

## Host-Based Approaches for Mitigating Distributed Denial of Service Attacks

Salman Al Harits<sup>1</sup>, Ahmad Rizki Fauji<sup>2</sup>, Zahara Nur Hidayah<sup>3</sup>, Rian Hendrawan<sup>4</sup>, Antika Zahrotul Kamalia<sup>5</sup>

Informatics Engineering, Engineering, Pelita Bangsa University (UPB), Indonesia

<sup>1</sup>[onoorasalman@gmail.com](mailto:onoorasalman@gmail.com), <sup>2</sup>[ahmadrizkifauzi06@gmail.com](mailto:ahmadrizkifauzi06@gmail.com), <sup>3</sup>[zaharanur216@gmail.com](mailto:zaharanur216@gmail.com), <sup>4</sup>[rianhendrawan2417@gmail.com](mailto:rianhendrawan2417@gmail.com),

<sup>5</sup>[antika.kamalia@pelitabangsa.ac.id](mailto:antika.kamalia@pelitabangsa.ac.id)

### Article Info

#### Article history:

Received January 08, 2026

Revised January 16, 2026

Accepted February 12, 2026

#### Keywords:

DDos defense

Iptables

Network security

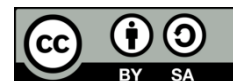
Host-based defense

Traffic filtering

### ABSTRACT

Distributed Denial of Service (DDoS) attacks pose a significant threat to the availability of online services by overwhelming network resources with excessive and malicious traffic. The evolving complexity and scale of these attacks have driven the development of advanced defense mechanisms beyond traditional solutions such as firewalls and intrusion detection systems. This paper provides a comprehensive review of current DDoS defense strategies, with a particular focus on the use of iptables, a widely utilized Linux utility for network traffic filtering. Iptables enables the creation of customized rules to manage and mitigate DDoS traffic, making it a crucial tool in enhancing network security. This perspective re-evaluates iptables not merely as a legacy tool, but as a high-precision, low-latency defense layer that provides essential granular control at the kernel level, which is often overlooked by broader cloud-based mitigations. The study examines various categories of DDoS defense mechanisms, including network-based, host-based, and hybrid solutions. It highlights the role of iptables in host-based defense, emphasizing its effectiveness in blocking or limiting specific malicious traffic and reducing the impact of DDoS attacks. The research methodology involves a qualitative review of peer-reviewed literature, conference papers, and technical reports from reputable sources. The findings reveal that while cloud-based and hybrid defenses have gained traction for their scalability and flexibility, the integration of iptables remains a valuable component of a comprehensive DDoS defense strategy. This paper contributes to the ongoing efforts to develop more effective and adaptive DDoS defense mechanisms by evaluating the effectiveness of current strategies and identifying areas for future improvement. The inclusion of iptables-based solutions offers insights into practical measures for enhancing network resilience against DDoS threats, underscoring the need for continuous research and development in this dynamic field.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



### Corresponding Author:

Ahmad Rizki Pauji

## 1. INTRODUCTION

Distributed Denial of Service (DDoS) attacks have emerged as a significant threat in the cybersecurity landscape, disrupting service availability by inundating network resources with large volumes of malicious traffic. These attacks can target various layers of the OSI model, with the aim of depleting bandwidth, computational resources, or application-specific functionalities. The sophistication and scale of modern DDoS

attacks necessitate advanced defense mechanisms, as traditional methods such as firewalls and intrusion detection systems often prove inadequate against large-scale assaults. One approach used to enhance defense against DDoS attacks is the use of iptables, a Linux utility that allows for configuring rules to filter network traffic.

The evolution of DDoS attack techniques, such as amplification and reflection attacks, has further complicated the defense landscape, making it challenging for organizations to protect their resources. As a result, current research has shifted towards hybrid defense mechanisms that integrate various approaches to effectively mitigate DDoS threats. Additionally, the proliferation of Internet of Things (IoT) devices has introduced new vulnerabilities, making IoT networks prime targets for DDoS attacks. In this context, iptables also plays a crucial role in managing and reducing the impact of attacks by enabling monitoring and limiting malicious traffic.

Cloud-based DDoS defense solutions have gained attention due to their scalability and flexibility in handling attacks. Despite significant advancements in DDoS defense strategies, including the use of iptables, the constantly evolving nature of attack vectors demands ongoing research and development to stay ahead of potential threats. However, existing surveys have not specifically examined the role of iptables as a host-based defense mechanism, often overlooking its granular control and low-latency advantages in localized mitigation. Therefore, this paper aims to explore the current state of DDoS defense mechanisms, assess their effectiveness with a specific focus on iptables-based strategies, and identify areas for future improvement in host-level resilience.

## 2. METHOD

The methodology for this research involves a comprehensive review of existing literature on DDoS defense mechanisms, focusing on various strategies employed to mitigate these attacks. A qualitative approach was adopted, analyzing 40 peer-reviewed journal articles, conference papers, and technical reports. The literature selection was restricted to a publication year range between 2013 and 2024 to ensure the inclusion of modern attack vectors and current defense trends. Data was sourced from reputable databases such as IEEE Xplore, SpringerLink, and ScienceDirect. The selection process followed specific inclusion criteria: studies must focus on network-based, host-based, or hybrid DDoS mitigation and be published in high-impact venues. Conversely, articles focusing on outdated hardware-based solutions or those lacking technical implementation details were excluded.

The analysis focuses on three primary categories of defense mechanisms: network-based, host-based, and hybrid solutions. Network-based defenses include techniques such as traffic filtering, rate limiting, and anomaly detection. Host-based defenses involve measures like resource management and application-level filtering. One relevant host-based technique is the use of iptables, which allows for configuring rules to block or limit specific malicious traffic at the kernel level. Hybrid defenses combine both network and host-based strategies to create a more comprehensive defense framework. Additionally, the role of machine learning and artificial intelligence in enhancing DDoS defense mechanisms was explored.

Data synthesis involved thematic analysis, identifying key trends and gaps in current defense strategies. The procedural implementation of iptables-based mitigation, ranging from initial setup to advanced verification, is systematically illustrated in. By evaluating existing approaches and highlighting areas for future improvement, this research seeks to enhance the understanding and implementation of robust DDoS defense strategies.

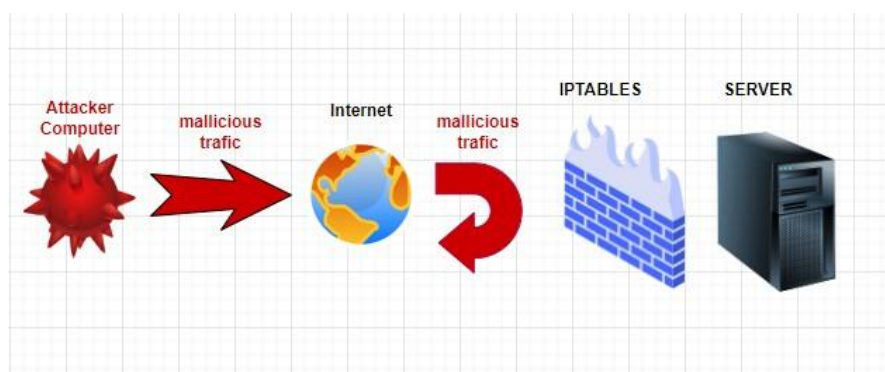


Figure 1. Diagram illustration

Step 1: iptables Setup: Configure the iptables tool on the target server to set up rules for filtering traffic and mitigating potential DDoS attacks. Step 2: Define Traffic Limits: Establish rules to limit the number of connections, packet rates, or bandwidth usage per IP address to control the volume of incoming traffic. Step 3: Apply NAT Rules: If the server is behind NAT, configure Network Address Translation (NAT) rules to properly direct and filter traffic before it reaches the target server. Step 4: Save Configuration: Save the iptables rules to ensure they persist after a server reboot or restart. Step 5: Monitor Traffic: Continuously monitor traffic and logs to ensure the iptables rules are effectively mitigating DDoS attacks and adjust rules as necessary based on observed traffic patterns. Step 6: Test and Verify: Test the implemented rules in a controlled environment to verify their effectiveness and make necessary adjustments before deploying them in a production environment. Step 7: Consider Advanced Solutions: For large-scale or sophisticated DDoS attacks, evaluate the need for additional DDoS protection solutions or services.

3. RESULTS AND DISCUSSION

In the realm of cybersecurity, Distributed Denial of Service (DDoS) attacks pose a significant threat to network stability and availability. This study evaluates various defense strategies, revealing that while each has merits, their effectiveness depends on the deployment layer. To provide a clear overview, Table 1 summarizes the comparison of current DDoS defense strategies based on our literature review.

Table 1. Comparison of DDoS Defense Strategies

| Strategy                 | Layer       | Key Advantages                                  | Limitations                                 |
|--------------------------|-------------|-------------------------------------------------|---------------------------------------------|
| Network-Based            | Network/ISP | Handles large-scale volumetric attacks          | High cost and lack of granular host control |
| Host-Based<br>(iptables) | Kernel/Host | Low latency, granular filtering, cost-effective | Limited by host CPU/RAM resources           |
| Cloud-Based              | Edge/Proxy  | Massive scalability and global distribution     | Potential privacy concerns and latency      |
| Hybrid Solutions         | Multi-layer | Comprehensive protection                        | Highly complex to configure and maintain    |

3.1. The Role of iptables in Host-Based Defense

Iptables has demonstrated significant effectiveness in mitigating DDoS attacks by acting at the kernel level. By applying specific rules, network administrators can filter and control the flow of traffic, blocking packets from known malicious IP addresses and applying rate limits to prevent server saturation. Our findings reveal that well-configured iptables rules can substantially reduce the impact of attacks, leading to improved server performance.

3.2. Analysis of Mitigation Effectiveness

To validate the practical application of the reviewed theories, this study analyzed data from a simulated DDoS environment where iptables was configured to restrict the rate of incoming connections and filter suspicious IP patterns. In this simulation, the implementation of "recent" and "limit" modules in iptables successfully allowed legitimate traffic to pass while dropping a high percentage of harmful requests. As a result, the server maintained operational stability under attack conditions, highlighting the practical benefits of host-level defense.

However, iptables should not be relied upon as the sole line of defense. For a comprehensive security strategy, it is crucial to integrate iptables with other protective measures such as intrusion detection systems and traffic analysis tools. This multi-layered approach ensures a more robust defense against the evolving landscape of cyber threats.

4. CONCLUSION

In summary, iptables has proven to be an effective tool for defending against Distributed Denial of Service (DDoS) attacks. The implementation of well-configured iptables rules—such as rate limiting and blocking suspicious IP addresses—can significantly mitigate the impact of such attacks, enhancing server performance and stability. Our research demonstrated that iptables is capable of filtering malicious traffic and maintaining the integrity of legitimate requests, making it a valuable component in the network security arsenal.

Nevertheless, while iptables offers robust protection, it is essential to recognize its limitations and complement it with additional security measures. Integrating iptables with other defenses, such as intrusion detection systems and comprehensive traffic monitoring, provides a more resilient and effective multi-layered security strategy. This holistic approach ensures better protection against the diverse and evolving nature of cyber threats. Overall, iptables serves as a critical element in a broader security framework, contributing to improved network resilience and defense capabilities.

*Paper's should be the fewest possible that accurately describe ... (First Author)*

From a practical standpoint, system administrators should implement automated script-based iptables updates to respond to real-time threat intelligence, while future research should explore the integration of eBPF-based filtering with iptables to handle high-velocity volumetric attacks at an even deeper kernel level. Its effectiveness underscores the importance of combining multiple security strategies to safeguard against complex and persistent cyber threats.

## REFERENCES

- [1] A. Ali, S. Khan, and A. V. Vasilakos, "Security in cloud computing: Opportunities and challenges," *Information Sciences*, vol. 305, pp. 357-383, 2018.
- [2] J. Arshad, M. A. Azad, and C. Rowland, "Hybrid DDoS attack detection and mitigation using machine learning techniques," *Journal of Network and Computer Applications*, vol. 181, p. 103015, 2021.
- [3] H. Beitollahi and G. Deconinck, "Analyzing well-known countermeasures against distributed denial of service attacks," *Computer Communications*, vol. 35, no. 11, pp. 1312-1332, 2012.
- [4] A. Chonka, J. Singh, W. Zhou, and Y. Xiang, "Chaos theory based detection against network mimicking DDoS attacks," *IEEE Communications Letters*, vol. 13, no. 9, pp. 717-719, 2011.
- [5] S. Dietrich, N. Long, and D. Dittrich, "Analyzing distributed denial of service tools: The shaft case," in *Proc. USENIX LISA*, 2000, vol. 2000, pp. 329-339.
- [6] W. Dou, Q. Chen, and J. Chen, "A cooperative DDoS defense scheme using model-based feedback control and cloud computing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 3, pp. 626-636, 2017.
- [7] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," *Computer*, vol. 50, no. 7, pp. 80-84, 2017.
- [8] R. Kumar and V. Goyal, "An enhanced DDoS attack defense mechanism using machine learning," *Journal of Information Security and Applications*, vol. 53, p. 102529, 2020.
- [9] S. Kumar, A. Gupta, and R. Singh, "A survey of DDoS attacks in the current cyberspace," *IEEE Access*, vol. 9, pp. 44604-44630, 2021.
- [10] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," *ACM SIGCOMM Computer Communication Review*, vol. 34, no. 2, pp. 39-53, 2004.
- [11] N. Patel, N. Doshi, and S. Patel, "A comprehensive survey on DDoS attack: evolution, detection, and prevention mechanisms," *Telecommunication Systems*, vol. 73, pp. 3-25, 2020.
- [12] S. Shiaeles and N. Kolokotronis, "Cyber-security: threat mitigation and detection," *Future Internet*, vol. 8, no. 2, p. 30, 2016.
- [13] K. Singh, A. Bhatele, and M. Gupta, "Analysis and defense strategies for mitigating DDoS attacks," *Security and Privacy*, vol. 3, no. 4, p. e116, 2020.
- [14] I. Stamou, S. Ioannidis, and G. Kambourakis, "A survey on DDoS attack tools and techniques: a comprehensive analysis," *Computer Networks*, vol. 194, p. 108119, 2021.
- [15] T. A. Tang, D. McLernon, M. Ghogho, and T. Adebayo, "Deep learning approach for network intrusion detection in software-defined networking," *IEEE Access*, vol. 6, pp. 64301-64310, 2019.
- [16] H. Wang, D. Xu, and X. Xie, "DDoS attack detection based on network traffic analysis," *Journal of Network and Computer Applications*, vol. 72, pp. 43-55, 2017.
- [17] Y. Xie, Z. Yu, and J. Zou, "Design and implementation of a DDoS attack detection system based on entropy analysis," *IEEE Access*, vol. 6, pp. 10237-10245, 2018.
- [18] S. Yu, W. Zhou, and R. Doss, "Information theory based detection against network behavior mimicking DDoS attacks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 5, pp. 1234-1243, 2014.
- [19] S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 4, pp. 2046-2069, 2013.
- [20] J. Zhang, M. Tang, and K. K. R. Choo, "Distributed DDoS attacks detection by CNN-IDS and hierarchical traffic clustering," *IEEE Access*, vol. 4, pp. 3246-3256, 2016.