Study of Failover Time in Site-to-Site VPNs Across Leading Firewall Vendors: Fortinet, Check Point, Palo Alto, and Cisco

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

2nd Mohammad Saedi
Department of Computer Science
City St Georg's University
London, United Kingdom
mohammad.saedi@citystgeorges.ac.uk

***Abstract*—Reliable failover performance is a critical factor in maintaining the availability of site-to-site virtual private networks (VPNs). This study presents a comparative analysis of failover times among four leading firewall vendors: Fortinet, Check Point, Palo Alto Networks, and Cisco. A controlled test environment was designed to evaluate how different configuration parameters and default settings influence the time required for VPN tunnels to recover after a link or device failure. The results highlight significant variations in failover behavior across vendors, with differences attributed to IPsec rekeying mechanisms, detection timers, and session handling strategies. By identifying the configurations that achieve the lowest failover times, this research provides practical guidance for network administrators and security engineers seeking to optimize high-availability VPN deployments. In addition, the study emphasizes the importance of fine-tuning IKE parameters to minimize downtime. The findings suggest that vendor specific optimizations play a greater role than hardware capacity in achieving fast recovery. Future work may extend this analysis by incorporating cloud-based firewalls and hybrid WAN environments for a broader perspective.**

Keywords—Site-to-Site VPN, Failover Time, IPsec, IKE, Firewall Vendors

I. INTRODUCTION

Secure and resilient connectivity between enterprise sites is a cornerstone of modern network infrastructure. Site-to-site VPNs remain a widely adopted method to connect disparate locations over public networks like the Internet, providing encrypted and authenticated paths using protocols such as IPsec [1]. VPNs ensure that sensitive data remains confidential while enabling continuous communication between branch offices, data centers, and cloud environments.

While throughput and encryption strength are commonly emphasized in vendor evaluations, failover performance that is, how quickly a VPN tunnel can recover after a network or device failure is equally critical. Downtime resulting from an outage, whether due to ISP link failure, hardware malfunction, or network disruption, can severely degrade productivity, disrupt business operations, and expose organizations to compliance and security risks. Consequently, efficient failover mechanisms and minimal recovery times are essential to sustaining operational continuity.

Different firewall vendors employ distinct strategies to handle VPN failovers:

- Cisco offers crypto map-based failover using IP SLA (Service Level Agreement) tracking to detect link failure and rapidly redirect VPN tunnels through backup interfaces [2].
- Fortinet provides options such as route-based VPN redundancy using BGP, static route failovers, or dynamic SD-WAN–based rerouting to maintain tunnel availability [3][4].
- Palo Alto Networks employs tunnel monitoring and static route path monitoring to dynamically reroute when tunnel health degrades [5].
- Check Point often leverages its ClusterXL high-availability system with stateful synchronization to preserve VPN states during failover [6].

Although failover is a shared requirement, implementations differ significantly. Protocol-level parameters, including Dead Peer Detection (DPD) timers, IKE rekey intervals, monitoring thresholds, and session persistence behavior often vary both across vendors and firmware versions. These variances directly impact

failover time and can result in markedly different recovery experiences under similar conditions, posing a challenge for network engineers who wish to design resilient, vendor-agnostic VPN infrastructures.

Despite the critical nature of failover performance, comparative studies across firewall platforms are scarce. Much of the existing knowledge comes from vendor-specific guides or anecdotal reports, while forum discussions highlight variability in downtime across implementations, such as systems described as "nearly instantaneous" versus those with delays of up to several minutes [7].

In parallel, emerging research has explored advanced VPN capabilities that push the boundaries of performance and security. For instance, a recent study demonstrated quantum-safe IPsec tunnels with 100 Gbps throughput using Quantum Key Distribution (QKD) over 46 km fiber, maintaining sustained high-speed and secure connectivity with sub-second key refresh rates [8]. Although such work primarily addresses encryption and throughput at scale, it underscores the importance of rigorous testing frameworks and performance benchmarking for both emerging and traditional VPN applications [9].

This study aims to fill the gap by offering:

- A comparative analysis of failover times across four prominent firewall vendors Cisco, Fortinet, Palo Alto Networks, and Check Point under controlled, standardized conditions.
- An evaluation of how key IPsec parameters (e.g., DPD settings, tunnel monitoring intervals, rekey timings) and vendor-specific monitoring features affect recovery latency.
- Actionable configuration recommendations to optimize failover performance, grounded in empirical evidence.

The contributions of this research are twofold. First, by benchmarking VPN failover times across vendors, it provides a performance baseline valuable to practitioners for making informed decisions. Second, by identifying which configuration parameters most effectively reduce failover latency, it offers practical guidance for network designers seeking to enhance resilience. Notably, this study highlights that optimal failover is not governed by hardware alone, but by fine-tuning protocol-level mechanisms and leveraging vendor-tailored features intelligently.

In conclusion, this research empowers organizations to deploy highly available site-to-site VPNs with minimal downtime in the best firewall vendor for the best fail-over time. By systematically comparing leading firewall solutions and highlighting configuration best practices, it supports robust network design and strengthens the broader domain of network resilience and high availability [10].

II. RELATED WORK

Previous research on IPsec optimization has explored various aspects of improving performance, efficiency, and reliability in 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. 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.

Tan (2006), investigates the performance of BGP/MPLS VPN failover functionality, focusing on the impact of link or node failures on message delivery latency. The study aims to understand how various protection mechanisms affect the performance of VPN services. The findings are relevant for designing resilient networks that maintain performance during failures [11].

Fischer (2019) compares the performance of state-of-the-art VPN solutions under stable versus unreliable network conditions. The study evaluates how different VPN protocols perform when network reliability varies, providing insights into their robustness and suitability for various environments. This comparison is crucial for selecting appropriate VPN solutions based on network stability [12].

Regarding VPN in cloud, in previous research presents a performance test of Azure site-to-site VPN latency. The tests simulate cross-region latency using Azure VPN Gateway and compare it with direct public IP connections. The findings offer insights into the performance implications of using VPNs in cloud environments[13], [14].

Ullah et al. (2020), conduct performance analyses of IPsec implementations over high-speed network links, providing enhancements to boost throughput and efficiency. The research identifies factors affecting performance and suggests optimizations for better utilization of high-speed links [15].

Despite extensive research on optimizing various aspects of IPsec, very little attention has been given to failover mechanisms in IPsec-based VPNs [16].

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 FTD environment [17].
Furthermore, it is found that the data flow is increased by using IPsec type Authentication Header (AH) protocol. Additionally, this proposed technique can satisfy a significant reduction in the delay caused by encryption by at least 15%, along with increasing efficiency and the throughput on the Internet. Moreover, the proposed cryptography enables the development of special processors for encryption with Field Programmable Gate Array (FPGA) chips that can be available in the form of devices attached to networks [18].
The security and privacy of data that travels through cyberspace have become an essential concern for the individual users and the organizations[19]. Apart from this, the government of many countries has also imposed many censorship rules on the way their citizens should use the Internet [20]. All this has resulted in VPNs becoming very popular as it allows the users and organizations to secure and largely circumvent their Internet connection. In a previous study three types of most common VPNs and present a comparative study of their features, performance, security and a few other aspects. Their research will offer a clear understanding of the users and help them make their decision on choosing the correct VPN based on their need and priority regarding security, speed, and cost [21].

III. MODEL AND PRELIMINARIES

A. Simulation Model

In the experiment, we evaluated the failover time of site-to-site VPN connections configured on 4 different firewall vendors 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 [22], Figure 1 shows the main topology.
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 [23].
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 isolated lab 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. The average failover time for each configuration was calculated and analysed to compare the performance of IKEv1 and IKEv2.

B. Experimental Process Setup

To analyse the optimal failover time in FortiGate, Cisco FTD, Checkpoint and Palo alto 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.

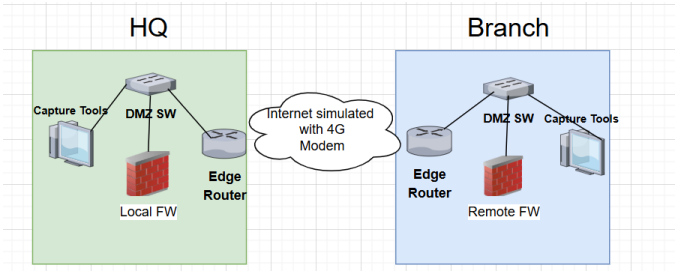

Fig.1: The main Topology for Test

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

1. Design four topologies (for four firewalls), 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 FTD-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 linux TCPDUMP packet capture, including tunnel status, Phase 2 timing, Comparison the results and finally Illustrate the results with diagrams.

C. Lab Scenario

This study examines the modification and analysis of IKEv1 and IKEv2 parameters within a site-to-site VPN across four different firewalls [24]. IKEv1 establishes secure tunnels through a two-phase negotiation, but its multiple message exchanges can increase setup time. IKEv2, an enhanced version, simplifies negotiation, reduces exchanges, supports automatic rekeying, and strengthens resistance against security threats, making it more suitable for modern, mobile, and cloud environments. By adjusting parameters such as encryption algorithms, lifetimes, and rekey intervals, the research compares how each protocol influences VPN failover performance, latency, and connection stability, helping optimize configurations across vendors and scenarios [25].

D. Different states for IKEV1 and IKEV2 for phase 2

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

Table 1
Different Variables in IKEv1 and IKEV2 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 identify them.

Table 2
The Constant Variables in Tests

	IKEV1/2
HASH Integrity	AES SHA
Authentication	Preshared key
DH	14
Lifetyme	28800

E. 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[20].

In Wireshark and Packet capture in Linux TCPDUMP, 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 [26].

F. Calculation failover time in Wireshark and Tcpdump:

The failover measurement process begins by confirming an active IPsec tunnel and sending continuous pings from local machine A to remote machine B, while Wireshark captures packet data for real-time analysis. A failover scenario is created by disabling the primary service provider connection, triggering SLA monitoring and rerouting traffic to the secondary provider. TCPDUMP logs are used to calculate failover duration as the interval between the last successful packet and the first response after rerouting. By adjusting IKEv1 Transform-set and IKEv2 Proposal parameters, the study evaluates cryptographic impacts, negotiation timing, and tunnel recovery performance under different configurations [27].

G. 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

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)

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

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 [28].

H. 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 [29]. This tool plays a crucial role in the research and is considered essential in the toolkit of every networking professional [30]. 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

I. Verification By Packet capturing in TCPDUMP

This project aims to verify the results using Linux 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. Figure 2 shows the sample TCPDUMP logs.

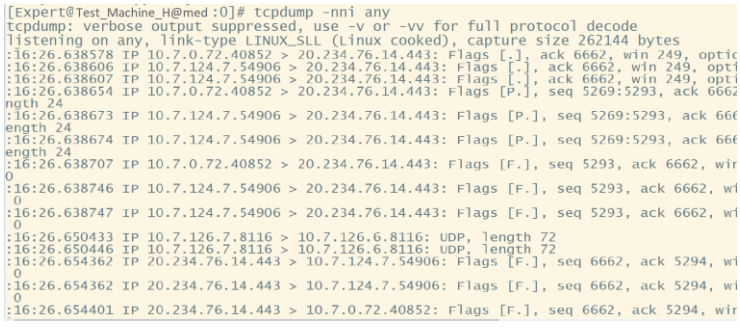

Fig. 2: The sample of Analysing and Calculation the failover time By TCPdump

IV. RESULTS

This study examined the key findings obtained from multiple measurements, with each test repeated three times to ensure reliability. The results from these repetitions were averaged to present a representative outcome for each step of the experiment.

A. Summary of the result

Among the firewalls tested, FortiGate consistently demonstrated the fastest failover times on average across all test scenarios. Following FortiGate, Check Point firewalls exhibited the next best performance, while Palo Alto firewalls showed moderate failover efficiency, and Cisco firewalls recorded the slowest failover times in comparison. The evaluation was carried out under multiple configurations to ensure comprehensive results. Specifically, for IKEv1, the tests were conducted across three distinct states, examining how variations in parameters such as encryption algorithms, key lifetimes, and rekey intervals influenced failover behavior. For IKEv2, a more advanced protocol, the study considered four different states, including additional features like automatic rekeying and improved negotiation mechanisms, to observe how these optimizations affected tunnel recovery. By analyzing the performance across these variables and states, the study was able to identify not only the relative ranking of firewall vendors in terms of failover efficiency but also how protocol configuration choices directly impact the speed and reliability of VPN tunnel recovery. These insights provide valuable guidance for network engineers seeking to optimize site-to-site VPN setups for critical business applications where minimizing downtime is essential. The experimental findings clearly show that IKEv2 provides superior performance compared to IKEv1 regarding redundancy timing and the efficiency of tunnel re-establishment. In particular, IKEv2 achieved noticeably faster failover and reconnection durations, making it better suited for network environments where high availability and minimal downtime are essential. These results highlight that IKEv2 represents a more optimized and reliable solution for IPsec tunnel deployment, especially in dynamic networks or setups requiring robust high-availability performance.

B. As previously discussed, the test prototype records three-time measurements for each step. Each step's time is calculated separately for each firewall.

Table 3

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

Failover Time IKEV1 Cisco (second)			
	AES	AES-192	AES-256
First	27	31	33
Second	26	33	36
Third	24	34	37

Table 4

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

Failover Time IKEV1 Fortigate (second)			
	AES	AES-192	AES-256
First	16	15	14
Second	12	17	15
Third	11	14	14

Table 5

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

Failover Time IKEV1 Checkpoint (second)			
	AES	AES-192	AES-256
First	19	18	20
Second	17	18	19
Third	17	16	17

Table 6

Failover Time for IKEV1 Tunnel in Test Result by changing the encryption in Cisco Palo Alto

Failover Time IKEV1 Palo Alto (second)			
	AES	AES-192	AES-256
First	27	26	25
Second	24	23	23
Third	22	24	21

IKEV1 Test Result: AES produced the shortest failover time in the IKEv1 tests, with an average of 11 seconds, based on three repeated test runs to ensure consistency and reliability of the results. Figure 3 shows this result by graphs.

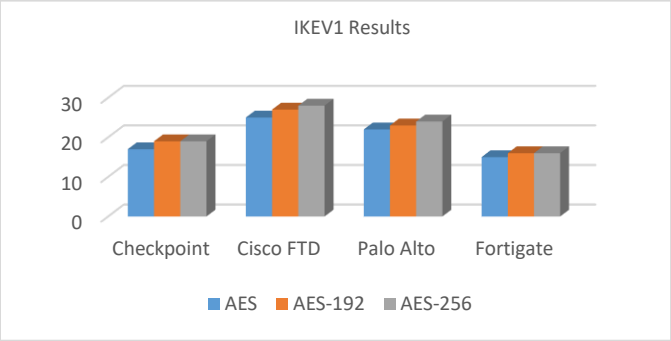

Fig. 3. Failover Time for IKEV1 Tunnel in the different configuration and different firewall

Table 7

Failover Time for IKEV2 Tunnel in Test Result by changing the encryption in Cisco FW

Failover Time IKEV2 Cisco (second)				
	AES-GCM-256-SHA512	AES-256 SHA256	AES-GCM SHA384	AES-192 SHA
First	23	23	30	33
Second	23	23	33	31
Third	24	24	31	34

Table 8

Failover Time for IKEV2 Tunnel in Test Result by changing the encryption in FortiGate FW

Failover Time IKEV2 Fortigate (second)				
	AES-GCM-256-SHA512	AES-256 SHA256	AES-GCM SHA384	AES-192 SHA
First	11	12	13	12
Second	13	13	12	13
Third	10	12	13	11

Table 9

Failover Time for IKEV2 Tunnel in Test Result by changing the encryption in Checkpoint

Failover Time IKEV2 Checkpoint (second)				
	AES-GCM-256-SHA512	AES-256 SHA256	AES-GCM SHA384	AES-192 SHA
First	23	20	14	14
Second	24	19	13	13
Third	21	24	15	15

Table 10

Failover Time for IKEV2 Tunnel in Test Result by changing the encryption in Palo Alto

Failover Time IKEV2 Palo (second)				
	AES-GCM-256-SHA512	AES-256 SHA256	AES-GCM SHA384	AES-192 SHA
First	23	20	24	23
Second	24	19	23	23
Third	21	24	24	25

IKEV2 Test Result: Across the four different IKEv2 configurations tested on the selected firewall vendors, FortiGate consistently achieved the best failover performance, followed by Check Point, while Palo Alto and Cisco trailed behind in similar patterns. This ranking was observed across all variations of cryptographic proposals evaluated, showing a clear distinction in how each vendor's implementation of IKEv2 handles tunnel recovery. Interestingly, the same trend was also reflected in the IKEv1 test scenarios, where FortiGate again led in failover responsiveness, followed by Check Point, with Palo Alto and Cisco demonstrating comparatively slower recovery times. These results underline that vendor-specific implementations and optimizations play a crucial role in determining overall VPN failover performance. The findings emphasize that organizations prioritizing fast reconnection and stable redundancy should carefully consider firewall vendor behavior in addition to protocol configuration when deploying site-to-site VPNs.

Figure {4 illustrates this comparative outcome across vendors.

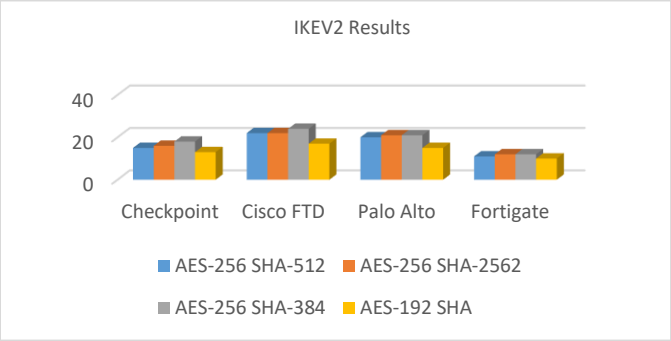

Fig. 4. Failover Time for IKEV2 Tunnel in the different configuration

V. DISCUSSION

In previous studies, research has largely focused on IPv4 and v6 tunneling, often concentrating on the analysis of various hashing and integrity mechanisms and sometimes limited to specific ports. The strength of the present study lies in its ability to provide a comprehensive comparative analysis across different environments and firewalls, evaluating them under a wide range of scenarios.

However, certain parameters were held constant in our experiments, which may have influenced the results. For instance, the network protocols used across all scenarios were fixed, and intermediate devices such as routers and switches were not varied. In addition, the OS (Operating System) models for each firewall could impact the result and if we upgrade JHF or major update it would be change the results. This study shows the results are so close together in Top vendor firewalls and IKEV2 is a little better than IKEV1. Based on the previous research the hashing with less numbers are better than high number in the encryption and decryption process so have a better failover time. For example, SHA is quicker than SHA256[31][32].

VI. CONSLUSION AND RECOMANDATION

In future research, a key focus could be on incorporating cloud-based firewalls into the benchmarking framework. This would involve evaluating and comparing firewalls from major cloud platforms such as Azure, AWS, and GCP. For example, cloud-native VPN solutions like Azure Native VPN, AWS VPN, and GCP VPN could be included in the analysis, allowing for a direct comparison of their performance and behaviour under similar conditions.

Moreover, when focusing on different firewall vendors, comparisons could be conducted by scheduling tests so that systems are evaluated within a closely matched timeframe. This would help minimize the influence of system aging or environmental changes on the results, ensuring that observed differences reflect the firewall configurations themselves rather than external factors. Addressing these aspects will enable future studies to provide a more comprehensive and reliable understanding of both traditional and cloud-based firewall performance across diverse scenarios. [33].

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] Romadhoni, M. K., Kenanga, L. S., Akbi, D. R., & Risqiwati, D. (2025). Performance Evaluation of Outgoing Interface Selection Method on Fortigate SD-WAN for Network Optimization. *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control*.

[2] Frahim, J., Santos, O., & Ossipov, A. (2014). *Cisco ASA: All-in-one Next-Generation Firewall, IPS, and VPN Services*. Cisco Press.

[3] Fabbri, R., & Volpe, F. (2013). *Getting started with fortigate*. Packt Publishing Ltd.

[4] Alvisyahri, M. G. (2023). PERANCANGAN DAN IMPLEMENTASI VPN METODE IPSEC SITE TO SITE MENGGUNAKAN FORTIGATE PADA PT. LINKSINDO MAKMUR. *Jurnal Jaringan Komputer dan Keamanan*, *4*(3), 1-10.

[5] Bezirganoglu, S. (2020). Securing Cloud with Palo Alto Networks Firewalls.

[6] Stiefel, B. J., & Desmeules, S. (2005). *Configuring Check Point NGX VPN-1/FireWall-1*. Elsevier.

[7] Hamed, H., Al-Shaer, E., & Marrero, W. (2005, November). Modeling and verification of IPSec and VPN security policies. In *13th IEEE International Conference on Network Protocols (ICNP'05)* (pp. 10-pp). IEEE.

[8] Alia, O., Huang, A., Luo, H., Amer, O., Pistoia, M., & Lim, C. (2024). 100 Gbps quantum-safe IPsec VPN tunnels over 46 km deployed fiber. arXiv.

[9] 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.

[10] Zhonghua, Y., & Lingda, W. (2016, August). Summary on network security visual analysis. In *2016 7th IEEE International Conference on Software Engineering and Service Science (ICSESS)* (pp. 989-991). IEEE.

[11] Tan, G. (2006). A performance analysis of BGP/MPLS VPN failover functionality (Master's thesis). Naval Postgraduate School.

[12] Fischer, T. (2019). Comparing VPN performance: State-of-the-art solutions in stable vs. unreliable networks. University of Skövde.

[13] Pudelko, M., Emmerich, P., Gallenmüller, S., & Carle, G. (2020). Performance analysis of VPN gateways. In Proceedings of the Networking Conference (pp. 1–9). IFIP.

[14] Aung, S. T., & Thein, T. (2020, February). Comparative analysis of site-to-site layer 2 virtual private networks. In *2020 IEEE Conference on Computer Applications (ICCA)* (pp. 1-5). IEEE.

[15] Ullah, S., Choi, J., & Oh, H. (2020). IPsec for high-speed network links: Performance analysis and enhancements. Future Generation Computer Systems, 107(C), 112–125.

[16] Jaha, A. A., Shatwan, F. B., & Ashibani, M. (2008, September). Proper virtual private network (VPN) solution. In *2008 the second international conference on next generation mobile applications, services, and technologies* (pp. 309-314). IEEE

[17] Choi, B., & Medina, E. (2023). Creating IPSec Tunnels on Palo Alto Firewalls. In Introduction to Ansible Network Automation: A Practical Primer (pp. 847-865). Berkeley, CA: Apress.

[18] Mahmmod, K. F., Azeez, M. M., & Ahmed, M. A. (2020, October). IPsec cryptography for data packets security within vpn tunneling networks communications. In *2020 International Conference on Electrical Engineering and Informatics (ICELTICs)* (pp. 1-8). IEEE.

[19] Khiat, A., Bahnasse, A., El Khaili, M., & Bakkoury, J. (2017). Study, evaluation and measurement of IEEE 802.16 e secured by dynamic and multipoint VPN IPsec. *Int. J. Comput. Sci. Inform. Secur.(USA)*, *15*(1).

[20] 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. *IEEE Access*, *8*, 139567-139586.

[21] Zhipeng, Z., Chandel, S., Jingyao, S., Shilin, Y., Yunnan, Y., & Jingji, Z. (2018, February). VPN: a boon or trap?: a comparative study of MPLs, IPSec, and SSL virtual private networks. In *2018 Second International Conference on Computing Methodologies and Communication (ICCMC)* (pp. 510-515). IEEE.

[22] Choi, J., Oh, H., & Ullah, S. (2022). Redundant IPsec tunnel using a single WAN connection. Fortinet Technical Tip.

[23] Zohaib, S. M., Sajjad, S. M., Iqbal, Z., Yousaf, M., Haseeb, M., & Muhammad, Z. (2024). Zero Trust VPN (ZT-VPN): A Cybersecurity Framework for Modern Enterprises to Enhance IT Security and Privacy in Remote Work Environments.

[24] Syal, R., & Malik, R. (2010). Performance analysis of IP security VPN. International Journal of Computer Applications, 8(4), 5–9.

[25] Rajore, T., Jithin, S., Gupta, A., Gambhir, K., Prithvi, A., & Chakravarty, S. (2025, June). VPN or Vpwn? How Afraid Should You be of VPN Traffic Identification?. In *2025 9th Network Traffic Measurement and Analysis Conference (TMA)* (pp. 1-11). IEEE.

[26] Strzęciwilk, D., Ptaszek, K., Hoser, P., & Antoniku, I. (2018). A research on the impact of encryption algorithms on the quality of vpn tunnels' transmission. In *ITM Web of Conferences* (Vol. 21, p. 00011). EDP Sciences.

[27] HASHIYANA, V., HAIDUWA, T., SURESH, N., BRATHA, A., & OUMA, F. K. (2020, May). Design and Implementation of an IPSec Virtual Private Network: A Case Study at the University of Namibia. In 2020 IST-Africa Conference (IST-Africa) (pp. 1-6). IEEE.

[28] Ćertić, S. (2024). Integrating multi-WAN, VPN, and IEEE 802.3ad for advanced IPsec. arXiv.

[29] Alia, O., Huang, A., Luo, H., Amer, O., Pistoia, M., & Lim, C. (2024). 100 Gbps quantum-safe IPsec VPN tunnels over 46 km deployed fiber. arXiv.

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

[31] 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

[32] Aung, S. T., & Thein, T. (2020, February). Comparative analysis of site-to-site layer 2 virtual private networks. In *2020 IEEE Conference on Computer Applications (ICCA)* (pp. 1-5). IEEE.

[33] Kurmala, H. K., Ardeli, R., & Iyer, P. (2017). *U.S. Patent No. 9,712,504*. Washington, DC: U.S. Patent and Trademark Office.