Miercom

July 2024

DR240109I

THALES

Miercom Independent Report on Thales Network Encryption Solutions

Table of Contents

1.0 Executive Summary

Thales engaged Miercom to conduct an independent review of their High Speed Encryption (HSE) network technologies. The devices tested were the Thales CN6140 Multilink Network Encryptor (CN6140) and the Thales CN4010 Network Encryptor (CN4010). Testing was comprised of throughput performance and data integrity tests to show the benefit of HSE employed in an enterprise with a preexisting network with a firewall. Overall, Thales HSE demonstrated greater efficiency and cost-effectiveness in encrypted performance compared to upgrading legacy firewall products to equivalent capacity. The findings showed that adding HSE to the network and disabling IPSec in fact reduce latency and jitter on the network that was resulting from the firewall, ultimately providing better network efficiency, stability, and security overall. HSE is vendor agnostic, and easily integrates into existing network architectures, making it a superior solution across the board for customers seeking to get the optimum return on investment for their network performance and security.

Key Findings:

- Bidirectional throughput testing proved the Thales CN6140 Multilink Network Encryptor (CN6140) capable of an average of 31.6% better performance than the same firewall using IPsec encryption in Unified Threat Management (UTM) mode at 10 Gbps. IPsec throughput was only 76% of the available link capacity, which is gated by the firewall throughput, meaning that 24% of the available bandwidth is not accessible. HSE encrypted throughput shown is 99.8% of the maximum link capacity, which is gated by the firewall throughput. The required encryption overhead causes the 0.2% loss. The throughput of CN6140 could operate at near the full 10G link capacity if a higher performance firewall was used.
- Bidirectional throughput testing proved the Thales CN4010 Network Encryptor (CN4010) capable of an average of 21.6% better performance than the same firewall using IPsec encryption in UTM mode at 1 Gbps. IPsec throughput was only 82% of the available link capacity, which is gated by the firewall throughput, meaning that 18% of the available bandwidth is not accessible. HSE encrypted throughput shown is 99.8% of the maximum link capacity, which is gated by the firewall throughput. The required encryption overhead causes the 0.2% loss. The throughput of CN4010 could operate at near the full 1G link capacity if a higher performance firewall were used.
- Bidirectional throughput testing proved Thales HSE appliances show no degradation of performance compared to firewall performance with encryption enabled. Thales encrypted throughput performance had an improvement of 21 – 31% compared to the firewall providing the encryption.

- Thales HSE appliances proved in testing no noticeable increase in latency. Both the CN6140 and CN4010 add less than ten microseconds of latency. While the higher end Fortinet firewalls did not add as much latency as the lower end firewall, using the CN4010 with IPsec disabled proved a 48% decrease in jitter and a 15% decrease in latency compared to those measured when using the firewall with IPsec encryption enabled. The findings showed that adding HSE to the network and disabling IPSec in fact reduce latency and jitter on the network overall that was resulting from the firewall with IPsec enabled.
- The Thales CN6140 and CN4010 solutions additionally showed an improvement in secure data transport, reducing data loss compared to that of the firewall using IPsec encryption with all security features enabled on the firewall.
- Thales HSE network encryption appliances achieved ZERO application transaction failures. No throughput or latency degradation was detectable with an enterprise mix of traffic (EMIX).
- Thales HSE appliances resulted in 1.5% less frame loss than the firewall deployed with IPsec. IPsec at times proved to over subscribe firewall resources including processor and memory allocation. Adding the HSE encryptor and disabling IPsec proved more reliable transport by offloading encryption processing from the firewall.
- Key management feature enhances secure data transport by automating key rotation which allows enterprises to improve data security and IT efficiency. This is a unique feature we found in HSE encryptors that we have not found available on NGFW products alone.

Miercom Engineers proved in hands-on testing of the CN6140 Multilink Network Encryptor and CN4010 Network Encryptor that the Thales security products delivered exceptional efficacy and superior encrypted throughput performance. The high-speed encryption provided by Thales HSE solution proves greater security and encryption performance than IPsec encryption. Based on these findings, Thales is awarded Miercom Certified Secure.

Congratulations Thales for achieving ***Miercom Certified Secure***."

Rob Smithers CEO, Miercom

2.0 Products Evaluated

Firewall encryption is resource intensive. Thales High Speed Encryption (HSE) appliances provide secure dedicated data encryption to eliminate strain on firewalls, allowing for better throughput performance and encryption without the need to upgrade the firewall, and even enable improved firewall performance.

Thales HSE product features:

- Protocol and application transparent
- Encrypts Unicast, Multicast, and Broadcast traffic
- Flexible encryption policy engine
- Per packet confidentiality and integrity with AES-GCM encryption
- Automatic key management
- Automatic network discovery and connection establishment
- Support for Jumbo frames
- Tamper resistant and evident enclosure, anti-probing barriers
- Hot swappable cooling fans
- Front panel access

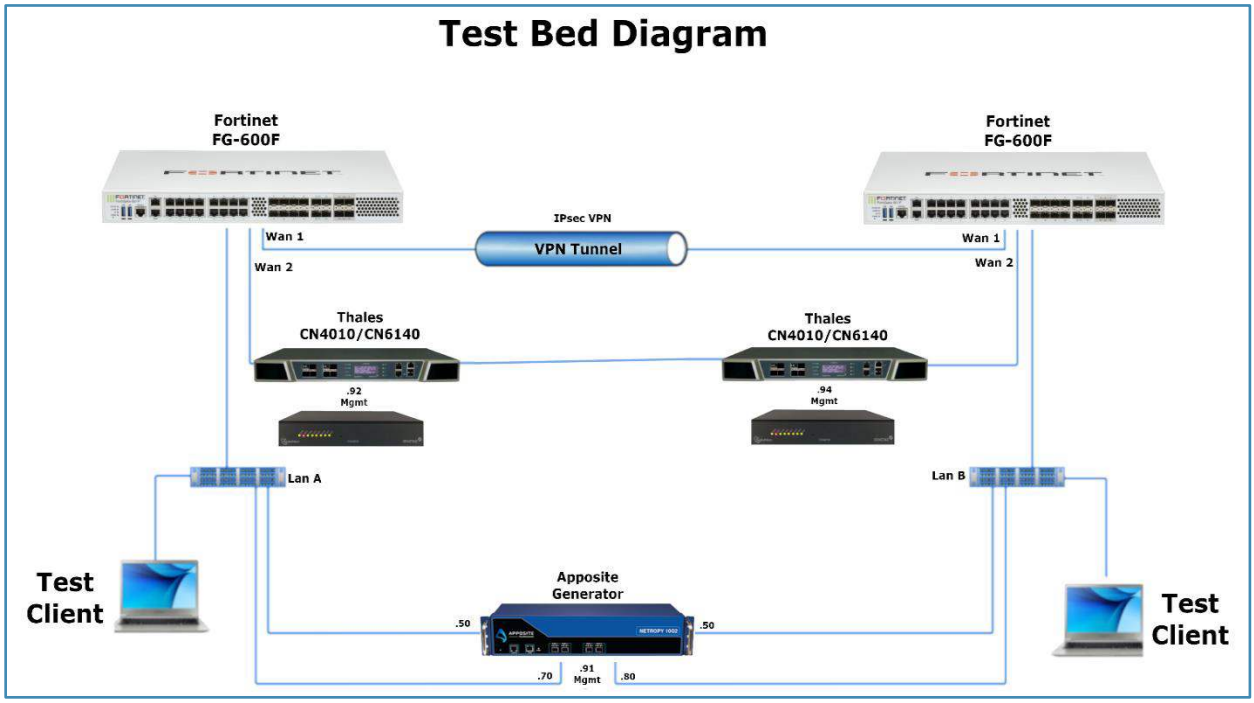
Thales CN6140 Multilink Network Encryptor

The CN6140 is a multi-port, high assurance encryptor that provides up to 40 Gbps (4x10) full line rate encryption for all communications including voice, video, and data.

Thales CN4010 Network Encryptor

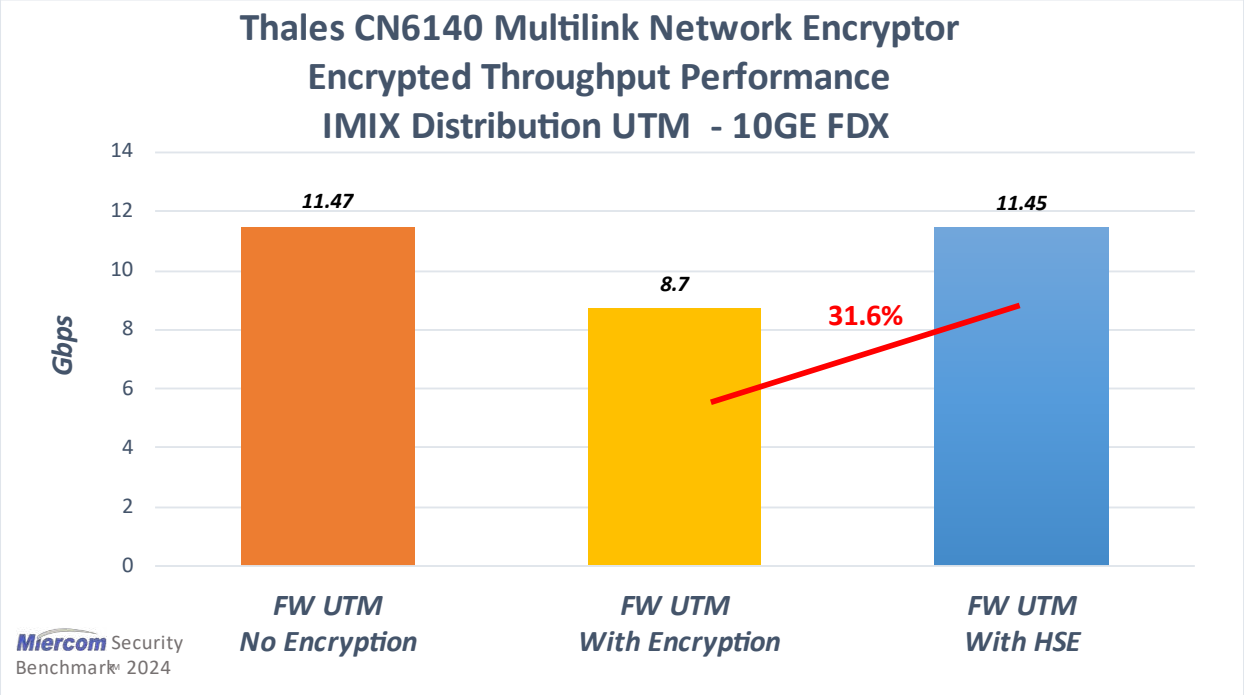
The CN4010 is designed for organizations with lower speed links, up to 1 Gbps network needs, and a small footprint, for all communications including voice, video and data.

3.0 How We Did It



The above diagram shows the Thales HSE between two Fortinet firewalls. Testing was repeated using the Thales CN6140 and Thales CN4010 models. Network load traffic was provided using an Apposite Traffic Generator (www.apposite-tech.com) using standard RFC 2544 as well as traffic distribution configured for IMIX (Internet Mix 7-64Byte, 4-512Byte, 1-1518 Byte Frame). The Firewalls were configured in full UTM mode (security features enabled). We tested first with the firewalls providing the IPsec encrypted tunnel (upper path VPN tunnel). We then repeated testing connecting the firewalls to the HSEs allowing those devices to provide the encryption. We compared these results of the encryption performance throughput.

4.0 CN6140 Multilink Network Encryptor Throughput Performance



Thales CN6140 Multilink Network Encryptor proved 31.6% better encrypted throughput than the firewall tested provides alone. Offloading the encryption from the firewall reduced the memory consumption by 25% and CPU process utilization by 35%. These resources can then be reallocated to providing advanced security protection features. Thales HSE enables the firewall to do what the firewall should be doing - protecting your network. Test above was single port pair full duplex 10GE (20 Gbps maximum)

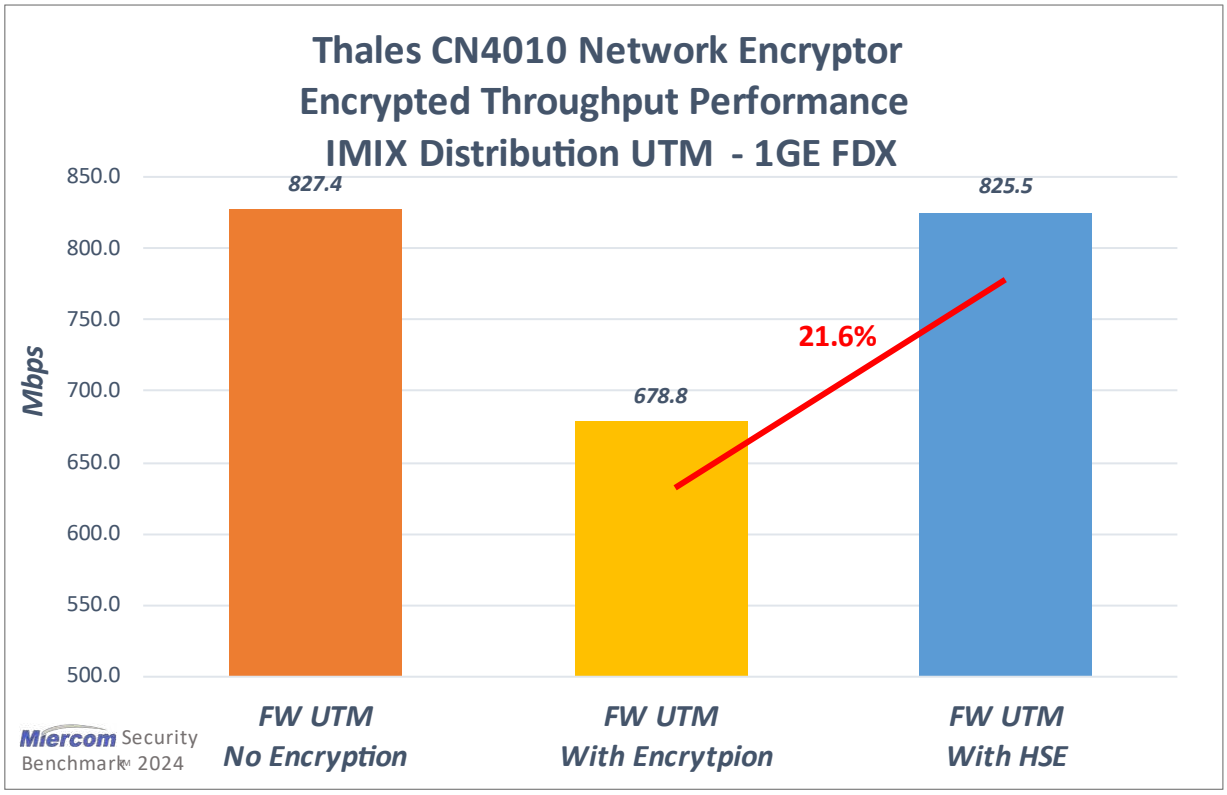
Protected firewall throughput is measured with full unified threat management (UTM) to include application awareness, malware detection, web filtering and deep packet inspection. This testing was conducted using a Fortinet FG-600F NGFW.

When baseline testing was conducted on the firewall without the Thales HSE, Miercom observed IPsec throughput capable of 76% of the available full link capacity, meaning that 24% of the available bandwidth is not accessible. When baseline testing Thales HSE solution, we observed 99.8% throughput of the maximum link capacity. The test results depicted above illustrate that when the Thales HSE is employed we achieve the overall best encrypted throughput although still gated by the firewall's ability to provide protected firewall throughput (Compare the orange to blue in the bar chart above). The 0.2% loss comparing throughput (orange to blue) is attributable to normal encryption overhead. The throughput

of CN6140 could operate at near the full 10GE link capacity (20Gbps FDX) if a higher performance firewall was used.

The cost to forklift upgrade firewalls to the next model with sufficient capacity can be as high as US$65,000. The same or better encrypted throughput performance can be achieved with the CN6140 for a significantly lower cost.

5.0 CN4010 Network Encryptor Throughput Performance



The Thales CN4010 Network Encryptor proved 21.6% better encrypted throughput performance than a firewall provides alone. Offloading the encryption from the firewall reduced the firewall memory and CPU process by 35% that could be reallocated to providing security protection features. This allows the firewall to do what the firewall should be doing - protecting your network.

As previously mentioned is baseline testing Miercom observed IPsec encryption reduces network throughput by over 24% compared to baseline UTM performance. In contrast, Thales HSE encryption maintains virtually identical throughput, significantly minimizing security overhead. This emphasizes the substantial performance penalty associated with IPsec encryption and highlights how Thales HSE effectively reduces this slowdown, ensuring secure and efficient network operations.

Protected firewall throughput is measured with full unified threat management (UTM) to include application awareness, malware detection, web filtering and deep packet inspection. This testing was conducted using a Fortinet FG-60F NGFW.

IPsec throughput was only 82% of the available link capacity, which is gated by the firewall throughput, meaning that 18% of the available bandwidth is not accessible.

HSE encrypted throughput shown is 99.8% of the maximum link capacity, which is gated by the firewall throughput. The required encryption overhead causes the 0.2% loss.

The throughput of CN4010 could operate at near the full 1G link capacity if a higher performance firewall was used.

The cost to forklift upgrade firewalls for this class product to the next model with sufficient throughput capacity can be as high as US$25,000.

Additionally using the CN4010 with IPsec disabled proved a 48% decrease in jitter and a 15% decrease in latency compared to those measured when using the firewall with IPsec encryption enabled. The findings showed that adding HSE to the network and disabling IPSec in fact reduce latency and jitter on the network that was resulting from the firewall, ultimately providing better network efficiency, stability, and security overall.

6.0 Encryption

Thales HSE appliances are preferred by the world's most secure organizations. They support standards-based, end-to-end authenticated encryption and client-side key management. Advanced crypto-agile security features include traffic flow security, support for a wide range of elliptic curves (Safe Curves, Brainpool, NIST). VLAN based encryption provides unique key pairs in hub and spoke environments to protect against misconfigured traffic. For high-assurance environments, the encryptors also support nested encryption.

Thales HSEs are certified by NIST – FIPS 140-2 Level 3, in process for FIPS 140-3, and certified by ANSSI – Common Criteria EAL 4+ and have been vetted by the US Department of Defense Information Systems Agency and by NATO, among others. Thales HSEs uphold security best practices such as authenticated end-to-end encryption, automated key generation and updates, and controlled access (separation of duties). Crypto-agile, Thales HSEs are quantum ready, and offer field upgradeable support for all four NIST PQC (Post Quantum Crypto) algorithm finalists, and more as they evolve.

7.0 Latency

Both the CN6140 and the CN4010 operate with a latency of less than 10 microseconds per encryptor. Miercom testing showed no noticeable increase in latency when encrypting data with Thales appliances rather than the firewall. While the higher end Fortinet firewalls did not add as much latency as the lower end firewall, using the CN4010 with IPsec disabled proved a 48% decrease in jitter and a 15% decrease in latency compared to those measured when using the firewall with IPsec encryption enabled. The findings showed that adding HSE to the network and disabling IPSec in fact reduce latency and jitter on the network overall that was resulting from the firewall with IPsec enabled.

8.0 Cost Benefit

Thales HSE appliances offer significant savings over firewall upgrades, particularly when taking licensing costs over time into consideration, as well as the added cost for upgrading to a higher capacity firewall.

The cost of upgrading from the Fortinet FG-600F to the Fortinet FG-1000F could cost up to US$44,241 for the hardware and an additional US$188,024 for five years, or US$37,604 per year, in licensing and support costs, according to pricing quoted by the vendor. The list price of US$40,000 for the CN6140 hardware is less than the Fortinet product. With licensing costs for the FG-600F remaining US$15,460 per year, savings can be up to **US$22,800** per year in licensing expenses by encrypting with the CN6140 rather than upgrading the firewall to the FG-1000F. The Thales CN6140 offers savings of 42.2% per protected Gb.

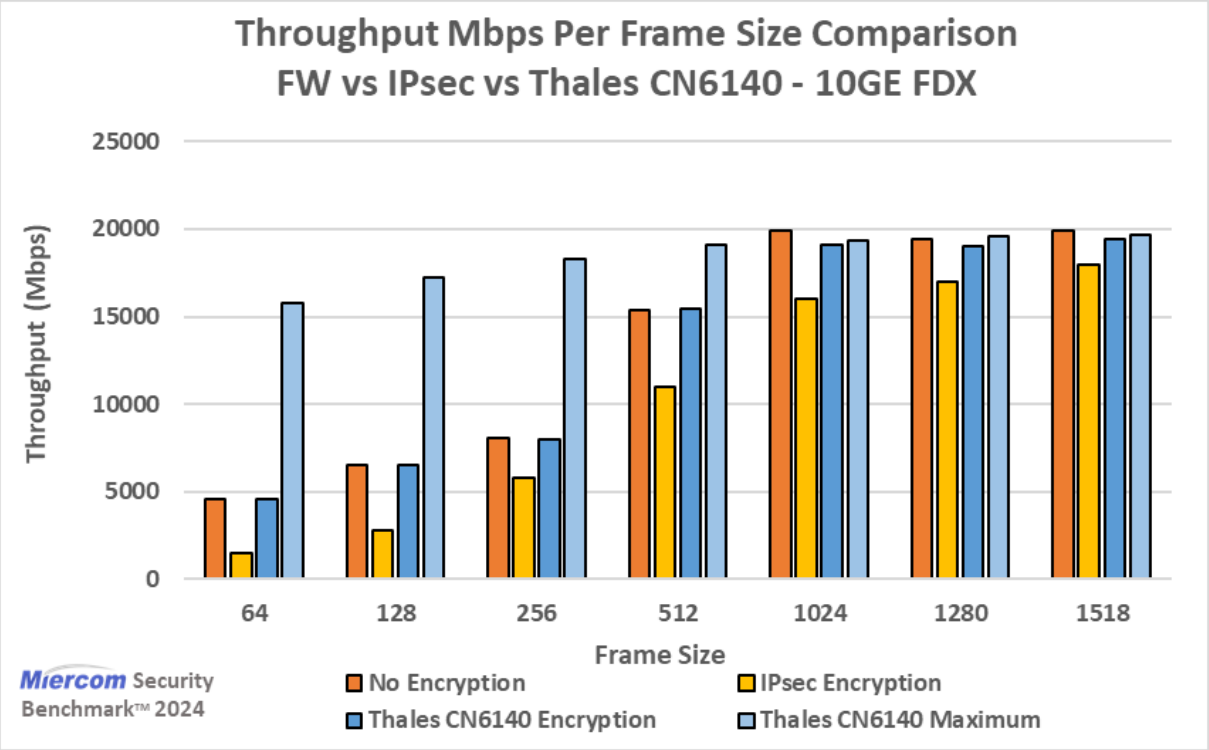
The CN4010 costs US$10,000, which is comparable to the cost of upgrading the firewall from the Fortinet FG-60F to the Fortinet FG-90G when considering the increased licensing expenses, not to mention the overheads involved in upgrade configuration, forklift upgrade, architectural changes, and the cost of the bandwidth itself. However, you could save up to **US$1,325** per year in licensing expenses alone, not to mention the associated costs and performance and security enhancements, therefore making the CN4010 the more cost-effective option especially if you do not plan to do a more significant upgrade.

	FG-60F + CN4010	FG-90G	FG-600F + CN6140	FG-1000F
Average Throughput with Services Enabled (Mbps)	825	750	11450	13000
Total Cost of Ownership (1 Year)	$ 10,000.00	$ 3,977.50	$ 40,000.00	$ 81,845.85
TCO per Protected Mbps (1 Year)	$ 12.12	$ 5.30	$ 3.49	$ 6.30
Total Cost of Ownership (5 Years)	$ 10,000.00	$11,287.50	$ 40,000.00	$232,265.25
TCO per Protected Mbps (5 Years)	$ 12.12	$ 15.05	$ 3.49	$ 17.87

9.0 RFC 2544 Throughput Test

RFC 2544 is a benchmark test methodology designed for testing performance and includes tests for throughput, latency, frame loss, and back-to-back frames.

The RFC 2544 test module enables users to test against packet sizes from 64 to 1518-byte frames. Throughput measures the highest rate at which the data can travel with no dropped packets. This is referred to as the available bandwidth.



The chart above shows standard RFC 2544 throughput test results for different frame size traffic loads with different topology configurations. The first bar "No Encryption" reflects the firewall only providing protected throughput without any encryption applied. This is highest rate possible the firewall can provide any protect throughput. The next bar "IPsec Encryption" reflects the observed throughput of the firewall providing protected throughput (security services on) while ALSO providing encryption. The next bar, "Thales CN6140 Encryption" reflects the observed protected encrypted throughput of the firewall AND HSE encryptor employed with the HSE providing the encryption service. The final bar "Thales CN6140 Maximum" reflects the maximum throughput the HSE encryptor was tested for 10GE FDX link. The CN6140 has capacity for 4x 10GE FDX links.

The HSE plus firewall solution throughput performance is far better than the firewall alone providing encryption service (IPsec Encryption). The last bar plotted "Thales CN6140 Maximum" is the best throughput possible with a 10 Gbps (20,000 Mbps for large frame size) restricted by the FDX 10GE firewall connection only.

The Thales CN6140 Multilink Network Encryptor proved 31.6% better encrypted throughput by enhancing the performance of the firewall under test. The Thales HSE offloads the encryption processing from the firewall thereby reducing the firewall memory consumed by 45% and reduces CPU processes by 35%. The resources saved using the Thales HSE solution allow the firewall to better allocate resources to provide security protection features. This allows the firewall to focus on protecting your network.

Protected firewall throughput is measured with full unified threat management (UTM) to include application awareness, malware detection, web filtering and deep packet inspection. This testing was conducted using a Fortinet FG-600F NGFW. The cost to forklift upgrade firewalls to the next model with sufficient capacity can be as high as US$65,000. The same or better encrypted throughput performance can be achieved with the CN6140 for a significantly lower cost.

The RFC 2544 tests clearly proved better protected encrypted throughput for all frame sizes when the HSE encryptors were employed versus the firewall providing encryption alone.

10.0 Conclusion

This evaluation of Thales HSE network technologies, specifically the Thales CN6140 Multilink Network Encryptor and the Thales CN4010 Network Encryptor, demonstrates superior performance and cost-efficiency compared to traditional IPsec encryption.

The findings showed that adding HSE to the network and disabling IPSec in fact reduce latency and jitter on the network that was resulting from the firewall, ultimately providing better network efficiency, stability, and security overall.

Both the CN6140 and CN4010 add less than ten microseconds of latency. While the higher end Fortinet firewalls did not add as much latency as the lower end firewall, using the CN4010 with IPsec disabled proved a 48% decrease in jitter and a 15% decrease in latency compared to those measured when using the firewall with IPsec encryption enabled. The findings showed that adding HSE to the network and disabling IPSec in fact reduce latency and jitter on the network overall that was resulting from the firewall with IPsec enabled.

The Thales CN6140 Multilink Network Encryptor achieves an average of 31.6% better performance in directional throughput compared to a firewall using IPsec encryption in UTM mode at 10 Gbps. It also reduces data loss, enhancing secure data transport. The Thales CN4010 Network Encryptor shows an average of 21.6% better performance than a firewall with IPsec encryption in UTM mode at 1 Gbps. Both the CN6140 and CN4010 exhibited higher overall protected, encrypted throughput, regardless of frame size.

Thales HSE appliances exhibit no degradation in performance, with encrypted throughput performance improving by 21-31% on average for the traffic profile compared to firewall providing the encryption. These appliances deliver exceptional throughput performance with an enterprise mix of traffic (EMIX), achieving zero application transaction failures and no detectable throughput or latency degradation. Thales HSE devices result in 1.5% less frame loss compared to firewalls with HSE, ensuring more reliable data transport.

Thales HSE appliances offer significant savings over firewall upgrades, particularly when taking licensing costs over time into consideration, as well as the added cost for upgrading to a higher capacity firewall including overheads involved in upgrade configuration, forklift upgrade, architectural changes, and the cost of the bandwidth itself.

Thales employs advanced encryption technology with revolving keys and a proprietary key exchange system, providing secure data transport, across on-premises, cloud(s), and hybrid environments, and helps to ensure compliance.

HSE is firewall vendor agnostic, and easily integrates into existing network architectures, making it a superior solution across the board for customers seeking to get the optimum return on investment for their network performance and security.

Based on these findings, enterprises seeking to enhance network security while maintaining high performance and cost-efficiency should consider deploying Thales HSE network encryption technologies. The Thales CN6140 Multilink Network Encryptor and the CN4010 Network Encryptor provide substantial performance improvements over IPsec encryption, ensuring efficient and secure data transport with minimal latency and frame loss. These devices are particularly suitable for organizations requiring high throughput and low latency in their network operations, such as financial services, healthcare, and large enterprises or even governments managing sensitive data across multi-cloud/hybrid environments.

11.0 About Miercom

Miercom has published hundreds of network product analyses in leading trade periodicals and other publications. Miercom's reputation as the leading, independent product test center is undisputed.

Private test services available from Miercom include competitive product analyses, as well as individual product evaluations. Additionally, Miercom services comprehensive certification and test programs, including Certified Interoperable, Reliability Assured, Certified Secure, and Certified Green. Products may also be evaluated under the Performance Verified program, the industry's most thorough and trusted assessment for product usability and performance.

12.0 Customer Use and Evaluation

We encourage customers to do their own product trials, as tests are based on the average environment and do not reflect every deployment scenario. We offer consulting services and engineering assistance for any customer who wishes to perform an on-site evaluation.

13.0 Use of This Report

Every effort was made to ensure the accuracy of the data contained in this report, but errors and/or oversights can occur. The information documented in this report may also rely on various test tools, the accuracy of which is beyond our control. This document is provided "as is," by Miercom and gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness, or suitability of any information contained in this report.

All trademarks used in the document are owned by their respective owners. By downloading, circulating, or using this report you agree to Miercom's Terms of Use. For full disclosure of Miercom's terms, visit https://miercom.com/tou.