SENETAS

Security without compromise

ETHERNET WAN ENCRYPTION SOLUTIONS COMPARED

TECHNICAL PAPER

INTRODUCTION

This technical paper examines the pros and cons of different WAN encryption solutions. It compares Senetas certified high-assurance encryption hardware with the application of the Media Access Control Security (MACsec) standard in other devices – highlighting important security and performance trade-offs.

The data protection risk landscape is constantly evolving, but the risks facing sensitive data in motion across WAN infrastructure is well known. The long list of data breaches over the past five years tells its own story: high-speed data networks are not inherently secure.

With data breaches widely acknowledged as being inevitable, IT professionals are shifting their focus away from beach prevention to breach protection. Many of the world's leading organisations have adopted data encryption as their optimal data protection technology.

Government agencies around the world have set demanding certification standards for encrypting sensitive transmitted data. Senetas' product legacy lies in meeting these rigorous demands through certified, high-assurance encryptors, dedicated to protecting sensitive data without compromising on network performance.

Commercial organisations have adopted the same rigorous standards and are using encryption to protect sensitive customer data, intellectual property and trade secrets across their metro and wide area networks.

Organisations of all types have become increasingly dependent upon high-speed data networks to conduct business as usual. From secure collaboration to cloud services, aggregated big data applications and the Internet of Things; data has become the currency of business.

Encryption protects the data itself in the event of a network breach. When prevention security technologies such as firewalls fail, encrypted data remains protected and the data is rendered useless in the hands of unauthorised users.

The case for encryption, then, is an easy one to make. However, as the market for encryption technologies has evolved, it has become apparent that not all encryption solutions are created equal.

Some have been developed with inherent weaknesses or inefficiencies, adding a significant network overhead that adds cost and complexity and compromises network and application performance.

With demand for Ethernet data security on the rise, encryption is increasingly implemented within conventional network equipment, such as routers and switches. Such encryption often uses IPsec at Layer 3 or MACsec for Ethernet frames at Layer 2.

Different approaches may be taken to implement and deploy network data encryption. It is important when evaluating these alternatives to understand the trade-offs and compromises in both data security and network performance that may apply.

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, relay and unauthorised traffic analysis.

MACsec

The IEEE MAC Security Standard (known as MACSec) is used to define connectionless data confidentiality and authentication. It is comprised of two separate standards:

- 802.1ae – defines frame format, encryption algorithms, 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. The MACsec security standard 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).

When transmitting data across a WAN using MACsec, the data will be encrypted and decrypted on every MACsec enabled device in the path. This means each intermediate network device in the traffic path has full visibility of the data. MACsec does not provide end-end[2] security.

The hop-by-hop data journey creates a security risk by leaving the data completely unprotected at each node; it is both highly inefficient and unnecessarily complex.

MACsec may be carried on pseudo-wire connections across a WAN, removing the need 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).

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.

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 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 the MACsec security standard and is also limited to hop-by-hop scenarios; restricting TrustSec use on direct connections. TrustSec may not be used on metro-Ethernet services, nor carrier-provided label switched services.

[1] Hop-by-hop is a term used to describe data's transit journey on a network. Each hop is when data reaches a device such as a switch.

[2] End-to-end is a term used here to describe the transmitted data's whole journey – where the data begins its journey encrypted until it completes its whole journey where it is then decrypted.

HIGH-ASSURANCE ETHERNET ENCRYPTION HARDWARE

Senetas high-speed encryption (HSE) hardware has been specifically designed to provide end-to-end data encryption across any type of data network topology; including service provider networks.

Senetas encryptors are used globally on Ethernet WAN infrastructures in point-to-point, hub and spoke, multipoint-to-multipoint and fully meshed environments.

If encrypted at Layer 2, there are no restrictions on the number of hops, intermediate nodes or service provider networks that may be protected.

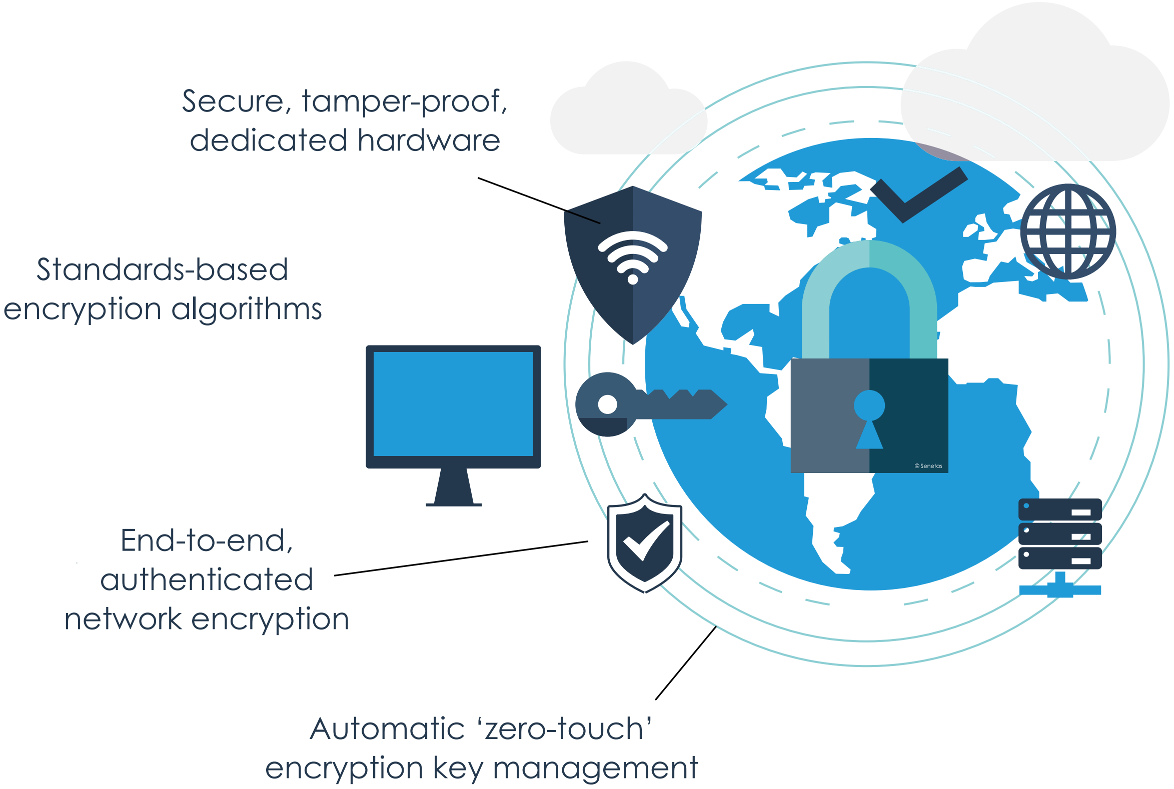
Many of the world's most secure organisations trust Senetas encryptors to secure sensitive data in motion across metro and wide area networks.

Senetas CN Series encryptors are used by governments, defence agencies, multi-national enterprises and Cloud service providers in more than 40 countries.

An essential component of the Senetas high-assurance promise is the provision of authenticated, end-to-end encryption. Data remains encrypted at every point throughout its journey across the network.

Senetas encryptors provide robust encryption security but are simple to implement and manage.

Senetas CN Series encryptors may be centrally managed over the network using the Senetas CM7 encryptor management application, which enables multiple encryptors to be provisioned and managed simply, across all topologies.


Secure, tamper-proof, dedicated hardware
Standards-based encryption algorithms
End-to-end, authenticated network encryption
Automatic 'zero-touch' encryption key management
© Senetas

ENCRYPTION OVERHEAD AND NETWORK PERFORMANCE

All encryption introduces some additional traffic on the network; something that is often referred to as the encryption 'tax'. The amount of tax is dependent upon how the encryption is implemented and the size of the network overhead may have a significant impact on network performance.

Encryption overhead generally comes from two prime sources:

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

The inserted overhead is minimal - 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 authentication features are all required. This leads to a trade-off among the security features used and the desired, or achievable, network performance.

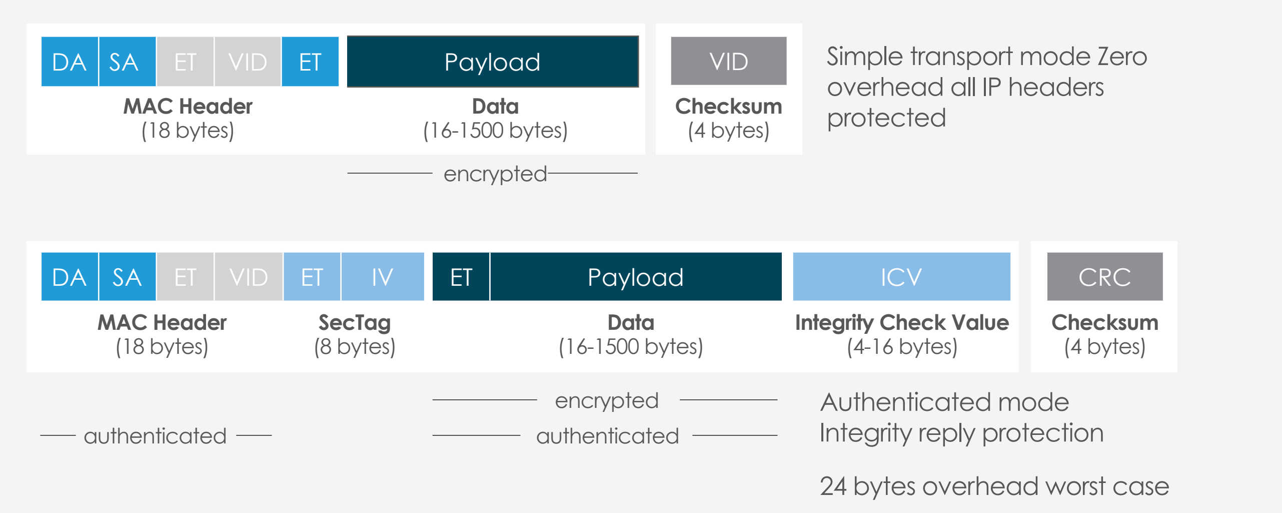
If confidentiality of the frame payload is the only requirement, then the per-frame overhead may be removed entirely.

Senetas CN Series encryptors provide efficient, native Ethernet encryption; ensuring the encryption tax is kept to a minimum. When using low-overhead transport mode under real world conditions, Senetas encryptors may achieve 100% line-rate for all packet sizes.

Senetas CN Series encryptors support a wide range of encryption modes, including:

- 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. High Speed Encryption Modes



Simple transport mode Zero overhead all IP headers protected

Authenticated mode
Integrity reply protection

24 bytes overhead worst case

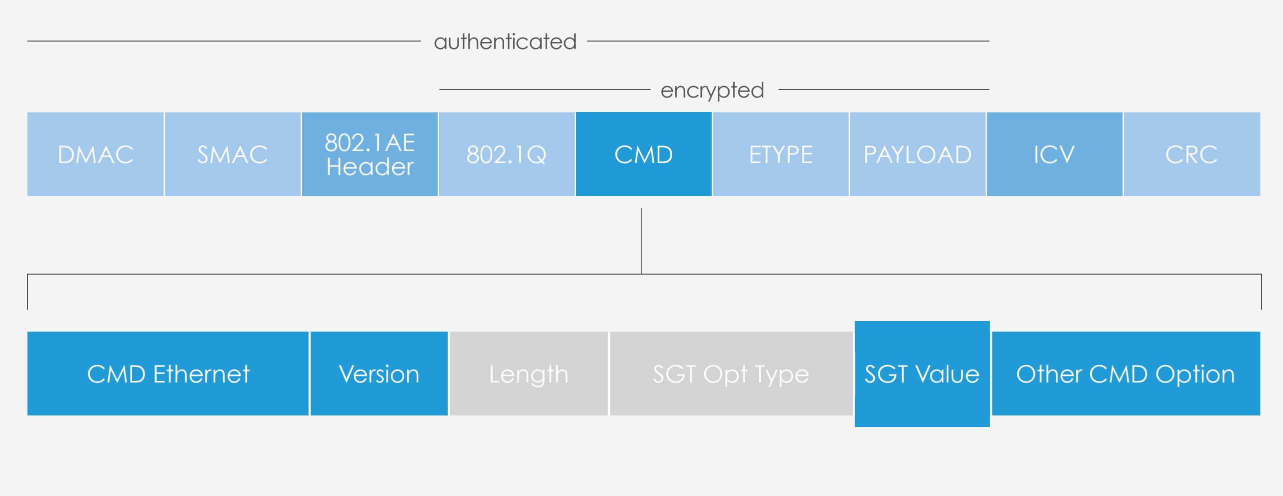
Note: Available encryption modes may vary by encryptor model, link speed and selected network mode (Line, VLAN, or Mac).

In the case of MACsec, there is an additional per-frame overhead of 32 bytes. If Cisco TrustSec is used this overhead is increased to 40 bytes, because an additional 8 bytes of Cisco metadata is present (see figure 2).

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 OTV (Overlay Transport Virtualisation), which adds another 42 bytes per frame; resulting in a total data overhead of 82 bytes per frame.

Figure 2. Cisco TrustSec



NETWORK THROUGHPUT

The per-frame overhead may have significant impact on the performance of the network and significantly reduce the 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 Senetas encryptors in transport encryption mode.

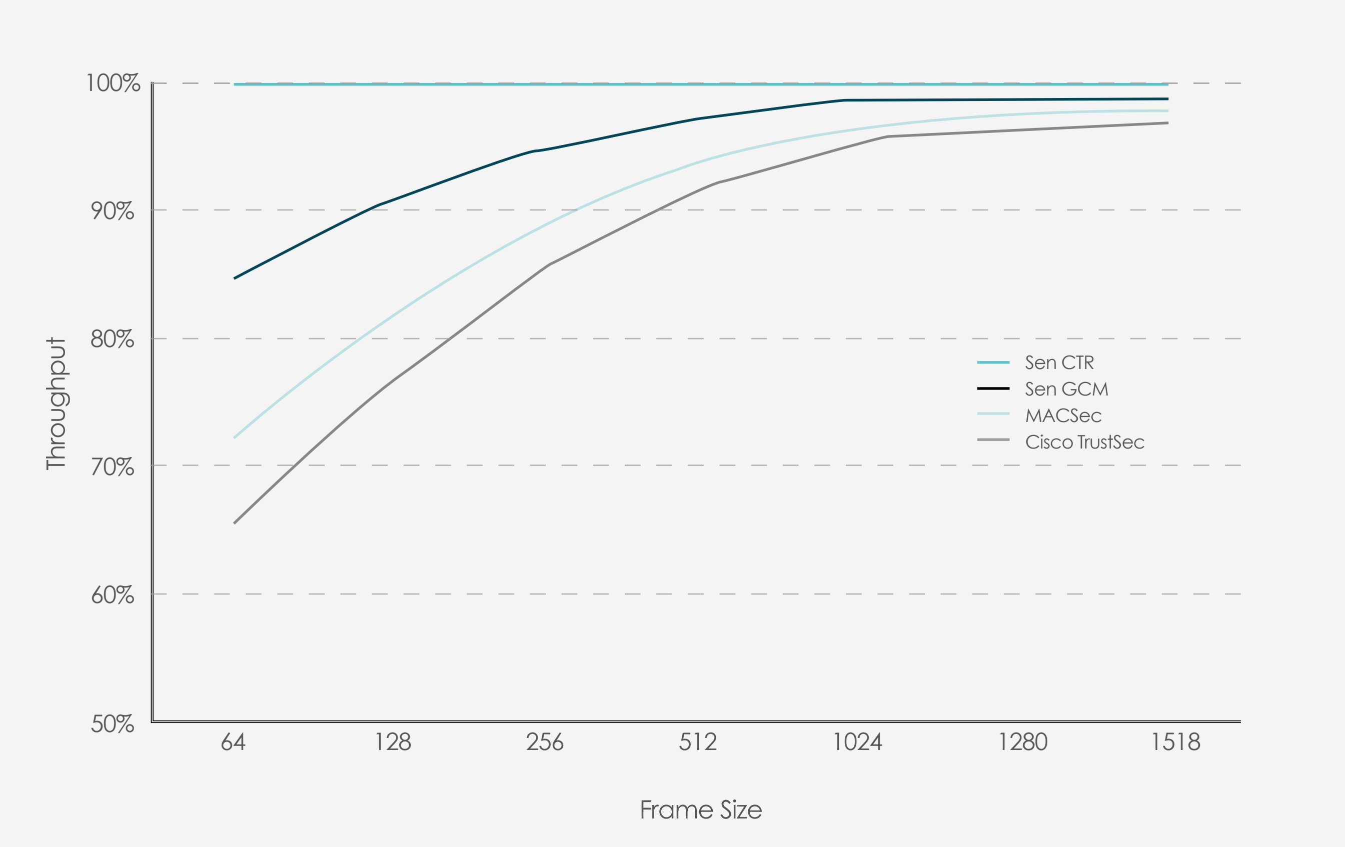
Even when using full authentication mode, Senetas CN encryptors may achieve nearly 90% throughput for small frames.

By contrast, the grey line at the bottom of figure 3 shows the throughput achieved for Cisco TrustSec with 40 bytes of overhead. In this mode, network bandwidth is reduced by nearly 35% for small and medium sized frames; limiting the scalability of the solution and making it unsuitable for heavily utilised connections.

Across a carrier Ethernet WAN link, using Cisco's OTV encryption, the data overhead nearly doubles; reducing the throughput even further.

RFC2544 testing1 demonstrates that the Senetas FPGA encryption engine may achieve 100% line-rate for all packet sizes when using low overhead transport mode. Under real-world conditions latency is just 6 microseconds at 10Gbps.

Figure 3 – Network throughput for 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 keep up with the maximum achievable throughput.

[1]Benchmarking methodology for network interconnect devices.

GLOBAL SUPPORT

Senetas encryption solutions are distributed and supported internationally (outside Australia and New Zealand) by Thales

Thales is the world leader in digital security and defence, servicing over 30,000 customers across 180 countries. Senetas products are sold by Thales under its brand.

ANZ PARTNER COMMUNITY

Senetas works directly with customers and their service providers across Australia and New Zealand. We provide technical consultancy and support to data networks providers, systems integrators and cloud service providers. Visit our **ANZ Partner Page** for full details.

© SENETAS CORPORATION LIMITED

www.senetas.com

Senetas is a leading developer of end-to-end encryption security solutions; trusted to protect enterprise, government, defence, Cloud and service provider network data in over 40 countries.

From certified high-assurance hardware and virtualised encryption, to secure file sharing and collaboration with data sovereignty control, all are based on the same crypto-agile platform and deliver security without compromise.

Regional Contacts:

Asia	**T:** +65 8307 3540	**E:** infoasia@senetas.com
Australia & New Zealand	**T:** +61(03) 9868 4555	**E:** info@senetas.com
Europe, Middle East & Africa	**T:** +44 (0)1256 345 599	**E:** infoemea@senetas.com
The Americas	**T:** +1 949 436 0509	**E:** infousa@senetas.com

GET IN TOUCH

Are you looking for a service provider to help you select and implement a network data encryption or secure file sharing and collaboration solution? Contact Senetas and we'll help you find the right one.

Senetas works with IT infrastructure service providers and systems integrators across the globe, to help specify the optimal cybersecurity solution for their customers' needs.

Customers may contact Senetas directly to discuss their requirements; or ask their service provider to speak to us on their behalf.

NETWORK DATA SECURITY WITHOUT COMPROMISE

Whatever your network security needs, Senetas has a network independent encryption solution to suit. Our multi-certified high-assurance encryptors protect data across networks operating at speeds from modest 100Mbps to ultra-fast 100Gbps and support all network topologies.

Our virtualised encryption solution, for virtual CPE and virtualised WAN, supports bandwidths of up to 15Gbps. It provides policy-based, end-to-end encryption across multi-Layer networks.

Senetas encryptors are recognised globally for delivering maximum data security and crypto-agility, without compromising network or application performance.

They are trusted to protect much of the world's most sensitive government, defence and commercial data.

SECURE COLLABORATION

SureDrop offers all the flexibility of a drop-box style solution, with the added benefit of best-in-class encryption security and 100% control over data sovereignty.

For customers seeking additional layers of content security, SureDrop is also available with the Votiro Secure File Gateway extension.

DISARM MALICIOUS CONTENT

Votiro Secure File Gateway leverages patented Content Disarm & Reconstruction (CDR) technology to protect your files from the most advanced, persistent cyber-attacks. It sanitises incoming files, eliminating the risks associated with zero-day or undisclosed attacks, whilst preserving 100% file functionality.

SENETAS