

Data in Motion Security Through a 5G Infrastructure



Thales trusted technology with 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) 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 as 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.

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.

> cpl.thalesgroup.com < [in](#) [tw](#) [f](#) [yt](#)

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us

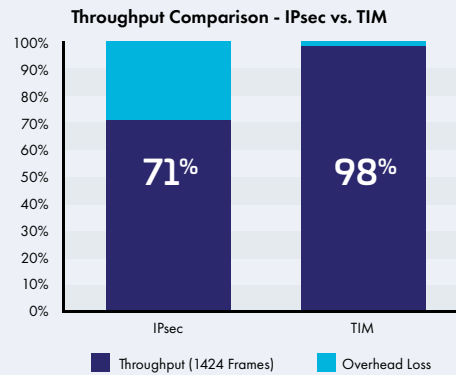


Figure 1 – IPsec vs. Thales Transport Independent Mode

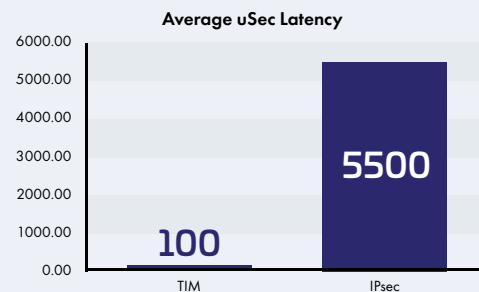


Figure 2 – IPsec vs. Thales TIM Latency over a 5G Infrastructure

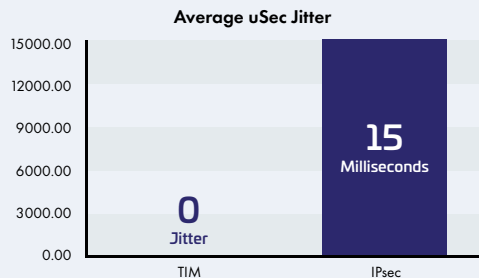


Figure 3 – IPsec vs. Thales TIM Jitter over a 5G Infrastructure

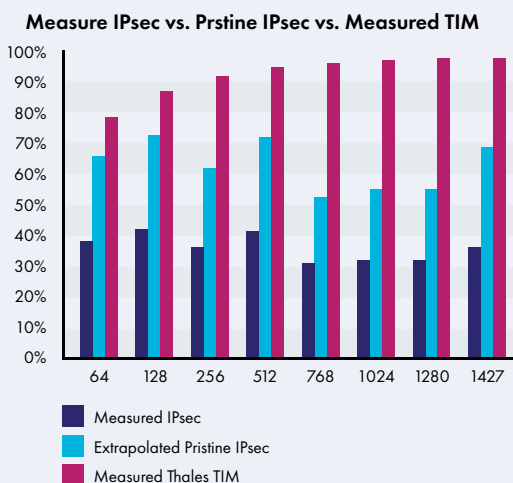


Figure 4 – Measured IPsec vs. Extrapolated Pristine IPsec vs. Thales 1G HSE with TIM