IDQ
FROM VISION TO TECHNOLOGY

USER CASE

REDEFINING SECURITY

Global Bank

IDQ Secures Global Wide Area Network

Multipoint 100 Megabit Ethernet Encryption

Centauris Layer 2 Encryptors

- Reliable field proven hardware
- Support for AES 256- bit keys
- Support for P2P and multipoint
- Leading FIPS & CC certification
- True full duplex wire speed encryption up to 10Gbps
- Low latency under 15 microseconds
- Single GUI and management platform for multiple protocols
- Secure remote management & upgrade

The Challenge

An international bank needed to upgrade their encryption infrastructure to meet new business requirements. Their commitment to customer confidentiality, the increasing demands of regulatory compliance and the need for real-time data flow led the bank to re-evaluate their technical situation in an environment where new technologies were rapidly being made available and where the total cost of ownership was decreasing.

Their existing solution was a 2 Mbps layer 2 E1/T1 link, which could no longer handle the amount of data required. The bank then tested a Layer 3 IPSec solution, but rejected this due to the relatively high cost, complexity of installation and lower throughput. Morever, 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.

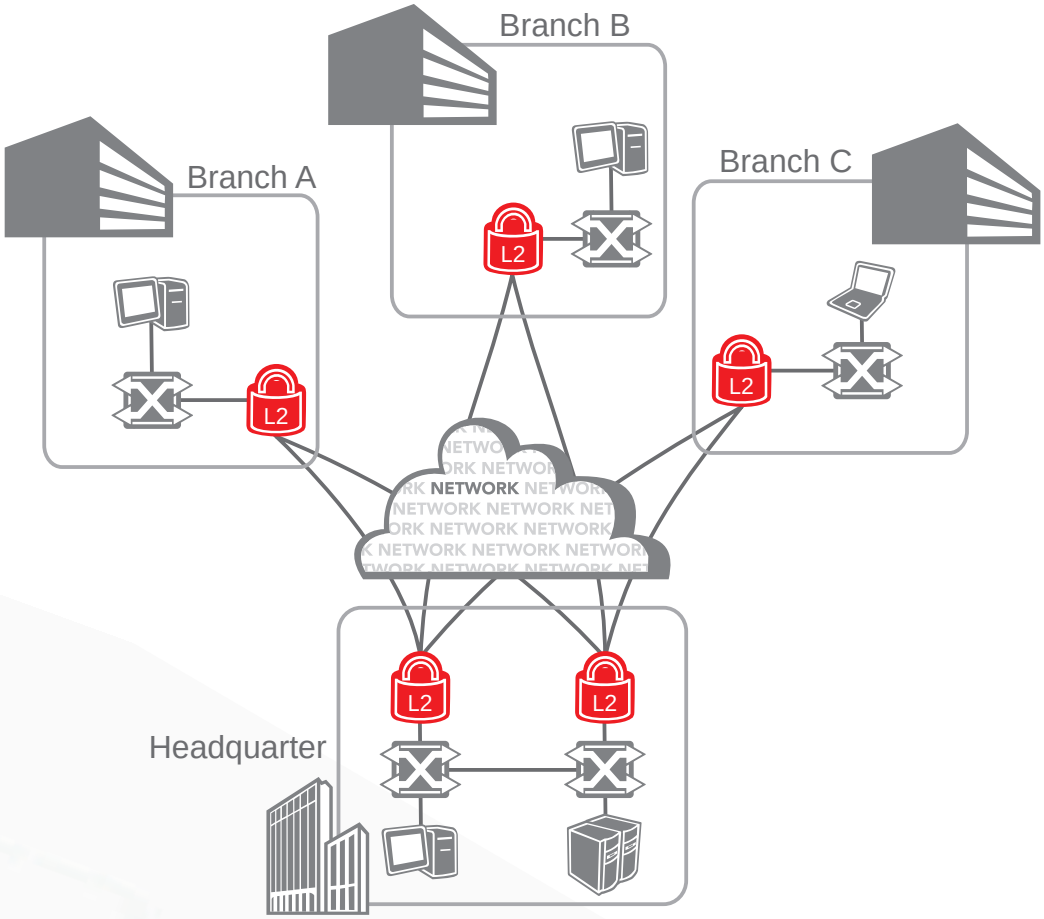
The challenge for the bank was to find a high-performance solution which was easy to deploy and maintain within a reasonable budget.

The Solution

The bank chose IDQ's Centauris Ethernet platform in partnership with COLT Telecom Group. IDQ's layer 2 platform provided high-throughput encryption on Colt's MPLS network, using 100% of the bandwidth with no packet loss in transport mode. The latency was tested at below 15 microseconds per encryptor pair, crucial for real time communications and banking applications. The Centauris 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 - Common Criteria EAL4+ & FIPS PUB 140-2 level 3 accreditation. They provided compatibility with 802.1Q, and the VLAN was left transparent for the carrier.

In addition, IDQ's encryption platform provided other 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). For VLAN-based multicast traffic, IDQ's intelligent group key system utilised one encryption key per secured connection.

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



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.

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. Solutions with a single point of failure (such as a separate key manager) are vulnerable to network problems since the encryption keys cannot subsequently be renewed. In the IDQ system, the keys are generated per secured connection and are renewed up to every 60 seconds, providing much greater resilience to common network problems. 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.

From a usability perspective IDQ's CypherManager graphic 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 the CypherManager 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.

The Results

After the success of the pilot project, the bank rolled out the IDQ encryption platform to their global WAN, incorporating over thirty branches on three continents.

Currently the headquarters uses two Gigabit Ethernet encryptors, and the branches are each equipped with a 1 Gigabit encryptor rate-limited to 100 Megabits. This allowed the bank to meet their Capex budget requirement at the time of installation, as they only paid for the bandwidth used. However they have the versatility to upgrade the branches to higher bandwidths in the future without changing the hardware.

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