Implementing Zero Trust Principles to Data in Motion for Improved Security and Performance over Physical and Virtual Networks

Joseph Warren
Viasat
Plantation, FL
Jwarre01@yahoo.com

ABSTRACT

For more than 25 years, IPSec/VPN has been the go-to solution of choice for both remote client network access and bulk encryption of critical infrastructure links. However, encrypted VPN is no longer suitable for today's remote clients, modern networks, and virtual infrastructures. Zero Trust Network Access (ZTNA) solutions are emerging to address the requirements of today's modern remote clients, while protection of physical and virtual network links continue to be implemented with legacy security techniques such as IPSec and MACSec. Zero Trust security, coupled with high efficiency and performance, are no longer optional requirements for critical network infrastructures and ominous pathways to the cloud. This paper presents a solution for implementing quantum-resistant, BYOE security for virtual and physical network infrastructures to physical and virtual endpoints.

ABOUT THE AUTHOR

Joseph Warren is Director of Viasat's Secure Networks Program business. Mr. Warren has more than 20 years of experience bringing data security solutions to market. Prior to his role at Viasat, Mr. Warren managed biometric, key management, and wireless LAN security solutions for commercial and U.S. military applications including the world's first WiFi solution certified to transmit U.S. classified data.

Implementing Zero Trust Principles to Data in Motion for Improved Security and Performance over Physical and Virtual Networks

Joseph Warren
Thales Cloud Protection and Licensing
Plantation, FL
Joe.Warren@ThalesGroup.com

INTRODUCTION

Today's networks are an endless array of wired, wireless, and software defined network connections. Together with diverse endpoints requiring everything from remote client access to high capacity site-to-site and site-to-cloud connections, securing network access and network pathways is a profound challenge to IT professionals. The advent of Cloud Services and AI routing techniques have placed even more demands on the methods used to secure the delivery of data. While IPSec/VPN has handled both secure client-side network access and bulk encryption for critical network links, VPN is no longer suitable for today's modern applications. Zero Trust Network Access (ZTNA) solutions are now available to address the deficiencies of VPN for remote users. These ZTNA solutions are more secure and more transport efficient than VPN. However, these solutions do not address requirements for bulk encryption of critical, high capacity links. Unlike VPN, ZTNA does not address both single-user network access and high capacity critical network connections. The Zero Trust concept requires a different approach for high capacity corporate networks communicating over an uncontrolled wide area network. In order to implement Zero Trust security and solve performance deficiencies of VPN, MPLS, and MACsec, security must be addressed separately from the transport layers.

SECURITY AND PERFORMANCE TO THE CLOUD

In an effort to reduce critical link transport inefficiencies of traditional IP connections to the cloud, Cloud Service Providers (CSPs) offer low latency connections through close proximity on-ramps that present themselves in the form of a Virtual Private Network, or an MPLS link in which layer-specific security solutions can be added. Security for these services are somewhat a patchwork of solutions based on the transport layer. Essentially, the transport layer dictates the security solutions. In some cases, a simple, unencrypted Virtual "Private" Network is the solution. However, one must be certain to understand the distinction between "Privacy" and "Security". For example, we can achieve privacy in a home by shutting the doors and lowering the window shades. However, this does not actually secure the home; it only provides privacy. To secure a home, windows and doors must have unbreakable locks with unbreakable glass, and the keys to those locks must be in the control of the homeowner at all times. Although Encrypted VPN is today's go-to solution for layer 3 data in motion security, it requires a high amount of transport overhead and provides little to no controls over the key material. Transport overhead and control over key material are two of the most important ingredients for providing zero trust principles that enable excellent performance with auditable security for all pathways to, and within, the physical and virtual network infrastructure

When applying a Zero Trust model to a high capacity network link, one must separately examine the terms "data", and "transport". Data is something that is very important to the owner. One can think of data as a bar of gold. When the owner of the gold wants to transport it to another place, the owner wants to ensure the gold is secure during its journey. The owner does not want to give anyone else access to the security. Additionally, the owner does not necessarily care whether the delivery service uses a big truck, a small car, an airplane or a helicopter. At the same time, the transport service does not want to be responsible for managing the security of that gold. The transport service is concerned with receiving a package and getting it to the final destination as quickly and efficiently as possible. Trouble occurs when the two concerns (security and transport) are in conflict of each other. This is the case of encrypted VPN. The conflict occurs when security requires interaction with the protocol layer. To resolve the conflict, data security and transport efficiency must reach a happy medium. This is required to ensure that the owner of the gold provides the best possible security without burdening the transport service with unnecessary weight that would flatten the truck's tires or prevent the airplane from taking off. This analogy works well when applied to securing high capacity critical links, especially virtual pathways to the cloud. Let us look at the way we store data in the cloud, otherwise known as "data at rest". When storing the bars of gold in the cloud, many companies leverage solutions

such as "Bring Your Own Encryption" (BYOE). BYOE enables the owner of the data to store their data in someone else's home (the cloud), while maintaining full control of the security of the data (the keys, the root of trust). It represents the best scenario for both parties since the cloud provider can concentrate on what it does best, which is storing data, while the data owner maintains control of the security. This system works well when applied to the dichotomy of data owner vs. service provider requirements for data at rest. To gain these same benefits for data in motion, a similar method would apply to the network link. IPSec does not meet these diverse owner/provider requirements. In fact, IPSec fails both the data owner and the service provider.

Why IPSec/VPN Fails both the Data Owner and the Service Provider

Today, IPSec is largely the default selection for securing almost all Layer 3 and Layer 4 pathways to the cloud. For some applications, such as single client remote access, IPSec/VPN might make sense, although ZTNA solutions are more suitable for modern applications, especially those running in the cloud. For other use cases, especially critical infrastructure and pathways to the cloud, IPSec/VPN is not a prudent choice. To begin with, IPSec/VPN is not efficient. It adds around 30% overhead on average to the transport layer. At smaller packet sizes, it adds as much as 60% to 70% overhead to the transport layer. This is an extreme burden on the transport layer. It forces the data delivery service to carry a lot of excess baggage that causes poor performance and a need for greater capacity. In some cases, the delivery service vehicle is not large enough to accommodate the excess baggage (MTU size limits) and the gold must be split in two pieces (data fragmentation) and carried by two vehicles, both of which require the excess security baggage. For the data owner, IPSec requires third party certificate authorities for the root of trust. In many cases, network administrators manage this root of trust, rather than the data owners. Referring back to our gold transport analogy, IPSec is akin to the owner of the gold handing it off to the transport company on a handshake with the promise that "someone else" will meet the security requirements. The owner has no control over the security of the gold. Additionally, who knows what the transport company will do? Maybe they will decide not to secure the data in an effort to get to the destination as quickly as possible. It is certainly not a zero trust model since the data owner does not have auditable control of the security. If the gold is missing, who exactly is responsible for the breach? As stated earlier, when it comes to securing the critical infrastructure, both security ownership and transport efficiency must be in check. In addition to being in check, the ownership and management of each must be separate functions (separation of duties). This ensures that provisioning of the best security with the most efficient transport and the identification of respective ownership for each are verifiable.

IPSec/VPN Transport Deficiencies

The IPSec standard has been around for quite a while. In basic terms, IPSec requires the establishment of "sessions" between sites, also known as tunnels. The more interconnected sites there are within the critical infrastructure, the greater the number of tunnels and each must be aware of every other site. The larger the network infrastructure, the more complex the tunnel configuration and management is. From an implementation and management perspective, this is why IPSec is better suited for single-user remote access than it is for large critical infrastructures. Management of a large-scale tunnel deployment is cumbersome and requires headcount to manage and monitor these session-based connections. In addition to the burden of tunnels, IPSec burdens the transport layer with a tremendous amount of overhead. The amount of overhead is approximately 30% on average. We calculate the percentage of overhead as a ratio of overhead to packet size. While IPSec overhead is somewhat stagnant, packet sizes can vary tremendously. For example, small Voice or Video packets will require the same amount of overhead as a large data packet or even a jumbo frame. In the case of voice and video, IPSec overhead can be as high as 70% of the total packet size. The basic diagram in Figure 1 below illustrates the amount of overhead that IPSec can inject into a UDP packet.

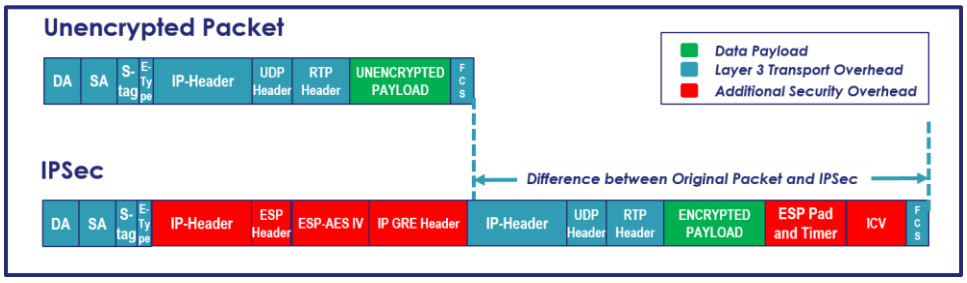

Figure 1 – Packet Size Comparison of unencrypted packet vs. VPN encrypted Packet

THE TRUE COST OF IPSEC IN THE CLOUD

When moving data to the cloud, there are many "pay as you go" and "capacity on demand" services that cause fluctuations in the overall bill. As an example, cloud providers charge for storing data. When signing up to these data storage services, many customers do not realize that there may also be a charge to move that data. The term "data egress fee" is sometimes applied to the fee placed on data that is moving out of the Virtual Private Cloud (VPC) environment. This charge might also occur even when moving data within the cloud in addition to moving data between public and private clouds. Regardless of whether or not a fee is charged, the amount of overhead that applies to each Gigabyte of egress data scales with usage and certainly affects network efficiency. When data is put into motion, we must account not only for the data itself, but also the transport overhead required to move data to its final destination. Let us examine a scenario where one might store 1 Terabyte of data in the cloud. Now let us say that you want to move that data from your cloud provider to another data center. We must add TCP/IP overhead to each packet once that data is set into motion. Let us assume that it works out to be about 8% or so of extra overhead depending on the packet size. So moving that data will require you to move 1TB of data plus the 8% TCP/IP overhead it needs to get the data to its final destination. If you want to secure that link from the cloud to the data center using VPN, approximately 30% of additional overhead is required to secure and transport the data. To move 1TB of data through an IPSec encrypted tunnel now incurs about 1.4TB of data egress fees to accommodate all of the transport and security protocol overhead

The Burden of Overhead

Granted, there really is no way to eliminate TCP/IP overhead when moving data over a Layer 3 network, so we can label that overhead as table stakes. However, adding 30% additional overhead to secure that data definitely adds significant overhead, and potentially cost in terms of data egress fees. Let us look at a 1Gbps connection between a customer site and the cloud. Certainly, the connection would not run at 100% capacity 24 hours a day, 7 days per week. Instead, we will examine a more realistic usage model, say 25% total usage. A 1Gbps link operating at 25% capacity per day would pass approximately 985,500 GB of data (including transport overhead) in a year over an unencrypted network. If one were to secure that same link using Encrypted VPN, an additional 30% IPSec overhead is required, resulting in an additional 295,650 GB per year just in overhead data. The result is an additional 30% per year increase in total data transfer to accommodate the VPN overhead (see Figure 2 below). Adding VPN results in a 30% overall increase in overhead and is a largely an inefficient use of precious bandwidth.

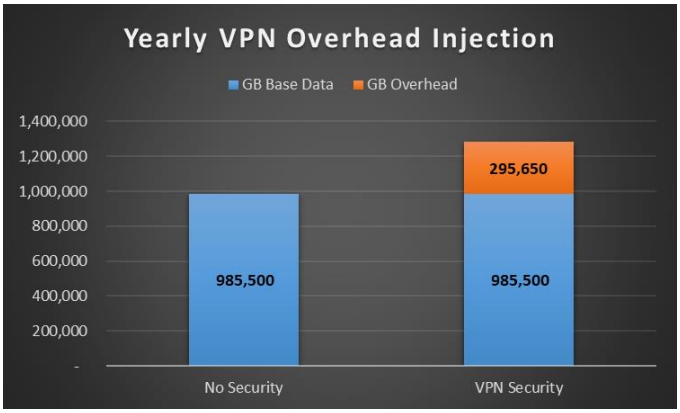

Figure 2 – Assumes 1Gbps link operating at 25% capacity.

BRING YOUR OWN ENCRYPTION – A MODERN APPROACH TO ZERO TRUST SECURITY

Transport Efficiency

Today's networks consist of a wide array of protocols and capabilities. MacSec for Layer 2 connections, MPLS for Layer 2.5, IPSec for Layer 3 and Layer 4, Artificial Intelligence Routing, Software Defined Networks, 5G, and satellite networks are just a few of the unlimited variety of networks and mediums. Each of these connection types are tethered to layer-specific security, some of which require single vendor, single provider end-to-end connections. This patchwork of protocol dependent (and sometimes vendor dependent) solutions certainly limits both connectivity and data security and greatly burdens manageability. Today's global connectivity is a menagerie of service providers, equipment providers, and diverse connections. Leveraging traditional security solutions, end-to-end security cannot

be guaranteed and certainly is not auditable. The coupling of security to transport layer stymies the concept of "separation of duties" between the administration of network security and network management functions. The best way to address the two conflicting interests of data security and data transport are to separate them from each other. By moving the encryption intelligence to the endpoints and controlling the root of trust, a formidable, quantum resistant security solution with unconstrained transport results. The insertion of a small instruction packet is the only requirement to provide the endpoints with the information needed to perform encryption and decryption functions while continuing to meet today's security certification requirements (see Figure 3). Insertion of this small instruction set, or shim, does not affect any standard or proprietary transport techniques (such as PEP, AI Routing, QoS, etc) and adds only 5% overhead to the original packet size. This technique enables the network to do what it does best, which is efficient routing and switching. It also provides a mechanism for providing the Zero Trust principles of Bring Your Own Encryption to the payload as addressed hereafter.

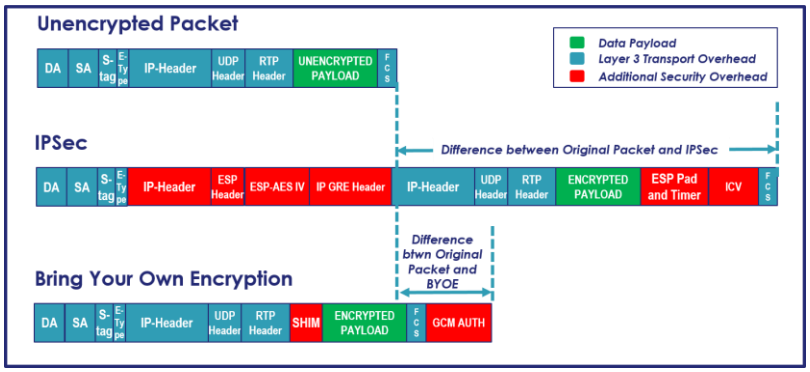

Figure 3 – Packet Size Comparisons: Unencrypted vs. IPSec vs. BYOE

Zero Trust Security Model

With the establishment that we can move security functions to the endpoints without affecting the transport layer, let us examine a Zero Trust security model for data in motion. To begin with, elimination of third party certificate authorities is necessary. The Zero Trust solution must be able to store its root of trust and key material within a FIPS 140-2 Level 3 hardware boundary whether on-prem or as a service. The important factor is that the root of trust and key material is in the auditable control of the data owner with no other outside entity able to gain access. This ensures that only the appropriate responsible entity can provide credentials to the endpoint, enabling them to encrypt and decrypt the transmitted and received data. No matter what path the data takes, no matter which layer the data requires, no matter which carrier the network lease resides, no matter what protocol enhancement techniques are used, and no matter where the credentialed endpoints may exist, the data travelling over these network paths are secure. The delivery of this Zero Trust data in motion security solution secures most any infrastructure including low-latency cloud on-ramp solutions such as Direct Connect and Express Route since there are no protocol dependencies. It can also be implemented over completely uncontrolled IP connections to the cloud as well as within the cloud (VPC to VPC) and between cloud providers. The result is a high performance, closed network with auditable security over all physical and virtual infrastructure links.

BRING YOUR OWN ENCRYPTION VS. IPSEC/VPN

As Zero Trust Network Access solutions for remote clients get deployed to solve the inadequacies of VPN, so too must a Zero Trust model be implemented on high-capacity infrastructure pathways to the cloud. Figure 4 shows just a few comparative benefits of Zero Trust Security as it compares to the 25-year-old VPN solution.

Capability	IPSec/VPN	BYOE
Overhead	30%	5%
Elimination of Security Associations (Tunnels)	No	Yes
Quantum Resistant	No	Yes
Elimination of Third Party Dependencies	No	Yes
Auditable Chain of Custody for Root of Trust	No	Yes
BYOE to Network Connections	No	Yes
End to End Security regardless of infrastructure	No	Yes
Separation of Duties	No	Yes

Figure 4 – IPSec vs. BYOE

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 are moving on premise or, in the very least, outside the CSP infrastructure, so that data can be stored safely on remote servers 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 root of trust. Control and ownership over the root of trust is now an on premise function, 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 the root of trust for data links, whether it is on-prem to on-prem, on-prem to cloud, cloud-to-cloud, or east-west data within the data center (See Figure 5).

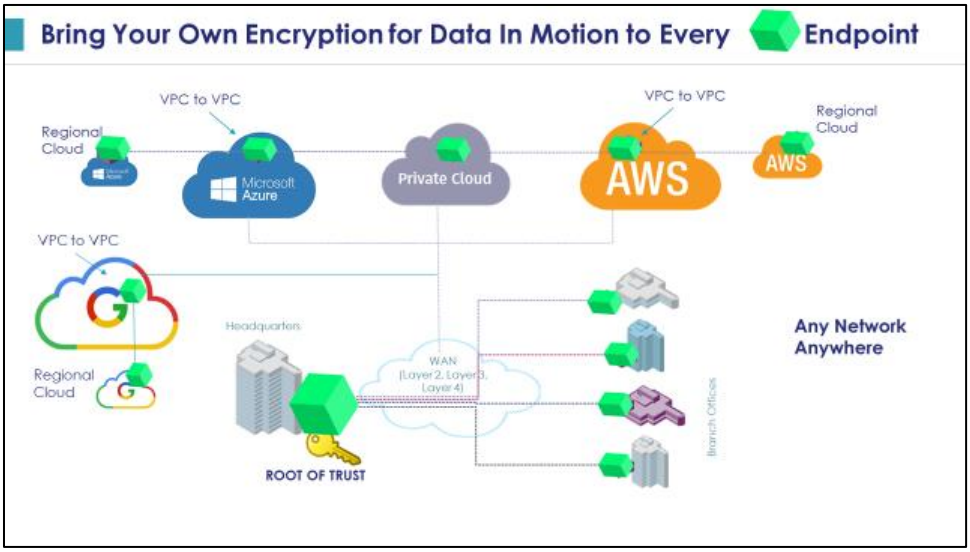

Figure 5 – Implementation of a Zero Trust Network through an unsecured WAN

Crypto Agility and Quantum Threats

The term crypto agility is important as it relates to a variety of independent security requirements. IPsec is deployed with traditional AES-256 algorithms using standard, globally available certificate authorities. When it comes to custom crypto requirements, IPSec solutions are stuck in the 1990s. VPN does not normally allow for hardened key delivery systems, Quantum Key Delivery systems, Quantum Random Number Generation, or an internally secured root of trust. Asymmetric encryption techniques used by solutions such as ASIC-based IPSec and MACSec devices, will require new hardware for the implementation of quantum algorithms. The eventual impact of Quantum threats will require forklift equipment changes in order to meet this inevitable threat. The BYOE architecture proposed in this paper leverages symmetric encryption, AES256 algorithms, and the elimination of third party certificates, which is recognized as quantum resistant today (Rao, Mahto, Yadav and Khan, 2021). As the world moves more and more toward new connections types including satellite, 5G, SDWAN and others, it is senseless to continue to implement 20th Century security techniques into 21st Century networks.

Separation of Duties

Data in motion security solutions often overlook the aspect of separation of duties. Because IPsec is bound to the transport layer and embedded into traditional network equipment, it is impractical to separate the administration of security from the administration of the network. 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 monitor and tune the network performance. 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 ensure that the achievement of both high levels of security and performance are independently manageable.

Data Transport Efficiency Comparisons: IPSec vs. Bring Your Own Encryption

Applying Zero Trust principles to the network connection provides improved security and better efficiency. As described earlier in our Zero Trust model, the implementation would add only about 5% additional overhead to the transport layer as compared to 30% overhead for IPSec. Figure 6 compares the amount of data moving over a 1Gbps link operating at just 25% capacity over the course of a year. The base data usage amount calculates to be about 985,000 GB per year. Adding IPSec/VPN security to that same link would add 30% overhead and bring the amount to almost 1,300,000 GB per year. Comparing that to the proposed Zero Trust solution which adds only 5% overhead, the total amount of data usage would be less than 1,035,000 GB per year. The proposed Zero Trust model achieves 25% improved efficiency over IPSec/VPN in addition to providing improved security.

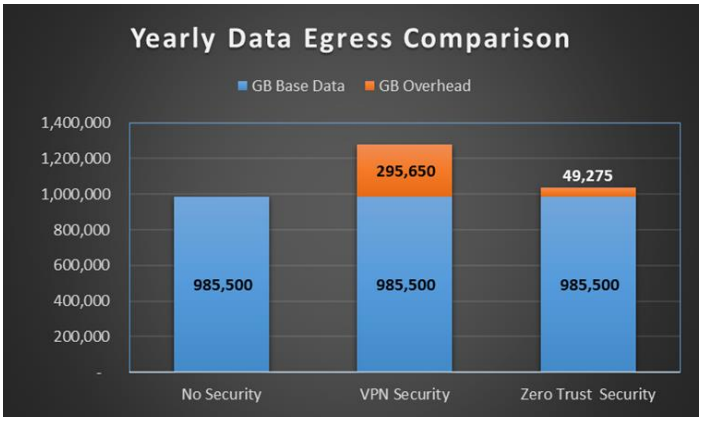

Figure 6 – Assumes 1Gbps link operating at 25% capacity.

THE BENEFITS OF A BRING YOUR OWN ENCRYPTION, DATA IN MOTION SECURITY ARCHITECTURE

Greater Security

The ability to provide controls and ownership of data in motion security is the primary rationale behind the Zero Trust model. Providing these capabilities, independent of network constraints, guarantees auditable security ownership from Point A all the way to Point B without any transport constraints. Protocols, network vendor equipment, and service providers can all be in the mix without transport concerns. Quantum resistance provides for solution longevity and fits 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 part of this upgradeable framework.

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 (see Figure 7). The comparative results in Figure 7 (Thales CPL, 2021) show a dramatic improvement in terms of bandwidth efficiency, latency, and jitter. It is clear that reduced overhead, and therefore packet size, helps to reduce latency and jitter since there is less data to encrypt and decrypt. Additionally, the IPSec solutions are multipurpose devices (Weberblog.net, 2022). The processor is shared in order to maintain

routing tables and/or firewall rules, in addition to encrypting and decrypting data. A single-purpose, non-transport-dependent BYOE capability has only a single dedicated function, which is to encrypt and decrypt data. With a 25% average overhead reduction as compared to IPsec, BYOE is clearly the modern data in motion security solution required to meet the security and performance demands of today's networks and cloud endpoints.

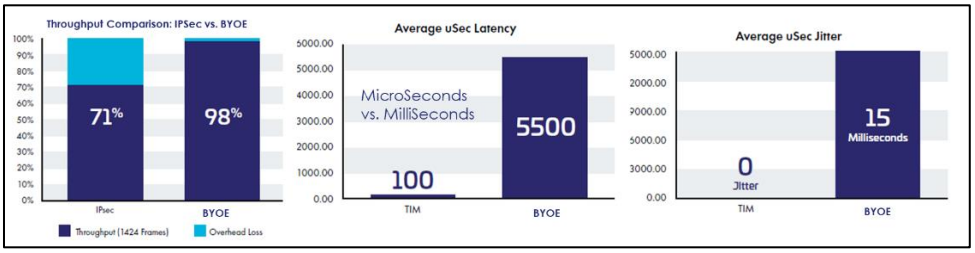

Figure 7 – Performance Comparison of IPSec vs. BYOE

Enhanced Connectivity

The placement of security intelligence at endpoints and the abstraction of security from the protocol layer enables complete independence from all transport dependencies, including service providers and equipment vendors. Mixing of network equipment providers, data handoffs between network service providers, movement between diverse cloud service providers, and traversal across multi-domain infrastructures with complete end-to-end security is only possible with protocol independence. Take, for example, a dataflow that utilizes an adversarial network or network equipment provider. Rather than being forced to share credentials with adversaries, the data is secured at its point of origin. Transport of the secure data passes unimpeded and without security dependencies. The data is secured with zero security dependencies. And since it is a single purpose security capability, encryption can be placed at any location without a need to change network architectures. If deep packet inspection is necessary, the decryption can occur immediately prior to a firewall handoff. Since end-to-end data transport security is provided, data can be passed between locations with zero trust between sites. GCM and optional Quantum-based data integrity checks can be used to eliminate man in the middle attacks. And since symmetric, AES256 encryption with a controlled root of trust is quantum resistant, there are no concerns over data mining for future use when Quantum Computing becomes mainstream.

Auditable Chain of Custody

Root of trust and key ownership can be maintained leveraging modern BYOK and BYOE hardware and/or services, including integration with external Hardware Security Module (HSM) and other FIPS 140-2 Level 3 certified, tamper resistant boundaries. With controls over security being limited to endpoints, access to and storage of crypto keys can be owned, managed, and contained. No one person or entity can decrypt data as it traverses through exponential variations in network equipment (including adversarial equipment providers), carriers, and service providers without the knowledge of the data owner and the assertion and confirmation of data integrity checks. There is only one entity in control of the root of trust for the encrypted data, while a multitude of entities are involved in the transport of that secure data.

CONCLUSION

Modern networks and cloud infrastructures have changed the way the world connects, computes, and stores data. The evolution of these new capabilities requires intelligent techniques to ensure security ownership of physical and virtual connections without impeding network performance and connectivity. It is time to discard relic security solutions of the past and prepare for the next generation of network connectivity. Separation of security from transport provides for the highest levels of security controls with the least amount of reliance on network topologies, equipment vendors, and ever-evolving transport methods. The BYOE architecture proposed in this paper is a future-proofed model needed to meet the demands of today's virtual and physical network infrastructures.

REFERENCES

Rao, Mahto, Yadav and Khan (2021). *The AES-256 Cryptosystem Resists Quantum Attacks*, https://www.researchgate.net/profile/Sandeep-Rao-4/publication/316284124_The_AES-256_Cryptosystem_Resists_Quantum_Attacks/links/58f999200f7e9ba3ba4d22b1/The-AES-256-Cryptosystem-Resists-Quantum-Attacks.pdf

Weberblog.net (2022). *Fortigate VPN Speedtests*, https://weberblog.net/fortigate-vpn-speedtests/

Thales CPL (2021). *Data In Motion Security Through a 5G Infrastructure*, https://cpl.thalesgroup.com/resources/encryption/data-in-motion-security-through-5g-infrastructure-white-paper