FUDMA Journal of Sciences (FJS)
ISSN online: 2616-1370
ISSN print: 2645 - 2944
Vol. 9 No. 12, December, 2025, pp 20 – 25
DOI: https://doi.org/10.33003/fjs-2025-0912-4049

EFFICACY AND LIMITATIONS OF FIREWALL CONFIGURATIONS IN PREVENTING NETWORK ATTACKS: A CONCEPTUAL REVIEW OF ARCHITECTURES AND RULE SETS

***[1]Adamu Bashir Ismail, [2]Mukhtar Ibrahim Hussaini, [1]Suleiman Abba Abubakar, and [1]Abdulmalik Ahmad**

[1]Department of Computer science and Technology, Umaru Ali Shinkafi Polytechnic Sokoto, Sokoto State, Nigeria.
[2]Department of Computer Science, Rayhaan University Birnin Kebbi, Kebbi State, Nigeria.

*Corresponding authors' email: biadamu377@gmail.com

ABSTRACT

Firewalls remain a central part of network security architectures, but their effectiveness is continually challenged by changing cyber threats and complex deployment settings. This conceptual review provides a full description of strengths and limitations of different firewall technologies, such as packet-filtering, stateful inspection, or next-generation firewalls (NGFWs) to combat modern network attacks. The study adopted a structured literature review methodology, analyzing peer-reviewed journal articles, conference papers, and authoritative reports published between 2010 and 2024 to identify key trends, challenges, and advancements in firewall research. This paper incorporates existing literature to investigate the relationship between firewall architecture, rule-set management and threat detection capabilities. The results revealed that while NGFWs are better defended against application-layer and encrypted threats by deep packet inspection (DPI), and intrusion prevention systems (IPS), they are much more complex than the NGFWs themselves are by providing much higher performance overhead and configuration complexity. It provides further work on the still significant issue of rule-set misconfiguration, as a source of security vulnerabilities, and new developments such as AI in adaptive security or Zero Trust architectures. This review concludes that a comprehensive approach to networking security consists of proper firewall technology combined with proper policy management and architectural best practices. Future research is designed to standardize AI-driven firewall evaluation and expand security frameworks in cloud-native and IoT environments.

Keywords: Firewall, Network Security, Next-Generation Firewall (NGFW), Rule-Set Configuration, Deep Packet Inspection, Zero Trust, Cybersecurity

INTRODUCTION

Cloud computing, growth of mobile workers and IoT have increased the surface area of network perimeter, but the network perimeter has evolved into a more dynamic and distributed boundary but now it is becoming a more porous perimeter due to the demands of cloud computing, mobile workforce trends, and IoT. Although modern security mechanisms and research have strengthened perimeter defenses, challenges still exist in maintaining consistent protection across such environments (Stallings, 2019). However, the increasing sophistication of cyber threats such as advanced persistent threats (APTs) and polymorphic malware keeps the effectiveness of traditional firewall configurations and static rule sets testing increasingly.

This highlights a persistent gap between the theoretical security potential of modern firewall technologies and their real-world performance under dynamic network conditions. Next-Generation Firewalls (NGFWs) offer advanced features but can cause misconfiguration and performance degradation (Hayajneh et al., 2013, Neupane et al., 2018). The Zero Trust model prohibits "never trust, always verify" in order to defend perimeter defense as the central principle of perimeter defense admonishes the original model.

This conceptual review is designed to combine existing literature with what is needed to critically consider the effectiveness and limitations of firewall configurations. These goals are threefold: (i) to describe a taxonomy of firewall technologies and architectures (ii) to assess their effectiveness against a variety of network attackers (iii) to discuss important trade-offs and emergent paradigms. By looking at the interplay between technology, policy and architecture, this paper provides an example of how firewalls can be applied as effectively in the present network landscape.

MATERIALS AND METHODS

Methodology

This review was designed as a systematic process to identify and analyze the pertinent literature. They searched the vast literature databases of IEEE Xplore, ACM Digital Library, Scopus and Web of Science. The search terms for the following things included "firewall configuration," "next-generation firewall (NGFW) performance," "firewall rule-set management," Deep Packet Inspection (DPI) overhead, "Zero Trust architecture," and "AI in network security." A total 20 sources from 2010 - 2024, the inclusion criteria were those journal articles, conference proceedings, books and authoritative reports from recognized bodies (e.g., NIST, SANS) who were published. By evaluating the literature under three criteria: i) effectiveness, ii) limitations – performance overhead, complexity and architectural constraints, and iii) evolution – new patterns and future directions.

Foundations of Firewall Technology: A Taxonomy

Core Principles and Operational Models

A firewall is a hardware, software, or combination of both systems that is designed to monitor, filter, and control the input/output traffic on a security rule that is designed to be set down for a specific security function (Stallings, 2019). Firewalls are barrier or gatekeepers between a trusted internal network and an anonymous external network such as the Internet (Kizza, 2024). Firewalls are a component of network security architecture and used to protect against unauthorized access, detect malicious actions and enforce security policies (Scarfone & Hoffman, 2009). They can be operating at different layers of OSI model, from network level to application level, for example, from inspecting HyperText Transfer Protocol (HTTP) or Domain Name System (DNS)

protocol and inspecting HTTP or DNS protocol (Gabriele & Ghafir, 2024).

Evolution of Firewall Technologies

Firewall technology has evolved significantly to address emerging threats.

Packet-Filtering Firewalls

At the network and transport layers, Layer 3 & 4, these are the easiest to operate, with IP addresses, port numbers and protocols being determined. They offer high performance but are not context aware, and can be easily invulnerable to IP spoofing and complicated attacks (Stallings, 2019).

Stateful Inspection Firewalls

Stateful inspection firewalls improve traditional packet filtering with an active state table and a current network connection state table. These firewalls detect active connections, such as TCP handshakes, that provide greater security than static packet filters by separating legitimate traffic packets from malicious packets of SYN flood attacks (Check Point, 2021). While packet filter and stateful firewalls need more resources than packet filters, they provide improved security, without significantly changing performance.

Proxy Firewalls (Application-Level Gateways)

An intermediary for different applications, proxy firewalls terminate and re-start connections on behalf of clients. This can allow deep content analysis but does provide latency and cannot be used for all applications (Kizza, 2020). Proxy firewalls are frequently used in environments that need strict content filtering education or corporate web gateways.

Next-Generation Firewalls (NGFWs)

Next-generation firewalls incorporate various security functions, including deep packet inspection (DPI), intrusion prevention systems (IPS), SSL/TLS decryption, and application-aware filtering decryption. This allows for large-scale control over applications and users, but costs high computational costs (Ahmad, 2025). NGFWs are particularly effective in modern networks where encrypted traffic and advanced threats are common, but their comprehensive inspection abilities can be a risk to performance compromises.

Cloud Firewalls (FWaaS)

Firewall-as-a-Service is a cloud-based, secure, cloud-native, multi-cloud security software that can be deployed in any cloud-based infrastructures and provide a secure system of security across distributed networks in hybrid and multi-cloud environments. (Gartner, 2022). They seamlessly integrate into cloud platforms and SD-WAN environments providing consistent security policies across distributed networks. Examples include Zscaler's cloud firewall, AWS Network Firewall, which serves hybrid or fully cloud-based environments.

Firewall Architectures and Deployment Strategies

Firewall architecture defines the direction and structure of the firewall in order to enforce security policies in the network. These deployment models estimate how traffic flows across security checkpoints and the isolation of different network segments. Figures 1–5 illustrate key firewall architectures examined in this review. Figure 1 shows the Bastion Host Architecture, which relies on a single fortified gateway between trusted and untrusted networks but introduces a single point of failure. Figure 2 depicts the Screened Subnet (DMZ) Architecture, where dual firewalls isolate public-facing servers in a DMZ for enhanced security. Figure 3 presents the Dual-Homed Host Architecture, using two NICs to separate external and internal traffic through proxy mediation. Figure 4 illustrates the Screened Host Architecture, combining a packet-filtering router and bastion host for layered inspection. Figure 5 displays the Multi-Tiered (Hybrid) Architecture, which integrates DMZ segmentation with Zero Trust and cloud-managed virtual firewalls for adaptive, multi-layered defense.

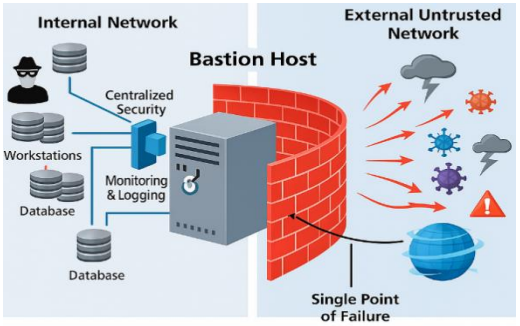

Figure 1: Bastion Host Architecture

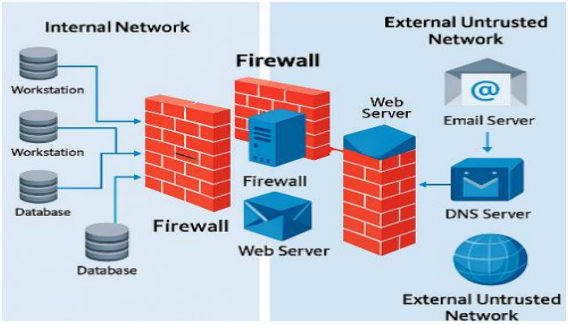

Figure 2: Screened Subnet (DMZ) Architecture

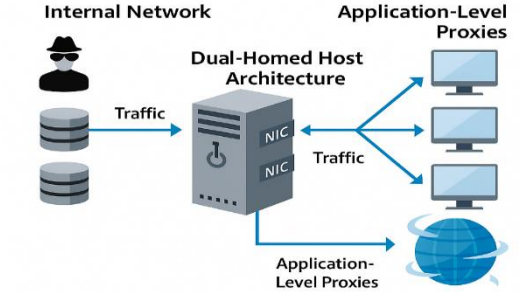

Figure 3: Dual-Homed Host Architecture

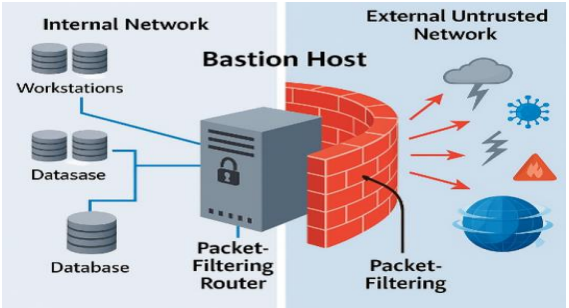

Figure 4: Screened Host Architecture

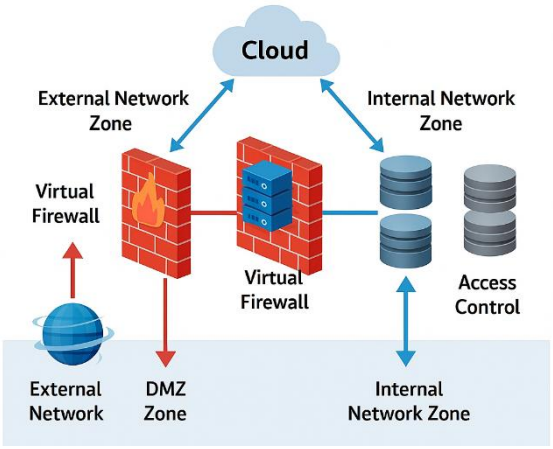

Figure 4: Multi-Tiered (Hybrid) Architecture

i. Bastion Host Architecture

The bastion host architecture employs a single, heavily fortified firewall that serves as the sole gateway between an internal network and external untrusted networks, typically the internet. This architecture is designed to withstand direct attacks, as the bastion host is deliberately exposed to potential threats. According to Stallings (2019), this approach centralizes security monitoring and logging but creates a single point of failure. Organizations with limited resources or simple network topologies often use bastion hosts, though they are less suitable for high-availability environments due to their lack of redundancy.

ii. Screened Subnet (DMZ) Architecture

The screened subnet, or demilitarized zone (DMZ), architecture is one of the most secure and widely adopted firewall deployment models. The firewall is used for either the two firewalls or a single firewall with dual interfaces to create a middle network portion of its network with public-facing services such as web servers, email servers, and DNS. In Scarfone and Hoffman (2009), they argue that this design can be characterized by creating the inner firewall which makes possible even in case a security threat blocks the DMZ. This architecture was used by organizations that need to secure outside access to services, while maintaining internal network integrity.

iii. ***Dual-Homed Host Architecture***

A dual-homed host architecture is a firewall with two Network Interface Cards (NICs) that connect one to the outside network and another to the internal network. In contrast to router-based firewalls, this design does not allow direct IP forwarding because all traffic must pass through application-level proxies or gateways. Kizza (2024) noted that this architecture is fine-grained over traffic control but requires proxy mediation, providing performance bottlenecks. For instance it is often used in environments in which traffic inspection is necessary, such as research institutes or secure government networks.

iv. ***Screened Host Architecture***

The screened host structure uses a packet filtering router and bastion host to create a layer of defense against the enemy. The router performs initial traffic filtering based on access control lists or ACLs; whereas the bastion host uses stateful or proxy-based inspection primarily to conduct deeper inspection. Gabriele and Ghafir (2024) show how this model is well-suited to mid-sized organizations for security and flexibility. But, it does not create the compartmentalization advantages of a DMZ that is better for high-risk environments.

v. ***Multi-Tiered (Hybrid) Architecture***

Modern networks increasingly employ multi-tiered architecture that blends traditional DMZ design with internal segmentation, often in line with Zero Trust models. The hybrid approach reinforces security by applying strict access controls between different network zones, including internal network zones. Clouds, particularly, benefit greatly through this architecture by synchronizing virtual firewalls with software-defined networking (SDN) to achieve dynamic policy enforcement.

The Centrality of Rule-Set Management

Firewall rule-sets consist of a list of instructions that a firewall employs to process network traffic by either dropping or permitting data packets depending on set parameters. The instructions serve the purpose of policy enforcement and help organizations regulate traffic depending on source and destination IP address, port, protocol, and several other attributes. Rule-sets are important in stipulating the working functionality of a firewall and how to determine which traffic is malicious or safe (Scarfone & Hoffman, 2009).Typically, each rule consists of five fundamental components:

i. ***Source Address:*** The network or IP address that network traffic is coming from.
ii. ***Destination Address:*** Shows the preferred IP address or network.
iii. ***Protocol:*** It defines the transport layer protocol (e.g., TCP, UDP, and ICMP)
iv. ***Port Number:*** specifies the actual application port being run (e.g., port 80 with HTTP).
v. ***Action:*** Determines whether the firewall should allow or deny the traffic.

The rules run within a hierarchical order, such that the firewall processes rules based on their order listed and takes action on the rule that matches the first traffic. As such, rule ordering within a rule-set is of crucial significance. A poorly organized rule-set can cause access by mistake or interfere with legitimate traffic (Kurose & Ross, 2021).

Types of Rules

i. ***Allows Rules:*** Permit specific traffic that matches rules.
ii. ***Deny/Drop Rules:*** Stop traffic, either quietly (drop) or with a rejection message (deny).
iii. ***Default Deny Rule:*** Typically positioned at the conclusion of the rule-set, this mechanism serves to obstruct all traffic that does not correspond with any

preceding rule, consequently upholding a principle of "least privilege" (Stallings, 2019).

Analyzing Efficacy against Modern Network Attacks

The efficacy of a firewall depends heavily on the attack vector being considered. Recent empirical and experimental studies provide insight into how well different firewall types handle conventional, application-layer, and encrypted attacks.

Conventional Attacks (e.g., DoS, Port Scans)

Stateful inspection firewalls remain effective against the majority of volumetric and reconnaissance attacks. For instance, firewall layers that have been augmented with the aid of deep learning have been able to attain over 97% detection of denial-of-service (DoS) traffic while keeping the false positives to a low rate (Dawadi, Adhikari, & Srivastava, 2023; Suthar & Patel, 2023; Talukder et al., 2025). Connection state monitoring can also be effective against port scanners; however, with increased traffic conditions and without hardware acceleration, the performance will be adversely affected (Suthar & Patel, 2023)

***Application-Layer Attacks (e.g., SQLi, XSS*)**

Packet-filtering and traditional state-based firewalls prove significantly inefficient against SQL injection (SQLi) and cross-site scripting (XSS) attacks due to the lack of proper capabilities to inspect payloads. Next-Generation Firewalls (NGFWs), with their integration of deep packet inspection (DPI) and intrusion prevention systems (IPS), show higher effectiveness, particularly with the supplementation of artificial intelligence models (Heino et al., 2022). A recent study employing deep learning approaches to web application firewalls showed detection effectiveness reaching nearly 90% against SQLi and XSS attacks (Dawadi et al., 2023). However, with the example of adversarial attacks by AdvSQLi, many commercial-grade web application firewalls (WAFs) are prone to evasion, thus exposing the vulnerability inherent to signature-based defense strategies (Qu et al., 2024).

Encrypted Traffic (TLS/SSL)

Encrypted traffic poses one of the strongest challenges to firewall effectiveness. Examining Transport Layer Security (TLS) flows frequently necessitates SSL/TLS decryption, a process that proves to be computationally expensive and causes latency and privacy issues. Benchmark research confirmed that having TLS decryption enabled can decrease throughput by 50–60% within commercial NGFWs, particularly using TLS 1.3 (Gigamon, 2023). AI-based adaptive firewalls can enhance detection precision against encrypted malware but with increased computational requirements and latency (Ahmad, 2025).

APTs and Zero-Day Exploits

Firewalls, including Next-Generation Firewalls (NGFWs), don't really fare that well against uncovering and preventing advanced persistent threats (APTs) and zero-day exploits. The overwhelming majority of commercially available firewalls rely on signature-based identification or general threat patterns that actually are reactive by design. They don't hold up very well against new or obfuscated attacks (Sommer & Paxson, 2010).

Critical Analysis of Inherent Limitations and Trade-Offs

Despite their evolution, firewalls face inherent limitations that challenge their efficacy in modern enterprise and cloud environments. These limitations often manifest as trade-offs between performance, scalability, usability, and architectural fit.

The Performance–Security Trade-Off

Higher-end NGFW features such as DPI, intrusion prevention, and SSL/TLS decryption can significantly slow down performance. Tests have proved that enabling SSL inspection can reduce throughput by 35–60% and induce higher latency, mostly on high-speed or encrypted traffic deployments (Gigamon, 2023; Ahmad, 2025). This creates bottlenecks in organizations with gigabit- or terabit-scale traffic that forces admins to make tradeoffs between network speed and depth of inspection.

Scalability Challenges

Traditional hardware firewalls provide limited flexibility and cannot adapt dynamically to heterogeneous workloads. Firewall-as-a-service (FWaaS) solutions that reside within cloud infrastructure offer higher scalability, while they add vendor lock-in issues, common accountability, and visibility (Liu et al., 2014). Hybrid methods that mix on-premises next-generation firewall (NGFW) devices with cloud-native controls increasingly come into scrutiny to strike a balance between flexibility and control.

The Human Factor in Configuration

Misconfigurations continue to be a key cause of firewall breaches. Overlapping of policies, overly complex graphical user interface (GUIs), and poor validation mechanisms cause mistakes by administrators. A recent systematic review of firewall misconfigurations reaffirmed that configuration complexity is strongly associated with exploitable vulnerabilities (Alkhalil et al., 2021). Usability studies add emphasis that security tools should be designed with human understanding; otherwise, they will too often not be effective (Furnell & Clarke, 2012). New approaches such as policy abstraction (e.g., ForestFirewalls) and verification automation are being made to tackle this problem.

Architectural Limitations in a Zero-Trust Era

Traditional firewalls rely on a perimeter-based security model that assumes a clear differentiation between an internal trusted network and an external untrusted network. But with the scenario of today's cloud-centric and remote-work environments, this model becomes ever increasingly obsolete. The Zero Trust security model advocates identity-based policies, perpetual verification, and micro segmentation, thus reducing reliance on perimeter firewalls as the sole enforcement mechanism (Rose et al., 2020; CISA, 2023). This conceptual shift calls for a reassessment of firewall deployment as part of an overall, multi-layered Zero Trust architecture rather than just a perimeter-based defense by itself.

Emerging Paradigms and Future Directions

The future of firewalls lies in greater intelligence and integration.

Towards Adaptive Security

The papers go on to discuss using Machine learning to detect anomalies and Reinforcement learning to adaptively tune rules. They will be able to respond to new attacks in real-time but will require significant computing resources and induce anxieties over adversarial attacks (Apruzzese et al., 2023).

Integration with Zero-Trust Architectures

Firewalls are being repositioned from perimeter guardians to policy enforcement points (PEPs) of a Zero Trust network. The initiative involves the installation of identity-aware proxies and micro segmenting to implement least-privilege access across the network (Rose et al., 2020).

The Future of Policy Management

The trend is towards intent-based networking and policies that are automatically generated by higher-security intentions, with less human error and ease of management of distributed, heterogeneous systems (He et al., 2023).

RESULTS AND DISCUSSION

Discussion

Synthesis and Conceptual Framework

This review demonstrates that the success of a firewall is not determined by technology alone but by the dynamic interrelationship between its architecture (placement and design), its configuration (the quality and sophistication of the rule-set), and the threat horizon that faces it. These conceptual models of selection and deployment will have to account for organizational context. For a high-performance data center, a basic packet-filtering firewall may be acceptable for internal segmentation. However, an e-commerce site demands an NGFW within a DMZ design to ward off attacks against web applications. The solution lies in aligning the capabilities and positioning of the firewall with the inherent security demands and performance limitations of the environment. The trend of developing adaptive, AI-based firewalls within a Zero Trust model holds the best future potential for keeping defense effective

.

CONCLUSION

Firewalls continue to be a core, if evolving, component of network defense. This overview drew a simple line: from simple packet filters, to integrated, application-savvy NGFWs, and now to intelligent, adaptive systems within Zero Trust architectures. The key problems here remain the performance costs of deep inspection, the management burden of rule-sets, and the design shift away from a hardened perimeter. The takeaway is that not one firewall technology or architecture is best suited to everyone. Successful security is about a defense-in-depth that employs firewalls judiciously, chosen, set up, and situated within the context of a comprehensive security ecosystem that takes in intrusion detection, threat intelligence, and robust identity and access control. Future success will be predicated on taking advantage of automation and artificial intelligence to control complexity while embracing the borderless nature of today's networks. In summary, each firewall defense method has its own pros and cons. Packet-filtering and stateful firewalls are easy to use and fast, but they don't do deep inspection. Next-Generation Firewalls (NGFWs) and proxy-based systems offer strong protection for applications and encrypted traffic, but they cost more to run and manage. Adaptive firewalls that run on the cloud and use AI improve scalability and threat response, but they need more computing power. The best way to do this is to use a layered, context-aware deployment that matches the types of firewalls to the needs of the organization. This will ensure a balanced defense between performance, adaptability, and security resilience.

REFERENCES

Ahmad, T. (2025). *AI-driven dynamic firewall optimization using reinforcement learning for anomaly detection and prevention*. arXiv. https://arxiv.org/abs/2506.05356

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science, 3*, 563060. https://doi.org/10.3389/fcomp.2021.563060

Apruzzese, G., Laskov, P., De Oca, E. M., Mallouli, W., Rapa, L. B., Grammatopoulos, A. V., & Di Franco, F. (2022). The role of machine learning in cybersecurity. *Digital Threats Research and Practice, 4*(1), 1–38. https://doi.org/10.1145/3545574

Check Point. (2021). *Stateful inspection technology*. Check Point Software Technologies. https://www.checkpoint.com/resources/stateful-inspection-technology

CISA. (2023). *Zero trust maturity model, version 2.0*. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/resources-tools/resources/zero-trust-maturity-model

Dawadi, B. R., Adhikari, B., & Srivastava, D. K. (2023). Deep learning technique-enabled web application firewall for the detection of web attacks. *Sensors, 23*(4), 2073. https://doi.org/10.3390/s23042073

He, K., Kim, D. D., & Asghar, M. R. (2023). Adversarial Machine Learning for Network Intrusion Detection Systems: A Comprehensive survey. *IEEE Communications Surveys & Tutorials, 25*(1), 538–566. https://doi.org/10.1109/comst.2022.3233793

Heino, J., Hakkala, A., & Virtanen, S. (2022). Study of methods for endpoint aware inspection in a next generation firewall. *Cybersecurity, 5*(1). https://doi.org/10.1186/s42400-022-00127-8

Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. *Computers & Security, 31*(8), 983–988. https://doi.org/10.1016/j.cose.2012.08.004

Gigamon. (2023, April 7). *Right-sizing decryption functionality for your network*. Gigamon Blog. https://blog.gigamon.com/2023/04/07/right-sizing-decryption-functionality-for-your-network

Hayajneh, T., Mohd, B., Itradat, A., & Quttoum, A. N. (2013). Performance and Information Security Evaluation with Firewalls. *International Journal of Security and Its Applications, 7*(6), 355–372. https://doi.org/10.14257/ijsia.2013.7.6.36

Kizza, J. M. (2024). Guide to computer network Security. In *Texts in computer science*. https://link.springer.com/book/10.1007/978-3-031-47549-8

Neupane, K., Haddad, R., & Chen, L. (2018). Next generation firewall for network Security: a survey. SoutheastCon. https://doi.org/10.1109/secon.2018.8478973

Qu, Z., Ling, X., Wang, T., Chen, X., Wu, S., & Zhang, Y. (2024). AdvSQLi: Generating adversarial SQL injections against real-world WAF-as-a-service. *IEEE Transactions on Information Forensics and Security, 19*, 1–14. https://doi.org/10.1109/TIFS.2024.3350911

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero trust architecture (NIST SP 800-207)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

Scarfone, K., & Hoffman, P. (2009). *Guidelines on firewalls and firewall policy (NIST SP 800-41 Rev. 1)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-41r1

Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. In *2010 IEEE Symposium on Security and Privacy* (pp. 305–316). IEEE. https://doi.org/10.1109/SP.2010.25

Suthar, F., & Patel, N. (2023). A survey on DDOS Detection and Prevention Mechanism.*Journal of Advances in Information Technology*, *14*(3), 444–453. https://doi.org/10.12720/jait.14.3.444-453
.

Stallings, W. (2019). *Network security essentials: Applications and standards* (6th ed.). Pearson.

Talukder, M. A., Khalid, M., & Sultana, N. (2025). A hybrid machine learning model for intrusion detection in wireless sensor networks leveraging data balancing and dimensionality reduction. *Scientific Reports*, *15*(1). https://doi.org/10.1038/s41598-025-87028-1

Liu, M., Dou, W., Yu, S., & Zhang, Z. (2014). A Decentralized Cloud Firewall Framework with Resources Provisioning Cost Optimization. *IEEE Transactions on Parallel and Distributed Systems*, *26*(3), 621–631. https://doi.org/10.1109/tpds.2014.2314672

Gabriele, L. G. F., & Ghafir, I. (2024). Firewalls: types, policies, security issues and best practices. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4709034