thalestct.com

THALES

MACsec FOR WAN AND HIGH-ASSURANCE ENCRYPTORS:

NETWORK SECURITY COMPARISONS

White Paper

What is MACsec?

MACsec is an encryption security standard (IEEE 802.1ae) from 2006 that was specifically developed for Local Area Network (LAN) security. MACsec is not a product nor encryption security solution itself, but a standard applied to an encryption solution's design.

Recently, the MACsec standard has been applied to networking devices to enable encryption, in addition to their networking functions. They are known as multi-purpose devices (hybrid encryption).
The MACsec standard specifies a set of protocols to meet the security requirements for protecting data traversing Ethernet LANs, hence its local network origins.

When originally developed to protect data on Local Area Networks, MACsec was intended to provide authentication and encryption of traffic between endpoints and the LAN switch.

MACsec is designed to intentionally decrypt traffic at each network hop so that switches can parse all traffic content before re-encrypting and sending securely to the next hop destination (hop-by-hop).

MACsec and WAN

Today the MACsec standard is also used to encrypt WAN communications links. On point-point links over dark fiber or pseudo-wire circuits, this is equivalent to encrypting a LAN hop.
On Carrier WANs, where there is active equipment in the core of the network, MACsec may or may not be suitable.

However, in recent years, cyber-attack vectors and the security requirements of Carrier Ethernet networks have caused network product vendors to add encryption.

Despite MACsec's LAN security origins, they adopted it for WAN encryption security. The application of the MACsec standard for WAN in network switches and routers varies from vendor to vendor.
A MACsec for WAN solution's suitability will be determined by:

- Security requirements (e.g. multi-purpose network device limitations)
- Network performance needs (e.g. latency and bandwidth overheads)
- Operational issues (e.g. unscheduled network down-time for patches)

Because MACsec for WAN is applied to vendors' networking switches and routers, they become multi-purpose devices, which has implications for both device performance and security.

Therefore, MACsec for WAN is not network, nor device, agnostic. As networks change and devices are added or changed, incompatibilities may arise.

Whatever the vendor application of MACsec for WAN, there are common performance, operational and encryption security issues in comparison to 'dedicated purpose-built' secure devices (high-assurance encryptors). In some cases, there are also security vulnerabilities.

These lead to recurring operational issues, such as unplanned network down-time for patching which is regularly published by vendors. Network performance issues include increased bandwidth overheads and higher latency.

What are 'high-assurance' encryptors?

'High-assurance' encryptors are "secure, single-purpose hardware appliances that are purpose-built and dedicated to performing network data encryption".

They feature four essential security attributes necessary to meet high-assurance requirements, otherwise known as security credentials. These are:

- A tamper proof/resistant, and evident, single-purpose hardware enclosure
- Provide 'end-to-end' authenticated encryption
- Use state-of-the-art 'client-side' embedded, automatic zero-touch encryption key management
- Use and adhere to standards-based encryption algorithms e.g. AES 256 and NIST curves

The term 'high-assurance' was given to differentiate these purpose-built dedicated appliance solutions from 'lower-assurance' solutions, such as:

- Multi-purpose and hybrid device solutions, e.g. routers/switches using MACsec encryption
- Software and virtualized network data encryption

The benefits of high-assurance

Because the primary purpose of network data encryption is long-term data security in the event of a breach, the term 'high-assurance' reflects the relative security differences among security solutions:

- The encryption host device's own security - encryption should always take place in a secure device, in a secure environment
- The encryption solution's overall security strength - encryption keys should be secure during their entire lifecycle and the algorithms used should be standards-based

Similarly, because high-assurance encryption solutions are single-purpose, they typically offer added benefits, such as:

- Low to near-zero performance impact on the data network – latency and data overheads
- No impact on network operations through unscheduled network shut-downs due to unplanned software (security) patching, such as those experienced by the use of multi-purpose network devices

Security as a key differentiator

Specifically, the key security differentiator is that single-purpose hardware appliance encryption platforms are purpose-built and developed by specialist data security and encryption organizations.

Their solutions have resulted from investment in extensive Research and Development (R&D), lengthy government standards-based certifications and independent penetration testing to provide network encryptors with the following characteristics:

- Solutions specifically developed for use on Carrier WANs
- A single-purpose secure appliance ensuring 100% separation of duties – exclusively encryption security
- Use of end-to-end encryption and state-of-the-art key management
- Field Programmable Gate Array (FPGA) based hardware – for maximum performance, in-field upgradability, enhancement flexibility, and solution future-proofing
- Agnostic to network equipment and Carrier infrastructure
- Support for all topologies including very large meshed networks

LAN and WAN security differences

The core difference between a MACsec encryption standard based network security solution and a high-assurance single-purpose solution lies in their origins.

MACsec was developed for LAN security, whereas high-assurance single-purpose solutions are specifically developed for WAN.

A Local Area Network (LAN) is local, under physical control of the customer, and doesn't share its infrastructure with other parties. This is the environment that MACsec was designed for.

MACsec uses 'hop-by-hop' encryption, leverages existing LAN infrastructure and uses encryption embedded in the network chip.

MACsec for WAN is the application of the MACsec encryption standard to network switch/router devices across networks. It is network and device specific.

Single-purpose 'high-assurance' hardware devices (encryptors) provide end-to-end network encryption. They are network and device agnostic.

While both are legitimate solutions, differences lie in their degrees of security and performance, and their operational impact.

The WAN threat landscape

Once customers use Ethernet outside their LAN, the threat environment changes. The outside network uses somebody else's infrastructure, which is shared by multiple parties.

Even if customers own the external infrastructure, security requirements increase as the level of control is eroded and others may have physical or logical access to the network.

One example of this is the ability to transmit MACsec Key Agreement frames across a Carrier network.

On Carrier Ethernet networks, a specific set of MAC addresses is used for processing control plane traffic to manage the Ethernet service. Customer frames using these MAC addresses can be "consumed" by Carrier equipment.

For that reason, any encryption solution should not use these well-known management addresses.

Is MACsec right for WAN?

MACsec uses extensible authentication protocol over LAN (EAPOL) for MACsec Key Agreement (MKA). As it happens, EAPOL's default address is one of those known addresses that is consumed causing the MKA session establishment to fail.

For 'hop-by-hop' Ethernet on a LAN, only the MAC addresses need to be visible for forwarding. By contrast, all virtual private variants of Carrier Ethernet are based on VLAN-IDs (802.1Q).

These VLAN-IDs need to be in the clear for Carrier Ethernet services to function correctly. Quality of Service (QoS) delivery also requires that the priority marking (802.1P) in the frame is readable and in the clear.

However, the MACsec standard specifies that the entire Ethernet frame after the MAC address should be encrypted. This renders both 802-1Q and 802-1P fields invisible in the Carrier network.
For these reasons, and more, many MACsec standard implementations are unsuitable for use in commercial Carrier networks a different approach to network encryption security and functionality is required.

An extension to the standard, known as MACsec EDE, addresses some of these issues, however it does not address all the functionality and security limitations and so it has not been adopted widely.

WAN security considerations

The following lists important WAN encryption security considerations and includes the views stated in independent cyber security experts' published papers.

These security considerations are not listed in any priority order and would differ according to specific customer situations.

Customers will balance their security, performance and operational requirements, applying varying levels of importance to each consideration.

However, it is important for customers to have a clear view of the trade-offs among security and other WAN considerations.

Security, solution longevity and a predictable Total Cost of Ownership (TCO) are key objectives when designing a WAN. The following factors should be taken into consideration:

- All traffic between sites should be encrypted (data and control/management planes)
- The threat scenario is the same for all traffic among the sites, thus all traffic must be secured at the same layer
- Encryption should take place in a secure device, in a secure environment
- True random number generation with high entropy should be used
- Encryption keys must be secure during their entire lifecycle
- Key management should be versatile and optimized for the task
- Support should be provided for all Ethernet topologies: point-to-point, point-to-multipoint, hub-and-spoke and multipoint-to-multipoint, fully meshed
- Users should have a choice of cryptographic primitives
- The solution should be crypto-agile – e.g. Through the use of FPGA-based, field-upgradeable processors rather than non-upgradeable ASICs
- The solution should be scalable, to provide security across the network
- Look for certification by independent security evaluations and audits: CC EAL 4+ or equivalent. FIPS 140-2 Level 3 or equivalent
- The solution should be network and network type agnostic – avoiding future incompatibilities
- Look at the latency and data overhead impacts on network performance, which may hide additional bandwidth costs
- Consider how the solution may involve higher unscheduled network down-time due to software and security patch updates
- Does the solution provide investment 'future- proofing' in the event of technology and threat vector changes?

Security, performance and cost

The encryption technology deployed within any network data security solution is just part of the overall security foundation.

What matters most to the overall strength of the solutions are:

- What is being encrypted?
- How is it being encrypted?
- Where is the encryption taking place?

At the outset, answers to these questions will determine if the security solution is fit for purpose.

It is true to say that a security solution must implement standards-based encryption primitives to provide confidentially and integrity protection of all network transmitted data, using authenticated encryption algorithms.

MACsec for WAN may not be the right/optimal choice when a customer is seeking an encryption solution that ensures:

- Security
- Stability
- Predictability
- Control

There are three primary reasons why:

Encrypt all traffic (not just the data)
Because all network traffic is subject to the same threats, be it at the data plane or the control plane, customers should ensure all traffic is protected with the same (equally strong) level of encryption security.

In many MACsec for WAN solutions, only the data plane is encrypted at Layer 2. Some of the control plane traffic is encrypted at Layer 4 (i.e. authentication, authorization and key agreement). The remainder of the control plane traffic remains unencrypted.

Only encrypt in a secure device
The optimal network encryption security solution is built within a secure tamper/proof and evident device – providing adequate physical protection against tampering and probing attacks.

The FIPS 140-2 Level 3 certification standard is the minimum benchmark for such protection in security devices.

FIPS certification also provides assurance that the encryption keys are being generated with sufficient security from an approved Random Bit Generator.

Optimism key management for 'end-to-end' encryption
Encryption key management should be optimized for all use cases and network topologies, versatile, and support unidirectional point-to-point keys and bi-directional group keys.

Key management should be optimized for end-to-end encryption (rather than hop-by-hop) and should generate both session and encryption keys from scratch; using a reliable source of entropy, such as a true random number generator.

WAN based MACsec solutions based on a 'hop-by-hop' design do not offer sophisticated group keying systems and derive their encryption and session keys from the same source.

MKA, the MACsec Key Agreement, is built on IEEE 801.11x, an authentication, authorization and access (AAA) solution for campus networks.

There are also two important operational issues, with significant operational implications, customers should consider:

Compatibility and interoperability
MACsec for WAN solutions (e.g. network equipment vendor solutions) are not widely "vendor agnostic" – i.e. are not 100% compatible with all network technologies/types, nor devices.

Some Carrier networks are unable to deliver end-to-end MACsec traffic due to Ethernet header and key agreement standard issues.

This issue has significant implications for overall life-cycle TCO. Typically, it does not arise with purpose-built high-assurance solutions.

Operational disruption
Multi-purpose MACsec based encryption solutions, where there is no separation of networking and security duties, are exposed to unscheduled network maintenance and shut-downs.

These arise when security patches to networking equipment (switches and routers) are released for unplanned implementation. Such events are common and cause operational disruption.

Unplanned patch implementation also adds to the solution's life-cycle TCO. If such patches are not implemented promptly there are increased risks that the security solution and/or networking devices are compromised.

Summary

A number of network equipment vendors use the MACsec encryption standard as the basis of their WAN data encryption solutions.

Rather than invest in developing a purpose-built and vendor agnostic encryption solution, they have adopted MACsec for their hybrid WAN security solution.

This approach provides a low-cost solution at a cost of security strength, network performance and operational issues. Where MACsec EDE is applied to a single-purpose hardware device, little or no cost advantage arises.

Whether the MACsec for WAN implementation is the more effective hardware (EDE) based type or the more common less effective multi-purpose (switch/router based) hybrid type, they share similar security limitations.

Since the MACsec standard was not designed, nor intended for WAN security, some Carrier networks are unable to deliver end-end MACsec traffic for two reasons:

- The MACsec standard encrypts Ethernet header fields such as MPLS labels, 802.1P and 802.1Q fields from the original Ethernet frame. As a result, any intermediary network device that requires those tags is not able to see them as the Ethernet frame crosses the underlying network between encrypted stations
- The MACsec Key Agreement standard uses an Ethernet packet type that is defined as a "well known" management packet. Many Carrier switches will not pass such frames end-end, thus preventing MACsec being used on such networks. (Some implementations provide proprietary extensions to work around these issues)

Due to their 'purpose-built, secure dedicated encryption appliance' attributes, high-assurance encryptors provide enhanced security capabilities and features without compromising network performance and network operations.

It should be noted that MACsec for WAN (multi-purpose or EDE dedicated appliances) may provide a legitimate encryption security solution under some circumstances.

This paper seeks to highlight the differences between purpose-built high-assurance encryptors and MACsec for WAN solutions; helping customers make informed decisions about what solution type best meets their specific security, performance and operational requirements. The section overleaf provides a security feature comparative table.

Security features comparison table

The following table compares MACsec for WAN and 'purpose-built secure, dedicated hardware appliance' (high-assurance encryptors) security features.

It is not intended to be a definitive selection guide, but a tool highlighting WAN encryption security functionality differences. Customers will differ in the importance they give to the features listed.

Security features	MACsec for WAN	Purpose-built, secure dedicated cryptographic appliance
Dedicated security function – separation of duties	No	Yes
Standards based encryption algorithms	Yes	Yes
Independent cryptographic certifications	Some	"Commonly more; and higher levels of certifications including: • FIPS 140-2 level 3 • Common Criteria • DODIN APL • NATO etc"
Uses tamper resistant/ proof enclosure	Not in router or switch	Yes
Has anti-probing hardware protection	Not in router or switch	Yes
Field-upgradeable firmware	No (ASIC based designs)	Yes (FPGA based design)
Hardware RNGs for secure key encryption generation	Some	Yes
Multiple encryption solution types (e.g. hardware and virtualized) and 100% interoperability	No	Yes – among those offering multiple solution types
Advanced features to protect against Traffic Flow Analysis	No	Yes
Dedicated GUI Management tools	No	Yes
Separation of duties through dedicated appliance	Not in router or switch	Yes
Fully flexible Ethernet network policies	No - limited	Yes – support for all topologies
Consistent latency for all traffic types	No (typically store-forward packet processing)	Yes (typically cut-through packet processing)
Self-healing' key management	No	Yes
Quantum-ready - support for quantum- safe cryptography	No	Some
Separation of duties (network vs security functions)	No	Yes
Suitable to meet NIST Cryptographic algorithm transitions (SP800-131A)	Some: • Requires crypto-agility that may be prevented by ASIC architectures • Encryption is just one small component in a switch or router solution	Most: • FPGA engines typically allow algorithms to be updated in the field • Dedicated security appliances prioritize encryption enhancements

References and notes

This discussion paper was authored by Senetas and is based on publicly available WAN security and MACsec for WAN information. Senetas' solutions are available for sale to the U.S. Federal Government exclusively through Thales Trusted Cyber Technologies.

The paper summarizes the primary information published by independent (non-vendor) technical experts. It recognizes how customers' requirements – security, performance and operational - differ.

Customers' choices are determined by the mix of, and relative importance of their security, performance and operational requirements and how they are met by specific vendors' solutions.

The following links are to source of independent expert papers, webinars and podcasts about data network security, encryption solution types and high-assurance Carrier Ethernet encryption security solutions.

- Carrier Ethernet Network Security papers: www.uebermeister.com/homepage.html
- Ethernet Encryption Webinar: www.ipspace.net/Ethernet_Encryption
- Transport and Network Security Primer: www.ipspace.net/Transport_and_Network_Security_Primer
- Independent network encryption security author, Christoph Jaggi: www.ipspace.net/Author:Christoph_Jaggi

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

About Senetas Corporation

Senetas is a leading developer of end-to-end encryption security solutions; trusted to protect enterprise, government, defense, Cloud and service provider network data in over 35 countries.

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