Data in Motion Security Through a 5G Infrastructure

Thales trusted technology combined with TCS global services to achieve Transparent, Quantum Resistant Security with Improved Performance and Auditable Compliance in 5G data in motion security.

Introduction

5G networks have unique requirements for both security and performance. From signaling and control plane data to the end-user experience, efficient use of bandwidth, low latency, and low jitter are non-negotiable mandates. 25-year-old security solutions, such as IPsec and VPN, are no longer viable solutions for 5G networks. Modern networks such as 5G, SDN and virtualized core infrastructures, require modern methods to maximize throughput while providing quantum-ready security. The Thales Transport Independent Mode (TIM) meets these 5G requirements for quantum-ready security, low jitter and low latency at 93% network efficiency.

5G Security and Network Performance

5G use cases will be widespread and varied. From enterprise data center backups to small office vital links to end users and Mobile Network Operators' backhaul signaling data, the diversity of packet sizes, protocols, and transport layers make consistency in security and performance impossible using traditional security methods. While IPsec might have met most requirements for 4G, 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 increases latency and jitter by milliseconds, rather than microseconds
- Security – Doesn't offer control over key management nor quantum safe encryption techniques

One of the major problems with older security solutions is that security is tied to the transport layer. IPsec is an optional feature of devices like routers and firewalls. 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. More horsepower can help to minimize these affects but unless both sides of the link have high-performance equipment, the slowest, highest latency link will prevail as the best-case scenario. By separating security functions from the transport layer, improved security and increased performance can be achieved. Thales has implemented Transport Independent Mode (TIM), which eliminates transport constraints and provides for the highest standards of network security.

> "5G requires large amounts of data to be transmitted at high speeds over shorter distances with low latency, near-zero jitter, and high throughput. Thales High Speed Encryptor's TIM (Transport Independent Mode) and TCS (Tata Consulting Services) provide solutions and services for the telco operators to overcome those obstacles by maximizing 5G security without compromising performance."
>
> – Chen Arbel, VP Business Development, 5G & Cloud Security, Thales

Performance Comparisons

Figure 1 clearly shows the dramatic throughput difference between IPsec and the Thales TIM implementation. IPsec achieved only 71% total performance under the device's best-case, sterile environment. The processing power (and price) of the IPsec endpoints as well the diversity in packet sizes provides for additional negative impact on performance. Smaller packets, such as voice and video, require the same amount of overhead as larger data packets. The result is a greater ratio of overhead to data. Figure 4 shows actual average IPsec performance over a live 5G infrastructure over varying packet sizes through 1Gbps capable devices. This real-life scenario of average performing IPsec devices highlights the dramatic affects that packet diversity and processing power have on overall performance. Although the IPsec manufacturer claims 1Gbps IPsec performance, it was discovered that this claim can only be achieved under specific test conditions leveraging higher performing devices at the end point and using aggregated WAN connections, a scenario that is highly costly and unlikely in real world testing. It is expected that higher-performing IPsec devices will produce better results however, pristine conditions yielded a best case of only 71% performance for IPsec. Based on these pristine conditions, we can extrapolate expected results. In comparison to TIM, it is clear that consistency of performance over diverse network conditions can be achieved.

Conclusion

5G promises to change the way the world connects., enabling connectivity for IOT, driverless vehicles, smart grid, health care provisioning, and a multitude of new and exciting capabilities . This increase in capabilities requires intelligent methods to secure links without impedance. It is time to discard relic security solutions of the past and prepare for the next generation of network connectivity and quantum security. As our networks and connectivity methods grow smarter, data in motion security solutions must also grow to defeat the limitations of network dependencies and security threats.

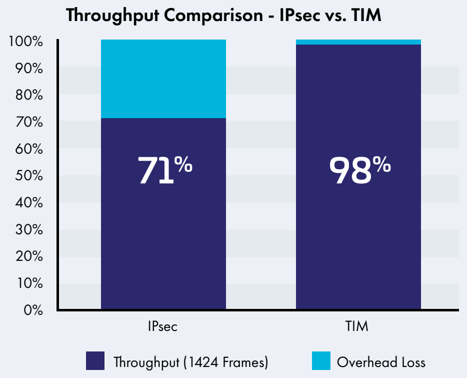

Figure 1 – IPsec vs. Thales Transport Independent Mode

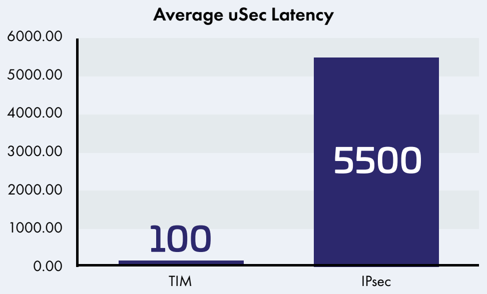

Figure 2 – IPsec vs. Thales TIM Latency over a 5G Infrastructure

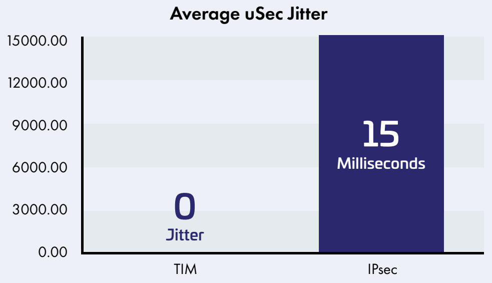

Figure 3 – IPsec vs. Thales TIM Jitter over a 5G Infrastructure

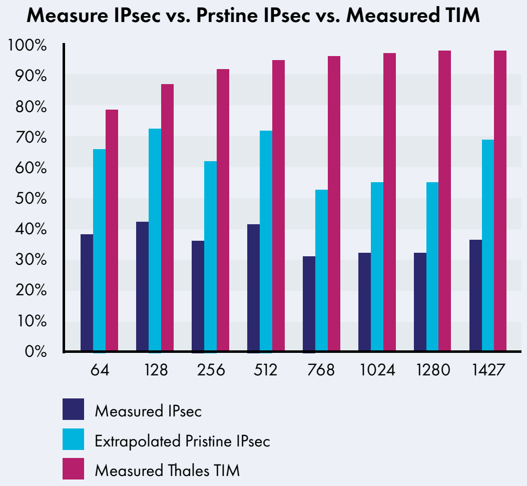

Figure 4 – Measured IPsec vs. Extrapolated Pristine IPsec vs. Thales 1G HSE with TIM

TATA

TATA CONSULTANCY SERVICES

About TCS

TATA Consultancy Services (TCS) is in business for last 50 years with consolidated revenues of USD 22 Billion in fiscal year 2019-2020 together with a consistent 25.14% CAGR since 1998. Currently for Q1FY21, revenue is $5,059 Million with employee strength 443676 representing 146 nationalities.

TCS is a pioneer amongst IT companies globally and a mega player offering consulting-led, integrated portfolio of IT & IT-enabled services delivered across all major geographies through a unique onshore-off-shore model i.e. 'Global Network Delivery Model™'. The model offers multiple levers of time zone, language, skills and local business knowledge to deliver high quality solutions across the globe, 24x7 with globally connected workforce, seamless integrated delivery processes & through multi-tiered infrastructure. This model has been adopted by all global competitors and is recognized as the benchmark of excellence in software development.

TCS has significant footprint in Telecommunication Industry, be it equipment manufacturers or telecom operators. As part of this line of business, TCS helps its customers in many aspects of their business, for e.g. - engineering services, network design and transformation, and operations.

All Telcos are in various stages of execution of their 5G Readiness/ rollout program. One of the key problems faced in these initiatives is the effective implementation of protection of data in motion.

A significant part of addressing the 5G security problem is dealing with the challenges posed by the requirements to secure data in motion.

Control and User Plane signaling data needs to be protected at various levels in 5G communication. There is a strong suggestion that IPSec be used to ensure the integrity of all signaling messages in order to ensure that rogue nodes do not get admitted to the network and that existing nodes are unable to tamper with signals not generated by them. There is a suggestion that certain types of control messages especially those that could reveal the identity of end user should also be encrypted so as to protect the privacy of a subscriber and the information about the movement of that subscriber in the network.

In the 5G scenario there may be specialized network slices that deal with latency critical applications or involve actuation of devices that carry out action in real world. Signaling in these situations needs to be strongly protected as well.

> " The scale and volume of data movement envisaged in 5G deployments require a sophisticated and nuanced approach to protecting data in motion. The HSE solution of Thales is scalable, quantum safe and high performance solution that can operate at layer 2, 3 or 4. This gives it a significant edge over a solution like IPSec."
>
> – Dr. Sundeep Oberoi – Global Head Of Cybersecurity TATA Consultancy Services (TCS)hales

In developing effective strategies and ensuring the highest level of security, the following challenges needed to be dealt with;

- Packet Size Overhead – IPSec in tunnel mode adds an additional IP header to every packet. This degrades throughput and latency
- In practical terms there are interoperability challenges between IPSec implementations of various vendors especially in IKE and Certificate format
- In certain scenarios portion of the physical network may be a daisy chain but may be configured as a hub and spoke logically. Here running logical IPSec tunnels may incur a performance penalty and it may be necessary to engineer tunnels keeping in mind the actual network topology. Maintaining this patchwork of tunnels can be complex

User plane data confidentiality is to be dealt at higher layers of the protocol (PDCP). The operator may provide different levels of encryption here but these deployments must conform to the legal interception and cryptographic regulations of the regions that the deployments is in. The user plane data confidentiality is not usually achieved by IPSec.

In a practical network with many thousands of network elements ensuring that all certificates are valid and are changed over smoothly when they expire with no loss of continuity demands the deployment robust key management. Given that quantum computing is rapidly advancing some attention has to be paid to quantum safe key distribution technology.

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.