10 Gigabit Ethernet encryptors between their headquarters and disaster recovery center. In addition, the QKD server provides forward-secrecy for the most sensitive long-term data. Due to the success of the first deployment, the encryption platform was rolled out to other areas of the company for both MAN and WAN applications.

> *"Our bank has been using IDQ's quantum safe encryption solutions for nearly a decade now. The system has proven to be robust, with high performance and no down time – really "set and forget", while providing the level of high security which our customers expect."*
>
> CISO, leading Swiss bank

ID QUANTIQUE SA
Chemin de la Marbrerie 3
1227 Carouge/Geneva
Switzerland
T +41 22 301 83 71
F +41 22 301 89 79
info@idquantique.com
www.idquantique.com