Journal of Artificial Intelligence and Engineering Applications

Website: https://ioinformatic.org/

15th June 2025. Vol. 4. No. 3; e-ISSN: 2808-4519

Comparative Analysis of Network Security: Firewall, IDS, and AI-Based Defense Against DDoS Attacks

Elsa Kristi Aprilia Tobing[1]*, Rara Eka Septya[2], Yustian Servanda[3]

[1,2,3]*Program Studi Teknologi Informasi, Fakultas Ilmu Komputer, Universitas Mulia*
elsatobing@students.universitasmulia.ac.id[1*], raraseptya@students.universitasmulia.ac.id[2], yustians@universitasmulia.ac.id[3]

Abstract

Distributed Denial of Service (DDoS) attacks have become one of the most significant threats in today's network security landscape. By overwhelming a network with excessive traffic, these attacks can disrupt service availability and render digital systems inaccessible. Various defense mechanisms have been developed to counter this threat, including firewalls for initial traffic filtering, Intrusion Detection Systems (IDS) for real-time anomaly detection, and Artificial Intelligence (AI)-based systems that can adaptively recognize new attack patterns. This study aims to analyze and compare the effectiveness of these three approaches in mitigating DDoS attacks. The method used is a literature review of selected scientific journals published between 2019 and 2024. The findings show that firewalls are effective for standard traffic filtering, IDS excels in early threat detection, and AI-based systems offer high accuracy with lower false positive rates. A combined implementation of these three methods is recommended to build a comprehensive and adaptive network defense system capable of withstanding increasingly complex DDoS threats.

Keywords: *Firewall, Intrusion Detection System, Artificial Intelligence, DDoS Attack, Network Security.*

1. Introduction

In the ever-evolving digital era, network security has become crucial in protecting information technology infrastructures from cyber threats, particularly Distributed Denial of Service (DDoS) attacks. DDoS attacks aim to flood a network or target system with extremely high and excessive traffic, making services unavailable to legitimate users or even causing a complete system failure [1]. Various security methods have been developed to counter these threats, including Firewalls, Intrusion Detection Systems (IDS), and Artificial Intelligence (AI)-based defense systems.

Firewalls, as a basic defense mechanism in network security systems, can be implemented through either hardware or software to filter data traffic and restrict unauthorized access between internal and external networks [2]. Iptables, a firewall feature in Linux, functions to filter packets and block access identified as potential DDoS attacks, thereby helping to maintain server performance and stability [3]. Implementing a firewall using Iptables on a Linux system has proven effective in resisting DDoS attacks on Apache2 servers and restoring server performance once the attack ceases [4].

Conversely, the Intrusion Detection System (IDS) is designed to detect suspicious activities within the network and provide alerts or notifications to prevent security breaches, including DDoS attacks [5]. These intrusions may include Ping Floods, Port Scans, DoS/DDoS attacks, and unauthorized access within the network [6]. IDS can be categorized into two main types: Signature-Based Detection, which uses predefined signatures to identify known attack patterns, and Anomaly-Based Detection, which detects unusual behaviors [7].

Meanwhile, AI-based approaches offer greater flexibility and detection accuracy in modern network security research. By leveraging machine learning techniques such as Support Vector Machines (SVM) and Decision Trees, these systems can classify network traffic based on complex statistical patterns and learn from historical data to recognize previously undefined attacks [8], [1]. In machine learning models, SVM is capable of detecting and classifying network traffic, allowing the system to distinguish between normal traffic and DDoS attacks [8], while Decision Trees can efficiently process large amounts of data with high speed and accuracy [1]. Furthermore, AI also promises operational efficiency through automated detection and mitigation processes, as it can handle large-scale data quickly and accurately.

Nevertheless, each approach has its own advantages and limitations. Firewalls are superior in terms of performance and simple implementation but are weak against anomaly-based attacks. IDS can quickly detect suspicious activity, but it lacks automated corrective capabilities. AI-Based Defense offers high accuracy and strong adaptability but requires significant computational resources and complex

data training. Therefore, a comprehensive comparative study is necessary to determine the most effective, efficient, and appropriate approach for tackling the constantly evolving DDoS threats.

Based on this urgency, this study aims to analyze and compare the performance of network security systems based on firewalls, IDS, and AI-Based Defense in mitigating DDoS attacks. The evaluation is conducted using parameters such as detection accuracy, response time, resilience to high-volume attacks, and error rates. This study is expected to contribute meaningfully to the development of network defense architectures that are not only technically reliable but also strategically relevant amidst the growing escalation of global cyber threats.

2. Research Methodology

This study employs a literature review method by examining six relevant journal articles published between 2019 and 2024. The selected journals are categorized into three groups: two journals discussing firewalls, two journals focusing on Intrusion Detection Systems (IDS), and two journals related to AI-based defense mechanisms. Each article is analyzed in terms of its research objectives, methodology, findings, and implications for DDoS mitigation strategies.

3. Results and Discussion

Based on the review of relevant scientific articles, six journals were identified as closely related to the topic of Network Security, specifically focusing on the use of Firewalls, Intrusion Detection Systems (IDS), and Artificial Intelligence (AI)-Based Defense mechanisms in mitigating Distributed Denial of Service (DDoS) attacks. The details of these journals are as follows:

Table 1: Literature Review Summary (Journal 1)

Author & Year	Rahmadaniar et al. (2024)
Technology	Firewall (Iptables)
Objective	To implement and evaluate the effectiveness of a firewall using Iptables in maintaining the security and availability of web services by protecting an Apache2 web server from DDoS attacks, as well as to provide a reliable open-source-based solution for network security systems.
Methodology	The method used was direct experimentation (system implementation and testing). The authors set up a target server running a Linux operating system and then configured the firewall using Iptables to block various DDoS attack patterns, including SYN Flood and UDP Flood. The testing involved simulating DDoS attacks using specific tools and analyzing the firewall's effectiveness based on server logs and performance metrics.
Findings	The Iptables firewall successfully detected and blocked most of the malicious traffic generated by DDoS attacks. After implementing Iptables rules, the server became more stable and less prone to downtime during attack simulations. Resource usage (CPU and memory) remained within safe limits after the firewall configuration was applied. The combination of Snort and Shorewall running simultaneously proved to be the most effective in detecting and blocking DoS attacks. In scenarios where either Snort or Shorewall was disabled, the system became more vulnerable and response times increased significantly during attacks. Activating both tools reduced the average network response time, especially when the number of attacks increased.
Implications	This study demonstrates that Iptables firewalls can serve as an effective and affordable solution to protect servers from DDoS attacks. Proper rule implementation can enhance server stability and security without the need for additional hardware. These results provide practical guidance for network administrators in managing and securing web infrastructure.

Table 2: Literature Review Summary (Journal 2)

Author & Year	Sumar et al. (2024)
Technology	Firewall (Shorewall)
Objective	To assess the effectiveness of Snort and Linux-based firewalls in detecting and preventing Denial of Service (DoS) attacks on web servers, and to analyze network performance during and after the attacks.
Methodology	This study employed an experimental method by simulating DoS attacks. The testing was carried out under several scenarios involving the activation and deactivation of Snort and Shorewall to evaluate server response times and the effectiveness of protection against the attacks.
Findings	The combination of Snort and Shorewall being active simultaneously showed the most effective results in detecting and blocking DoS attacks. In scenarios where either Snort or Shorewall was inactive, the system became more vulnerable, and response times increased significantly during the attacks. Activating both tools reduced the average network response time, especially as the number of attacks increased.
Implications	This study highlights the importance of integrating an IDS and a firewall to strengthen network security against DoS attacks. Such an implementation can serve as an effective defense model for open-source-based systems with limited resources.

Table 3: Literature Review Summary (Journal 3)

Author & Year	Aulianita et al. (2021)
Technology	Intrusion Detection System (IDS) + Mikrotik Router
Objective	To investigate and evaluate the effectiveness of implementing an IDS and firewall configuration on a Mikrotik router in detecting and blocking DDoS attacks, specifically UDP Flooding attacks.
Methodology	The research was explanatory in nature and conducted through DDoS attack simulations using the UDP Unicorn application. The authors performed testing before and after applying the firewall configuration by monitoring bandwidth usage, CPU load, and system response to the attacks.
Findings	Before the firewall was configured, the DDoS attack caused a bandwidth spike of up to 44.6 Mbps and CPU usage increased to 31%, resulting in the router becoming slow or unresponsive. After the firewall configuration was applied, the attack was successfully detected and blocked, stabilizing the system and maintaining network accessibility.
Implications	This study shows that the combination of IDS and filter rules on a Mikrotik router can enhance network resilience against DDoS attacks, offering a practical and affordable security solution that can be implemented with accessible hardware.

Table 4: Literature Review Summary (Journal 4)

Author & Year	Syujak et al. (2024)
Technology	Intrusion Detection System (IDS) + Deep Packet Inspection (DPI)
Objective	To utilize Deep Packet Inspection (DPI) technology combined with an Intrusion Detection System (IDS) as an innovative approach for early detection of DDoS attacks.
Methodology	This study employed a quantitative experimental approach through the development and testing of a system architecture that integrates a Snort-based IDS with a DPI module. The system was tested in a simulated network environment using the CIC-DDoS2019 dataset. Evaluation parameters included True Positive Rate (TPR), False Positive Rate (FPR), latency, and throughput.
Findings	The integration of DPI and IDS resulted in an improved DDoS attack detection accuracy of up to 94.7%, along with a low false positive rate. The system also handled high-throughput network traffic efficiently, indicating its effectiveness for deployment in large-scale networks.
Implications	This research makes a significant contribution to the development of adaptive and scalable network security solutions. Integrating DPI into IDS overcomes the limitations of header-only analysis and enhances system effectiveness against complex attacks such as HTTP Flood, SYN Flood, and UDP Flood. The study also opens opportunities for further development, including the integration of artificial intelligence to improve detection of more diverse and sophisticated attack patterns. This implementation can serve as an effective defense model for open-source systems with limited resources.

Table 5: Literature Review Summary (Journal 5)

Author & Year	Sihombing et al. (2019)
Technology	AI (Support Vector Machine Algorithm)
Objective	To develop a DDoS detection and mitigation system implemented within a Software-Defined Network (SDN) architecture using the Support Vector Machine (SVM) algorithm. The system is designed to differentiate between normal and attack traffic and mitigate the impact on the target host.
Methodology	This study used an experimental machine learning approach, where network traffic data was collected from flow entries in an OpenFlow switch. Features such as packet standard deviation, number of source IPs, and number of flows were used to train the SVM model. The test environment was built using Mininet in a virtual SDN network. Detection was conducted in real-time, and mitigation was implemented by adding flow rules to the switch to block attack traffic.
Findings	The system successfully detected DDoS attacks with an average accuracy of 96.83% and an average detection time of 67.80 ms. It also reduced the number of attack packets reaching the victim host (from 1,855 to 864). High detection accuracy (95–98%) was achieved for various attack types, including SYN Flood, UDP Flood, and ICMP Flood.
Implications	This study demonstrates that applying the SVM algorithm within SDN architecture enhances the effectiveness of DDoS detection and response. Practically, the system can be deployed in real SDN environments as a proactive and reactive cybersecurity solution. Additionally, this research paves the way for further development of machine learning-based detection methods and their application to other types of attacks.

Table 6: Literature Review Summary (Journal 6)

Author & Year	Syahputra et al. (2020)
Technology	AI (Decision Tree Algorithm)
Objective	To develop a system for detecting and mitigating DDoS (Distributed Denial of Service) attacks in a Software Defined Network (SDN) architecture using the Decision Tree algorithm. The study focused on detecting UDP Flood attacks and mitigating them by dropping packets.
Methodology	The study used the Decision Tree algorithm to classify network traffic (normal vs. DDoS attack). The dataset used was CICIDS 2017, which includes UDP Flood attack data. The system was implemented in an SDN controller, which monitored incoming packets and identified whether they were part of an attack. If identified as an attack, mitigation was performed by blocking packets from the attack source.
Findings	The system successfully detected UDP Flood attacks with an accuracy of 99.95%. During testing, it effectively reduced the number of attack packets reaching the victim host. Mitigation was performed by closing the port of the attack source for 10 seconds, which significantly reduced the impact of the attack on the network.
Implications	This study contributes to the development of machine learning-based detection and mitigation systems in SDN environments to combat DDoS attacks, particularly UDP Flood. The system can be implemented in real SDN networks and offers an efficient solution for minimizing service disruptions caused by DDoS attacks. It also opens up opportunities for further research to expand detection to other attack types and improve accuracy using larger datasets.

Based on several journals reviewed, the author examined six studies focusing on network security, specifically on the use of firewalls, Intrusion Detection Systems (IDS), and Artificial Intelligence (AI)-based defense systems in mitigating Distributed Denial of Service (DDoS) attacks.

The first journal, titled "Implementasi Firewall Menggunakan Iptables untuk Melindungi Server dari Serangan DDoS," discusses the effectiveness of using iptables as a firewall on the Linux Ubuntu operating system to detect and block DDoS attacks, particularly the Slow HTTP Attack type. The study simulates an attack using the tool slowhttptest with 500 simultaneous connections, showing that the Apache2 server experiences significant lag when unprotected. After applying iptables rules including blocking attacker IPs and limiting SYN connections, server access returned to normal. Log analysis showed that the attack was successfully stopped after the 64th attempt. The mitigation system achieved a 95% accuracy rate in recognizing, stopping, and preventing repeated attacks without disrupting legitimate user access. The advantages of this method include its simplicity, configuration flexibility, and effectiveness in maintaining web service availability, making it suitable as an initial defense for small- to medium-scale networks [4].

The second journal, titled "Sistem Keamanan Jaringan Terhadap Serangan DOS Menggunakan Snort dan Firewall Berbasis Linux OS," proposes the integration of Snort IDS and the Shorewall firewall to detect and prevent DoS attacks, particularly Slowloris and SlowHTTPTest. The system was tested in four scenarios: without any security system, with Snort only, with Shorewall only, and with both enabled. Testing involved 100 to 10,000 attack connections. The results show that when Snort and Shorewall were both active, server response time was significantly reduced, from 3,465 ms to only 1,356 ms under 10,000 attack packets. The system consistently detected and blocked all attacks, with detection accuracy approaching 100% for the tested attack types. The main strength of this approach lies in

its efficiency and effectiveness in handling DoS attacks using open-source solutions, making it ideal for small- to medium-scale network implementations [2].

The third journal, titled "Penggunaan Metode IDS dalam Implementasi Firewall pada Jaringan untuk Deteksi Serangan DDoS," discusses the integration of Intrusion Detection System (IDS) methods with firewall configuration on MikroTik routers to detect and prevent DDoS attacks, particularly UDP Flooding. The attack simulation was carried out using the UDP Unicorn tool targeting the MikroTik router, resulting in bandwidth spikes up to 44.6 Mbps and CPU usage reaching 31%. To counter the attack, the authors implemented an IDS-based firewall with filter rules and tarpit actions to automatically detect and block attacker IP addresses. IDS identified suspicious traffic patterns, while the firewall filtered and blocked unauthorized connections. The system achieved a detection accuracy rate of 96%, successfully recognizing and blocking most attack traffic without disrupting legitimate users. The router remained stable, bandwidth returned to normal, and users experienced no issues after the configuration was applied. The main advantage of this approach is its efficiency in securing networks using low-cost, open-source solutions, offering adaptive and real-time protection against DDoS attacks [5].

The fourth journal, titled "Integrasi Deep Packet Inspection dengan Intrusion Detection System (IDS) untuk Identifikasi Serangan DDoS dalam Jaringan Skala Besar," proposes integrating Deep Packet Inspection (DPI) technology with IDS to enhance DDoS detection in large-scale networks. The system was tested using the CICDDoS2019 dataset with scenarios including HTTP Flood, SYN Flood, and UDP Flood, types of DDoS attacks based on application and protocol layers. Results showed that integrating DPI and IDS increased the True Positive Rate (TPR) from 87.4% to 95.2% and reduced the False Positive Rate (FPR) from 12.6% to just 4.8%. While latency slightly increased from 3.2 ms to 5.8 ms, this trade-off was considered acceptable for the significant improvement in detection accuracy. The system also demonstrated the ability to handle high throughput up to 10 Gbps, making it suitable for large-scale network infrastructure. A key advantage of this approach is DPI's ability to analyze payload content, allowing it to detect attack patterns that conventional header-based IDS may miss [7].

The fifth journal, titled "Implementasi Sistem Deteksi dan Mitigasi Serangan Distributed Denial of Service (DDoS) menggunakan SVM Classifier pada Arsitektur Software-Defined Network (SDN)," develops a DDoS detection and mitigation system in an SDN environment using the Support Vector Machine (SVM) algorithm. The system utilizes data from flow entries on OpenFlow switches to extract network features such as packet count deviation, source IP quantity, and flow entry ratio. The SVM model then classifies whether the traffic is malicious or not. Tests were conducted in a simulated network topology using Mininet, involving various attack types including SYN Flood, UDP Flood, and ICMP Flood. The system achieved an average detection accuracy of 96.83% with an average detection time of 67.80 ms. After detection, the system automatically added flow rules to filter out malicious traffic. The number of attack packets reaching the victim host dropped from 1,855 to 864, demonstrating effective mitigation. This study shows that machine learning, specifically SVM, can provide real-time solutions to DDoS threats in SDN environments [8].

The sixth journal, titled "Deteksi Dan Mitigasi Serangan DDoS Pada Software Defined Network Menggunakan Algoritma Decision Tree," implements a Decision Tree algorithm on the SDN controller to detect and mitigate UDP Flood-type DDoS attacks. The system uses the CICIDS2017 dataset and classifies incoming packets at the controller before they are forwarded to the target host. If identified as an attack, packets are blocked using a drop packet method. The results show a detection accuracy of 99.95% with a recall rate of 100%, meaning all attacks were successfully detected. Mitigation effectively reduced both packet-in and packet-out traffic during the attack. Additionally, quality of service (QoS) metrics such as throughput and jitter improved after the detection and mitigation system was activated, indicating that the system not only blocked attacks but also maintained stable network performance [1].

4. Conclusion

This study has presented a comparative analysis of three major defense mechanisms against Distributed Denial of Service (DDoS) attacks: Firewall, Intrusion Detection Systems (IDS), and Artificial Intelligence (AI)-based approaches. The findings from six selected journal articles between 2019 and 2024 demonstrate that each method offers unique advantages in mitigating DDoS threats. Firewalls, particularly Iptables and Shorewall, are effective for basic traffic filtering and protecting server availability, especially when configured with complementary tools like Snort. IDS solutions, including those enhanced with Deep Packet Inspection (DPI), are proficient in detecting anomalies in real-time and can significantly improve detection accuracy when integrated properly. Meanwhile, AI-based approaches using algorithms such as Support Vector Machines and Decision Trees offer the highest accuracy and adaptability, making them suitable for detecting complex and evolving attack patterns.

However, no single solution provides comprehensive protection on its own. Firewalls may struggle with zero-day or behavioral-based attacks, IDS often requires manual intervention for mitigation, and AI-based systems demand significant resources and training data. Therefore, a hybrid implementation that combines the simplicity of firewalls, the detection strength of IDS, and the adaptive intelligence of AI offers the most robust strategy to counter modern DDoS threats. Future research is encouraged to explore integrated frameworks and real-time coordination among these tools to achieve scalable, automated, and intelligent network defense architectures.

References

[1] Q. Syahputra, D. Akbi, and D. Risqiwati, "Deteksi Dan Mitigasi Serangan DDoS Pada Software Defined Network Menggunakan Algoritma Decision Tree," *Repositor*, vol. 2, no. 11, pp. 1491–1502, 2020, doi: 10.22219/repositor.v2i11.795.

[2] M. H. Dar and S. Z. Harahap, "IMPLEMENTASI SNORT INTRUSION DETECTION SYSTEM (IDS) PADA SISTEM JARINGAN KOMPUTER," *JURNAL INFORMATIKA*, vol. 6, no. 3, pp. 14–23, Sep. 2017, doi: 10.36987/informatika.v6i3.1619.

[3] M. R. H. Tambunan and S. N. Neyman, "Implementasi Firewall pada Linux untuk Pencegahan Dari Serangan DoS," *Journal of Technology and System Information*, vol. 1, no. 4, pp. 1–10, 2024, doi: 10.47134/jtsi.v1i4.2648.

[4] I. Rahmadaniar, D. A. A. Tondang, B. S. Fernando, and A. Setiawan, "Implementasi Firewall Menggunakan Iptables untuk Melindungi Server dari Serangan DDoS," *Journal of Internet and Software Engineering*, vol. 1, no. 3, pp. 1–10, 2024, doi: 10.47134/pjise.v1i3.2564.

[5] R. Aulianita, N. Musyaffa, and R. Martiwi, "Penggunaan Metode IDS dalam Implementasi Firewall pada Jaringan untuk Deteksi Serangan Distributed Denial of Service (DDoS)," *Jusikom: Jurnal Sistem Komputer Musirawas*, vol. 6, no. 2, pp. 94–104, 2021, doi: 10.32767/jusikom.v6i2.1411.

[6] R. Fauzi, Y. Muhyidin, and D. Singasatia, "Sistem Keamanan Jaringan Komputer Berbasis Teknik Intrusion Detection System (IDS) Untuk Mendeteksi Serangan Distrubuted Denial Of Service (DDOS)," *Jurnal Sains Komputer & Informatika (J-SAKTI*, vol. 7, no. 1, pp. 72–86, 2023, doi: 10.30645/j-sakti.v7i1.

[7] A. R. Syujak, K. Diantoro, V. Yuni T, A. Soderi, and P. A. Sucipto, "Integrasi Deep Packet Inspection dengan Intrusion Detection System (IDS) untuk Identifikasi Serangan DDoS dalam Jaringan Skala Besar," *Jurnal Minfo Polgan*, vol. 13, no. 2, pp. 1971–1975, Dec. 2024, doi: 10.33395/jmp.v13i2.14324.

[8] J. C. J. Sihombing, D. P. Kartikasari, and A. Bhawiyuga, "Implementasi Sistem Deteksi dan Mitigasi Serangan Distributed Denial of Service (DDoS) menggunakan SVM Classifier pada Arsitektur Software-Defined Network (SDN)," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, vol. 3, no. 10, pp. 9608–9613, 2019, [Online]. Available: https://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/6476