thalestct.com

THALES

Ethernet WAN Encryption Solutions Compared

White Paper

Executive Summary

This White Paper describes the comparative security and performance benefits of Ethernet WAN data security solutions. We compare the benefits of Thales Layer 2 high speed encryption hardware with integrated encryption using MACsec or TrustSec.

Introduction

Network data security risks are well known, including serious data breaches at the Data Link Layer – Layer 2 – in Wide Area Networks (WANs) and carrier-connected network services.

Consequently, encryption of sensitive data is adopted by the world's most secure organizations and market leaders as the optimal information security technology.

Government agencies have set demanding certification standards for encrypting sensitive transmitted data. Thales's product legacy lies in meeting these rigorous demands through purpose-designed certified high speed encryptors, dedicated to protecting sensitive data – without compromising network performance.

Similarly, commercial organizations adopt encryption as the optimal approach to protecting sensitive data transmitted across their Wide and Metropolitan Area Networks that interconnect their different sites. As their business plans increase demand for cloud and data center services and big data technologies, their WANs rapidly grow, exposing the organizations to new and serious threats.

Simply put, encryption protects the data itself in the event of a network breach. When 'prevention security' (e.g. firewalls etc.) technologies fail, encrypted data is protected – the data is rendered useless in unauthorized hands.

However, as various Layer 2 encryption technologies have evolved, many come with security weaknesses and inefficiencies. Some add significant network overheads that compromise network performance, which also proves costly. Other encryption technologies add significant complexities when other network devices are present, such as in large or more complex 'multi-point-to-multi-point' topologies.

As market demand for Ethernet data security increases, encryption is increasingly being implemented in conventional network equipment such as switches or routers. They often use IPSec for encryption of network traffic at Layer 3, or the Media Access Control Security standard (MACsec) for encryption of Ethernet frames at Layer 2.

While different approaches may be taken to the implementation and deployment of network data encryption; when evaluating different solutions it is important to understand the trade-offs (and compromises) in both data security and network performance that may apply.

The Issue – Protecting Ethernet Network Transmitted Data

For maximum data protection on both LAN and Ethernet WANs sensitive data should be encrypted. Ethernet network traffic that is not encrypted is vulnerable to a variety of attacks such as snooping, spoofing, tampering, replay and unauthorized traffic analysis. Each attack type results in sensitive data getting into attackers' hands.

The MACsec security standard was designed specifically to provide port based security across Local Area Networks (LANs); CN high-speed encryptors are purpose-designed to protect data transmitted across Metropolitan and Wide Area Networks including Carrier Ethernet services regardless of the topologies and architectures used.

Whether the WAN is a simple point-to-point or highly complex multi-point-to-multi-point fully meshed network; CN encryptors provide maximum encryption security without compromising network performance.

MACsec

Known as MACsec, (802.1AE) the IEEE MAC security standard defines connectionless data confidentiality and authentication to enable secure communications on Local Area Networks. MACsec is defined by two IEEE standards:

- 802.1ae - defines the frame format, encryption algorithm, data authentication and Ethernet frame processing
- 802.1x-2010 - defines port based authentication and the MacSec Key Agreement protocol MKA.

MACsec is a security standard originally designed for LAN use - to prevent network data sniffing and unauthenticated access to network resources. MACsec was specifically designed to secure 'hop-by-hop'[1] network connections requiring every port at the end of an Ethernet segment to be MACsec compliant (trusted).

However, when transmitting data across WANs using MACsec, the data will be encrypted and decrypted on every MACsec enabled device in the path. This means that each intermediate network device in the traffic path has full visibility of the data. Therefore, MacSec does not provide 'end- end security'2.

This 'hop-by-hop' data journey causes a serious WAN security risk by leaving the data completely unprotected at each node. The hop-to-hop data journey is also highly inefficient and unnecessarily complex.

MACsec may be carried on pseudo-wire connections across a WAN, which removes the requirement for each hop to support the protocol. Pseudo-wires provide a LAN emulation capability by encapsulating the Ethernet traffic with an additional header so that it may be sent across the native transport network e.g. MPLS, IP or SONET networks.

However, when the underlying transport network itself is an Ethernet service, pseudo-wires are unnecessary because they introduce a significant overhead and additional complexity. In this case native encryption at the Ethernet frame Layer is much preferred for efficiency.

Therefore, it is for these important reasons that MACsec is not a suitable protocol for use on carrier-connected Ethernet WANs.

MACsec Implementations

MACsec is a common feature in modern Ethernet switches and may be used to enable strong data security on Ethernet links, providing data confidentiality and integrity using GCM- AES-128 encryption.

MACsec is commonly implemented on switch downlink ports where it is used to protect local area Ethernet segments. For example Cisco switches support MACsec on downlink ports but do not support it on 'switch-to-switch' uplinks. To encrypt inter-switch data, Cisco switches use a proprietary extension known as TrustSec.

TrustSec is based on MACsec and therefore is also limited to 'hop-by-hop' scenarios. These restrict TrustSec to use on direct connections. Hence TrustSec may not be used on metro-Ethernet services nor carrier-provided label switched services.

High-Speed Encryption Hardware and Network Fit

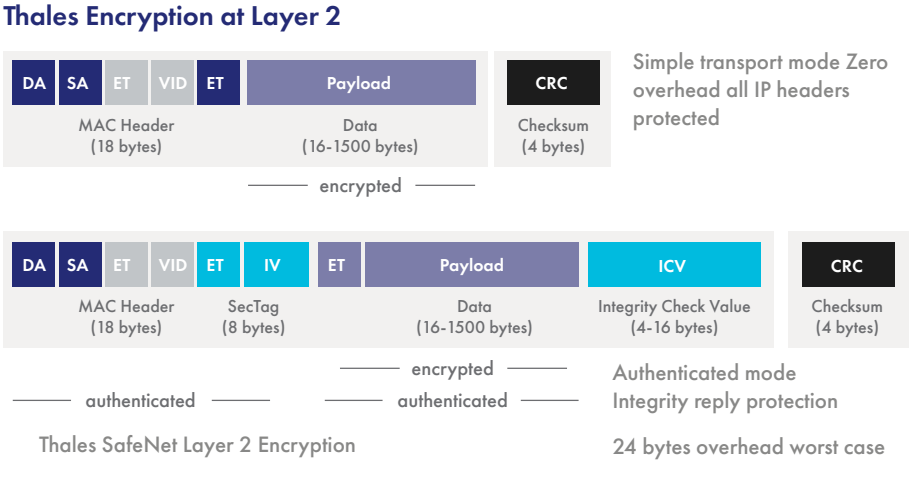
By comparison, High Speed Encryptors (HSE) have been specifically designed to provide end-to- end data encryption across any type of data network topology, including service provider networks. HSE encryptors are used globally on WAN infrastructures in point-to-point, hub and spoke and fully meshed environments. Provided that the underlying carriage is Layer 2 there are no restrictions on the number of hops, intermediate nodes or service provider networks that may be protected.

CN encryptors are extensively used by many of the world's most secure organizations and market-leaders to protect sensitive information transmitted across a wide range of global, international and national WAN infrastructures.

Most importantly, at every point in the network the encryption-protected data remains encrypted and is not decrypted until it reaches an authenticated encryptor at the intended destination! There are no weak-points in the hardware encryption process and the data's journey – there are no security 'gaps'.

The encryptors' 'HSE policy' is very powerful yet simple to implement and manage. CN encryptors may be centrally managed over the network using the CM7 or SMC encryptor management applications, which enables a large number of encryptors to be setup quickly and simply across all topologies.

Figure 1 –High Speed Encryption modes



The Encryption 'Tax' – Encryption Overheads and Network Performance

All encryption necessarily introduces some additional traffic on the network - often referred to as the encryption 'tax'. This tax depends upon how encryption is implemented as well as any specific security features required. The size of that overhead may significantly impact the performance of the network.

Generally, encryption overheads arise from:

- Network frames that are inserted by encryptors - to ensure encryption keys are regularly updated between and among encryptors and for the purpose of remote encryptor management
- Additional per-frame overheads – to provide synchronization, packet integrity and data origin authentication. The amount of data overhead is dependent upon the encryption mode used.

The inserted overhead is typically minimal (far less than 0.1% of the network link); however the per-frame overhead is higher and may range from 0 to 82 bytes per frame.

The highest per-frame overhead occurs when confidentiality, frame integrity and data origin authentication features are all required, leading to a trade-off among the security features used and the desired/achievable network performance.

If confidentiality of the frame payload is the only requirement then the per-frame overhead may be removed entirely.

The CN encryptor platform provides highly efficient native Ethernet encryption - ensuring the encryption tax is absolutely minimal. When using 'low overhead' transport mode under real world conditions, Thales encryptors may achieve 100% line rate for all packet sizes!

CN encryptors provide a wide choice of encryption modes, which include:

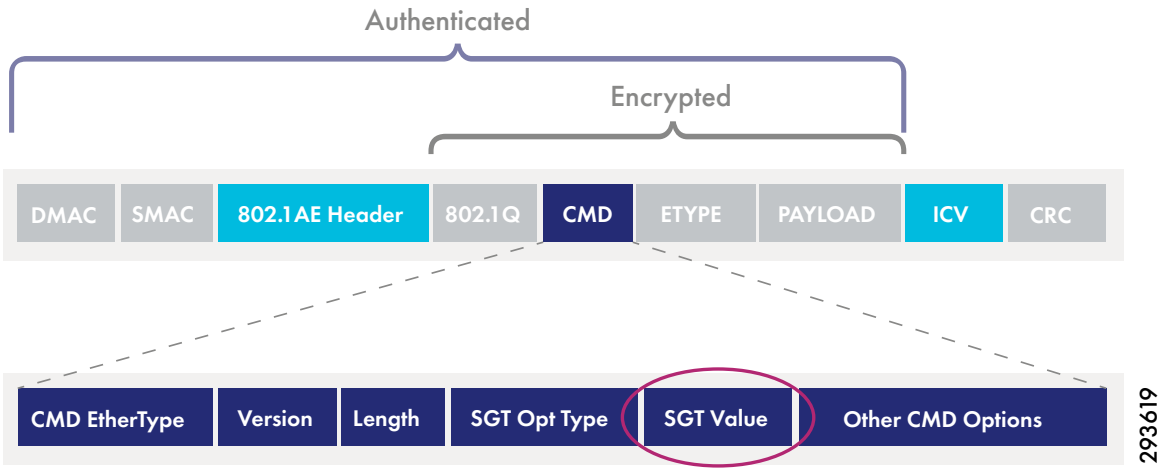
- Fully authenticated mode: 24 byte per frame overhead providing confidentiality, frame integrity, data origin authentication and replay protection
- Simple transport mode: Between 0-8 bytes per frame overhead providing confidentiality and replay protection

Figure 1 shows the encrypted frame format, the user may configure the mode using the CM7 encryptor management tool.

Note: Available encryption modes may vary by encryptor model, link speed and selected network mode (i.e. Line, VLAN or Mac).

In the case of MACsec it has an additional per frame overhead of 32 bytes and Cisco TrustSec increases this overhead to 40 bytes because an additional 8 bytes of Cisco metadata is present - see Figure 2.

Figure 2—Cisco TrustSec



Further, when using Cisco TrustSec over a carrier-connected network it is necessary to encapsulate the entire Ethernet frame inside an IP packet that is transported over Ethernet.

Cisco refers to this as 'Overlay Transport Virtualization' (OTV), which adds another 42 bytes per frame – resulting in a total data overhead of 82 bytes per frame! For details refer to: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/ Borderless_Networks/Unified_Access/BYOD_Design_Guide/ BYOD_Network_Design.html

Figure 3—Network throughput for different encryption modes

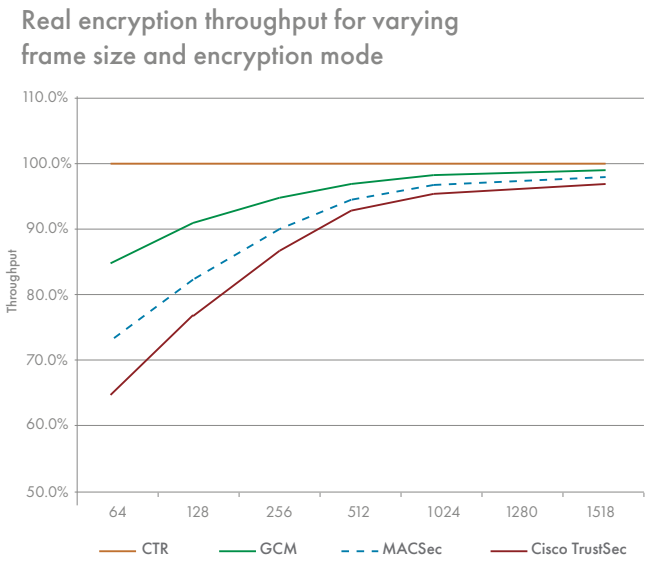


Figure 3 shows the achievable throughput for different frame sizes in several different encryption modes.

Note: figure 3 shows the theoretical (not measured) throughput that is achievable given the per-frame overhead. These are therefore best case scenarios that assume the encryption engine can actually keep up with the maximum achievable throughput.

Figure 3 shows the achievable throughput for different frame sizes in several different encryption modes.

Note: figure 3 shows the theoretical (not measured) throughput that is achievable given the per-frame overhead. These are therefore best case scenarios that assume the encryption engine can actually keep up with the maximum achievable throughput.

The per-frame overhead may have a significant impact on the performance of the network and significantly reduce network throughput. This overhead also imposes a significant financial cost of 'lost' network performance.

The top-most line in figure 3 shows that 100% throughput may be achieved for all frame sizes when using Thales encryptors' transport encryption mode. Even when using full authentication mode CN encryptors may achieve nearly 90% throughput for smaller frames. Generally, the vast majority of frames are 256 bytes or smaller so with MACsec/TrustSec most customers will pay a high penalty of encryption of >30% on average and twice that of the Thales High Speed Encryptor solutions. See figure 4.

By contrast, the red line at the bottom of figure 3 shows the throughput achieved for Cisco TrustSec with 40 bytes of overhead. In this mode the network bandwidth is reduced by nearly 35% for small and medium sized frames thus limiting the scalability of the solution and making it unsuitable for heavily utilized connections. Across a carrier-connected Ethernet WAN link, using Cisco's OTV encryption, the data overhead is nearly doubled. This data overhead significantly reduces the throughput even further.

Significantly and in contrast, RFC2544 testing3 demonstrates that the FPGA encryption engine may achieve 100% line rate for all packet sizes when using low overhead transport mode under real world conditions. Latency is approximately 6 microseconds at 10 Gbps.

Encryptors' Hardware Security

CN high-speed encryptors are purpose-designed and built to the highest government certification standards they have been independently tested by international testing authorities and hold all four major certifications for cryptographic products.

The certifications held among the various CN platform model encryptors are:

- DoDIN APL Approval
- FIPS 140-2 level 3
- Common Criteria EAL4+ and EAL2+
- CAPS Baseline
- NATO Green Restricted

Thales encryptors include strong physical protection to prevent tampering or probing of the encryptors, such as attempts to access encryption keys.

Further, hardware random number generators generate genuine random encryption keys that are stored securely within the encryptors' protected physical enclosures.In addition the keys are protected in hardware and managed with ease using Thales High Speed Encryptor management solutions.

Router or switch based encryptors are not designed to provide an equivalent level of physical or virtual security. Consequently, this means that critical security parameters such as keys and passwords may be considerably more vulnerable and susceptible to physical compromise without such protection mechanisms.

The use of network devices such as routers and switches as encryptors also fails to provide the optimal separation of duties between network and security management duties. Separation of duties is often referred to as a data security best practice. Due to proprietary implementations, most routers and switch based encryptors are not interoperable with other vendors. This results in double vendor lock in. Thales encryptors are vendor agnostic.

Conclusion

Thales TCT delivers a complete set of solutions that offer an unparalleled combination of robust security, high performance, and minimal cost and administrative overhead. With these solutions, you can address critical security threats while maximizing the value of your investments.

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., protects the most vital data from the core to the cloud to the field. We serve as a trusted, U.S. based source for cyber security solutions for the U.S. Federal Government. Our solutions enable agencies to deploy a holistic data protection ecosystem where data and cryptographic keys are secured and managed, and access and distribution are controlled.

Contact Us: For more information, visit www.thalestct.com

3465 Box Hill Corporate Center Drive, Suite D, Abingdon, MD 21009 • 443-484-7070 • info@thalestct.com
thalestct.com