|Jurnal Jaringan Komputer dan Keamanan |JJKK|Vol. 6| No. 2|June|Year 2025|

Next-Generation Firewall Design Using an Intrusion Prevention System (IPS) Method for Securing the Web Portal Server of Universitas Bina Darma

Viren Pranata [1*]

Abstract

Network security is a crucial requirement for digital communication systems, particularly for institutions that rely heavily on web-based services. The design and implementation of network security systems must address increasing cyber threats, particularly unauthorized access, malware infiltration, and Distributed Denial-of-Service (DDoS) attacks that disrupt service availability. This study aims to design a Next-Generation Firewall (NGFW) using an Intrusion Prevention System (IPS) to detect and prevent potential attacks on the Universitas Bina Darma web portal server. The research applies the Action Research Method through four structured stages: Diagnosing, Planning Action, Taking Action, and Evaluating Action. The system was developed and tested through vulnerability assessments, firewall configuration, and IPS rule implementation. The results show that the NGFW with IPS effectively blocks cyberattacks, secures system vulnerabilities, and provides real-time intrusion detection capabilities. The study concludes that implementing an NGFW with IPS significantly enhances server security and performance.

Keywords

Next-Generation Firewall, IPS, network security, cyberattack prevention, UBD web portal.

Article History

Received 01 April 2025
Accepted 24 June 2025

How to Cite

Pranata, V. (2025). Next-Generation Firewall Design Using an Intrusion Prevention System (IPS) Method for Securing the Web Portal Server of Universitas Bina Darma. ***Jurnal Jaringan Komputer dan Keamanan,*** *6*(2), 87-92.

[1*] Universitas Bina Darma, Indonesia, Corresponding email: virenpranata@gmail.com

Introduction

The growth of digital services across institutions has increased the importance of cybersecurity as a foundational element supporting daily operations. Organizations today face escalating threats such as hacking, unauthorized system infiltration, malware distribution, and Distributed Denial-of-Service (DDoS) attacks, all of which can severely disrupt service availability and data integrity (Iannaa et al., 2022). Maintaining a secure digital environment is therefore not merely an operational need but a strategic requirement, especially for institutions that rely heavily on web-based interactions.

Technological advancements have significantly transformed the education sector, where most academic, administrative, and communication processes now utilize online platforms. Universities depend on integrated information systems for activities ranging from course registration and e-learning to digital document management and public information services. As one of the leading higher education institutions, Universitas Bina Darma (UBD) is deeply reliant on web-based services to facilitate academic operations and ensure continuity of digital learning environments. Consequently, any disruption to access or system performance directly impacts the quality of academic services and institutional productivity.

To mitigate such risks, firewalls play a critical role as the frontline defense mechanism in network security. A firewall manages and filters traffic between internal and external networks, inspecting packets to prevent unauthorized access or malicious activity (Rohmatullah et al., 2022). Traditional firewalls, however, are no longer sufficient to counter modern, sophisticated cyber threats. As cyberattacks evolve, the need for security devices capable of deeper inspection and contextual understanding becomes increasingly urgent.

This need has given rise to Next-Generation Firewalls (NGFWs), which integrate advanced security features such as deep packet inspection (DPI), application control, intrusion prevention systems (IPS), and real-time anomaly detection. Unlike conventional firewalls, NGFWs can detect complex attack patterns and block threats based not only on IP or port but also on user identity, application behavior, and traffic anomalies. This capability is essential in identifying stealthy attacks such as encrypted malware communication, protocol abuse, and application-layer intrusions.

Among the most common cyber threats faced by institutional networks are backdoor intrusions and SYN Flood attacks. Backdoor attacks allow unauthorized actors to bypass security controls and gain hidden access to a system, posing a severe risk to data confidentiality and administrative integrity. Meanwhile, SYN Flood attacks target server resources by overwhelming them with incomplete handshake requests, causing service degradation or complete downtime (Y Maarikhan, A. Priyadi, & Santoso, 2023). These attacks can cripple critical university services, including academic portals, internal dashboards, and online administrative systems.

Given the centrality of the UBD web portal as the primary communication and academic management platform, securing its infrastructure is a priority. Strengthening its protection mechanisms is essential to avoid system downtime, prevent data leakage, and ensure uninterrupted access for students, lecturers, and administrative staff. Based on these needs, this study focuses on the design and implementation of a Next-Generation Firewall

equipped with an Intrusion Prevention System (IPS) as a proactive and adaptive solution to secure the UBD web portal server against evolving cyber threats.

Methodology

This study adopts the Action Research Method, which consists of four iterative stages: Diagnosing, Planning Action, Taking Action, and Evaluating Action. This method enables real-time problem-solving and continuous refinement of the system.

Diagnosing

This stage identifies issues affecting the UBD web portal server, including vulnerabilities exploited by attackers, outdated firewall configurations, and insufficient traffic filtering mechanisms. The diagnostic phase also collects system logs, server specifications, and network topology to understand potential points of intrusion.

Planning Action

Based on the diagnosed problems, solutions are planned to enhance server security. These include:

- Conducting vulnerability scanning using automated tools
- Designing firewall filtering rules
- Implementing IPS to detect and block suspicious patterns
- Configuring layered security policies
- Preparing hardware and software components for NGFW deployment

The planning phase produces a structured framework for securing the server.

Taking Action

The implementation stage includes:

- Installing and configuring the firewall system
- Setting up IPS rules and signatures
- Conducting penetration tests to evaluate attack resilience
- Testing firewall performance during simulated threats
- Verifying that blocked traffic matches known attack signatures

This stage ensures the firewall operates as an effective security barrier against real cyber threats.

Evaluating Action

The evaluation stage compares system performance before and after NGFW implementation. Indicators include:

- Firewall alert logs
- Blocked malicious traffic
- Server response time
- Reduction in vulnerability scores

The evaluation confirms whether the implemented system successfully enhances server security.

Results

Firewall Configuration Results

The NGFW was successfully configured with IPS enabled. Firewall rules were created to filter traffic based on:

- Source and destination IP
- Protocol type
- Port usage
- Suspicious packet behavior

IPS signatures were activated to detect backdoors, brute-force attacks, and DDoS-related anomalies.

Vulnerability Scan Results

Vulnerability scanning identified several weaknesses in the UBD web portal server related to open ports, outdated services, and potential attack vectors. These vulnerabilities were mitigated by applying IPS rules and adjusting firewall policies.

Attack Simulation Results

Simulated attacks demonstrated the following:

- Backdoor attempts were detected and blocked
- Unauthorized login attempts were prevented
- SYN Flood attempts were throttled before reaching server resources
- Malicious port scanning was rejected automatically

Firewall Log Analysis

After implementing the NGFW with IPS, logs recorded:

- Increased number of blocked intrusion attempts
- Reduced server response latency
- No successful intrusion incidents
- Significant decrease in malicious requests

These results show that IPS enhanced visibility and protection against modern attacks.

Discussion

The effectiveness of the Tarpit Firewall against simulated attacks is summarized in Table 3.2.

The findings indicate that implementing a Next-Generation Firewall with IPS substantially improves the security posture of the UBD web portal server. Modern cyberattacks often bypass traditional firewalls; therefore, adding IPS provides deeper inspection and proactive blocking capabilities.

IPS enables recognition of attack signatures such as:

- Abnormal SYN packets
- Brute-force login patterns
- Malware communication attempts
- Exploit payloads during intrusion attempts

The firewall's ability to filter traffic based on port, protocol, and packet characteristics contributes significantly to preventing unauthorized access. Furthermore, integrating IPS allows real-time mitigation before attacks reach critical services.

The results confirm that an NGFW with IPS is not only effective for detection but also capable of real-time attack prevention, reducing the risk of downtime and data breaches. This aligns with previous research emphasizing the importance of layered network defense strategies.

Conclusion and Recommendations

This study concludes that the application of an NGFW with IPS significantly improves the security of the Universitas Bina Darma web portal server. The system successfully:

1. Detects and blocks potential cyber threats
2. Prevents unauthorized access to server resources
3. Mitigates SYN Flood and backdoor attacks
4. Enhances server stability during high-risk conditions
5. Reduces vulnerability exposure through automated filtering

The IPS-enhanced NGFW demonstrates superior performance compared to traditional firewalls, offering a reliable and proactive security solution for institutional web servers.

Disclosure Statement

The authors declare no conflicts of interest associated with this research.

Acknowledgments

The authors would like to thank Universitas Bina Darma for providing the facilities, access, and support necessary for completing this study.

References

Aenab, M., Honeine, R., & Darweesh, A. H. (2023). Securing network communication using optimized firewall rules and AI-based anomaly detection. International Journal of Information Security, 22(4), 1–15.

Iannaa, F., Linares, C., & Paulo, R. (2022). The importance of data security in business operations. Journal of Information Systems Security, 10(3), 215–228.

Rohmatullah, D., Putra, A., & Setiawan, R. (2022). Firewall design using packet filtering for corporate networks. Jurnal Keamanan Siber, 6(2), 102–110.

Y Maarikhan, A., Priyadi, A., & Santoso, I. (2023). Analysis of SYN Flood attacks using modern cybersecurity frameworks. Jurnal Teknologi Informasi dan Komunikasi, 11(1), 33–40.

Biographical Notes

VIREN PRANATA is a researcher in cybersecurity and network infrastructure at Universitas Bina Darma. His research interests include firewalls, intrusion detection systems, and web security.