Idea: Future Research
Volume 1, Issue 3, Oct 2023 Published by:
ISSN 2987-1565 (Online) | ISSN 2987-2715 (Print) Ideas for Future Research and Technology

Implementation of Network Security System Using Firewall Technology and Intrusion Detection System (IDS)

Carel Adelard[1], Osric Penrod2
[1,2] Fakultas Sains & Teknologi (FST), Universitas Papua Madani Jayapura (UPMJ), Papua

Introduction

In an increasingly digital world, the security of network systems has become a paramount concern for organizations, governments, and individuals alike. As businesses and services move online, the volume of sensitive data being transmitted across networks has grown exponentially, making networks vulnerable to a wide range of cyber threats, including unauthorized access, data breaches, and denial-of-service attacks. The need to protect these networks is critical to ensure the confidentiality, integrity, and availability of the data being exchanged(Aldossary & Allen, 2016).

Network Security is a set of practices, policies, and technologies aimed at protecting a network from various types of security breaches. Traditional network security systems relied primarily on firewalls to prevent unauthorized access(Stewart, 2013). However, as cyber threats have evolved, relying solely on firewalls is no longer sufficient to guarantee network safety. Firewalls, while effective in controlling incoming and outgoing traffic based on security rules, are limited in their ability to detect internal threats, sophisticated attacks, and zero-day vulnerabilities.

To address these gaps, Intrusion Detection Systems (IDS) have been developed. IDS are designed to monitor network traffic for suspicious activities and detect potential threats in real-time(Kenkre et al., 2015). While IDS can detect attacks and intrusions, they cannot prevent them; hence, combining IDS with firewalls offers a more comprehensive approach to network security. The integration of these two technologies firewalls for controlling access and IDS for monitoring and detecting intrusions forms a layered security model that improves defense against both external and internal attacks.

A firewall is a network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules. Firewalls act as a barrier between a trusted internal network and untrusted external networks, such as the internet. Their primary function is to enforce security policies by either allowing or blocking traffic based on factors like IP addresses, port numbers, protocols, or application behaviors.

Corresponding Author: Carel Adelard (careladelard@gmail.com)

Firewalls can be classified into several types, such as packet-filtering firewalls, stateful firewalls, and application-level gateways (proxy firewalls). Each type serves the same basic function filtering traffic but they vary in terms of their depth of inspection and the level of detail at which they analyze the network traffic(Iglesias & Zseby, 2015). For example, packet-filtering firewalls operate at the network layer and examine each packet of data individually, while application firewalls can inspect traffic at the application layer to detect malicious activity such as web application attacks.

The primary role of a firewall is to prevent unauthorized access to an internal network while allowing legitimate communication. It can block incoming threats such as hackers or malware attempting to exploit network vulnerabilities. Additionally, firewalls can be configured to monitor outgoing traffic, ensuring that sensitive data is not leaked or transmitted outside the network without proper authorization. By defining clear rules about what traffic is allowed and what is blocked, firewalls reduce the attack surface and minimize the likelihood of successful external intrusions.

An Intrusion Detection System (IDS) is a security technology designed to detect and monitor network traffic for signs of malicious activity or policy violations(Bace & Mell, 2001). Unlike firewalls, which primarily focus on preventing unauthorized access, an IDS is built to identify suspicious activity that may have already bypassed the firewall or originated from within the internal network. IDS systems are typically deployed to monitor network traffic in real time and analyze it for abnormal patterns or behaviors that may indicate a security threat, such as a network intrusion or an attack in progress(Garcia-Teodoro et al., 2009).

IDS technologies can be broadly categorized into two types: signature-based and anomaly-based systems. Signature-based IDS works by comparing network traffic against a database of known attack patterns or signatures. If the traffic matches a predefined signature, the IDS generates an alert. Anomaly-based IDS, on the other hand, establishes a baseline of normal network behavior and alerts administrators when there are deviations from this baseline, which could indicate a potential security threat(Viegas et al., 2017). While signature-based systems excel at detecting known threats, anomaly-based systems are better at identifying previously unseen or novel attacks.

The primary role of an IDS is detection and monitoring. It acts as a security tool that provides real-time alerts when potentially harmful activities are observed within the network(Boukerche et al., 2007). Although an IDS does not directly block traffic like a firewall, it can provide valuable insights into the nature of an attack, enabling network

administrators to respond swiftly and mitigate damage. IDS also plays a key role in providing visibility into network activity, helping to identify both external and internal threats that may go unnoticed by traditional security measures.

While firewalls and IDS serve different functions, they are often used together to create a layered defense strategy. Firewalls primarily focus on preventing unauthorized access by filtering traffic at the network perimeter, while IDS focuses on detecting and alerting administrators to suspicious activities that could indicate a breach or an attack.

By combining the two, organizations can achieve both proactive defense and reactive detection. Firewalls act as the first line of defense by blocking malicious traffic, while IDS provides an additional layer of vigilance, helping to identify threats that might slip through the firewall or originate internally(Hedbom, 2001). Together, they offer a robust security framework that helps ensure the integrity and safety of a network.

Despite the growing adoption of firewall and IDS technologies, many organizations still struggle with effectively implementing and managing these systems(Anwar et al., 2017). The complexity of configuring firewalls and IDS to work in tandem, along with the challenges of minimizing false positives and ensuring real-time responses to threats, often hinders optimal performance. Additionally, advancements in cyber-attacks, such as advanced persistent threats (APT) and polymorphic malware, continue to test the efficacy of traditional security measures(Laurenza, 2020).

This research focuses on the implementation of a network security system using firewall technology and an IDS, aiming to design and evaluate an integrated solution that enhances network defense capabilities. The study will explore the interplay between firewalls and IDS, the effectiveness of this integration in mitigating modern cyber threats, and the technical challenges involved in deploying such systems(Kuipers & Fabro, 2006). By investigating real-world case studies, methodologies, and best practices, this research aims to contribute valuable insights into how organizations can improve their network security posture by combining these two critical security technologies.

Research Problem Statement

In today's interconnected world, the security of digital networks is more important than ever. As organizations increasingly rely on the internet and networked systems to carry out business operations, the threat landscape has become significantly more complex and sophisticated. Cyber-attacks, ranging from malware and phishing attempts to advanced persistent threats (APTs) and data breaches, pose significant risks to both private and public sector organizations(Alshamrani et al., 2019). These attacks can

result in financial losses, reputational damage, regulatory fines, and a loss of consumer trust. In response, businesses and institutions are investing heavily in network security measures to protect their valuable data and maintain business continuity.

Two critical components of a comprehensive network security strategy are firewalls and Intrusion Detection Systems (IDS). Firewalls serve as the first line of defense by filtering network traffic and blocking unauthorized access based on predefined security rules. On the other hand, IDS are designed to monitor network activity in real-time, detecting and alerting administrators to potentially harmful or abnormal behaviors(Sobh, 2006). While both technologies play vital roles in protecting networks, they are often deployed separately, with firewalls focusing on blocking unwanted traffic and IDS providing threat detection and alerts.

Despite their individual importance, there are several challenges associated with the deployment and integration of these two systems(Shahin et al., 2017). First, the complexity of configuring firewalls and IDS in a manner that optimizes both performance and security is a significant hurdle for many organizations. The balance between allowing legitimate traffic and blocking malicious data can be difficult to achieve, especially with the growing volume of network traffic and evolving cyber threats(Yaacoub et al., 2020). Furthermore, IDS may generate false positives, creating a challenge in identifying true security breaches while avoiding unnecessary alerts that could overwhelm security teams.

Second, firewalls and IDS systems, when used independently, do not provide a comprehensive solution to network security. Firewalls alone may not be sufficient to detect and respond to sophisticated attacks that bypass them, and IDS may struggle to prevent attacks from occurring in the first place(Rash, 2007). Therefore, integrating these two technologies into a cohesive network security system could potentially provide enhanced protection, offering both proactive measures (through the firewall) and reactive measures (through the IDS).

However, despite the advantages of combining firewalls and IDS, there are limited studies exploring the effective implementation and evaluation of such integrated systems. Many existing studies focus on the standalone performance of each technology, rather than assessing how they work together to strengthen network defense(Skopik et al., 2016). Moreover, the performance of integrated firewall and IDS systems in real-world environments, including their ability to minimize false positives, enhance detection capabilities, and optimize response times, remains underexplored.

The research problem, therefore, lies in exploring the implementation and integration of firewall technology and Intrusion Detection Systems (IDS) to create a more effective and comprehensive network security solution. The challenge is to design and evaluate a system that not only combines the capabilities of firewalls and IDS but also overcomes the technical difficulties associated with their deployment, configuration, and operation. Specifically, the research will focus on investigating how the integration of these two technologies can enhance network security, reduce the incidence of false positives, improve threat detection and response times, and ultimately provide more robust protection against both external and internal cyber threats. This research aims to fill the gap in existing literature by offering practical insights into how organizations can deploy and manage an integrated firewall and IDS system for more effective network security.

Novelty of Research

The novelty of this research lies in its focus on the integration and optimization of firewall technology and Intrusion Detection Systems (IDS) to create a more robust and effective network security solution. While firewalls and IDS are established and widely used technologies in network security, they are often deployed in isolation, each serving distinct and limited functions within a broader security framework. Firewalls are primarily focused on filtering traffic and blocking unauthorized access, whereas IDS are designed to detect suspicious or anomalous network behaviors and generate alerts(Strand, 2004). Although these systems can be highly effective on their own, the true potential of network security can only be realized when they are strategically integrated to complement each other.

What sets this research apart is the attempt to develop a unified approach that not only combines the capabilities of both firewalls and IDS but also addresses the technical challenges associated with their integration. In most existing studies, these two technologies are examined independently, with little emphasis on their combined impact or how they can be fine-tuned to optimize performance in real-world scenarios. By focusing on the synergistic benefits of integrating these systems, this research offers a fresh perspective on improving the efficiency and effectiveness of network security architectures(Rawat & Reddy, 2016).

One of the primary innovations of this research is the exploration of real-time, adaptive integration of firewalls and IDS, aiming to enhance threat detection and prevention while minimizing false positives(Ghorbani et al., 2009). While firewalls typically rely on predefined rules and signatures to block malicious traffic, IDS systems often struggle with false alarms due to the complexity and variability of network traffic. This research aims to investigate how the integration of these technologies can leverage their

complementary strengths firewalls' ability to block harmful traffic and IDS's ability to detect and alert on anomalies to create a more adaptive security model that dynamically adjusts to emerging threats without overwhelming administrators with unnecessary alerts.

Furthermore, the research addresses the operational challenges that organizations face when implementing and managing separate firewall and IDS systems. Integrating these systems in a manner that reduces the complexity of configuration, enhances user experience, and provides seamless monitoring is a novel approach that has not been extensively explored in the literature(Serhani et al., 2020). By developing an integrated network security framework, this research aims to provide practical solutions to the technical difficulties associated with the deployment and maintenance of firewall and IDS systems, which are often considered separate silos in current network security practices.

Another significant novelty of this research lies in its real-world application. Many studies focus on theoretical models or laboratory simulations, which may not fully capture the complexities and dynamics of actual network environments. This research emphasizes practical, hands-on implementation, aiming to evaluate the performance of integrated firewall and IDS systems in live environments(Eliot et al., 2018). The research will assess key performance indicators such as detection accuracy, false positive rates, and response times, offering actionable insights into how organizations can effectively deploy and manage integrated network security systems.

In summary, the novelty of this research stems from its unique approach to integrating firewall technology and IDS into a cohesive, adaptive network security solution. It goes beyond conventional methods by addressing the challenges of managing these technologies in tandem, optimizing their complementary functions, and testing the integrated system in real-world scenarios(Lamnabhi-Lagarrigue et al., 2017). By doing so, the research promises to make a significant contribution to the field of network security, providing a more comprehensive, effective, and user-friendly solution for safeguarding digital infrastructures in an increasingly complex threat landscape.

Plan for the results and discussion of this research

The results and discussion section of this research will focus on presenting and interpreting the findings of the study, evaluating the performance of the integrated firewall and Intrusion Detection System (IDS) solution in real-world network environments. The section will be structured to provide a comprehensive analysis of the data collected during the implementation and testing phases, comparing the performance of the integrated system to traditional standalone firewall and IDS setups.

The discussion will also explore the implications of the findings, assess the effectiveness of the integration, and provide recommendations for further improvements.

Before diving into the results, the research will provide an overview of the experiment setup, including the network architecture, the configuration of both the firewall and IDS, and the integration methods used. This section will detail the specific parameters that were tested, such as network traffic volume, the types of attacks simulated (e.g., DoS attacks, malware, SQL injection), and the methods used for data collection. The experimental setup will be described to give readers a clear understanding of the context in which the results were generated.

The research will focus on several key performance metrics to assess the effectiveness of the integrated firewall and IDS system. This metric will evaluate the accuracy of the IDS in identifying malicious activities and unauthorized access attempts that pass through the firewall. The discussion will examine how well the IDS integrates with the firewall in detecting and responding to attacks that bypass the firewall's filtering mechanisms. A critical challenge in both firewall and IDS technologies is the generation of false positives alerts for benign activities that appear malicious. The results will assess the rate of false positives generated by the integrated system, comparing it with the rates of standalone firewalls and IDS. A successful integration should ideally reduce false positives, ensuring that security teams are not overwhelmed by unnecessary alerts.

The speed at which threats are detected and responded to is essential in a network security system. The results will analyze the average response time of the integrated system compared to standalone setups, focusing on how quickly the IDS can detect an attack and how effectively the firewall can block it. The integration of firewall and IDS systems should ideally not significantly degrade network performance. This section will assess the impact of the integrated security system on network throughput, latency, and resource utilization, comparing the results to baseline network performance without security measures.

The ultimate measure of success is the ability of the integrated system to defend against and mitigate network security threats. The results will include a comprehensive evaluation of how well the integrated system addresses both external and internal security threats, offering a comparative analysis with traditional, non-integrated configurations.

Once the results have been presented, a detailed comparative analysis will follow. This will involve examining the differences in performance between the standalone firewall,

standalone IDS, and the integrated firewall-IDS system. The comparison will highlight the strengths and weaknesses of each configuration, focusing on factors such as detection accuracy, false positives, response times, and network performance.

The discussion will explore how the integrated approach enhances the capabilities of both systems. For example, it will be shown how the firewall's traffic filtering capabilities can complement the IDS's anomaly detection, resulting in improved security without introducing a disproportionate number of false positives. The research will also explore whether the integrated system provides quicker and more accurate responses to attacks, and whether it reduces the administrative burden of managing two separate systems.

References

Aldossary, S., & Allen, W. (2016). Data security, privacy, availability and integrity in cloud computing: issues and current solutions. *International Journal of Advanced Computer Science and Applications*, *7*(4).

Alshamrani, A., Myneni, S., Chowdhary, A., & Huang, D. (2019). A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. *IEEE Communications Surveys & Tutorials*, *21*(2), 1851–1877.

Anwar, S., Mohamad Zain, J., Zolkipli, M. F., Inayat, Z., Khan, S., Anthony, B., & Chang, V. (2017). From intrusion detection to an intrusion response system: fundamentals, requirements, and future directions. *Algorithms*, *10*(2), 39.

Bace, R. G., & Mell, P. (2001). *Intrusion detection systems*.

Boukerche, A., Machado, R. B., Jucá, K. R. L., Sobral, J. B. M., & Notare, M. S. M. A. (2007). An agent based and biological inspired real-time intrusion detection and security model for computer network operations. *Computer Communications*, *30*(13), 2649–2660.

Eliot, N., Kendall, D., & Brockway, M. (2018). A flexible laboratory environment supporting honeypot deployment for teaching real-world cybersecurity skills. *IEEE Access*, *6*, 34884–34895.

Garcia-Teodoro, P., Diaz-Verdejo, J., Maciá-Fernández, G., & Vázquez, E. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. *Computers & Security*, *28*(1–2), 18–28.

Ghorbani, A. A., Lu, W., & Tavallaee, M. (2009). *Network intrusion detection and prevention: concepts and techniques* (Vol. 47). Springer Science & Business Media.

Hedbom, H. (2001). *On the Self-Protection of Firewalls and Distributed Intrusion Detection systems*. Citeseer.

Iglesias, F., & Zseby, T. (2015). Analysis of network traffic features for anomaly detection. *Machine Learning*, *101*, 59–84.

Kenkre, P. S., Pai, A., & Colaco, L. (2015). Real time intrusion detection and prevention

system. *Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014: Volume 1*, 405–411.

Kuipers, D., & Fabro, M. (2006). *Control systems cyber security: Defense in depth strategies*. Idaho National Lab.(INL), Idaho Falls, ID (United States).

Lamnabhi-Lagarrigue, F., Annaswamy, A., Engell, S., Isaksson, A., Khargonekar, P., Murray, R. M., Nijmeijer, H., Samad, T., Tilbury, D., & Van den Hof, P. (2017). Systems & control for the future of humanity, research agenda: Current and future roles, impact and grand challenges. *Annual Reviews in Control*, *43*, 1–64.

Laurenza, G. (2020). *Critical infrastructures security: improving defense against novel malware and Advanced Persistent Threats*.

Rash, M. (2007). *Linux Firewalls: Attack Detection and Response*. No Starch Press.

Rawat, D. B., & Reddy, S. R. (2016). Software defined networking architecture, security and energy efficiency: A survey. *IEEE Communications Surveys & Tutorials*, *19*(1), 325–346.

Serhani, M. A., T. El Kassabi, H., Ismail, H., & Nujum Navaz, A. (2020). ECG monitoring systems: Review, architecture, processes, and key challenges. *Sensors*, *20*(6), 1796.

Shahin, M., Babar, M. A., & Zhu, L. (2017). Continuous integration, delivery and deployment: a systematic review on approaches, tools, challenges and practices. *IEEE Access*, *5*, 3909–3943.

Skopik, F., Settanni, G., & Fiedler, R. (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers & Security*, *60*, 154–176.

Sobh, T. S. (2006). Wired and wireless intrusion detection system: Classifications, good characteristics and state-of-the-art. *Computer Standards & Interfaces*, *28*(6), 670–694.

Stewart, J. M. (2013). *Network security, firewalls and VPNs*. Jones & Bartlett Publishers.

Strand, L. K. (2004). *Adaptive distributed firewall using intrusion detection*.

Viegas, E. K., Santin, A. O., & Oliveira, L. S. (2017). Toward a reliable anomaly-based intrusion detection in real-world environments. *Computer Networks*, *127*, 200–216.

Yaacoub, J.-P. A., Salman, O., Noura, H. N., Kaaniche, N., Chehab, A., & Malli, M. (2020). Cyber-physical systems security: Limitations, issues and future trends. *Microprocessors and Microsystems*, *77*, 103201.