TRAFFIC FLOW SECURITY USING SENETAS HIGH-ASSURANCE ENCRYPTORS

TECHNICAL PAPER

SENETAS

Security without compromise

Traffic Flow Security (TFS) is the technology that provides protection against damaging data network "traffic analysis". This paper discusses the significance of high-speed communications network traffic analysis, the risks it imposes and how Senetas has incorporated TFS in selected encryptors.

NETWORK TRAFFIC ANALYSIS

Traffic analysis is the process of intercepting and examining data about communications network data flows (traffic) in order to deduce information from patterns in the network communications. Simply put, the data being analysed is not the information itself, but "data about the data being transmitted".

It is apparent that surveillance of private and public communications networks is occurring on an unprecedented scale around the world. Even high-speed fibre optic communications links (once thought to be "tamper-proof") are vulnerable to eavesdropping using readily available, low cost tools.

The risks from eavesdropping and surveillance of high-speed communications networks are not limited to information theft, privacy, tampering or other cyber-crimes. While the information itself may be encrypted and protected from such security risks, networks and the data they transmit must also be protected from potentially damaging "traffic analysis".

Even when network data is securely encrypted, network traffic analysis risks remain. Although traffic analysis does not reveal the data content, it does expose users' networks to risks of 'inferring' activities, which expose users to other potentially serious threats.

Traffic analysis has broader risk implications in commercial applications. Due to increasing volumes of meta data traffic analysis will identify a range of network and user behaviours. This paper explains how Senetas has incorporated TFS within its encryptor firmware to prevent and defeat traffic analysis risks.

While defence, military and other government applications lead to the development of TFS, commercial organisations are increasingly experiencing the threats of traffic analysis.

Examples of traffic analysis threats include: equities; trading manipulation, business financial transaction activities and identity interpretation.

For these reasons, Senetas has introduced TFS as an additional feature of highspeed encryptors.

BACKGROUND

Media reports of information breaches – eavesdropping, tampering and other breaches of highspeed communications networks – have increased in their frequency and severity. Commercial, government and not-for-profit organisations globally are alarmed by the threats caused to economies, government secrets, commercial intellectual property and citizen privacy.

By focusing on protecting the data itself, encryption provides assurance that the information will be meaningless to unauthorised parties in the event of a successful network breach. However, commercial and government organisations are not only concerned about protecting the information itself; they are also concerned that the alleged cyber-criminals include trusted organisations, such as governments and government agencies.

Increasingly prevelant communication network breaches have highlighted the importance of protecting the data itself; understanding that even the best "perimeter" protection technologies (used to protect the communications networks) may eventually be breached. By protecting the information itself, even a successful breach will not result in a data loss.

Encryption of sensitive information is the optimal solution because it ensures both the privacy and integrity of data as it travels across high speed networks to its intended destination. It also provides the assurance that should the network perimeter protection fail, the information itself is protected by encryption.

Encryption provides this assurance of information protection by "scrambling" the contents of each packet of data being transmitted from one location to another. Risks to transmitted data are not confined to 'theft' and eavesdropping. Risk of the input of 'rogue' data and the re-direction of data are also serious. Encryption ensures that the information itself cannot be read or tampered with by unauthorised parties.

The issue of the need to protect the information while being transmitted is addressed by encryption. However, an important issue remains – the risks of unauthorised analysis of the network's data flows (traffic). This data provides information such as the patterns of network traffic and behaviour. Traffic flow data is not the information traffic itself and therefore is not scrambled nor hidden from unauthorised eyes.

TRAFFIC ANALYSIS RISKS

Many will wonder what cyber-criminals could hope to gain from network traffic analysis. How will that information be used as a security threat? The answer is simple; unauthorised monitoring and analysis of network traffic enables cyber-criminals to gain valuable knowledge such as whether the network is busy or quiet; the delay between transmitted packets and the mix of big and small packets being transmitted.

The traffic patterns may seem inconsequential but they are potentially valuable to cyber-criminals as they may be used to both infer and deduce information about the nature of the communications transmitted that is otherwise purposefully hidden.

- **Defence application** – the volume of network traffic entering or leaving a military command centre is likely to be correlated with the state of alertness of that facility and could, in certain circumstances, provide evidence of likely future military activity.
- **General application** – Network traffic volumes and transmission patterns (such as regularly busy periods) may help guide attempts to eavesdrop and capture large quantities of uncrypted data. At certain times, the traffic flow may give an indication as to the type of data being transmitted.
- **Commercial application** – the use of silence suppression in VoIP calls is commonly used to reduce bandwidth but has the side - effect of revealing the length of talk spurts during a conversation. These spurts may be analysed using modern statistical and data mining techniques and used to identify the person talking, even if the VoIP traffic is encrypted.

Exploiting patterns in data traffic flows to deduce information is a technique widely used in military intelligence. However, in the commercial sector, traffic analysis is an increasing concern for computer and network security due to the high volumes of metadata now available.

Defeating, or preventing traffic analysis requires the ability to hide the data patterns by generating a constant traffic flow that is independent of the real data being transmitted. The objective is to obfuscate the timing behaviour of the native traffic by inserting additional information so that the traffic observer sees only a constant stream of invariant data.

A simple analogy is to consider a train spotter watching an infinitely long train of identical railway boxcars.

Some of the boxcars will contain valuable freight; others will be empty, but the observer has no way of telling them apart because they all look the same.

The technology used to defeat traffic analysis is Traffic Flow Security.

TFS AND NETWORK PROTOCOL TRAFFIC SECURITY

Some less commonly used communications network protocols provide TFS natively because of their synchronous framing structure. But more commonly used protocols today do not.

For example, Synchronous Optical Networks (SONET) use a fixed size frame which is sent every 125 micro seconds. As a result, it is impossible for an observer to detect traffic patterns when eavesdropping on an encrypted SONET network because the fibre optic cable is always 100% utilised.

Contrastingly, other widely used protocols, such as Ethernet, do not provide native TFS protection. Ethernet is an asynchronous protocol that sends data in variable sized frames.

Therefore, an eavesdropper monitoring an Ethernet network will see irregular traffic flows of variable frame lengths and frequency. Variations in the network utilisation, average frame size, inter-frame timing and header addresses will all be visible and may be exploited using statistical techniques such as Bayesian analysis or hidden Markov models.

SENETAS TFS IMPLEMENTATION

For the first time, Senetas is introducing TFS technology within its commercial Etherent encryptors, operating at rates from 10Mps to 10Gbps.

TFS will be available on all Senetas CN4000 and CN6000 series encryptors, with customers free to choose to activate TFS or not. It will provide native transmission security on point-to-point Eithernet networks.*

The Senetas high-assurance encryptors provide wire speed encryption of all data on Ethernet Layer 2 communications links. Information is encrypted in hardware using the AES-256 algorithm. They provide 'carrier-grade' protection of data transmitted without the additional costs of compromising network performance that typically comes with other encryption solutions.

TFS is an additional mode of operation now made available for the first time among the Senetas CN series encryptors. It provides native transmission security on point-to-point Ethernet networks.

A TFS feature-enabled Senetas encryptor generates and transmits fixed size encrypted Ethernet frames at a constant frame rate from the WAN-facing network port. The TFS enabled encryptor encrypts the entire contents of all Ethernet frames that are received on the local port and ensures that no MAC addresses, other header information or payload data is exposed.

The generated frame is called a transport frame, which consists of one or more client frames received from the LAN interface and any padding necessary to ensure the frame is completely filled. The transport frame is encrypted and transmitted at a constant frequency even in the absence of client frames as shown in Figure 1.

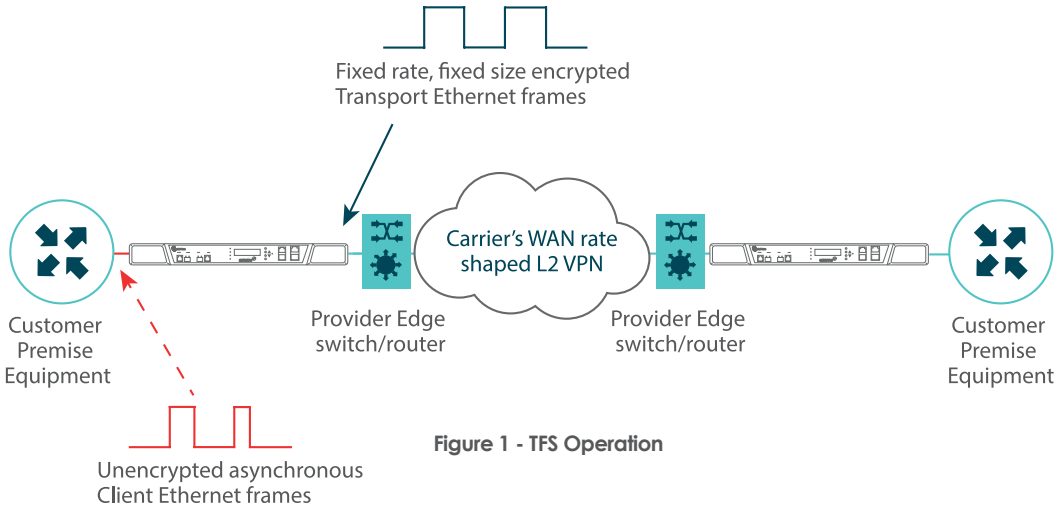


Figure 1 - TFS Operation

TFS mode may be enabled between a pair of Senetas Ethernet encryptors that are connected across both dark fibre connections or across a carrier/service provider Layer 2 VPN, such as VPLS, or an MEF service such as E-LAN

The Layer 2 data network connection must have the following characteristics:

> The WAN service is a Layer 2 VPN that may be rate shaped

> The VPN service preserves the transmission order of frames across the WAN, such that network frames are not reordered between encryptors

Note: TFS is not currently supported in point-to-multipoint or multipoint-to-multipoint topologies.

TRANSPORT TO CLIENT FRAME MAPPING

Unencrypted client frames received on the local interface are encapsulated in one or more transport frames as shown in Figure 2. When client frames are not available the transport frames are padded with random data.

In the example shown:

> Transport frame N+1 carries the configurable frame header, client frame 1 and some padding

> Transport frame N+2 carries the configurable frame header, client frame 2 and part of client frame 3

> Transport frame N+3 carries the configurable frame header, the remainder of client frame 3 and some padding

> Transport frame N+4 carries the configurable frame header and padding (no client frame available)

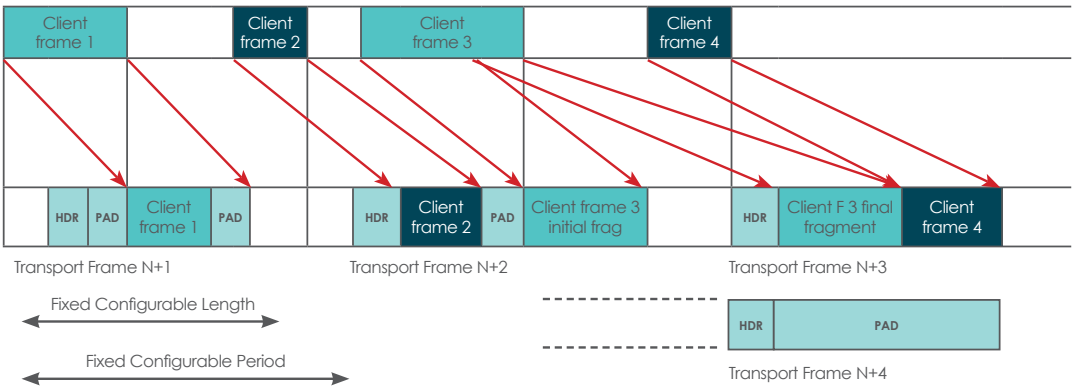


Figure 2 - Transport Frame Assembly

Figure 3 shows how a client frame is reassembled from received transport frames. All transport frames containing fragments of a client frame must completely arrive before the decrypting encryptor will start to send the client frame to the remote LAN.

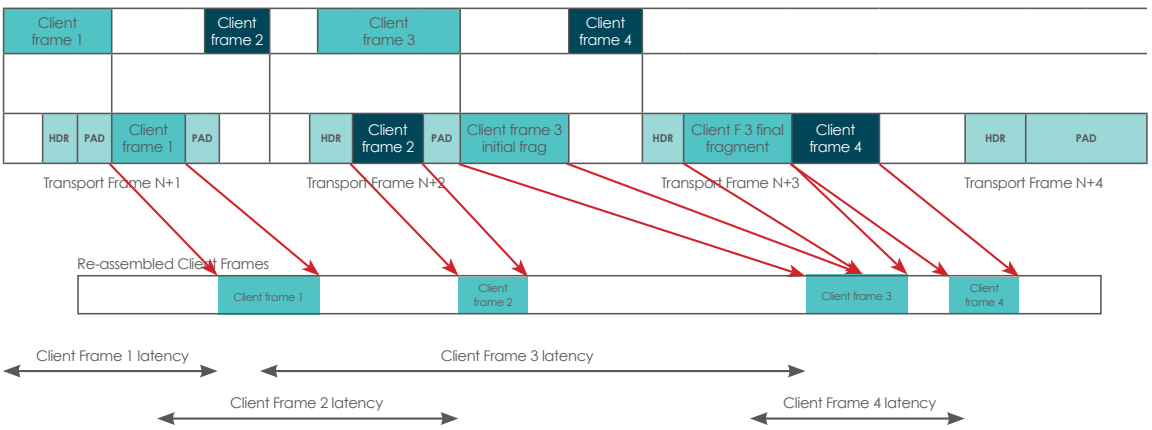


Figure 3 - Reassembly of Client Frames

TRANSPORT FRAME FORMAT

The transport frame format is shown in Figure 4 and consists of a fixed header, a shim for synchronisation and the encrypted payload.

The transport frame header is between 12 and 82 bytes long and is user configurable. In the simplest case, this header comprises only destination and source MAC addresses. The encryptor allows for more complex headers that may include VLAN tags and multiple MPLS labels if required for transport across the VPN connection.

The transport frame header is identical for all transport frames and is treated as a simple fixed sequence of bytes that are manually configured from the management GUI and simply added to each frame upon transmission.

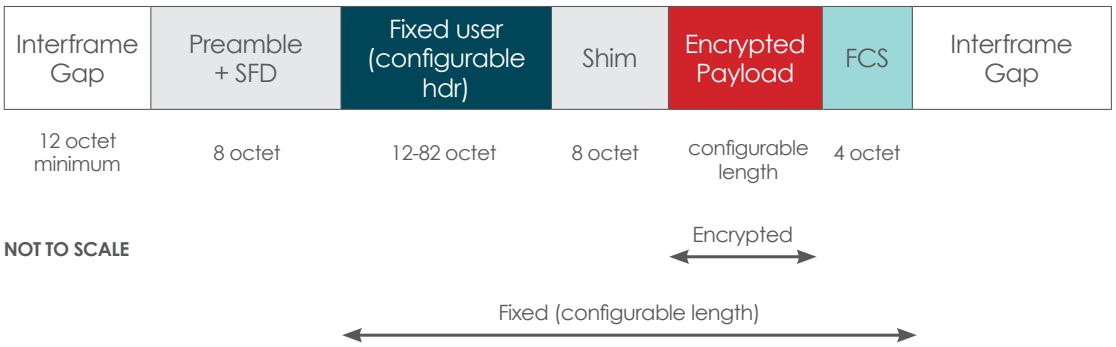


Figure 4 - Transport Frame Format

SENETAS TFS POLICY CONTROLS

Senetas's TFS management GUI provides considerable flexibility to control the size and rate of the transmitted transport frames. The transport frame length is fully configurable as is the transmission rate measured in frames per second or as a percentage of the available bandwidth*.
(*Note: The configured bandwidth should be set to a value less than 100% to allow in-band management and key update traffic to be sent between encryptors.)

Figure 5 shows the management interface for configuring the TFS options.

The Senetas management interface allows full configuration of the transport frame header, which may be between 12 bytes (just source and destination MAC addresses) to 82 bytes (more complex e.g. VLAN, MPLS, IP headers etc.).

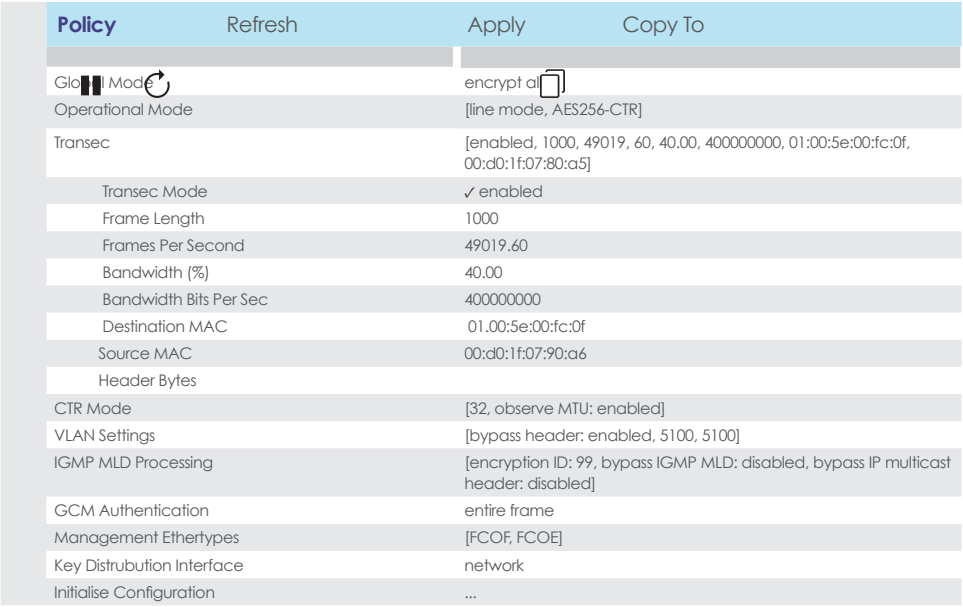


Figure 5 - Transport Frame Format

By default, all client frames received by the encryptor are either encrypted or discarded and no traffic is bypassed. However, practical experience on many service provider networks has shown that it is occasionally necessary for customer premises equipment (e.g. a router or switch) to be able to communicate with the provider's edge router or switch in order for end-to-end communications to work. This is typically required when service providers use Ethernet OAM (Operations Administration & Management) to administer, manager and maintain network connectivity for purposes such as fault management, performance monitoring and link layer discovery.

To allow for this communication the TFS featured encryptor retains the capability to optionally bypass certain well-known protocols used for operations and maintenance (i.e. control plane) purposes as shown in Figure 6.

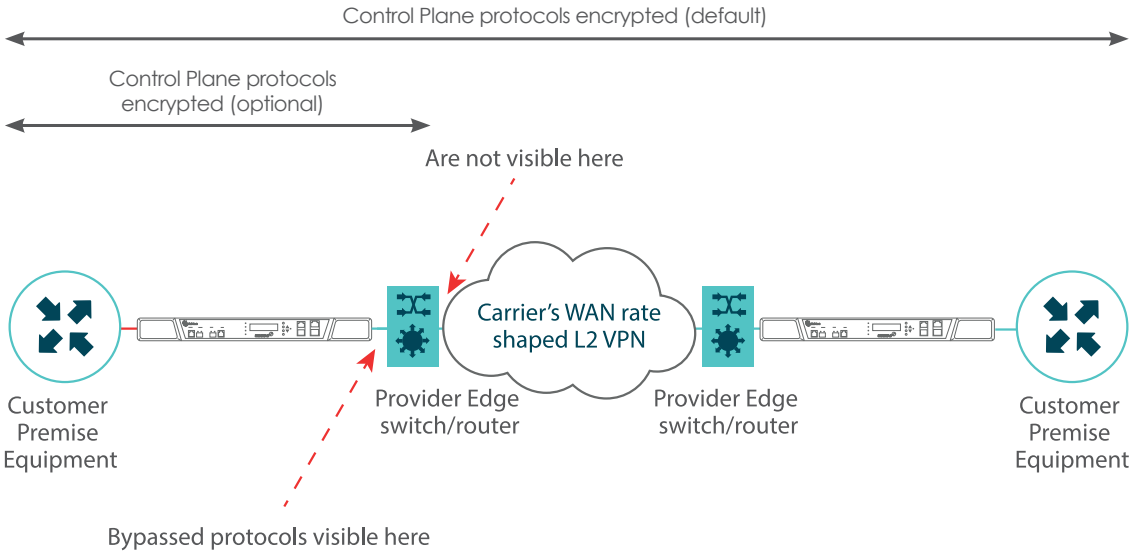


Figure 6 - Control Plane Traffic

Most control plane protocols are identified by a reserved MAC address and may include the following:

Multicast MAC address	Protocol
01:80:C2:00:00:0*	Link Constrained Protocol (LCP)
01:80:C2:00:00:00	Spanning Tree Protocol (STP)
01:80:C2:00:00:01	MAC Pause Frame
01:80:C2:00:00:02	Link Aggregation Control Protocol (LACP)
01:80:C2:00:00:03	Port Access Protocol
01:80:C2:00:00:0e	IEEE Link Layer Discovery Protocol (LLDP)
01:00:5e:00:00:**	Routing Protocol (e.g. OSPF)
01:00:0c:cc:cc:cc	Cisco VTP/DTP/CDP
01:00:0c:cd:cd:d0	Cisco L2TP
01:00:0c:dd:dd:dd	Cisco CGMP
01:00:0c:cc:cc:cd	Cisco SSTP

Table 1 - Typical Control Plane Frames

Encryption policy allows for each control plane protocol to be independently configured so that it may be bypassed through the encryptor without modification. The bypass ability is disabled by default to ensure that no traffic is bypassed unless explicitly enabled.

TFS PERFORMANCE CONSIDERATIONS

The transport frame length and transmission rate are both configurable and will affect the efficiency and latency of the encrypted connection.

Short transport frames are less efficient than long transport frames because the ratio of header to client data is higher. However, short transport frames have lower latency because, on average, less data needs to be buffered before reassembly.

Figure 7 shows an example of the available client bandwidth as a function of client frame size for three different configured transport frame lengths. The graph shows that efficiencies above 90% are easily achieved by choosing the appropriate transport frame length.

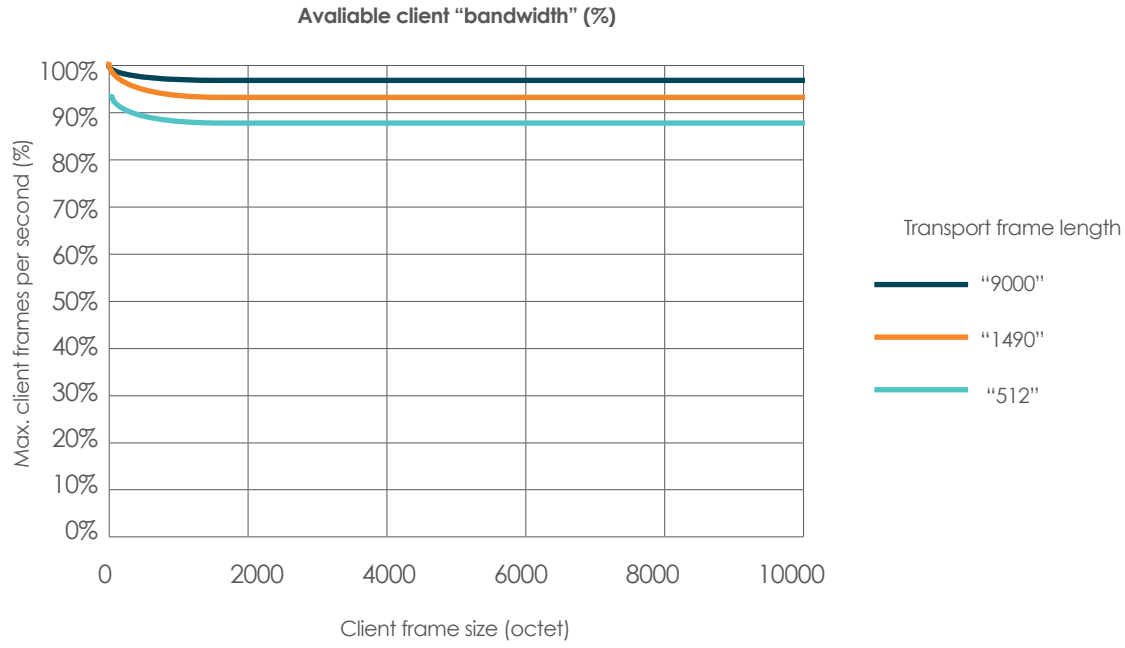
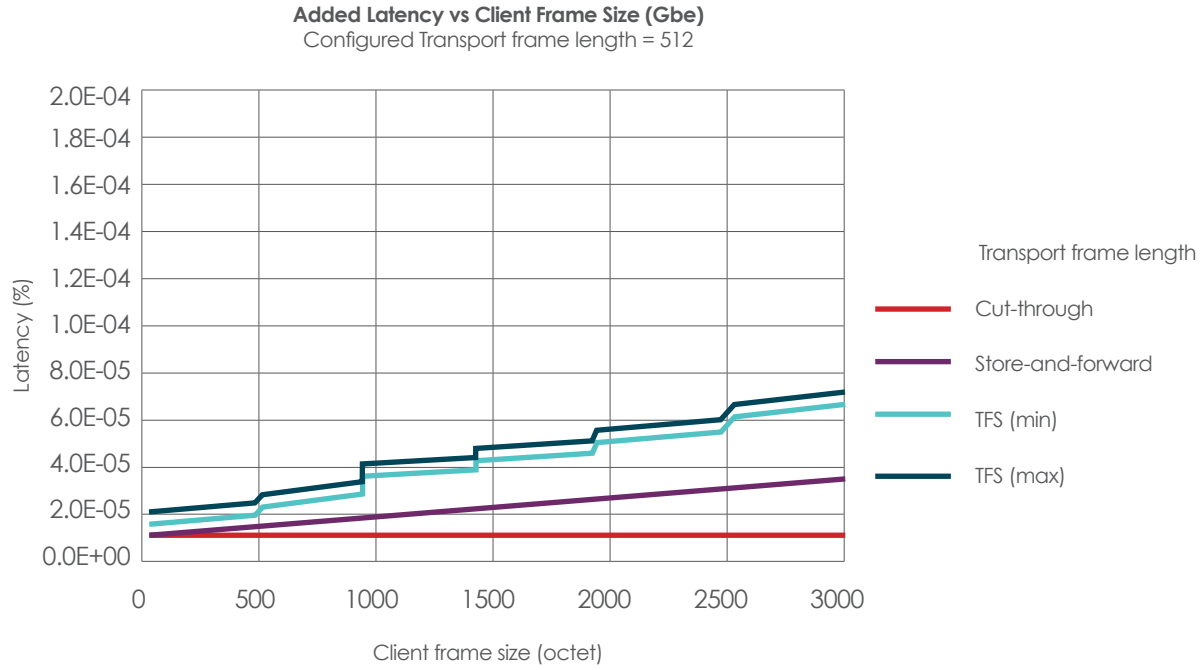


Figure 7 - Transport Efficiency



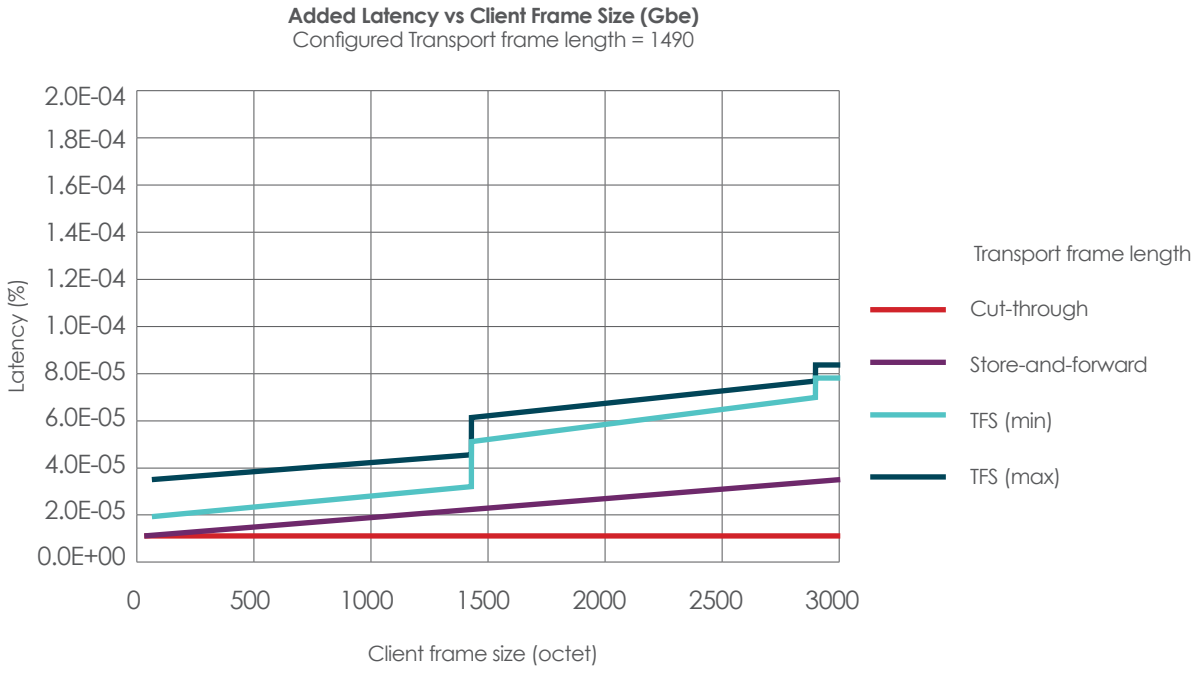


Figure 8 – shows examples of the variation in end-to-end latency across different client frame lengths dependent upon the configured transport frame length.

SUMMARY

While sensitive data being transmitted across high-speed communications networks should be protected against eavesdropping, theft, redirection and input of rogue data through high-assurance encryption; the traffic behaviour information itself may also need to be protected from unauthorised analysis and behaviour monitoring, which may give rise to other security risks.

Traffic behaviour monitoring and analysis expose organisations to both specific and general risks. The broader risks of increasing volumes of metadata involve analysis of user and organisational behaviour.

The more specific risks of Traffic Analysis involve activity behaviour that may expose the organisation and/or its users to a number of threats.

Protecting network traffic from Traffic Analysis involves TFS "masking" the data to eliminate any changes in behaviour and traffic patterns, thus rendering Traffic Analysis meaningless.

High-speed transmitted data across Ethernet communications networks may now be protected from the risk of Traffic Analysis. Senetas encryptors' inclusion of TFS mode security technology makes that possible for the first time.

TFS provides a defence against Traffic Analysis by disguising patterns in the network data flows and may be enabled on point-to-point links across a dark fibre or service providers' Virtual Private Network(VPNs).

GLOBAL SUPPORT AND DISTRIBUTION

Senetas CN series encryptors are supported and distributed globally by Gemalto under its SafeNet encryption brand.

Gemalto also provides pre-sales technical support to hundreds of accredited partners around the world; including systems integrators, networks providers, cloud and data centre service providers, telecommunications companies and network security specialists.

For more information click here.

TALK TO SENETAS OR OUR PARTNERS

Senetas and Gemalto also work with customers' existing data network service providers, systems integrators and information security specialists to specify the optimal high-assurance encryption solution for their needs.

Wherever you are, simply contact Gemalto or Senetas to discuss your needs. Or, if you prefer, your service provider may contact Gemalto or Senetas on your behalf.

HIGH-ASSURANCE NETWORK ENCRYPTION

Whatever your Layer 2 Ethernet network security needs, Senetas has a high-assurance solution to suit. They support modest 10Mbps to high-speed 10Gbps links and multi-port 10x10Gbps links.

Scalable, agile and easy to use; Senetas high-assurance encryptors provide maximum security without compromising network performance.

SENETAS CORPORATION LIMITED

E info@senetas.com
www.senetas.com

Senetas manufactures high-assurance Layer 2 Metro Area and Carrier Ethernet network encryptors. They support all Layer 2 protocols and topologies.

Our multi-certified encryptors are used by some of the world's most secure organisations, including governments and defence forces; commercial and industrial enterprises; Cloud, data centre and telecommunications service providers in more than 30 countries.

TFSDOC-TP-0816