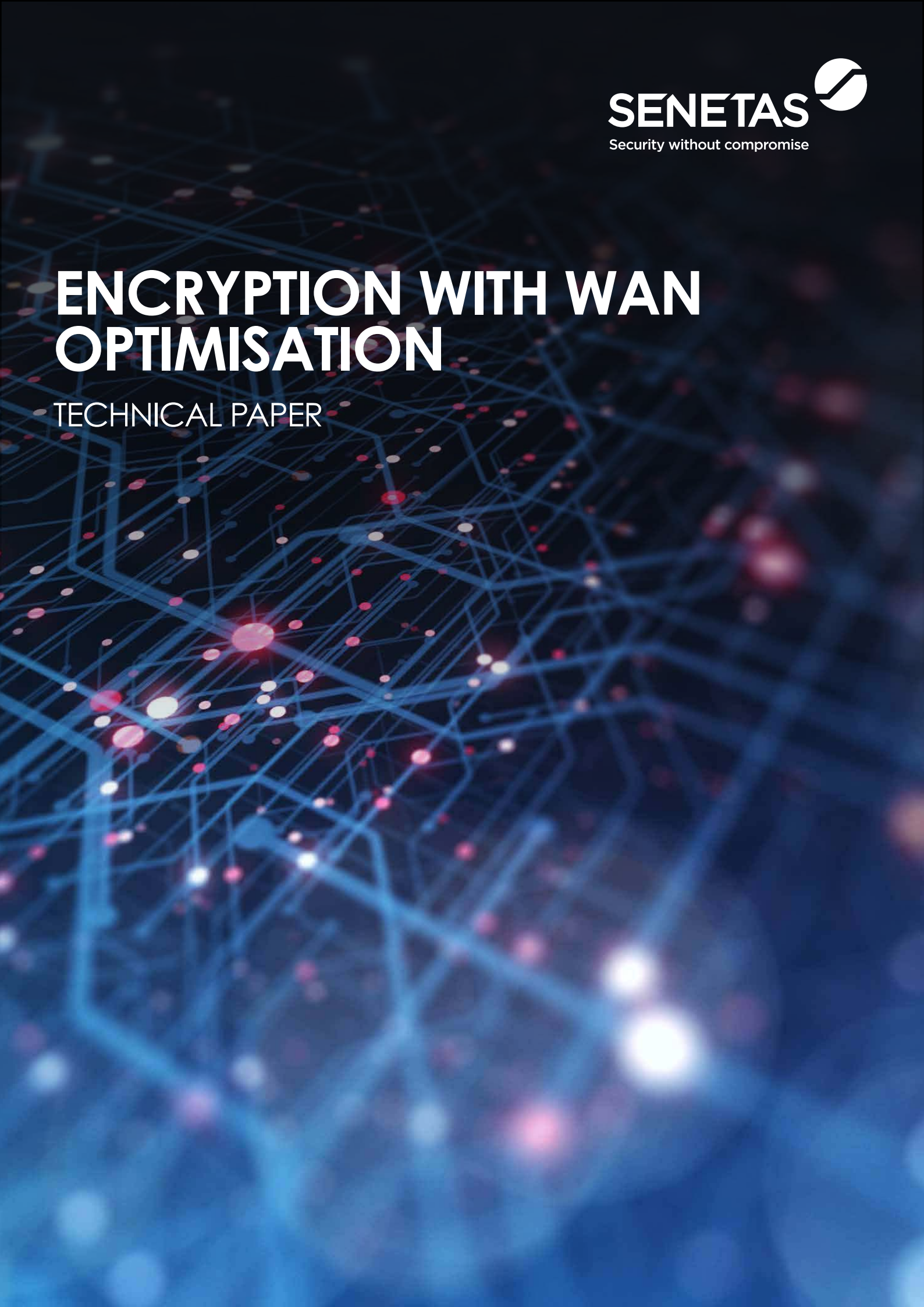
SENETAS

Security without compromise

ENCRYPTION WITH WAN OPTIMISATION

TECHNICAL PAPER



ENCRYPTION WITH WAN OPTIMISATION

WAN optimisation is a widely used technology that improves the efficiency of network data transmission.

Senetas Ethernet encryptors secure traffic at wire speeds across wide area Ethernet services to provide protection of the data transmitted.

This paper discusses the scenario where both encryption and optimisation are used across a Wide Area Network (WAN) and the design considerations required.

WAN optimisation overview

WAN optimisation (also called acceleration) is the term for a collection of policies and technologies that can increase the efficiency of data transmission across network infrastructure by reducing bandwidth requirements and improving transaction response times.

The benefits of WAN optimisation include cost savings, due to lower bandwidth needs and traffic; and improved network performance due to reduced latency (delay).

WAN optimisation includes a series of techniques that modify and/or optimise the way that software applications, protocols and data flows behave and includes mechanisms such as:

- Data compression – reduces the volume of information that needs to be sent across the network
- Deduplication – eliminates the transfer of redundant data across the WAN
- Protocol optimisation – improves the efficiency of network protocols using techniques such as window-size scaling and local acknowledgements
- Application streamlining – reduces 'chattiness' and round trip interactions in software applications or protocols such as CIFS, NFS and Microsoft Exchange
- Traffic shaping – controls the data flow on a per user or per application basis

WAN optimisation technologies may be implemented in either a dedicated hardware appliance or as client software.

WAN optimisation and network data security

WAN optimisation changes the headers and payloads of network traffic to provide more efficient information exchange across a network. Whilst common optimisation techniques such as compression and tokenisation do provide some level of data hiding or obscurity as a side effect, true protection/confidentiality of transmitted data still requires strong encryption techniques.

Some WAN optimising appliances do provide point-point encryption across a WAN. This is typically implemented using IPSec tunnels at Layer 3. Encrypting at Layer 3, whilst secure, secure adds significant overheads to transmitted data due to the size of the IPSec tunnel header, and this increases the WAN bandwidth requirements.

Increasing bandwidth due to Layer 3 encryption reduces much of the efficiency achieved from gains through traffic optimisation. Additionally, IPSec has a variable performance that can depend on the characteristics of the network traffic (eg packet size and traffic type) which is therefore not consistent across all traffic classes.

When possible, the optimal approach is to use very low overhead encryption technologies, such as Layer 2 hardware encryption.

Senetas CN series encryption devices are purpose built appliances that perform traffic encryption in dedicated silicon using a cut-through architecture. This allows for constant, very low latencies that are independent of packet size and provides predictable "jitter" free data transmission.

Using this approach, it is possible to provide overhead free encryption of the optimised traffic and achieve the maximum possible throughput and best response times across the WAN, whilst ensuring complete privacy of the transmitted information.

WHY IS CERTIFICATION IMPORTANT?

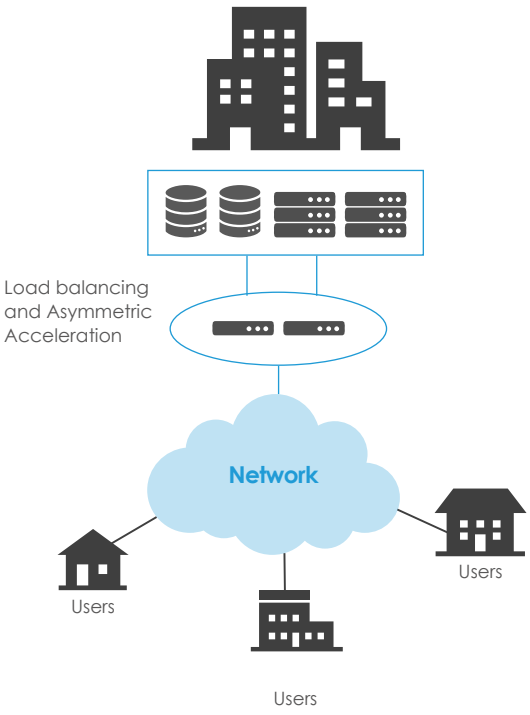


FIGURE 1 – ASYMMETRIC OPTIMISATION

WAN optimisation and encryption interoperability

WAN optimisation techniques rely on visibility of the protocols and data inside each packet. For this reason, once encrypted, network traffic cannot be accelerated.

Careful thought therefore needs to be given to the coexistence of encryption and optimisation appliances in any network environment.

WAN optimisation approaches

WAN optimisation can be deployed in either symmetric or asymmetric topologies.

Asymmetric optimisation, as shown in Figure 1, refers to the use of one or more devices at a single location that unilaterally improve performance by spreading load across multiple servers or other devices. In this scenario all optimisation is done at one central location. No additional software or appliances are required for users who connect to that location.

Symmetric optimisation, on the other hand, requires pairs of appliances (or an appliance and optimisation client software), which collaborate to optimise traffic flows between them – see Figure 2.

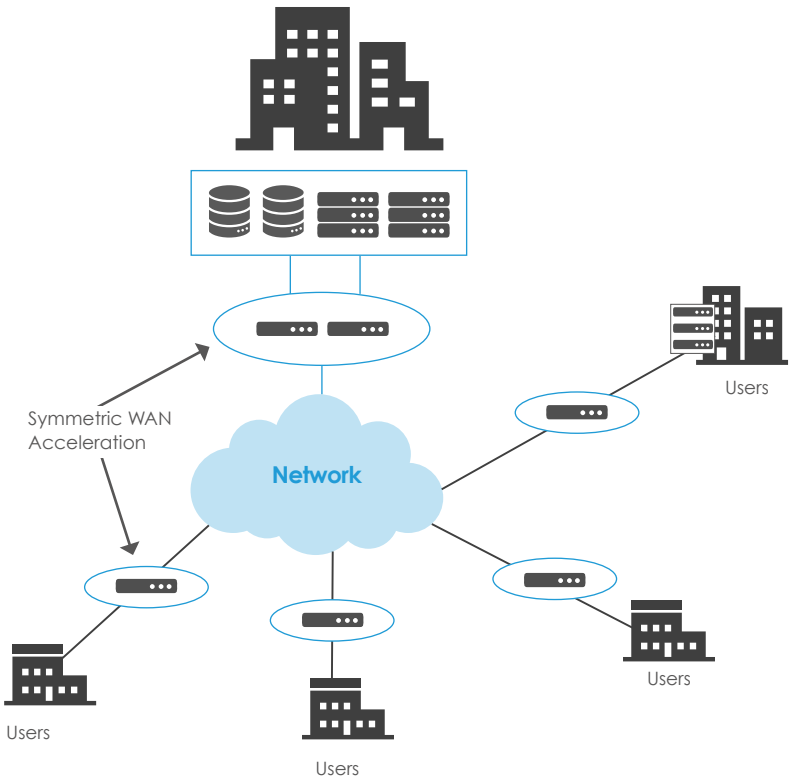


FIGURE 2 – SYMMETRIC WAN ACCELERATION

WAN optimisation appliances can be located at different places in the network. The simplest method is to locate the appliance in-line either before or after the WAN gateway router, as shown in Figure 2.

An alternative is to use out-of-path or stub optimisation using a protocol such as Web Cache Communication Protocol (WCCP) - see Figure 3. This provides a mechanism to redirect traffic flows in real time from a router to an accelerator that is located on a separate stub. It is an ideal way of implementing WAN optimisation or content-caching, it also has the benefit that it is easy to have multiple devices at a single site for redundancy or load balancing.

In this implementation, traffic is redirected from the gateway router to the WAN optimiser and then back through the gateway before being transmitted to the WAN.

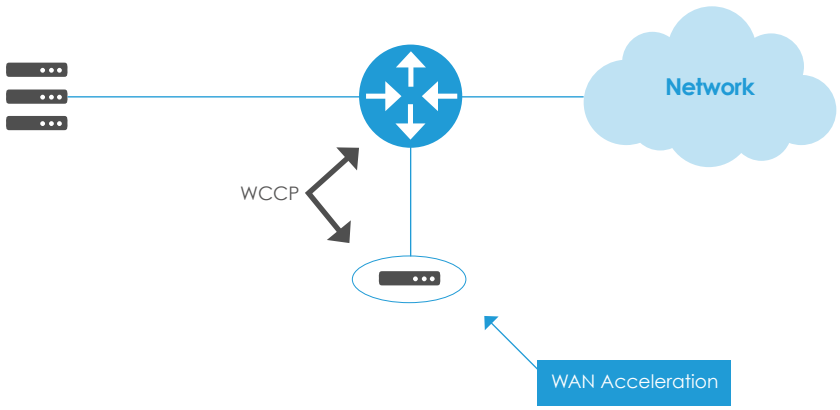
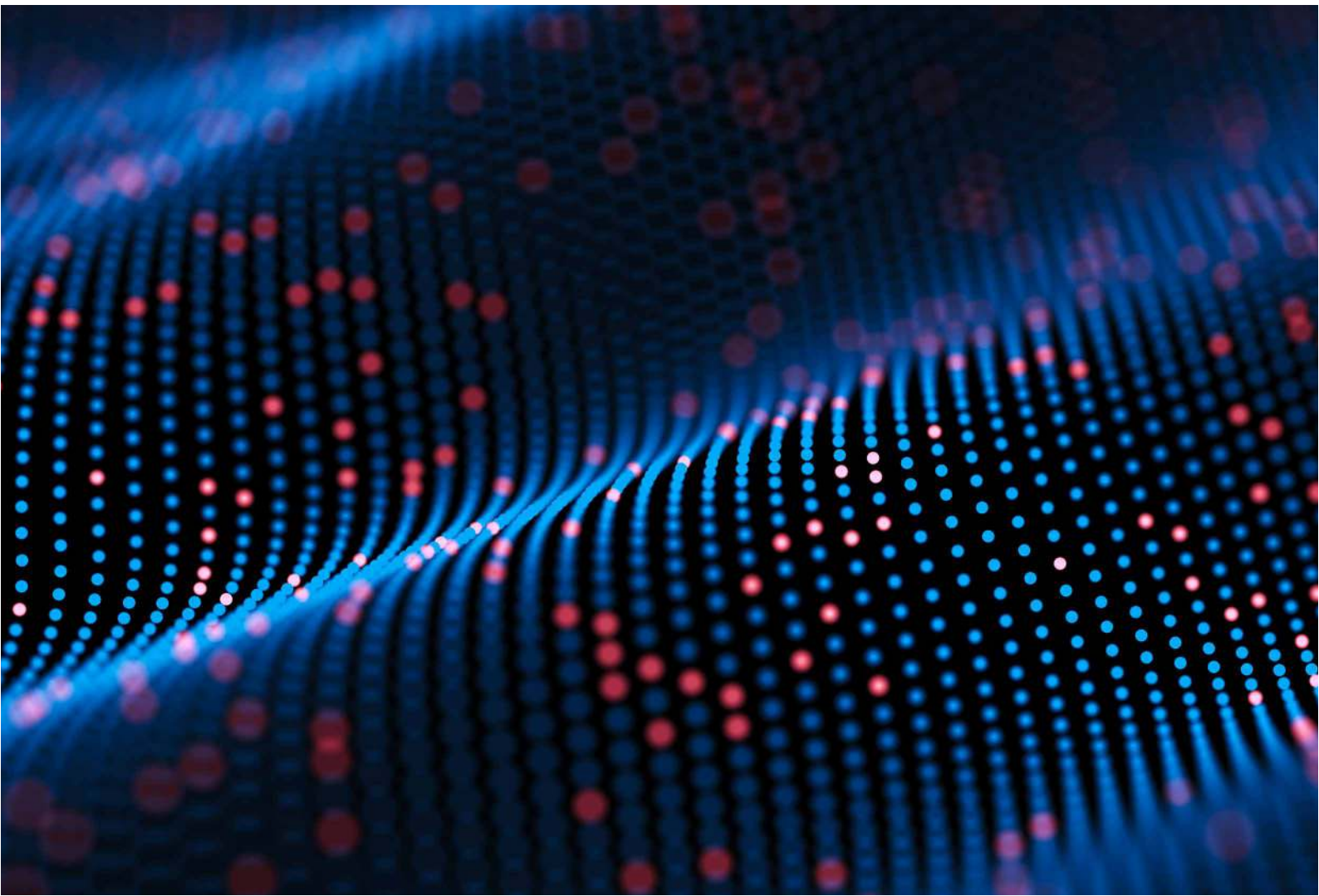


FIGURE 3 – OUT OF PATH WAN ACCELERATION



In all cases, and regardless of the optimisation implementation, it is vital to ensure that the encryption appliance is located on the WAN side of the optimisation appliance, so that incoming traffic is always decrypted prior to reaching the optimiser as shown in Figure 4.

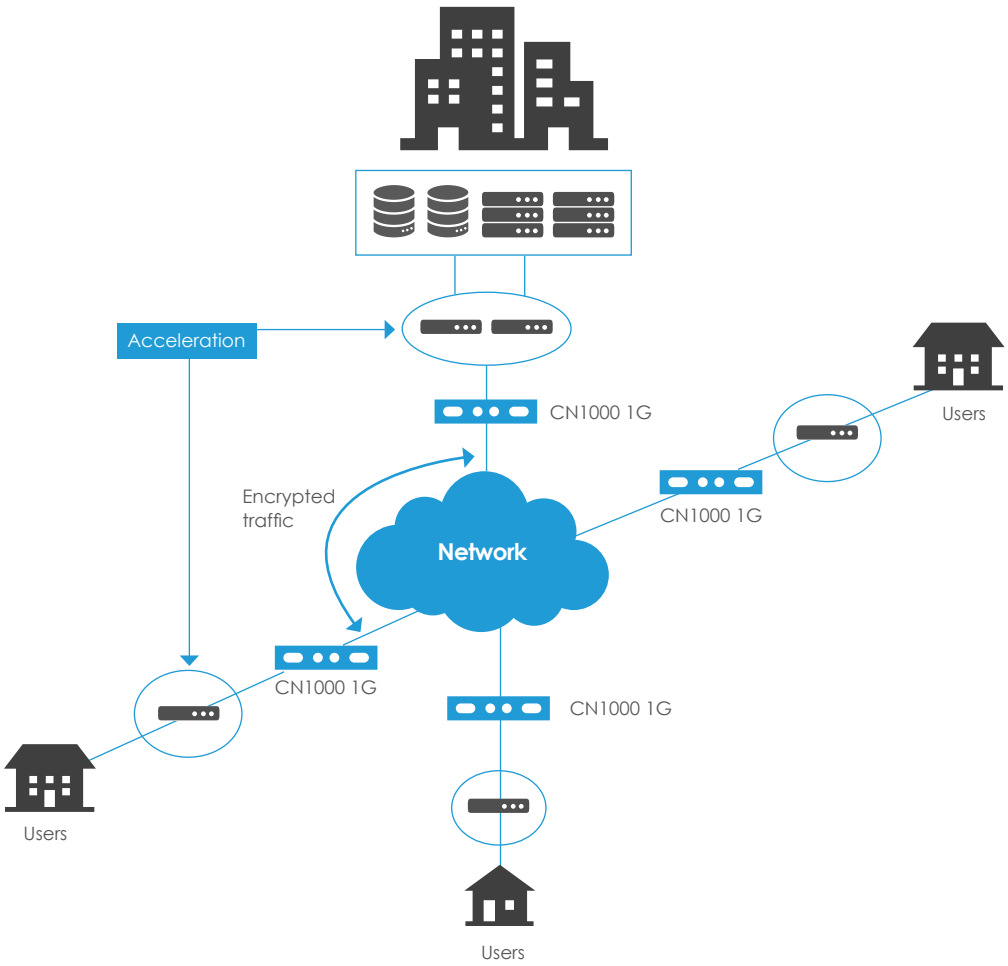


FIGURE 4 – ENCRYPTED NETWORK

Layer 2 encryption operates at the data link layer and is therefore independent of protocol modifications that occur at Layer 3 or above. For this reason, no special configuration or policy settings are required in a Layer 2 encryptor to secure network traffic that has been optimised.

Summary

WAN optimisation provides powerful techniques

to accelerate network performance and reduce transaction response times. However, the technologies themselves generally provide no inherent security. Therefore, encryption is required when the transmitted information is confidential or sensitive.

Deploying a high overhead encryption technology such as IPSec to accelerated traffic reduces much of the benefit achieved from the WAN optimisation/acceleration.

The combination of WAN optimisation and Layer 2 encryption technologies provides the most efficient way of providing the optimal performance and security for data transmission across Layer 2 WANs.

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.

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