Investigating the Effectiveness of Firewalls in Computer Security and Privacy

Mohammad Arsalan Mahmood
MSc Cybersecurity
University of Bradford
Word count 1951 – excluding references

***Abstract*— Firewalls have been at the core of network and system security. My paper will cover the extent to which firewalls remain effective in defending and counterattacking modern cyber threats. I will utilize real-life examples such as the Colonial Pipeline ransomware attack alongside the Target data breach. This study shows a critical evaluation of traditional and next-generation firewalls alongside examining how these tools can be integrated with Zero Trust models and intrusion detection systems. I have concluded that firewalls are vital; however, they must evolve into a broader, adaptive security framework.**

***Keywords*— firewalls, network security, privacy, intrusion prevention systems, zero trust architecture.**

I.INTRODUCTION

Firewalls have been a foundational tool in defending digital infrastructure throughout the timelines of online systems. Firewalls were initially developed to monitor and control the flow of traffic between internal and external networks. Their role evolved to cover complex, multilayered environments including cloud computing, mobile access, and remote connectivity (Scarfone & Hoffman, 2009). However, regardless of these advancements, there are still concerns about how effective firewalls are in addressing the advanced tactics used by modern cyber adversaries.

An example that I have covered is that of the 2021 Colonial Pipeline ransomware incident. In this incident, the perimeter defences were in place; however, the threat actors exploited and utilized exposed credentials and achieved lateral movement within the network, bypassing static firewall controls (Bozorgmehr & Smith, 2023, Section 4.3). Similarly, the Target data breach in 2013 included a similar approach whereby attackers leveraged third-party vendor access – a HVAC company – to infiltrate the network and access critical, sensitive financial data. This failure to implement network and system segmentation allowed the breach to spread further than the initial access point and attack the wider system despite preexisting firewall configurations (Lin, Tuttle & Cheng, 2016, Section 4).

The use of real-world examples pinpoints the necessity of re-evaluating firewall capabilities considering contemporary security expectations, and my aim is to investigate the effectiveness of firewalls and next-gen firewalls in securing modern systems and supporting digital privacy. This paper will cover firewall integration with foundational frameworks such as Zero Trust Architecture (Rose et al., 2020) and how this interlinks with intrusion detection systems. By utilizing academic literature, technical guidelines, and case analysis, this paper explores whether firewalls remain independently effective or must function as a piece in a larger puzzle in terms of broader security.

II. THE EVOLUTION OF FIREWALLS

The idea of a firewall originated in the 1980s with the intention of monitoring and directing the flow of traffic between networks. The earliest concept focused on filtering packets based on static rules, which were simple and became out of use as network threats became more serious and dangerous (Scarfone and Hoffman, 2009).

A. ***Packet Filtering Firewalls*** *– First-generation firewalls operated at the network layer by examining the headers of individual packets. Set rules were configured to allow or deny traffic based on IP address, port, and protocol. Packet filters were resource-efficient; however, they lacked the intelligence to understand context and were not able to inspect payload data, leaving systems vulnerable to spoofing, fragmented attacks, and port scanning (Scarfone and Hoffman, 2009, p.5).*

B. ***Stateful Inspection*** *– To address these issues, stateful inspection emerged. These systems maintained a table of active connections, allowing them to monitor traffic flow and make more intelligent decisions, such as tracking TCP protocols. However, as encrypted traffic and malware increased, stateful inspection mechanisms struggled with visibility and detection precision (Chowdhary et al., 2018).*

C. ***Application-Aware Proxy Firewalls*** *– With the rise of web applications, proxy firewalls became crucial. Operating at the application layer, they served as intermediaries between users and servers and inspected protocol-specific commands such as HTTP and FTP. This helped prevent attacks like SQL injection, though they introduced latency and scaling issues due to protocol reassembly and analysis (Stankovic and Simic, 2010).*

D. ***Next-Gen Firewalls*** *– These systems combined stateful inspection with deep packet inspection, intrusion prevention, application identification, and user-based policies. They detect malicious payloads in encrypted traffic and leverage real-time threat intelligence, but require frequent updates and skilled configuration (Heino, Hakkala and Virtanen, 2022).*

E. ***Cloud-Based Firewalls*** *– As businesses migrate to cloud platforms, traditional perimeter-based firewalls fail to adapt. Solutions like AWS and Azure embed firewall logic into each virtual machine, supporting identity-based access, micro segmentation, and dynamic enforcement. This reflects a shift toward context-aware security aligned with Zero Trust principles (Theodoropoulos et al., 2023, pp. 772–775).*

III. EVALUATING EFFECTIVENESS OF FIREWALLS IN THE MODERN SECURITY LANDSCAPE

Firewalls have served as essential security tools across industries all over the world; however, the question remains whether they can offer stand-alone protection. They offer many capabilities such as traffic filtering, access control, and protocol enforcement, but evolving attack techniques, encryption, and decentralisation of infrastructure all pose huge risks to traditional firewall design. An example of this is the Colonial Pipeline ransomware attack in 2021. What occurred is that the attackers bypassed the firewall protection by exploiting VPN credentials that had been compromised. Even though perimeter controls were in place, the firewalls failed to detect lateral movement and the ransomware payload within the system. The main reason being a lack of segmentation and monitoring (Bozorgmehr and Smith, 2023). This clearly shows that without proper integration with detection tools and identity-based controls, firewalls are not able to prevent breaches on their own.

Another key example of this would be the Target data breach. This incident showed us that attackers can exploit third-party access and how lateral movement works. In this specific case, attackers used stolen credentials from a third-party vendor – HVAC – to gain access to the internal system. What was apparent was that firewalls had been misconfigured, and due to poor segmentation, attackers were able to access more sensitive systems and then exfiltrate over 40 million credit card records (Data breach: analysis, countermeasures and challenges, 2022). In addition to this, the increasing use of end-to-end encryption in network traffic poses more challenges to traditional firewalls. Encrypted traffic cannot be inspected without the pairing of SSL/TLS interception or dedicated decryption appliances, which introduces the issues of latency and privacy concerns. As a result, threat actors can mask command-and-control activity, malware delivery, and data exfiltration throughout encrypted traffic whilst bypassing perimeter controls entirely (Heino, Hakkala and Virtanen, 2022).

If firewalls are properly configured and integrated into a multi-layer defence strategy, firewalls can play a crucial role. Next-gen firewalls can offer deep insight into packets, user-aware access policies, and application-layer visibility, and these are effective when deployed with tools such as SIEM, IDS/IPS, and Zero Trust Network Access (Theodoropoulos et al., 2023). To summarise, firewalls do remain an important line of defence but only when their capabilities are extended through integration, monitoring, and correct policy enforcement. They are no longer sufficient as isolated controls, especially against lateral movement, insider threats, and encrypted attack vectors.

IV. FIREWALLS IN MODERN SECURITY ARCHITECTURE

In contemporary cybersecurity frameworks, firewalls have adapted from a singular perimeter defense to an integral part of a more advanced multi-layered security architecture. Their role now is to monitor traffic, enforce security policies, and respond to threats in real time.

Integration with Zero Trust Architecture *– This model ensures that security is predicated on the phrase "never trust, always verify," which requires continuous authentication of users and devices. Firewalls that act alongside ZTA as Policy Enforcement Points ensure that access requests comply with security rules. This integration allows firewalls to be context-aware and able to adapt to dynamic network conditions and user behaviours (Rose et al., 2020, pp. 12–14).*

SIEM Integration *– Modern firewalls are significant log generators; however, their usage depends on integration with SIEM tools that can analyse and correlate logs from different sources. The increasing usage of encrypted traffic poses challenges for inspection. Implementing SSL/TLS inspection allows firewalls to decrypt and analyse encrypted traffic to ensure that threats are not hidden. This process allows for increased security monitoring (Sangfor Technologies, 2025).*

IDS/IPS Systems *– Firewalls may block traffic based on static rules, while IDS/IPS systems analyse behavioural anomalies. However, when integrated, they offer stronger protection, allowing firewalls to react to lateral movement and behavioural anomalies. This combination is discussed in adaptive architecture proposals such as Ahmadi (2025), where automated updates improve firewall policies in real time.*

Cloud-Based and Containerised Environments *– In cloud systems, firewalls are distributed and integrated into systems. For example, Kubernetes uses CNI plugins (e.g., Calico) to apply network policies at the pod level. Theodoropoulos et al. (2023, pp. 771–775) describe how services combine and how cloud services provide east-west traffic controls, replacing traditional perimeter models.*

AI and Behavioural Firewalls *– New research has covered the idea of machine learning-driven firewalls adapting to traffic anomalies over time. These systems can leverage retraining software from SIEM, EDR, and behaviour profiling to create autonomous response policies (Ahmadi, 2025, p. 4).*

V. ***LIMITATIONS AND FUTURE CHALLENGES***

Limitations

1. *Firstly, there is the reactive nature of threat dependency. NGFWs and traditional firewalls operate on predefined sets of rules and threat signatures. This limits their effectiveness against sophisticated attacks. As presented by ArmorPoint (2024), firewalls are known to be configured against known threats, making them less effective against zero-day exploits and evolving malware.*
2. *A major issue with encrypted traffic is that the increased usage of protocols such as HTTPS and SSL/TLS poses significant challenges for firewalls. Encrypted traffic is able to hide malicious activities, which renders regular inspection methods ineffective. Without proper detection capabilities, firewalls would not be able to detect threats from an encrypted data stream.*
3. *Limited visibility in cloud environments – As organisations migrate to the cloud, traditional firewalls struggle to provide the correct visibility and control. The dynamic nature of cloud environments, alongside the ever-changing nature of services, complicates the deployment of consistent security policies.*

Future Challenges

The integration of AI and ML presents both challenges and opportunities. While AI can enhance threat detection and response times, it introduces issues such as model training, false positives, and the need for continuous learning. Research by Ahmadi (2025) discusses the design and deployment of retrainable firewalls, showing the need for real-time adaptability.

Adapting to Zero Trust models – The shift towards ZTA requires firewalls to move beyond perimeter-based defences. Implementing ZTA involves continuous verification of users and devices, micro-segmentation, and strict access controls. The Cloud Security Alliance (2025) highlights how AI is used to strengthen ZTA by enabling real-time threat identification and adaptive access control.

The growth of IoT devices ensures that firewalls must adapt to manage the diverse and often resource-constrained nature of IoT devices, ensuring secure communication and limiting unauthorised access.

Evolving regulatory landscapes mean that firewalls must not only provide robust security but also support compliance with standards such as GDPR, HIPAA, etc. Ensuring that firewall implementation aligns with these regulations can be a challenge.

Vi conclusion

This paper has set out to answer the following question – How effective are modern firewalls in securing computer environments, and what limitations must we understand to ensure future resilience? After utilising academic references, studies, and frameworks, we have concluded that firewalls alone are an incomplete component of modern cybersecurity strategy. Next-gen firewalls offer capabilities such as deep packet inspection, application filtering, and integration with SIEM and Zero Trust. The effectiveness of this depends on configuration, context, and real-time integration.

They still face issues with encrypted traffic, policy enforcement, and cloud scalability. The research highlights that firewalls must evolve from static perimeter tools to a more dynamic approach embedded in modern architecture. New technologies such as AI rule adaptation and distributed policy enforcement suggest positive future directions but still require rigid design and oversight. Ultimately, firewalls are most effective not individually, but as a component within a multi-layered, intelligence-driven security framework.

REFERENCES

Check the university referencing style here:
http://www.brad.ac.uk/library/help/referencing/referencing/

1. *Scarfone, K. and Hoffman, P., 2009. Guidelines on Firewalls and Firewall Policy. NIST Special Publication 800-41 Revision 1. [online] Gaithersburg, MD: National Institute of Standards and Technology. Available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf [Accessed 11 Apr. 2025].*
2. *Bozorgmehr, N. and Smith, S., 2023. Analysis of the Colonial Pipeline Cybersecurity Incident. [online] ResearchGate. Available at: https://www.researchgate.net/publication/387104186_Analysis_of_the_Colonial_Pipeline_Cybersecurity_Incident#fullTextFileContent [Accessed 11 Apr. 2025].*
3. *Lin, X., Tuttle, H. and Cheng, M., 2016. Third-party risk and network vulnerabilities: Lessons from the Target data breach. Computers & Security, 59, pp.44–56. Available at: https://www.sciencedirect.com/science/article/pii/S0167404816000043?via%3Dihub [Accessed 11 Apr. 2025].*
4. *Rose, S., Borchert, O., Mitchell, S. and Connelly, S., 2020. Zero Trust Architecture. NIST Special Publication 800-207. [online] Gaithersburg, MD: National Institute of Standards and Technology. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf [Accessed 11 Apr. 2025].*
5. *Chowdhary, A., Huang, D., Alshamrani, A., Sabur, A., Kang, M. and Kim, A., 2018. SDFW: SDN-based Stateful Distributed Firewall. [online] arXiv. Available at: https://arxiv.org/abs/1811.00634 [Accessed 11 Apr. 2025].*
6. *Stankovic, S. and Simic, D., 2010. A Holistic Approach to Securing Web Applications. [online] arXiv. Available at: https://arxiv.org/abs/1001.3479 [Accessed 11 Apr. 2025].*
7. *Heino, J., Hakkala, A. and Virtanen, S., 2022. Study of methods for endpoint aware inspection in a next generation firewall. Cybersecurity, 5(1), p.25. Available at: https://cybersecurity.springeropen.com/articles/10.1186/s42400-022-00127-8 [Accessed 11 Apr. 2025].*
8. *Theodoropoulos, T., Rosa, L., Benzaid, C., Gray, P., Marin, E., Makris, A., Cordeiro, L., Diego, F., Sorokin, P., Di Girolamo, M., Barone, P., Taleb, T. and Tserpes, K., 2023. Security in Cloud-Native Services: A Survey. Journal of Cybersecurity and Privacy, 3(4), pp.758–793. Available at: https://www.mdpi.com/2624-800X/3/4/34 [Accessed 11 Apr. 2025].*
9. *Bozorgmehr, N. and Smith, S., 2023. Analysis of the Colonial Pipeline Cybersecurity Incident. [online] ResearchGate. Available at: https://www.researchgate.net/publication/387104186_Analysis_of_the_Colonial_Pipeline_Cybersecurity_Incident#fullTextFileContent [Accessed 13 Apr. 2025].*
10. *Data breach: analysis, countermeasures and challenges, 2022. Data breach: analysis, countermeasures and challenges. [online] ResearchGate. Available at: https://www.researchgate.net/publication/365721658_Data_breach_analysis_countermeasures_and_challenges [Accessed 13 Apr. 2025].*
11. *Sangfor Technologies, 2025. SSL Inspection: The Essential Guide to Securing Encrypted Traffic. [online] Available at: https://www.sangfor.com/glossary/cybersecurity/ssl-inspection [Accessed 13 Apr. 2025].*
12. *Ahmadi, S., 2025. Adaptive Cybersecurity: Dynamically Retrainable Firewalls for Real-Time Network Protection. [online] arXiv. Available at: https://arxiv.org/abs/2501.09033 [Accessed 13 Apr. 2025].*
13. *ArmorPoint, 2024. The Limitations of Firewalls in Modern Security. [online] Available at: https://armorpoint.com/2024/01/04/the-limitations-of-firewalls-in-modern-security/ [Accessed 13 Apr. 2025].*
14. *Ahmadi, S., 2025. Adaptive Cybersecurity: Dynamically Retrainable Firewalls for Real-Time Network Protection. [online] arXiv. Available at: https://arxiv.org/abs/2501.09033 [Accessed 13 Apr. 2025].*
15. *Cloud Security Alliance, 2025. How is AI Strengthening Zero Trust? [online] Available at: https://cloudsecurityalliance.org/blog/2025/02/27/how-is-ai-strengthening-zero-trust [Accessed 13 Apr. 2025].*