City Research Online

City St George's, University of London

Citation: Rezaeianfardouei, H., Townley, M. & Saedi, M. (2026). Reducing Failover Latency in Cisco ASA Site-to-Site VPNs Through IPsec Parameter Tuning. 2025 IEEE Conference on Dependable, Autonomic and Secure Computing (DASC), pp. 108-114. doi: 10.1109/DASC68382.2025.00021 ISSN 2837-0740 doi: 10.1109/DASC68382.2025.00021

This is the accepted version of the paper.

This version of the publication may differ from the final published version. To cite this item please consult the publisher's version.

Permanent repository link: https://openaccess.city.ac.uk/id/eprint/36010/

Link to published version: https://doi.org/10.1109/DASC68382.2025.00021

Copyright and Reuse: Copyright and Moral Rights remain with the author(s) and/or copyright holders. Copies of full items can be used for personal research or study, educational, or not-for-profit purposes without prior permission or charge, unless otherwise indicated, provided that the authors, title and full bibliographic details are credited, a hyperlink and/or URL is given for the original metadata page and the content is not changed in any way. For full details of reuse please refer to City Research Online policy.

City Research Online: http://openaccess.city.ac.uk/ publications@citystgeorges.ac.uk

Reducing Failover Latency in Cisco ASA Site-to-Site VPNs Through IPsec Parameter Tuning

1st Hamed Rezaeianfardouei
Network Secure Engineer
FrasersGroup
Sheffield, United Kingdom
rezaeian.hmd@gmail.com

2nd *Mark Townley*
Department of Computer Network and Cybersecurity
Sheffield Hallam University
mark.townley@shu.ac.uk

3rd Mohammad Saedi
Department of Computer Science
City St Georg's University
London, United Kingdom
mohammad.saedi@citystgeorges.ac.uk

Abstract—Numerous businesses rely on site-to-site Virtual Private Networks (VPNs) to establish secure and reliable communication between geographically dispersed locations. VPNs extend local infrastructure over public networks by integrating authentication and encryption to protect data in transit. Among the various VPN protocols, Internet Protocol Security (IPsec) is one of the most widely adopted, providing robust security through methods such as confidentiality, integrity, and authentication. Cisco Adaptive Security Appliance (ASA) is a common hardware solution for implementing IPsec VPNs. In modern business environments, ensuring minimal downtime and rapid failover after a VPN link failure is critical, as disruptions can significantly impact operational performance. This research focuses on evaluating the convergence time of Site-to-Site VPNs across two carrier networks by analyzing different IPsec parameters. Through simulations on Cisco ASA, various cryptographic algorithms and hashing methods were tested to determine their impact on failover times. Using CML (Cisco Modeling Lab) and Wireshark for simulation and analysis, the study reveals that AES encryption with lower hashing complexity leads to faster failover times. The findings highlight an inverse relationship between security levels and failover performance, underscoring the trade-offs between security and availability in IPsec VPN deployments.

Keywords—IPSEC, Site to Site VPN, ASA, Convergence time, Optimal failover time

I. INTRODUCTION

A site-to-site VPN is crucial in securely connecting multiple nodes of infrastructure, such as branch offices and headquarters, to simulate the experience of being on the same local network. IPsec plays a critical role in this setup, ensuring secure tunnelling and data encryption. Previous research has explored various aspects of IPsec configuration in site-to-site VPNs, particularly in terms of encryption protocols, and security parameters. The network security experts investigated changes in the IP packets header among ESP and AH variables in two protocol modes (Transport Mode and Tunnel Mode) [1]. Building upon these studies, researchers have also analyzed the overhead effects of data transmission in IPsec networks, specifically examining the impact of TCP throughput [2]. The investigation involved assessing how encryption influences both data size and transmission speed. In addition, several studies on IPsec have introduced novel approaches to integrating anti-replay protection with high-availability mechanisms in IMS environments [3]. The aim of this research is to investigate how to configure IPsec VPN variables effectively on Cisco ASA devices to achieve the best possible failover times. Failover refers to the process of switching to a backup network path or system when the primary one fails, in order to minimize the downtime and maintain network availability and business continuity[4]. Improving failover efficiency in site-to-site VPNs can enhance the operational resilience of organizations, especially those with multiple branch offices reliant on seamless connectivity[5].

This Paper will explore key configurations, such as encryption types, integrity mechanisms, and failover policies in IPsec VPNs. Through the experiment and testing, we aim to answer the central question: How can we configure IPsec VPN on Cisco ASA to achieve optimal failover time? Additionally, this research will address related sub-questions [15], such as which encryption methods and integrity algorithms provide the best convergence time and how to improve the performance of VPN phases in different network configurations.

The outcome of this research will provide businesses with practical insights into enhancing the failover time of their VPNs, thus improving network availability between their branches and headquarters. By examining these configurations, this study will contribute to better understanding how network performance and security can be balanced to meet organizational needs. Finally, this research will provide clear answers to the raised questions and open avenues for further exploration into site-to-site VPN performance optimization [8]. The comparison

between IKEv1 and IKEv2 is necessary because both protocols are still widely deployed in production networks, and their differences in negotiation mechanisms, failover handling, and rekeying efficiency can significantly influence VPN failover latency.

II. Related WORK

Previous research on IPsec optimization has explored various aspects of improving performance, efficiency, and reliability in Virtual Private Networks (VPNs). Researchers have studied the impact of different encryption and hashing algorithms on the overall performance of IPsec. Studies often compare some protocols such as AES, 3DES, and SHA-256 to determine their computational overhead and latency in secure communication [5]. For Key Exchange Protocols, several works have analyzed the efficiency of IKE (Internet Key Exchange) phases, particularly IKEv1 versus IKEv2, in reducing latency during session establishment [5]. Optimizing the handshake process has been a major focus in minimizing connection setup delays. Previous research in network security initially assessed the performance implications of IPsec by employing Openswan, an open-source implementation of the protocol. The study primarily concentrated on the tunnel mode of operation and the ESP protocol, as this configuration is extensively employed for establishing VPN [6]. Regarding performance under load, the scalability of IPsec has been a popular topic, examining how it performs under high traffic loads. Research in this area has focused on the ability of devices to handle high volumes of encrypted traffic without degrading performance, often by optimizing hardware acceleration techniques. Several types of research about performance measurements have been seen, including delays and packet loss, raised a different view to address the issue of IPsec anti-replay counters and IKEv2 Messages ID counters becoming unsynchronised [8]. These works highlight the trade-off between security strength and processing speed. Also based on the previous research, IPsec decreases the throughput of the network connections[7].

Some studies have explored payload compression to improve the efficiency of IPsec VPNs. By reducing the size of data packets before encryption, researchers aimed to enhance throughput and reduce latency. IPsec links between two LANs interconnected via a WAN. The routing protocol utilised within the WAN was the BGP. While in this research this research is trying to keep the IPsec connection redundancy in Cisco ASA by IP route static and SLA concept[9]. For Multi-Tunnel Optimization, Studies have also focused on optimizing multi-tunnel scenarios, where multiple IPsec tunnels are used simultaneously. Researchers have investigated techniques to balance traffic across tunnels for improved performance and fault tolerance. Among security appliances used for IPsec tunnel implementation and convergence time analysis, Cisco ASA is considered one of the leading candidates based on the latest Gartner evaluations. However, this investigation can be extended to include other vendors such as FortiGate, Check Point, and newer solutions like Cisco Firepower [10]. Researchers have explored the integration of Quality of Service (QoS) mechanisms with IPsec VPNs to prioritize certain types of traffic, ensuring that critical data receives the necessary bandwidth and reduced latency. The utilisation of T-CAM classification in IPsec architectures has the potential to enhance cost-effectiveness. In simpler terms, it can considerably reduce the size of TCAM while maintaining the speed of search and matching operations [11]. We can find an investigation about IPsec processors. Factually, the studies examined IPsec processors to enhance the efficiency of tunnels. They introduced a high-performance in-line network security processor with a configurable IPsec processor. This processor smoothly integrates two built-in 32-bit CPU cores and an IPsec protocol processor on a System-on-Chip. Most research on VPN Site-to-Site primarily focuses on general theoretical concepts, with little attention given to operational discussions [12]. Despite extensive research on optimizing various aspects of IPsec, very little attention has been given to failover mechanisms in IPsec-based VPNs.

Specifically, there is a lack of studies examining the optimal failover time when a site-to-site IPsec VPN connection encounters disruption. This gap in the literature underscores the significance of our work, which aims to analyse failover performance by manipulating IPsec VPN variables in a Cisco ASA environment [13].

III. Model and PRELIMINARIES

A. Simulation Model

In the experiment, we evaluated the failover time of site-to-site VPN connections configured on Cisco ASA devices using both IKEv1 and IKEv2 protocols. The tests were conducted by manipulating key IPsec VPN variables, including rekey intervals and key negotiation times, to observe their impact on failover performance [14].

To simulate realistic network conditions, link delays and traffic generators were configured to emulate typical WAN behavior. Each node was configured with identical security policies to isolate the impact of the protocol used. The topology included failover triggers such as interface shutdowns to initiate VPN renegotiation. Results were logged and analyzed through Wireshark and syslog event timestamps to ensure measurement precision. Failover times were measured using network monitoring tools, and each test was repeated three times to ensure accuracy[15].

The average failover time for each configuration was calculated and analysed to compare the performance of IKEv1 and IKEv2. This Research designs two topologies in CML for the study scenario, including eight nodes distributed across three areas with two IP ranges. Fig 1 provides a detailed illustration. The study will evaluate failover time by capturing packets and calculating the average after three trials for each category of VPN variables.

B. Experimental Process Setup

To analyse the optimal failover time in a Cisco ASA VPN site-to-site setup, we conducted a series of structured experiments. These experiments focused on manipulating IPsec VPN variables to assess their impact on failover performance.

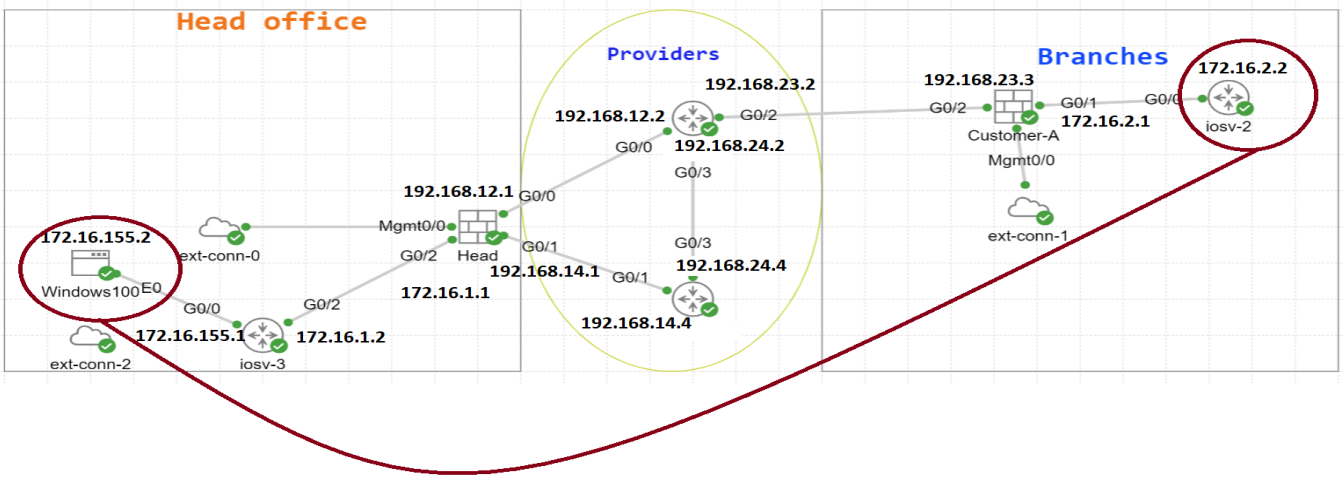

Fig.1: Topology of research and Path of test for Packet Filtering Process in Both Scenarios

This section outlines the testing process in this research, structured into six key steps:

1. Design two topologies in CML, Configure the IP connectivity based on the IP plan for public and private, Set up static IP routing between HQ and Providers, Set up static IP routing between Branche and Providers.
2. Configure crypto for IKEV1/V2 includes Create three common transform-sets configuration, Create four standard proposals configuration.
3. Configure tunnelling using IPsec behavior and key-share mechanism, create an access-list to enable reachability between IP public and Private, Set-up two SLA and Tracking Configuration on HQ to ensure redundancy between ASA-HQ and two carriers
4. Adjust three transform-set variables three times, measuring and averaging failover time for re-establishing connectivity between local and remote private segments.
5. Adjust four proposal variables three times, measuring and averaging failover time for re-establishing connectivity between local and remote private segments.
6. Record monitoring results using Wireshark and CML packet capture, including tunnel status, Phase 2 timing, Comparison the results and finally Illustrate the results with diagrams.

C. Lab Scenario

This research designs two network topologies in CML to simulate the research scenario, incorporating eight nodes across three areas with two IP ranges. The following section provides a detailed description of the topologies and their components. Topologies:

One: Implements the IKEv1 configuration for the IPsec tunnel. Transform sets will be configured in this topology.

Two: Implements the IKEv2 configuration for the IPsec tunnel. Multiple proposals will be set in version two to establish IPsec connectivity.

I. VARIABLES MANIPULATION

In the research scenario, the IKEV1 and IKEV2 parameters will be manipulated. IKEv1 is a protocol used to establish secure site-to-site VPN tunnels, utilizing a two-phase negotiation process to exchange keys and authenticate peers. It also involves multiple message exchanges to set up and manage the VPN connection. IKEv2 is a more advanced protocol designed to streamline and secure the establishment of VPN tunnels. It incorporates features like simplified message exchanges, improved NAT traversal, and support for mobility MOBIKE (Mobility and Multihoming Protocol) [17].

A. Different states for IKEV1 and IKEV2 for phase 2

IKEV1 Transform-Set and IKEV2 proposal: The Crypto configuration for the VPN tunnel in IKEV1 and IKEV2 will be manipulated by changing the encryption parameters[17] shown in Table 1.

TABLE 1 CRYPTO CONFIGURATION

	IKEV1	IKEV2
State 1	AES-SHA	AES-GCM-256 SHA512
State 2	AES-192-SHA	AES-256 SHA256
State 3	AES-256-SHA	AES-GCM SHA384
State 4		AES-192 SHA

It is supposed that the phase 1 configuration and Policy Attribute for both versions of IKE are constant and should remain unchanged throughout. Table 2 identifies them.

TABLE 2 CONSTANT VARIABLES

	IKEV1/2
HASH **Integrity**	AES SHA
Authentication	Preshared key
DH	14
Lifetime Sec	28800

B. Packet Filtering Process

After manipulating the parameters, the packet will be filtered to calculate the convergence time. Convergence time denotes the duration required for a network to regain stability following a topology change, such as the occurrence of a link failure or its recovery[18].

In Wireshark and Packet capture in cml, the icmp packet will be filtered for both sides of the tunnel and identify the timestamp for each test step. The convergence time will be calculated by subtracting the first and last times. Wireshark allows me to assess the convergence time of network protocols by inspecting the timestamps and packet sequences within the captured data [16].

C. Calculation failover time in Wireshark:

The calculation of failover time begins by verifying that the IPsec tunnel is active and functioning. A continuous ping is initiated from the Windows desktop on the local side (IP address 172.16.155.2) to the remote side's private IP address (172.16.2.2), as illustrated in Fig 1. Simultaneously, Wireshark is used to capture packets along this communication path to monitor any disruptions. To simulate a failover scenario, the primary provider connection is manually brought down. As a result, the system's SLA monitoring and tracking mechanisms are triggered, prompting the routing table to switch to the secondary provider in order to maintain connectivity to the remote branch IP address. Wireshark and packet captures in the Cisco Modelling Labs (CML) environment are then analysed to determine the exact failover time. This failover time is calculated as the duration between the moment the last successful packet is received from the remote side and the moment the first reply is received after the routing switch. To further evaluate the impact of different cryptographic configurations, the Transform-set in IKEv1 and the Proposal in IKEv2 are modified, and the process is repeated. This method is also applied to measure timing differences in phase 1 and phase 2 negotiations to obtain a comprehensive understanding of tunnel recovery behaviours under various conditions.

D. Equations

To develop a formula, we can consider key variables that influence failover time in site-to-site VPNs, such as:

T_f: Failover time (the total time it takes for the VPN to re-establish after a failure)

T_{r1}, T_{r2}, T_{r3}: Recorded failover times during the three test runs

N: The number of test runs (3 in this case)

T_{avg}: Average failover time

Three failover times (T_{r1}, T_{r2}, T_{r3}) have been recorded for each scenario. The average failover time (T_{avg}) was computed as the meaning of these runs, and the difference between IKEv1 and IKEv2 was derived from the corresponding averages.

We could define the average failover time for the three tests as:

$$T_{avg} = \frac{T_{r1+}T_{r2+}T_{r3}}{N}$$

Formula for Failover Time Comparison (IKEv1 vs IKEv2)

$$\Delta T = T_{avg}^{IkEv1} - T_{avg}^{IkEv2}$$

where:

T_{avg}^{IkEv1} is the average failover time for IKEv1,

T_{avg}^{IkEv2} is the average failover time for IKEv2, and

ΔT represents the difference in failover times between the two protocols [19].

E. Analysing the result by Wireshark

Wireshark is the most common tool among network administrators and researchers to identify and resolve network problems, to examine network activities, to investigate security breaches, and to verify application behavior across the network [16]. This tool plays a crucial role in the research and is considered essential in the toolkit of every networking professional [20]. In this research, Wireshark was installed on Windows desktop on both Remote and Local sides. Each test captured the packets in Wireshark to check the state of IPsec tunnel reachability (Fig 2).

F. Verification By Packet capturing in CML

This project aims to verify the results using CML Packet Capture tool. After each step, a separate capture is taken and analyzed to ensure the data's reliability and relevance. While it is unlikely that the results in Wireshark and Packet Capture will be identical, due to the influence of various parameters, they should exhibit the same overall pattern at each step.

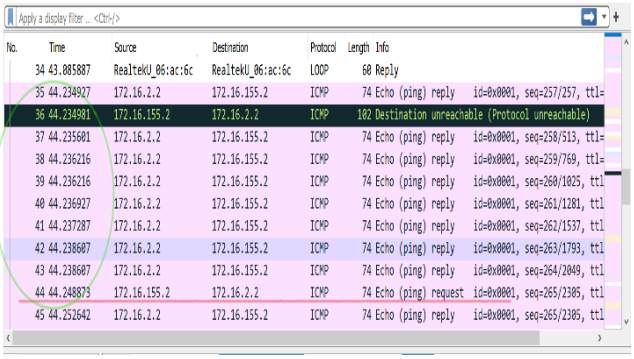

Fig. 2. The sample of Analysing and Calculation the failover time By Wireshark

I. RESULTS

This paper explored the principal discoveries derived from all of measurements repeating the test three times to find valuable conclusions, and the average was presented as that step result [15].

A. Summary of the result

The experimental results clearly indicate that IKEv2 outperforms IKEv1 in terms of redundancy timing and overall tunnel re-establishment efficiency. Specifically, IKEv2 demonstrated significantly faster failover and reconnection times, making it a more suitable choice for environments where uptime and responsiveness are critical. These findings support the conclusion that IKEv2 offers a more optimized solution for IPsec tunnel deployment, particularly in dynamic or high-availability network scenarios.

B. As previously discussed, the test prototype records three-time measurements for each step. Each step's time is calculated separately as the average of the local and remote sides.

Table 3

Failover Time for IKEV1 Tunnel in Test Result by changing the encryption.

Failover Time for IKEV1(Seconds)						
	AES		AES-192		AES-256	
	Local	Remote	Local	Remote	Local	Remote
First	12.81	13.9	13.31	14.29	16.51	16.92
Second	13.54	13.41	14.7	15.87	16.91	16.23
Third	14.63	12.32	15.45	15.6	16.72	16.43
Average	13.36	13.21	14.47	15.23	16.71	16.52

IKEV1 Test Result: AES produced the shortest failover time in the IKEv1 tests, with an average of 13.28 seconds, based on three repeated test runs to ensure consistency and reliability of the results. Figs 3 shows this result by graphs.

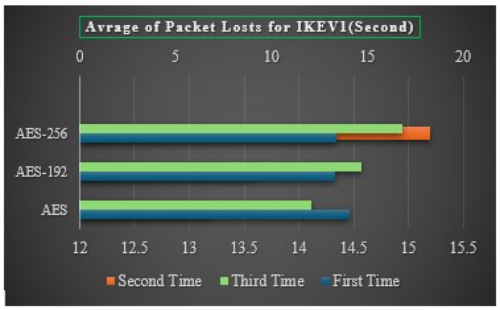

Fig. 3. Failover Time for IKEV1 Tunnel in the different configuration

Table 4

Failover Time for IKEV2 Tunnel in Test Result by changing the encryption and integrity.

Failover Time for IKEV2 (Second)								
	AES-GCM-256 SHA-512		AES-256 SHA-256		AES-GCM SHA-384		AES-192 SHA-1	
First	17.2	15.2	12.4	11.2	10.6	11.2	7.5	13.4
Second	12.3	14.4	12.6	12.5	11.4	11.1	8.4	9.5
Third	14.2	12.2	15.1	13.2	10.4	10.3	5.3	8.2
Average	14.5	13.9	13.3	12.3	10.8	10.8	7	10.3

IKEV2 Test Result: Among the various encryption and integrity combinations evaluated, the configuration using AES-192 with SHA-1 demonstrated the shortest failover time in the IKEv2 test scenarios, averaging 8.6 seconds across multiple trials. This result highlights the efficiency of Galois/Counter Mode (GCM) in increasing cryptographic overhead, as it combines encryption and authentication in a single operation. The tests were repeated three times to ensure consistency, and minimal variance in the results further validated the reliability of this configuration. The performance advantage is particularly noticeable in time-sensitive environments where rapid tunnel reestablishment is critical. Additionally, SHA-512, though computationally intensive, with AES-GCM-256 does not have optimized failed over time. These findings suggest that for deployments prioritizing both strong security and minimal downtime during link failures, AES-256 with SHA-256 offers a compelling solution under IKEv2 to have middle level of security and fail-over time. Figs 4 shows this result by graphs.

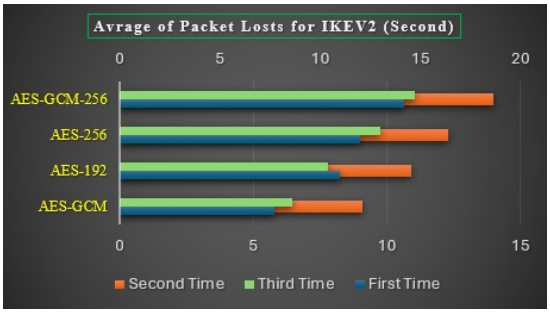

Fig. 4. Failover Time for IKEV2 Tunnel in the different configuration

C. Discussion

In most of the previous experience with IPsec tunnels, the project fixed connections after missing the Uplinks. This study wanted to take advantage of the time for data transactions, so several solutions were suggested. First, it is necessary to think about redundancy routing, which means one answer must be chosen SLA Static Routing or BGP. In addition, the selection of IKEV1 and IKEV2 to deploy the IPsec configuration. At that time, IKEV2 and BGP were selected for the failover link, but now, based on the research results, if the timing is more important than security, the configuration of IKEV2 with the lowest hashing algorithm, such as AES, is better. This approach does not imply fully sacrificing security but instead emphasizes achieving an appropriate trade-off between efficiency and protection, tailored to the specific requirements of the application. In cases such as VoIP, live video streaming, or systems that rely on real-time data, improved performance can enhance both the quality of service and overall reliability. Conversely, in contexts where stringent security standards are critical, organizations may still opt for more robust encryption protocols, accepting the associated performance costs [21]. Overall, the findings highlight that with thoughtful tunnel configuration and strategic protocol choices, IPsec tunnels can be optimized for greater adaptability and responsiveness especially in networks that experience frequent disconnections or require mobility support.

D. Conslusion and Recomandation

For future research projects, this study offers several recommendations to expand upon the current findings. Firstly, the research focused only on commonly used hashing algorithms due to time constraints; therefore, it would be valuable in future studies to explore a broader range of security parameters, including less commonly tested configurations. Additionally, conducting experiments in real-world environments is significantly more beneficial than relying solely on simulators. In this regard, future research could be performed using physical Cisco ASA devices instead of software-based simulators to obtain more realistic and applicable results. Moreover, it would be worthwhile to extend the research scope to include newer generations of Cisco firewalls, such as Cisco Firepower Threat Defense (FTD), or even alternative vendors like Palo Alto, Check Point, or FortiGate, to provide a more comprehensive evaluation. Future investigations could also benefit from using the BGP routing protocol instead of SLA-based mechanisms for configuring redundancy links on carrier networks. BGP may offer better performance in terms of routing convergence time, which is critical in redundancy scenarios [22]. Future studies should also consider high traffic loads and large enterprise environments to better understand how scale impacts VPN failover performance.

Acknowledgements

This research has been supported by the Pump Priming Research Scheme and institute of Cyber Security, funded by City's George's, University of London

REFERENCES

[1] Sakib, M., & Singh, J. (2020). Simulation based performance analysis of IPSec VPN over IPv6 networks. International Journal of Electronics Engineering, 12(2), 92-104.

[2] Abolade, O., Okandeji, A., Oke, A., Osifeko, M., & Oyedeji, A. (2021). Overhead effects of data encryption on TCP throughput across IPSEC secured network. Scientific African, 13, e00855. doi:10.1016/j.sciaf.2021.e00855

[3] S. T. Aung, & T. Thein. (2020). Comparative analysis of site-to-site layer 2 virtual private networks. Paper presented at the - 2020 IEEE Conference on Computer Applications(ICCA), 1-5. doi:10.1109/ICCA49400.2020.9022848

[4] Nguyen, L. T., Nguyen, H. D., Nguyen, L. D., Chu, N. H. T., & Van Ngo, V. (2022, October). High Availability Solution for IPsec in IP Multimedia Subsystem. In 2022 13th International Conference on Information and Communication Technology Convergence (ICTC) (pp. 1290-1294). IEEE.

[5] Kumar, J., Kumar, M., Pandey, D. K., & Raj, R. (2021). Encryption and Authentication of Data Using the IPSEC Protocol. In Proceedings of the Fourth International Conference on Microelectronics, Computing and Communication Systems: MCCS 2019 (pp. 855-862). Springer Singapore.

[6] Shue, C. A., Gupta, M., & Myers, S. A. (2007). Performance Analysis and Enhancement, Paper presented at the - 2007 IEEE International Conference on Communications, 1527-1532. doi:10.1109/ICC.2007.256

[7] Palomares, D., Migault, D., & Laurent-Maknavicius, M. (2013). Failure preventive mechanism for IPsec gateways. 2013 Third International Conference on Communications and Information Technology (ICCIT), 167-172.

[8] Singh, M. (2017). Connectivity between two distant sites with automatic failover to IPsec (Order No. 10262849). Available from ProQuest Central; ProQuest Dissertations & Theses Global. (1892482810). Retrieved from

[9] Niu, L. Wu, L. Wang, X. Zhang, & J. Xu. (2011). A configurable IPSec processor for high performance in-line security network processor. Paper presented at the - 2011 Seventh International Conference on Computational Intelligence and Security, 674-678. doi:10.1109/CIS.2011.154

[10] Aliev, W. S., Chae, & H. Kim. (2017). The cost-efficient architecture of IPsec classification engine with TCAM. Paper presented at the 2017 13th International Computer Engineering Conference (ICENCO), 20-25. doi:10.1109/ICENCO.2017.8289756

[11] Bevans, R. (2022). Guide to Experimental Design | Overview, 5 steps & Examples, scribbr.

[12] Kurniawan, D. E., Arif, H., Nelmiawati, N., Tohari, A. H., & Fani, M. (2019, March). Implementation and analysis ipsec-vpn on cisco asa

firewall using gns3 network simulator. In Journal of Physics: Conference Series (Vol. 1175, No. 1, p. 012031). IOP Publishing

[13] Juma, M., Monem, A. A., & Shaalan, K. (2020). Hybrid end-to-end VPN security approach for smart IoT objects. Journal of Network and Computer Applications, 158, 102598. doi:10.1016/j.jnca.2020.102598

[14] Hauser, F., Häberle, M., Schmidt, M., & Menth, M. (2020). P4-IPsec: Site-to-site and host-to-site VPN with IPsec in P4-based SDN. doi:10.1109/ACCESS.2020.3012738

[15] Chandra, V., & Hareendran, A. (2018). Research Methodology (pp. 330-334)

[16] Bock, L. (2022). Learn Wireshark: A Definitive Guide to Expertly Analyzing Protocols and Troubleshooting Networks Using Wireshark. Packt Publishing, Limited.

[17] Basit, Z., Tabassum, M., Sharma, T., Furqan, M., & Quadir Md, A. (2022). Performance analysis of OSPF and EIGRP convergence through IPsec tunnel using multi-homing BGP connection. Materials Today: Proceedings, 62, 4853-4861. 10.1016/j.matpr.2022.03.

[18] Camilo, B. C. V., Couto, R. S., & Costa, L. H. M. K. (2018). Assessing the impacts of IPsec cryptographic algorithms on a virtual network embedding problem. Computers & Electrical Engineering, 71, 752-767. doi:10.1016/j.compeleceng.2017.06.025

[19] Dharma, F. W. P., & Suharjito. (2021). Enhancing branch office network availability using cloud EoIP gateway. Procedia Computer Science, 179, 574-581. doi:10.1016/j.procs.2021.01.042

[20] Julia, I. R., Suseno, H. B., Wardhani, L. K., Khairani, D., Hulliyah, K., & Muharram, A. T. (2020, October). Performance evaluation of first hop redundancy protocol (FHRP) on VRRP, HSRP, GLBP with routing protocol BGP and EIGRP. In 2020 8th International Conference on Cyber and IT Service Management (CITSM) (pp. 1-5). IEEE.

[21] Schweiger, O., Foerster, K. T., & Schmid, S. (2021, December). Improving the resilience of fast failover routing: TREE (tree routing to extend edge disjoint paths). In Proceedings of the Symposium on Architectures for Networking and Communications Systems (pp. 1-7).

[22] Sholihah, W., Rizaldi, T., & Novianty, I. (2019). Information and communication system technology with VPN site-to-site IPsec. Journal of Physics. Conference Series, 1193(1), 12012–.

Streefkerk, R. (2023). Qualitative vs Quantitative Research | Differences, Examples & Methods, scribbr