International Law Enforcement HD CCTV Network

Major CCTV network and surveillance services provider chooses Thales high-assurance encryptors to protect European law enforcement CCTV network-transmitted data.

Thales CN Series encryptors enable certified data security and integrity without compromising CCTV network's performance.

Our customer is a specialist in delivering secure surveillance information. They work with governments and multinational corporations on the most complex and critical HD CCTV surveillance challenges within the regulatory, law enforcement, defence and critical infrastructure sectors.

Working with a law enforcement organization in Northern Europe the challenge was to design a secure video distribution infrastructure that would allow sensitive HD CCTV streams to be securely distributed across the whole country.

CCTV technology is commonly used to help protect high-profile locations such as international borders, airports, public buildings, military bases, oil and gas facilities, public spaces and mass-transit systems.

In more recent years, CCTV applications have seen an increased demand for real-time streaming of high-definition images. This has proved challenging for some data security systems, which typically reduce image quality and suffer from latency-driven streaming delays.

Demand for live HD video is apparent across many industries and has led to a proliferation of network video traffic; much of which is sensitive in nature and must be securely and efficiently transmitted across communication infrastructures.

CCTV data requires protection against privacy breaches, the input of rogue data and any unauthorized access that may adversely affect the CCTV data's integrity. These are particularly important issues amongst law enforcement and regulatory compliance applications.

Efficient HD video distribution/streaming (typically involving large volumes of data) uses multicast transmission protocols to ensure data is only sent to devices that have requested it.

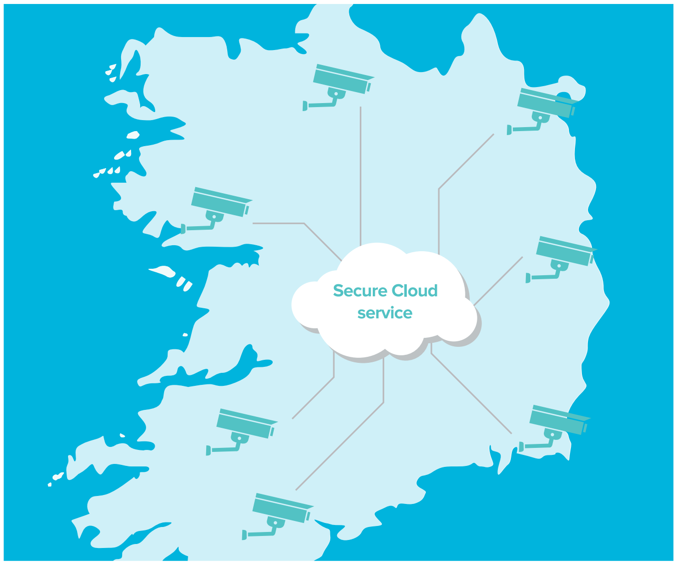

Figure 1 – CCTV Network

Evaluating the alternatives

One of the first solutions considered was based on a regular Layer 3 (Internet Protocol) routed data network; with all traffic to be encrypted using the common IPSec security protocol.

IPSec is an industry standard for securing data across Layer 3 routed data network environments and is optimized for use on "best-effort" networks such as the Internet.

However, securing data at Layer 3 has several limitations, especially when high-performance delivery of the HD CCTV feeds is required.

Speed restrictions, latency and excessive network overheads would impact on image quality, network performance and overall data security.

Encrypting at Layer 3 would not provide the high-assurance, high-performance solution necessary to meet the client's exacting standards.

There are also technical issues of complexity that arise when encrypting at Layer 3. To help overcome these limitations, IPSec encryption solutions typically require customers to increase network bandwidth (by up to 30%), which comes at a considerable cost

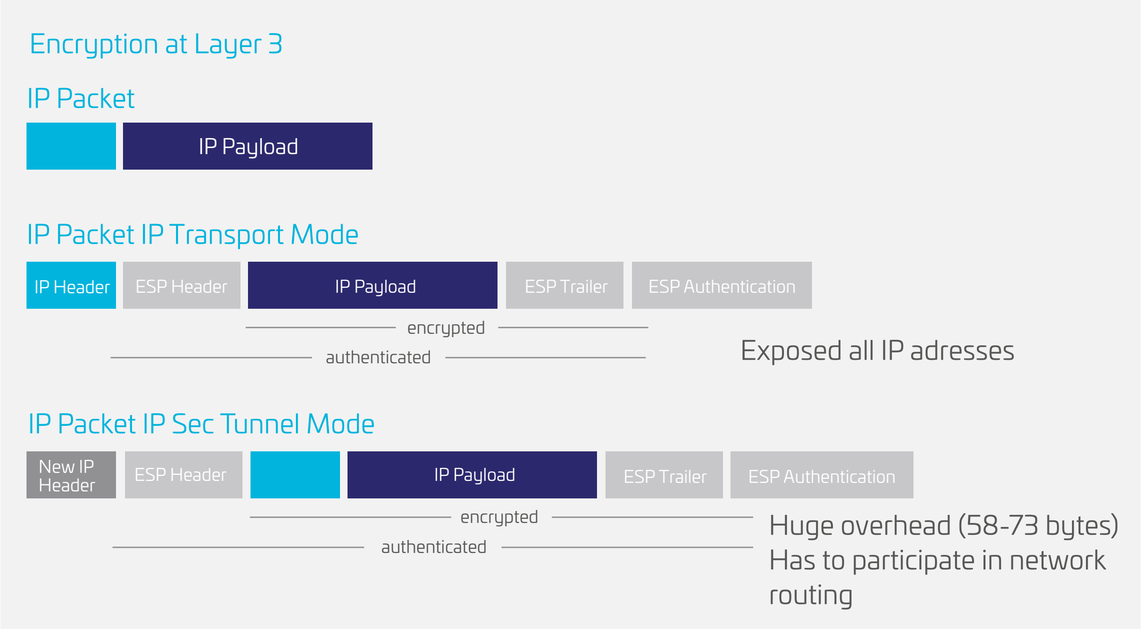

Figure 2 – IPSec encryption overhead

Multicast Transmission

Securing multicast encryption at Layer 3 is problematic, because the underlying network requires additional routing protocols to support multicast traffic such as the Protocol-Independent Multicast (PIM) routing family.

These protocols provide an additional level of complexity when required to interoperate with IPSec encryption. In practice the issue is that much of multicast IP traffic is encapsulated using GRE (Generic Routing Encapsulation) tunnels to allow the simpler encryption of unicast traffic, albeit with far higher overheads. Consequently, when encrypting at Layer 3, the underlying data network and equipment need to be of a higher specification.

Data delivery is inefficient for large scale multicast deployments and these "hidden" costs were a significant factor in the choice of solution.

Thales High-Assurance Encryption Solution

With the limitations and disadvantages of transmitting encrypted multi-location CCTV data across Layer 3 network links clearly identified, an alternative network architecture was required.

Thales proposed an alternative based on a Layer 2 WAN service with high speed encryption at the Ethernet layer. Thales CN high-assurance encryptors would not add overhead to the network data, offer near-zero latency and have no impact on other network assets.

At Layer 2, Thales encryptors provide far simpler "set and forget" implementation and ongoing management; making the solution much more efficient, both technically and financially.

The Thales encryption solution is optimized for network services such as Metro Ethernet E-LAN, E-LINE or E-TREE, Layer 2 MPLS (VPLS) or across simple point-to-point dark fibre and WDM (Wavelength Division Multiplexor) connections.

Layer 2 encryption occurs at the data link layer on Ethernet networks. As a result, the Ethernet payload is encrypted but the Ethernet header (including MAC addresses & VLAN identifiers) is unmodified; allowing transmission across service provider networks.

The Ethernet payload fully encapsulates the IP header and IP payloads, which are also encrypted; providing the additional security benefit of hiding all IP addresses in the transmitted data.

Encryption at Layer 2 can deliver 100% encrypted throughput, at speeds up to 10 Gbps, with little or no additional per frame overhead.

Also, because encryption occurs at the data link layer, no special configuration or protocols are required to encrypt multicast or broadcast traffic.

To ensure efficient multicast data transmission across a Layer 2 network, protocols such as IGMP or MLD are often deployed between hosts and routers. Network switches may also perform IGMP monitoring to listen in on the IGMP conversation, allowing them to maintain a map of links that need IP multicast streams.

This mechanism maintains data network efficiency by only delivering frames where they are needed. By allowing IGMP/MLD traffic to be bypassed (when required), a Layer 2 encryptor allows the network to continue operating with maximum efficiency without requiring any underlying changes
to its operation.

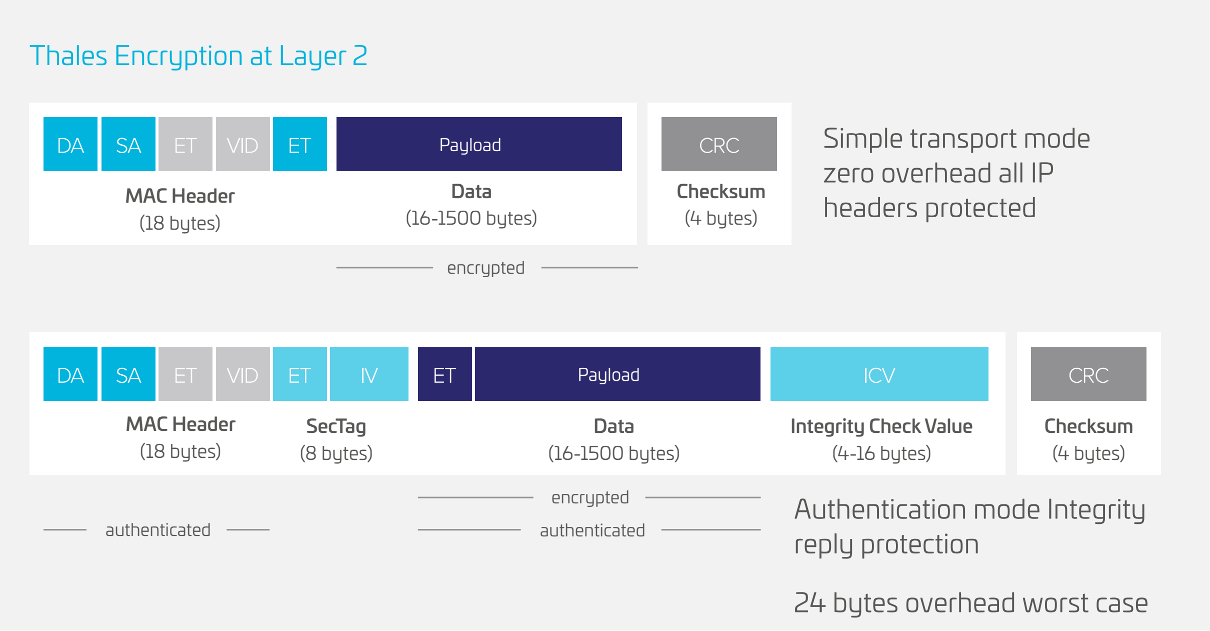

Figure 3 – Ethernet encryption overhead

Customer Benefits

The performance benefits and network efficiencies associated with Thales high-assurance encryptors were instrumental in the CCTV service provider's decision to implement the Thales solution.

Thales CN encryptors were chosen to secure data transmitted from over 100 end-points across Northern Europe.

By minimizing latency, network overheads and technical complexities, Thales CN encryptors maximize the available bandwidth for the customer's use, helping to reduce both management time and cost.

Thales high-assurance encryptors provide certified information security and network performance is maximized for delivery of both multicast and unicast traffic. Simple, automatic 'zero-touch' key management ensures that encryption scales efficiently to the largest deployments.

Near-zero latency is enabled by Thales' unique technology – purpose built hardware encryption engines that perform cut-through processing of network traffic at wire speed.

Tamper-resistant chassis provide protection to all encryption keys and user credentials at government-certified levels.

Thales CN encryptors are certified by all leading international, independent testing authorities: FIPS, Common Criteria, CAPS and NATO.

Large numbers of encryptors are easily and securely managed using CM7; Thales' remote management software. Using SNMPv3, this tool provides simple, secure remote management either out-of-band or in-band using the encrypted Ethernet port.

Benefits Summary

Flexibility:
Thales' unique Field Programmable Gate Array technology enables customisation flexibility.

Interoperability:
All CN encryptors are interoperable, providing an efficient long-term investment.

Zero impact:
Thales CN encryptors have no impact on other network assets and require no network changes during implementation.

Reliability:
Thales encryptors provide 99.999% uptime in the most demanding 24/7 availability environments.

Upgradability:
Among the various CN encryptors, many have field replaceable and upgradeable components.

Scalability:
Unlike other encryption solutions, Thales CN series encryptors are scalable to as many as 300 connections.

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.

Figure 4 – CN6010 Network Encryptor

> cpl.thalesgroup.com <

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