Energy Operator Protects Critical Infrastructure Using High Speed Encryptors from Thales

The Business Need—Critical Infrastructure Protection

A major UK energy company needed to connect to other electricity providers via the National Grid Network. Data within the energy network is of critical national importance so security mandates stipulate that the highest levels of security must be deployed. The prominent energy company needed a robust, dedicated encryption solution to secure their data in motion and allow it to access the National Grid Network, covering the great majority of Great Britain.

Communications, emergency services, energy, food, and other critical infrastructure industry sectors are high value targets for cyber-criminals. Whatever the intent - rogue nation states, terrorists, espionage – these industries' IT systems are subject to multiple attack vectors, where vulnerabilities may be maliciously exploited. These institutions store and transport some of the world's most sensitive data. As well, they typically need to move huge volumes of information through their vast high-speed global data networks.

The Solution—Data in Motion Encryption

The primary business need of the energy company was to connect data from its control center to the National Grid Network. The only fail-safe solution to ensure data is secure as it travels across the network is encryption. Furthermore, the encryption solution should be de-coupled from any specific network architecture and accredited against recognised world-wide security standards.

In order to access the network, the energy company needed to meet the National Grid's strict security mandates it requires of all energy companies. Most importantly, the data must be encrypted because network lines can be physically tapped and data stolen or manipulated. Moreover the encryption must have controls in place to ensure that it is not disabled or bypassed. This is because National Grid understands the importance of separation of duties for network encryption.

After consulting security professionals on how best to achieve the requirements, the energy company was advised to use a dedicated and certified network encryption system rather than using native MACsec encryption as it does not meet the required standards.

For a network encryption solution to be truly robust and provide long-term data protection (well beyond the useful life of the data), it must be a "high-assurance" solution. So-called 'hybrid' encryption devices – such as network routers/ switches with embedded encryption or those using MACSec or similar standards (not originally intended for WAN and MAN security) provide "low assurance" data protection.

By contrast, Thales High Speed Encryption solutions are certified by the world's leading independent testing authorities as suitable for government and defence applications. They are purpose-engineered for dedicated, high-assurance network data security.

Thales network encryptors' security credentials include all four, essential high-assurance features:

- Secure, tamper-proof hardware; dedicated to network data encryption
- State-of-the-art encryption key management; featuring secure, client-side key storage
- End-to-end, authenticated encryption
- Standards-based encryption algorithms

Thales Network Encryptors are also the first to offer Transport Independent Mode (TIM) - network layer independent (Layer 2, Layer 3, and Layer 4) and protocol agnostic data in motion encryption.

The energy company selected the Thales CN6010 Network Encryptors (CN6010), an easy-to-use platform that is user configurable to provide transparent and high-assurance FIPS and Common Criteria certified network encryption at full line rate speeds up to 1 Gbps.

With the pandemic in full swing, deployment was done remotely in spring 2020. Despite the challenging conditions, the solution was fully designed, delivered installed and signed off for use within three months from the first contact with Thales.

The Benefits—Security and Speed

Using the encryption appliances for communications throughout the network provides the energy company optimal security, and speed.

Security—As the data is encrypted, any hacker attempting to tap the traffic would get only useless material, and would therefore have no chance of being able to manipulate the data for their own purposes. Furthermore, Thales High Speed Encryptors can immediately detect manipulated data packets and the devices would then shut down the compromised transmission. At the same time, the devices would switch traffic to a second secure network connection so the traffic can be delivered to the destination via a different route.

Performance— Energy networks deal with real-time data, so any encryption technology needs to operate at full line speed and add minimal latency. Using Field Programmable Gate Array (FPGA) technology, the Thales CN6010 Network Encryptor's architecture enables real-time data processing and high throughput. This ensures consistent low latency across all packet sizes for maximum performance—less than 8µS at 1 Gbps. Throughput is maximized in a zero protocol overhead mode. A 1U unit, it operates with minimal power and rack space consumption.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.