cpl.thalesgroup.com

THALES

Data in Motion Security Through a 5G Infrastructure

White Paper

Contents

Introduction

Today's networks are an interconnected menagerie of diverse mediums. Copper, Fiber, WiFi, Satellite and LTE are just a few examples of the diverse paths that data packets can travel through on the way to their final destination. Beyond these wired and wireless links, there are a number of diverse transport protocols to contend with, each of which have layer-specific security solutions that can affect both connectivity and performance. For far too long, security of data in motion has been handcuffed to the massive overhead constraints of IPsec and stifled by network interoperability issues associated with MACsec.

5G connectivity promises to break traditional paradigms of data delivery by providing network connectivity virtually everywhere. To accommodate this new paradigm in diverse data delivery, the building out of 5G infrastructures is underway. And beyond user data itself, the requirements for high throughput with low latency and jitter are critical to signaling and management plane. From edge to tower, from backhaul to core, from Edge to Cloud, 5G enables use cases that can range from low data rate traffic bursts to 100Gbps core to core connectivity. 5G networks require new techniques for data in motion security in order to accommodate the diverse range of 5G use cases…a single solution that combines enhanced security, boundless interoperability, and optimized performance is required to meet the demands of 5G networks. The Thales Transport Independent Mode (TIM) meets the 5G requirements for quantum-ready security, low jitter and low latency at 98% network efficiency.

5G Security and Network Performance

5G use cases will be widespread and varied. For example, the requirements for secure data delivery of a driverless car can be quite different from the requirements of an enterprise data center backup, a small office vital link, or the Mobile Network Operators' backhaul control plane data. The diversity of packet sizes, protocols, and transport layers make consistency in security and performance impossible using traditional security methods. IPsec has not changed much since implemented back in the 1990s , the same era that Windows 95 was released. While IPSEC is suitable for most 4G use cases, it is far from qualified for 5G because of the following reasons:

- Bandwidth - IPsec Overhead can consume up to 35% - 50% of the bandwidth
- Latency - IPsec Increase latency and jitter by milliseconds, rather than microseconds
- Security – Doesn't offer control over key management nor quantum safe technology

MACsec greatly reduces the overhead associated with IPsec but is limited to Layer 2 (Ethernet) and it comes with its own set of constraints that affect security, performance, and interoperability. Both MACsec and IPsec are older technologies and are delivered on multi-purpose platforms that do not meet today's performance requirements nor the quantum threat challenges of the not-so-distant future.

One of the major problems with older security solutions is that security is too closely associated with the transport layer. IPsec is a feature of devices like routers and firewalls for purposes of convenience. Aside from the obvious overhead inefficiency required at the transport layer, these multi-function devices are busy making transport, routing, and filtering decisions for each frame. The additional burden of encrypting and decrypting each packet injects overall poor performance in terms of throughput, latency and jitter. Over the years, increases in processing power helps minimize these affects but unless both sides of the link have high-performance equipment, the slowest, highest latency, highest jitter link will prevail as the best-case scenario. In the text below, we will examine why IPsec and MACsec are antiquated solutions for 5G networks in terms of both security and connectivity.

IPsec

IPsec tunneling has been the go-to security solution of layer 3 networks for more than 25 years. Since the inception of IPsec, networks have changed dramatically, yet the fundamental constraints of IPsec remain. Originally designed to protect lower-speed networks operating at 10 to 100 Mbps, IPsec fulfilled the requirements of encrypting data in motion. Even though it adds an average of 5 milliseconds of latency (Figure 1) and 15 milliseconds of jitter to the network (Figure 2), it was a burden that the network team took on as a cost of business to secure their connections. As network speeds advanced to speeds of 1Gbps and 10Gbps, IPsec continues to be the go-to strategy. After all, it is a readily available, familiar solution that network administrators heartily accept….some without question. To keep pace with the growing speed and capacity of the network links, network equipment vendors added encryption accelerators and proprietary twists in an effort to compensate for the poor performance in terms of latency and jitter. This helped reduce some of the latency concerns (for a price) but certainly did not solve the overhead burden. As voice and video over IP continues to proliferate, the burden of overhead gets proportionately worse. With IPsec, smaller packets still require the same amount of overhead as large packets so the ratio of overhead to data becomes exponential. In controlled testing under pristine conditions, IPsec achieved a best case of 71% network performance (see figure 3).

Still, many network administrators view IPsec overhead as a cost of business and they continue to deploy it as a matter of convenience or because no comparable alternative exists. As network speeds continue to increase to 10Gbps, 100Gbps and even 400Gbps, IPsec is finally reaching its accepted break point and many markets have moved to Layer 2 encryption for higher speeds. For Layer 2, there are real-time hardware encryption solutions that operate at speeds of up to 100 Gbps while adding no more than 4 microseconds of latency. These solutions should be considered as an alternative to MACsec for 5G however, most are limited to layer 2 or require a tunnelling mode that is not optimal for Layer 3.

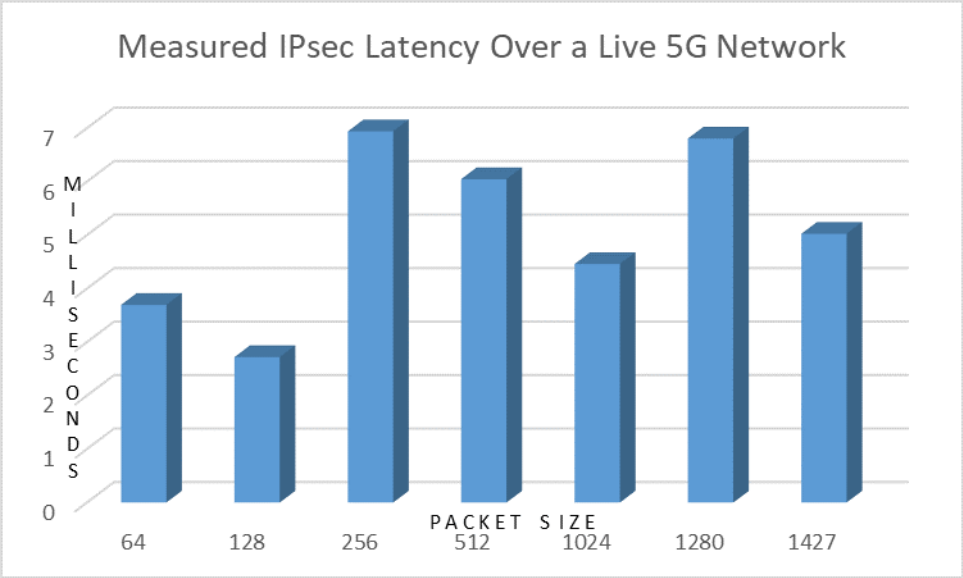

Figure 1 – An average of 5 milliseconds of IPsec Latency measured

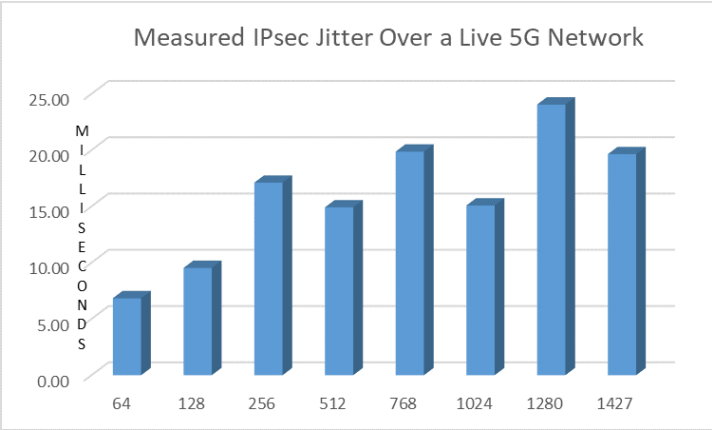

Figure 2 – An average of 16 milliseconds of Jitter measured

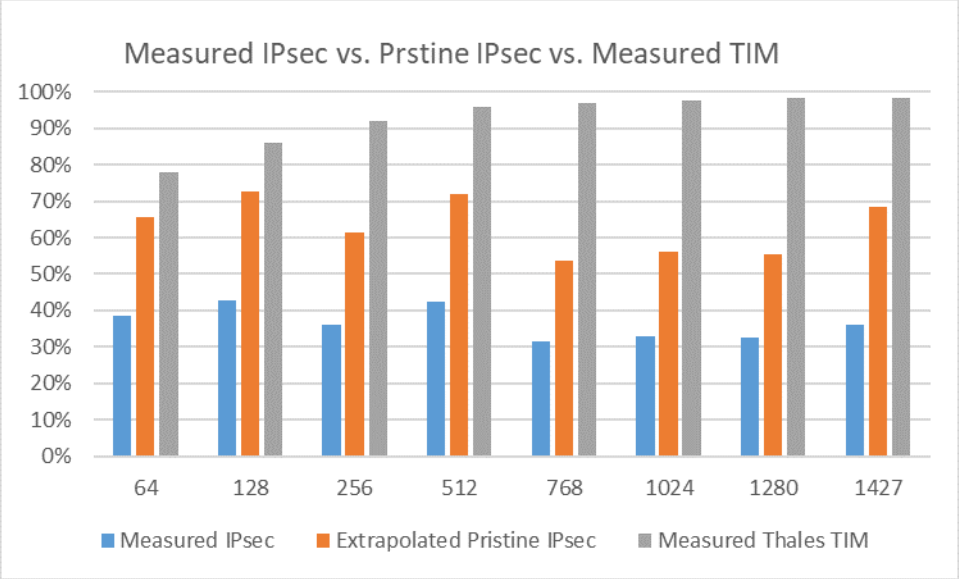

Figure 3 – Measured IPsec vs. Extrapolated Pristine IPsec vs. Thales 1G HSE with TIM

Constraints of Traditional Data In Motion Security Solutions

Both IPsec and MACsec provide little to no control over Key Lifecycle Management, the foundation under which encryption solutions are built. With IPsec and MACsec, second- and third-party certificate authorities are required, multiple network administrators have access to devices, and it is highly likely that no single entity (if any at all) retains ownership of the life cycle management of the keys that include, key entropy, key rotation, key storage, or key destruction. An auditable end-to-end security guarantee is not viable. 5G networks will undoubtedly require mandatory and auditable security requirements for backhaul to core as well as within the core itself. Small offices, enterprise IT organizations, and end users alike desire control and management over their security while service providers desire a mechanism for additional services to monetize links through customer-controlled, value added security provisioning. These uses cases can only be applied when control over the key material can be securely delivered, controlled, and managed.

Key Ownership and Compliance

Today, security professionals are placing more and more emphasis on key ownership. Terms like Bring Your Own Key (BYOK) and Bring Your Own Encryption (BYOE) are not just buzzwords. They are meaningful security concepts required for organizations to not only protect their data assets, but to be able to prove they control the security of these assets. Rather than trust that Cloud Service Providers (CSPs) will protect the data stored within their cloud, security administrators are taking ownership. Management of encryption keys security of data are now on premise so that data can be stored safely on a remote cloud server with full accountability. If audited, the customer can guarantee their control over the security of their data assets. No one on premise or in the cloud can access that data without the encryption keys. Control and ownership over keys are all on premise functions, without a need for second- and third-party vendors or a multitude of employees with their hands in the pie. The fundamental basis of a solid security solution is control and ownership of key materials. 5G core infrastructures can manage their own keys and service providers can monetize customer-managed end-to-end security of the links, from site to site or site to cloud.

Crypto Agility

The term crypto agility is important as it relates to variety of independent security requirements. IPsec and MACsec are usually limited to traditional AES-256 algorithms using standard, globally available certificate authorities. When it comes to custom crypto requirements, traditional data in motion security solutions are stuck in 1990. MACsec leverages low-cost hardware and mostly software-based random number generators for key entropy. With MACsec and IPsec, there are no easy ways to change key entropy functions, algorithms, key management, or certificates authorities. The eventual impact of Quantum threats will require forklift equipment changes in order to meet this inevitable threat. It's just a matter of time and solutions that provide quantum resistance today while allowing software upgrade paths to quantum compliance later, will serve as security solutions for today's and tomorrow's networks. 5G networks will require a solution that is Quantum resistant out of the gate, with an ability to be software upgraded to quantum compliance as these new standards get closer to ratification.

Separation of Duties

Data in motion security solutions often overlook the aspect of separation of duties. Because IPsec and MACsec have such close ties to the transport layer and embedded into traditional network equipment, it is impossible to separate the administration of security from the administration of the network. This can only be achieved through implementation of a security solution that is completely agnostic to the network transport layer. Access to security controls should be limited, monitored, and audited by a group that dedicates itself to standards implementation and compliance while allowing network administrators to tune the network. This ensures a high quality of network performance while preserving the integrity of the security. Each function can focus on their expertise, providing for the greatest level of security and performance through local and wide area infrastructures. Protocol agnostic security solutions with little to no impact on network performance ensures that both high levels of security and performance can be achieved independently of each other even when provided as a packaged solution.

5G Performance Considerations

Network Independence: Abstraction of Security from the Transport Layer

As discussed, both IPsec and MACsec are each integral parts of their respective network layers. This presents several serious constraints for both the security and the transport of data. By abstracting the security functions from the transport layer, we can achieve full security with Network Independence. Thales has implemented this revolutionary technique called Transport Independent Mode, or TIM for short. By implementing 21st century security techniques eliminating the overhead and constraints of network protocols, TIM becomes a realization. Security and transport are two different subjects and therefore we must deal with them separately in order to provide the best possible security with no transport constraints. The overlook of this amazingly simple concept cannot continue. Security with TIM is necessary for consistency across the diverse use cases and requirements of 5G infrastructures.

Performance: IPSec vs. TIM in an Operational 5G Network

Overhead and Latency Comparisons

The data presented within this paper are from tests performed over a live 5G network infrastructure. Since IPsec performance is greatly dependent upon the cost and processing power of the devices, this paper presents two sets of IPsec data points. One set of IPsec data points show the firewall Manufacturer's claims extrapolated to varying packet sizes under optimal conditions, described as "pristine" conditions. The other set of data points shows actual tested results using off-the-shelf hardware on both ends under normal network operating conditions, described as "measured" results. In all cases, the Thales TIM results were obtained under normal network operating conditions (measured). The goal is to compare the performance differences between traditional IPsec implementations (both "pristine" and "measured") against the Thales Transport Independent Mode. The test results show that in all tests, TIM outperforms IPsec in terms of Latency, Jitter, and Throughput.

Transport Independent Security achieves an average of 98% efficiency (a mere 2% opportunity loss) while IPsec achieves only 40% efficiency (a whopping 60% opportunity loss across diverse packet sizes). See Figure 4. This "average" opportunity loss is significant affected by diverse packet sizes. Smaller packets have a greater ratio of overhead, since IPsec overhead remains constant. 5G networks will have greater mixes of voice and video and the results of these mixed frame sizes are reflected in these tests.

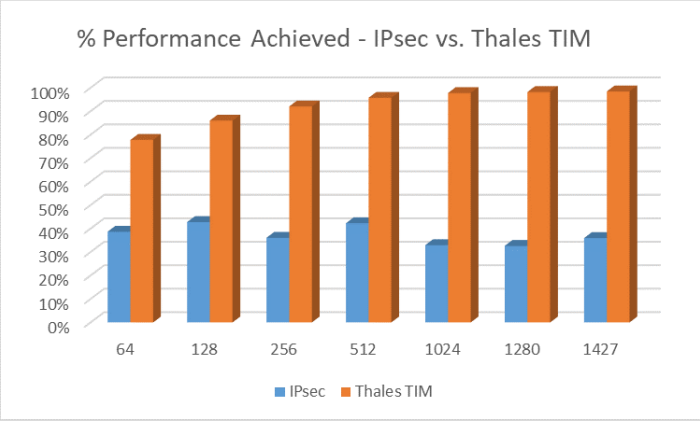

Figure 4 – IPsec measured vs. Thales Transport Independent Mode (TIM) security

When considering application layer use cases such as Teledoc, Zoom, Microsoft Teams and other voice and video dependent applications, we must take into account the effects of security on Latency and Jitter. These are critical measurements that can have profound effects on the user experience. Dropped UDP voice packets and choppy video are just two unacceptable side effect of latency and jitter. Comparing IPsec against the Thales TIM security implementations, we again see that the Thales TIM solution significantly outperforms the old school IPsec technique (see figure 5and figure 6).

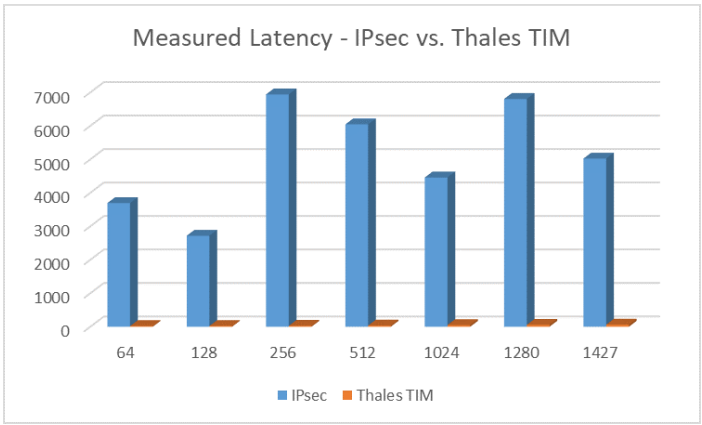

Figure 5 – IPsec vs. Thales TIM Latency over a 5G Infrastructure

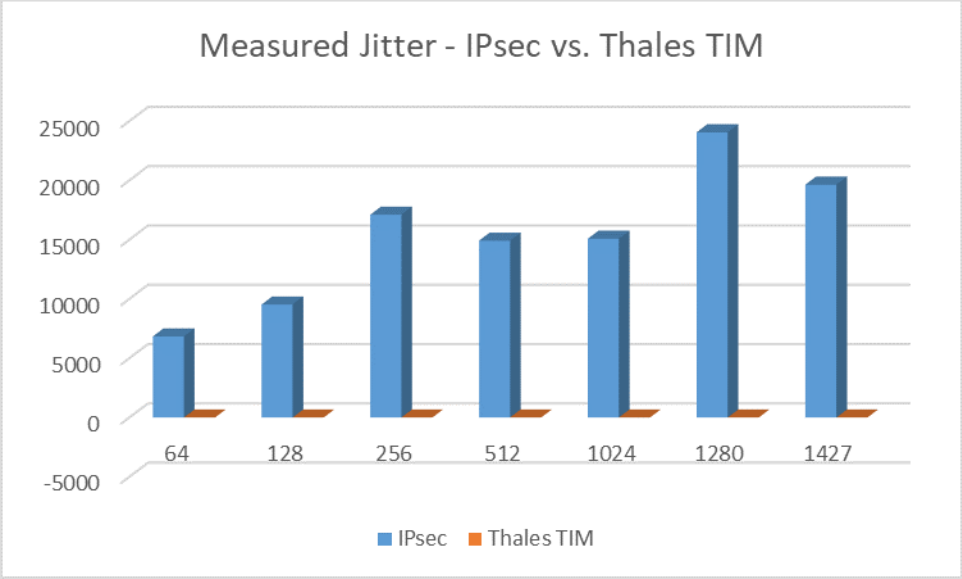

Figure 6 – IPsec vs. Thales TIM Jitter over a 5G Infrastructure

Security: IPsec vs. TIM in a 5G Network

The test data clearly shows the performance improvement that Transport Independence achieves over traditional IPsec solutions in the major categories of Latency, Jitter, and Throughput. Since security should never be compromised in favor of performance (or vice versa), it is important to evaluate the security differences between Transport Independent Security and IPsec.

The Benefits of TIM in a 5G Infrastructure

Greater Security

The ability to provide controls and ownership of data in motion security is the primary rationale behind enhanced security. Providing these capabilities independent of network constraints means that auditable security ownership can be guaranteed from Point A all the way to Point B without any network constraints. Protocols, network vendor equipment, service providers and telcos can all be in the mix without worry about interoperability issues, dependences or transport concerns. Quantum resilience, meaning the ability to provide quantum resistance today and upgradeable quantum compliance tomorrow, factor in for longevity solutions that fit the bill for today's and tomorrow's networks. Standards compliance to meet international and industry-specific mandates with the flexibility to meet unique and custom sovereign requirements are key aspects to an agile security solution.

Better Performance

Breaking the paradigms of old security mainstays, Transport Independence places the security intelligence at the endpoints, rather than within the protocol itself. The result is a drastic reduction in overhead with increased performance and network capacity. Showing a 25% average performance benefit over IPsec, Transport Independent Security is clearly the future of securing data in motion over wired, wireless, and software defined network infrastructures.

Enhanced Connectivity

The placement of security intelligence at endpoints and the abstraction of security from the protocol layer enables complete independence from all network dependencies. Mixing of network equipment providers, data handoffs between telcos, movement between diverse cloud service providers, and traversal across multi-domain infrastructures with complete end to end security is only possible with protocol independence.

Auditable Compliance

With controls over security being limited to endpoints, access to and storage of crypto keys are known and contained. No one person or entity can decrypt data as it traverses through exponential variations in network equipment, carriers, and service providers. From Silicon Valley to India, from Eastern Europe to China, the data can traverse freely throughout the network without concern of data interception and exposure. HIPPA compliance can be guaranteed from a remote doctor's office to the hospital or insurance company's data center.

Conclusion

5G promises to change the way the world connects. Opening up the world to traditional networking use cases, 5G will also enable connectivity for IOT, driverless vehicles, smart grid, health care provisioning, and a multitude of new and exciting capabilities all requiring connectivity. This increase in capabilities requires intelligent techniques to secure links without impedance. It is time to discard relic security solutions of the path and prepare for the next generation of network connectivity. As our networks and connectivity methods grow smarter, data in motion security solutions must also grow to defeat the limitations of outsider reliance and network dependencies.

Thales encryption solutions

If your data is worth anything, it's worth encrypting. Thales is a global leader in the development of end-to-end encryption technologies. Our solutions protect sensitive data for a wide range of commercial, government, industrial and defence customers.

From certified high-assurance hardware and virtualised encryption to secure file-sharing; all Thales solutions share a common high-performance encryption platform and are used to protect sensitive network data around the world. Thales encryption solutions have been trusted to protect much of the world's most sensitive information for more than 20 years.

They are used to protect everything from government and defense secrets to citizens' identity and intellectual property, financial transactions to real-time CCTV networks and critical national infrastructure control systems.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

THALES

Americas
Arboretum Plaza II, 9442 Capital of Texas Highway North,
Suite 100, Austin, TX 78759 USA
Tel: +1 888 343 5773 or +1 512 257 3900
Fax: +1 954 888 6211 | E-mail: sales@thalesesec.com

Asia Pacific – Thales Transport & Security (HK) Ltd
Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East
Wanchai, Hong Kong | Tel: +852 2815 8633
Fax: +852 2815 8141 | E-mail: apacsales.cpl@thalesgroup.com

Europe, Middle East, Africa
350 Longwater Ave, Green Park,
Reading, Berkshire, UK RG2 6GF
Tel: +44 (0)1844 201800 | Fax: +44 (0)1844 208550
E-mail: emea.sales@thales-esecurity.com

> cpl.thalesgroup.com <