cpl.thalesgroup.com

THALES
Building a future we can all trust

International Bank chooses Thales High Speed Multilink Encryptors to Protect Global WAN

An international bank needed to upgrade its Wide Area Network (WAN) encryption solution to enable secure and instant access to customer data from any of its 30+ locations on three continents. The bank implemented Thales High Speed Encryptors, providing it with the high performance security needed to maintain compliance, ensure client privacy, and gain real-time access to sensitive data.

Business Need

An international bank wanted to address its commitment to customer confidentiality, increasing regulatory compliance demands and the need for real-time data flow more effectively. To do so, it needed to upgrade its encryption infrastructure. It required a high-performance solution which was easy to deploy and maintain within a reasonable budget.

The bank's existing solution was a Layer 2 E1/T1 link, which could no longer handle the amount of data required. The bank tested a Layer 3 IPSec solution, but rejected this due to the relatively high cost, complexity of installation and lower throughput. Moreover, since IPSec encryption added significant overhead to the message length, the routers in turn fragmented and reassembled the packets causing technical problems with the packet re-assembly as well as higher latency.

The Solution

Working closely with their multinational telecommunications company, the bank chose Thales's High Speed Encryption solution. Thales partnered with Senetas (an Australian company specializing in high speed network data encryption) and ID Quantique (a Swiss leader in quantum- safe crypto solutions) to develop, deliver and support its newest High Speed Encryption (HSE) solution.

Senetas and ID Quantique determined a Thales CN Series Encryptor was the best fit for the bank's network and security architecture, because it provides:

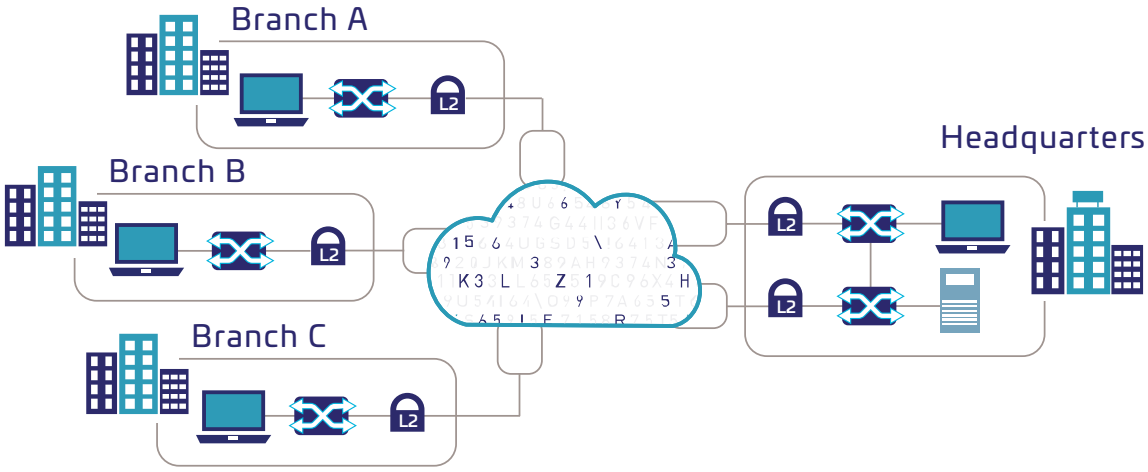
- Reliable field proven hardware
- Support for AES 256- bit keys
- Support for P2P and multipoint
- Designed for FIPS & Common Criteria certification
- True full duplex wire speed encryption up to 10 Gbps
- Low latency under 7.5 microseconds per appliance
- Single GUI and management platform for multiple protocols
- Secure remote management and upgrade
- State-of-the-art encryption and key management

The Benefits

Following a successful pilot project, the bank rolled out the encryption platform to their global WAN, incorporating over thirty branches on three continents. Redundant devices were used for the hub at the bank headquarters, and other Thales HSE CN series dedicated encryptors were used at the end points in the WAN, depending on the bandwidth requirements and the space available in the branch offices. Currently the branches are using rate-limited encryptors, with bandwidths from 100 Mbps to 1 Gbps, allowing the bank to pay only for the bandwidth used (helping them to meet their Capex budget requirements) but also providing them the flexibility to upgrade the branches without changing the hardware. The links at the headquarters are 10 Gbps.

SENETAS
Security without compromise

IDQ



- **High performance -** The Layer 2 platform provided high-throughput encryption on the telco's MPLS network, using 100% of the bandwidth with no packet loss in transport mode. Meeting network standards (IEEE 802.1Q) the VLAN was left transparent for the carrier.
- **Low latency -** The solution provided the low latency that was crucial for the bank's real time communications and banking applications (Latency was tested at below 7.5 microseconds per encryptor, and 15 microseconds per pair).
- **Designed for security -** The encryptors are based on the leading 256-bit AES cipher (Advanced Encryption Standard) in CTR/CFB mode and are certified to the highest commercial standards – currently in process for Common Criteria and FIPS 140-2 Level 3 certification.
- **Multicast -** For VLAN-based multicast traffic, Thales' intelligent group key system utilized one encryption key per secured connection. This means, for example, that the headquarters could securely videoconference with Branch A and Branch C, without Branch B being able to access the communication.
- **Scalable architecture -** The encryption platform provided critical benefits to enable both security and versatility in a point-to-multipoint architecture. The products support different traffic for varied applications – for example, unicast (standard), multicast (finance information to traders, secure videoconferencing, etc.) or broadcast (automated equipment info exchange, etc.).
- **Intelligent Key Management –** The architecture of the Intelligent Group Key system also provided a higher level of security in case of partial network failure – essential for global banking operations in countries with variable SLAs. Providing much greater resilience to common network problems, the keys are generated per secured connection and are renewed up to every 60 seconds. In the event of a partial network outage or loss of connectivity between two network areas, the keys are still renewed and continue to function as required in each separate part of the remaining network.

Challenge

- The global financial institution's existing encryption solution was a Layer 2 E1/T1 link, but as the bank grew it couldn't handle the amount of data required for access to real-time customer data.

Solution

- The bank, under guidance from Senetas and ID Quantique, chose the Thales High Speed Encryptors to secure its global WAN.

Benefit

- The high-performance encryptors provides the high-throughput encryption needed to ensure customer confidentiality, maintain regulatory compliance, and gain access to real-time data.

- **Management -** The Thales Encryptor Manager CM7 (CM7) graphic management platform user interface facilitated the every-day remote management of the network, the keys and the encryptors through a secure SNMPv3 connection. The bank was able to monitor real-time status and configuration changes easily. Different levels of user rights within CM7 allowed separation of duty between the network and security teams, with mission critical functions reserved for the administrator role. In addition the topology of the network and the addition or deletion of encryptors could be managed while the encryptors were still functioning, either in manual or in auto-discovery mode.

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.

> cpl.thalesgroup.com <

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us