cpl.thalesgroup.com

THALES
Building a future we can all trust

Network encryption ensures safety of massive data transfers between collection and processing centers.

Analysts predict annual sales of 12 million fully autonomous vehicles by 2035. As automobiles become more connected, manufacturers are collecting enormous data packets to gather insights aimed at capitalizing on customer behavior, understanding product performance, and predicting failures. Automobile manufacturers and mobility companies face enormous challenges protecting that data and preserving privacy. This case study explores the collaboration between the IT company collecting the data, the data center provider that stores and analyzes the data, and the Thales High Speed Encryptors (HSE) that secure data collected from autonomous driving cars as it travels between collection sites and processing centers.

The Business Need—IoT Data Protection

A software developer for autonomous driving and advanced driver-assistance systems collects massive amounts of data from its test automobiles. Using the sense-think-act model of automation, the developer's goal is to get cars to drive better than humans. Studying the good, the bad, and the proficient behaviors of the self-driving cars helps them come closer to realizing their goal every day. With IoT use cases, networks are increasingly more complex and multi-layered. Where networks were once centered around an isolated data center, they are now distributed amongst the cloud, a broad range of applications, and multiple devices—in this use case, cars.

To meet these challenges, the software developer needed a collection and processing solution for the petabytes of data constantly collected from its vehicles. The solution required a flexible and scalable platform. A multinational company specializing in big data provides the collection centers for data analyzation and processing. In addition to collection, it was vital to protect the data as it moved from the automobiles to the data center and back. Using IPsec VPN to secure the data in motion was costly, slow, and not built to move this amount of data.

The Solution—Data in Motion Encryption

The data center provider selected Thales CN6140 Multilink Network Encryptor (CN6140), and packaged the high-speed encryption solution into their offerings (hosting and other services), which was then sold back to the software developer as a managed service. The decision to implement network encryptors instead of IPsec was driven by performance, security, and budgetary needs, which Thales encryptors bested the competition on all three. By encrypting data in transit using high assurance Thales network encryptors, data being transmitted between the vehicles and the data center cannot be exposed or manipulated.

The CN6140 is the ideal solution for this performance-intensive environment, with high demands for scalability. The CN6140 is a high-assurance, high-speed encryption solution that provides maximum security and performance, and is certified to the highest security standards.

The Benefits—Security, Speed, Scalability

Thales CN6140 met the customer's needs for flexibility and scalability, while saving it money and increasing performance.

Performance

The CN6140 is a high-performance multilink encryptor, operating in full-duplex mode at full speed without loss of packets. It offers up to 40 Gbps (4x10) scalable, high assurance data in motion encryption.

Scalability

With the CN6140, the provider has the ability to scale from 4x1 Gbps to 4x10 Gbps in one cost effective, multi-channel appliance. The provider started at 10 Gbps, and plans to scale to 40 Gbps. The multi-port design makes this encryptor variable, with speed licenses up to 40 Gbps (4x10 Gbps), easy to install and highly cost-effective. Devices can be field upgraded on site with ease, for maintenance, feature enhancements and security updates.

Security

Preferred by the world's most secure organizations, the tamper resistant CN6140 is certified to Common Criteria EA4+ and FIPS 140-2 Level 3 requirements and supports standards based, end-to-end authenticated encryption and client-side key management.

Separation of Roles

Physical and virtual separation of duties ensures that only authorized users can access the keys. Encryption keys are generated and stored securely in hardware within the device's tamper-resistant enclosure. Any unauthorized attempts to physically extract the keys will result in device zeroization.

Costs

A top concern of the data center provider was cost. With IPsec, it's not uncommon to experience a 30% increase in overhead to Data Egress Traffic, which leads to an increase in costs. By switching from IPsec to Thales HSE, the data center provider saved money and increased performance and bandwidth, while protecting its data-in-motion with scalable, high-assurance encryption, built for modern networks.

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.