SENETAS
Security without compromise

IN CONTROL AT LAYER 2: A TECTONIC SHIFT IN NETWORK SECURITY.

WHO SHOULD READ THIS WHITE-PAPER: NETWORK ARCHITECTS / MANAGERS, DATA SECURITY MANAGERS, CIOs, CSOs.

EXECUTIVE SUMMARY

Network hacking and corporate espionage are on the rise and set to intensify. Information security risks remain commonplace, and most organisations need to increase vigilance. At the same time, stakeholders have increasing expectations that their information will be secure in the hands of other organisations.

In early 2013, Australian Prime Minister Julia Gillard quoted cyber security incidents as having risen by 42% over the last two years – announcing $1.46 billion in funding for a new Canberra-based cyber security centre to emphasise the threat.[1]

At the data network level, traditional Internet Layer 3 (IPSec) security is not well suited to modern environments. It is complex to administer, does not scale well to larger settings, and with its considerable overhead, can compromise network performance by up to 50%.

The network security industry is on the verge of a widespread shift towards Layer 2 Ethernet networks (LAN & WAN). We're seeing significant growth in Layer 2 networks for a variety of reasons – not least of all technology advances. They scale better, are more cost effective and deliver higher quality of service, and it's also easier to control and manage.

But most critically perhaps - as compared with Layer 3 (IPSec) encryption – Layer 2 networks can be secured and encrypted with dedicated appliances without any loss of speed and performance. This paper analyses the threat to networks, lays the case for Layer 2 network security, and draws on third party reports and customer stories to keep you up to date and informed, answering the important question: why is it becoming essential to encrypt your network at Layer 2?

INTRODUCTION: WHAT IS THE THREAT?

All across the globe, fibre-optic cable networks are used to transport important and large volumes of data. They have long been considered the fastest and most reliable method of moving information for just about every industry – and certainly for the critical finance, telecommunications, pharmaceutical and government sectors.

As such, the need for data to travel securely between sites is essential. But fibre-optic networks have become increasingly vulnerable as data theft and hacking technologies have become less expensive and easier to obtain and use.

As this paper will outline, while cyber-warfare between nation states may justifiably preoccupy media and Government interests, corporate and commercial espionage is just as real and must be considered in the security plans for every organisation. Internal network security alone is not sufficient as information traveling between sites can be intercepted without a great degree of difficulty.

As analyst firm IDC reported in 2009, "Industrial espionage is worth billions of dollars... some hackers have the capability to attack and exploit optical networks to collect information or introduce dangerous data that can halt or disable networks."[2]

Hacking methods

The IDC report, entitled *'Fiber-Optic Networks: Is Safety Just an Optical Illusion?'* describes the inexpensive methods that hackers can now use to compromise Ethernet networks, as follows:

Splice method – most common, this technique taps into the fibre by breaking the cable to monitor data. Hackers can easily abuse carrier maintenance points such as Y-bridges or splice-points.

Splitter/coupler method – by bending the cable, a small amount of light will escape from the cable. A hacker with the appropriate, commonly available photo-detector equipment can then capture this light and the data it carries.

Optical tapping method – requires little interference with the fibre. Sensitive photo-detectors are placed around the optical cables, capturing the small amount of light (and hence data) that naturally radiates off the cables.

Several known fibre-optic data theft incidents have come to light in recent years using these particular methods.

Here are a few examples:

A) About 10 years ago, US security forces discovered an illegally installed eavesdropping device in Verizon's optical network. It was believed someone was trying to access the quarterly statement of a mutual fund company prior to its release—information that could have been worth millions.

B) Reported in the Wall Street Journal (March 2008), roughly 4.2 million credit card details from Hannaford, a supermarket business, were stolen via optical tapping methods.

C) Information Security Magazine published a November 2006 story claiming criminals are unlawfully monitoring Dutch and German police networks, as well as the networks of pharmaceutical giants in the UK and France. The same article goes onto report that three main trunk lines of Deutsche Telekom were breached at Frankfurt Airport in Germany.[2]

As far back as 2003, author Wolfgang Müller-Scholz explained in a Wolf Report document titled *'The Silent Conspiracy'*, "the eavesdropping of fiber optic cables, the primary telecommunication veins, is much easier than previously believed. Just a little light is enough to fully copy even the biggest volumes of data, such as live video, completely unnoticed."

Worryingly, the Wolf Report at the time surveyed 36 German fibre network operators about their security – 75% chose not to respond to the survey. "Only one carrier showed courage and conceded under the condition of anonymity, that their network was poorly protected."[3]

Today, networks face a growing threat, although awareness around the vulnerability of fibre optic networks has increased. The latest Trustwave report, *"2012 Global Security Report"* interrogated a huge number of 2011 incidents, known breaches, tests and results from forensic investigations.

It was likely this report the Australian Prime Minister quoted with regard to a 42% increase in network attacks between 2010 and 2011. According to the same report, when it comes to how attackers infiltrate, 61.2% of attacks are executed via remote access and almost 20% remain of unknown origin, indicating client side attacks and insufficient network monitoring. Regarding the harvesting of data, information theft most commonly occurs when data is in transit, amounting to 62.5% of attacks. This last statistic supports the concerns documented in this paper around the proliferation of optical tapping methods.[4]

It is clear that fibre optic networks must be protected to ensure that security and privacy of information is not compromised.

AN INDUSTRY SHIFT TO LAYER 2 ETHERNET NETWORKS

Before we look at the security credentials of Layer 2 networks, it's worth discussing their increasing popularity based on technological needs.

As network traffic continues to grow in both volume and reach, organisations and network operators are embracing the benefits of Layer 2 Ethernet WAN services.

This growing uptake is supported by analyst firm IDC, which reported in late 2012 that adoption rates for Ethernet services in the United States are soaring, driving revenue from $5.2 billion in 2012 to an estimated $9.2 billion in 2016. We're also seeing an increase in the renewal and purchasing of Ethernet networks for both European organisations and those in the Asia Pacific region – and this is due to a variety of reasons.

IDC states that drivers include high-bandwidth applications such as data-centre connectivity, disaster recovery/business continuity measures, and data storage replication.[5]

For operators, Ethernet services are flexible, economical and provide plenty of opportunity for differentiation through end-to-end SLAs, security and bandwidth on demand. They also provide a path for customers to migrate off older frame relay, Asynchronous Transfer Mode (ATM) and private line technologies.

Ethernet has always dominated the LAN but is growing in popularity in the WAN because of its simplicity, scalability, low latency and cost-effectiveness. Layer 2 Ethernet services such as VPLS (an acronym for Virtual Private LAN Services) effectively transform the WAN into a large Ethernet switch giving organisations the operational efficiency of managing a single technology in both the WAN and the LAN.

Purchasing Ethernet services allows an organisation to get more bandwidth for less money as well as improved scalability and reliability. In many cases migration from legacy services such as ATM is being forced by carriers when existing contracts expire and those services are no longer on offer.

Carrier Ethernet providers now offer both point-to-point and multipoint services at rates from 512Kbps to 10Gbps and can connect multiple geographically dispersed sites in a scalable and efficient manner.

Additionally, Layer 2 WAN services give enterprises the benefit of controlling their own routing and avoid the need to expose their routing infrastructure to their service providers.

Further to the IDC synopsis on market drivers, we believe the next growth phase in Layer 2 Ethernet connectivity is being driven by the convergence of voice and data in the enterprise; cloud computing; and the consolidation of business data centres.

NETWORK SECURITY: LAYER 2 VS. LAYER 3

But what about security on Layer 2 networks? Is it any better or any worse than on Layer 3 links? Certainly, security of transmitted information is always a concern regardless of whether the WAN service is at Layer 2 (Ethernet) or Layer 3 (Internet).

Unfortunately misleading terms and obfuscation abound. Service provider networks are often characterised as being secure through terms such as "Virtual Private Networking" (VPN), which can cause widespread confusion to users.

The term VPN here is misleading in the sense that the word 'private' is not a synonym for encrypted. Although each customer does see a logically private network service it still runs on a shared infrastructure, which means all that is separating one customer's data from another is a tag or label that the core switches utilise for customer separation.

This means that if there is accidental or malicious mis-configuration in the network which results in data being sent to the wrong destination then that information will certainly be exposed. Secondly unencrypted traffic is still vulnerable to snooping (tapping, splicing and coupling – as described in this paper) anywhere in its journey from source to destination if, for example, an attacker can get access to the physical network at any point.

Just as with all security, if the cost of an attack is less than the value of the information – incentive is there and this can pose a genuine threat. In general, service providers do not provide "privacy by default" and any information transmitted comes with no guarantee of confidentiality, unless appropriate measures are taken to protect it. It is vital therefore that organisations understand this reality and factor it into their risk management decisions.

How do you secure Layer 2 and how does this compare with Layer 3 security?

Generally speaking, users expect the highest levels of security but not at the expense of degraded network performance. This was the historical trade off between usability and security. In the past when you used encryption it was understood that the price of confidentiality was a *reduction in network throughput performance* and increased complexity.

That performance trade off still exists today when using traditional Layer 3 IPSec solutions. The significant performance implications are due to the large 'per packet overhead'. Additionally, IPSec does not scale well in large meshed networks.

However, the positive news for Layer 2 users is that encryption at Layer 2 can be implemented in a simple, scalable way with little or no impact on network performance. This is achievable because Layer 2 networks are inherently simpler in general, provide in order delivery of frames, and do not have IP subnetting complexities to deal with.

This means that Layer 2 hardware encryption devices can be deployed that:

- Are fully autonomous and operate independently in point to point or large meshed environments
- Are transparent to all network applications and higher Layer protocols
- Can be deployed without requiring changes to other network devices
- Allow full line rate encrypted communications at up to 10Gbps
- Automatically discover the network topology and establish connections with peers
- Encrypt all unicast and multicast voice, video and data traffic

As secured wired and wireless point-to-point connections over WANs continue to proliferate, Layer 2 encryption is understood to better serve organisations with a superior security solution and greater network performance, also overcoming the operational complexities associated with traditional IPSec applications.

Consequently, organisations are increasingly looking at Layer 2 security solutions as simpler and less expensive to manage, particularly as changes within the WAN do not affect the encryptor's operation.

In summary, the shift to Layer 2 encryption – we believe – centres around the *lowest possible impact on network performance*, it's transparency to media, and the fact that it reduces IT complexity. This allows business and Government to reduce costs in meeting data protection and privacy regulations.

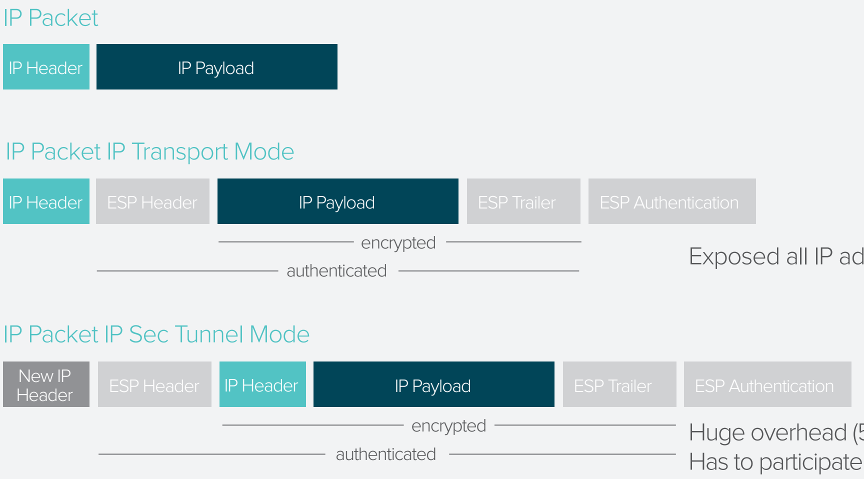
Analyst view on Layer 2 security

IDC Makes an important point about Layer 2 networks: *"A network can be secured at Layer 2 without loss of performance – (even) up to 10Gbps."* [2]

The underlying issues are whether Virtual Private Networks can be sufficiently secure and the role of encryption. Then the question is how efficiently an effective encryption solution can be applied. Encrypting at Layer 2 is optimal because it does not impose performance degradation.

The following graphs illustrate the difference between IPSec Layer 3 network security versus Ethernet encryption at Layer 2.

Encryption at Layer 3



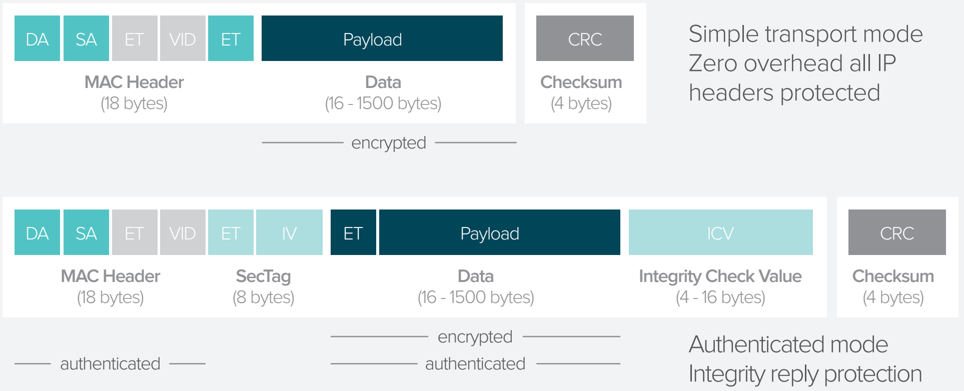
Exposed all IP addresses

Huge overhead (58-73 bytes)
Has to participate in network routing

Senetas Layer 2 encryption

A look at an IP packet with its payload in both, IPSec ESP transport mode and tunnel mode, reveals the inefficiencies caused by the encryption mode at the packet level.

Senetas Encryption at Layer 2



Simple transport mode
Zero overhead all IP headers protected

Authenticated mode
Integrity reply protection

Senetas Layer 2 encryption

24 bytes overhead worst case

A transport mode encryption at Layer 2 is able to encrypt the entire IP packet including the IP header without requiring any tunneling. Tunneling alone generates 20-40 bytes of avoidable overhead and adds noticeable latency and slowdown of performance.

Attributes of Dedicated Encryption Appliances for Layer 2 networks

Security - Dedicated appliances are optimised for security and meet the highest requirements.

Performance – Dedicated appliances are optimised for performance. There is no competition for the available resources between different functions.

Upgradeability – Dedicated Layer 2 encryptors tend to be specified and architected in a way that allows the expansion of the functionality at a later point in time.

Costs - The average product life of a dedicated encryption appliance exceeds that of an integrated appliance by 3-4 years, leading to lower cost of the dedicated encryption appliance over the entire product life. The initial cost savings of the integrated appliance turn into higher cost over time.

CASE STUDY – AUSTRALIAN FEDERAL GOVERNMENT (SENETAS CUSTOMER)

Senetas encryption solutions have been designed to provide high speed Layer 2/3 encryption of data in transit over public and private networks. This Australian government agency (a Senetas customer) is responsible for providing integrated control and monitoring of border security.

Challenge

The agency had implemented a closed circuit television system to monitor a number of major transport hubs. The video traffic was centrally monitored from a remote location. Due to the sensitive nature of the video information and the risk of interception between camera and monitoring station, it was a requirement that the video streams should be protected by encryption.

Solution

The client had been encrypting the video stream using a Layer 3 IPSec solution. This appeared to operate successfully at first, but trials indicated it introduces significant latency resulting in degradation of the video quality.

The Customer approached Senetas regarding a Layer 2 encryption solution, opting for an initial Proof of Concept (POC) using a pair of Layer 2 Ethernet encryptors running at 100Mbps. Testing indicated that the Senetas encryptors did not impair the quality of the video or the ability to remotely control the cameras.

Benefits

While Layer 3 IPSec encryption was suited to encrypting IP packets over a routed network infrastructure, this introduced significant packet overheads and high variable latency. This was the trade-off necessary to support operation over fully routed backbones.

The Senetas Layer 2 Ethernet solution operated at the data link layer and provided wire speed encryption at rates from 10Mbps to 10Gbps with little or no additional overheads. The solution combines the benefits of complete confidentiality with scalable line rate performance across point-to-point or fully meshed topologies.

CONCLUSION

This paper has analysed the realistic threats to fibre optic Ethernet networks – both at the LAN and WAN level. Due to a number of known optical hacking methods, and several documented cases of corporate and government information espionage – it is reasonable to conclude that proper security of Ethernet networks is a critical endeavor for all organisations.

IPSec-based encryption and security does not scale well in large networks, and can slow down network performance due to significant per packet overhead. Dedicated Layer 2 network encryption appliances, alternatively, provide the necessary security levels and can be implemented in a simple, scalable way with little or no impact on network performance.

And this is why we're seeing a widespread shift towards Layer 2 Ethernet networks – in the Asia Pacific region along with Europe and the United States.

This white paper has been co-authored by Julian Fay, CTO, Senetas Corporation and Simon Galbally.

ABOUT SENETAS CORPORATION LIMITED

Senetas Europe is a wholly owned subsidiary of Senetas Corporation Limited (ASX:SEN), specialising in high-speed network encryption. Our Layer 2 encryptors provide the last, best line of defence for data in transit for governments, the public sector and leading commercial organisations worldwide.

We manufacture the world's only triple-certified, high-speed data encryptors; certified to Common Criteria (Australia and International), FIPS (US) and CAPS (UK) as suitable for government and defence use.

Our products are used to secure network data for cloud computing services, payment systems, big data applications, CCTV networks, datacentres and critical infrastructure and control systems in more than 25 countries.

Senetas encryptors are suitable for networks of all types from point-to-point to fully meshed, multipoint network infrastructures. Our core products operate from 10Mbps up to 10Gbps and support Ethernet, Fibre Channel, SONET/SDH and LINK protocols. These high performance devices use AES 256bit encryption and operate in full-duplex mode at full line speed with no packet loss; delivering security without compromise.

For more information on Senetas Europe visit our website: **www.senetas-europe.com**

[1] ARN Magazine, February 6, 2013

[2] *'Fiber-Optic Networks: Is Safety Just an Optical Illusion?'* IDC, 2009.

[3] *'The Silent Conspiracy'* The Wolf Report, 2003

[4] Trustwave 2012 *Global Threats and Trends*.

[5] IDC press release: *'Robust Ethernet Service Adoption Forecast to Drive U.S. Revenues to $9.2 Billion by 2016, IDC Says'* November 1, 2012.