ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26may1407

A Comprehensive Evaluation of the Operational Differences Between Intrusion Detection Systems and Intrusion Prevention Systems in Modern Network Security Infrastructures

Sanu Momodu Kabiru[1]; Biralatei Fawei[1]

[1]Department of Computer Science, Niger Delta University, Wilberforce Island, Bayelsa State, Nigeria

Publication Date: 2026/05/29

Abstract: The growing reliance on computer networks to conduct crucial operations has led to increased vulnerability to cyber-attacks in the form of unauthorized access attempts, malware, denial of service (DoS) attacks, and other cyber intrusions. As a result, Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) have emerged as necessary components of today's computer network infrastructure to combat these threats. An Intrusion Detection System monitors computer network traffic for any suspicious activities, whereas an Intrusion Prevention System actively blocks all kinds of attacks to provide real-time protection. While both these systems have been designed with the purpose of improving computer network security, they exhibit many differences in operational process, impact on computer network performance, and effectiveness in different scenarios. This research paper examines these two types of security mechanisms by designing a computer network simulation using the Cisco Packet Tracer software application. For the purposes of this study, a realistic LAN was set up consisting of various networking devices, including routers, switches, client workstations, and servers. The IDS was configured in monitoring mode to detect and analyze computer network traffic, while the IPS was put into inline mode to inspect and block any malicious activity. All the attack scenarios used in this experiment included a DoS attack (Ping flood), attempts at unauthorized access, and port scanning operations in order to provide a fair comparison of system performance. Metrics that were analyzed include detection rate, response time, false alarm rate, and performance impact on the computer network. According to results obtained through the conducted experiment, IPS performed better in terms of providing more accurate detection rates, faster response times, and lower false alarm rates owing to its preventive features. IPS was found to have a negative influence on computer network performance because of the need to block malicious packets. On the contrary, IDS has proven to be efficient in terms of monitoring computer network traffic without affecting its performance, albeit at the expense of slower response times and a high number of false alerts. In conclusion, IDS has been proven to be more effective than IPS when it comes to surveillance and forensics, but when compared to IPS, which gives real-time protection against attacks, IDS lacks this feature. It is also important to note that each security strategy has its own merits, but at the same time, each strategy involves some degree of sacrifice regarding efficiency and effectiveness.

How to Cite: Sanu Momodu Kabiru; Biralatei Fawei (2026) A Comprehensive Evaluation of the Operational Differences Between Intrusion Detection Systems and Intrusion Prevention Systems in Modern Network Security Infrastructures. *International Journal of Innovative Science and Research Technology*, 11(5), 2316-2322. https://doi.org/10.38124/ijisrt/26may1407

I. INTRODUCTION

Rapid development and deployment of information and communication technologies have revolutionized the manner of interaction and exchange of information between organizations, governments, and individuals. Today computer networks are integral to many activities within different industries ranging from banking and medicine to defense and education. At the same time, computer networks have become increasingly vulnerable to different security threats, such as illegal access, data thefts, virus attacks, and even distributed denial-of-service attacks. Thus, network security became a crucial concern in current computing environment. Different security systems were developed to ensure the integrity of computer networks; however, intrusion detection system (IDS) and intrusion prevention system (IPS) remain highly important and relevant today. The main function of any IDS/IPS is the identification and neutralization of all forms of attack. The difference between the two systems lies in their functionality – while IDS detects attacks and generates alerts about them, IPS detects and prevents attacks. Therefore, the focus of this paper will be IDS vs. IPS. Intrusion Detection System Intrusion detection system is intended to monitor network traffic and the activity

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26may1407

of computers for any suspicious behaviors. Basically, IDS identifies policy violation or attack based on predefined set of actions. It should be noted that IDS is not able to prevent attacks. All it does is generating alarms about the possible threat. Thus, although IDS is very helpful in monitoring network activities and preventing attacks, IDS cannot prevent an attack directly. This shortcoming makes intrusion detection systems inferior to intrusion prevention systems. Intrusion Prevention System Intrusion Prevention System is an enhancement of IDS because it detects as well as prevents attacks on networks. Unlike IDS, IPS works inline with network traffic and therefore has the ability to analyze all incoming data flows in real-time mode and take measures to counterattack. The development of cyberattack complexity required the consistent improvement of the IDS and IPS technologies. Signature-based methods that were effective against traditional viruses and malware were ineffective in detecting novel types of attacks that had no signatures. Therefore, modern cybersecurity systems are based on a variety of other approaches, including anomaly detection, machine learning algorithms, and artificial intelligence-based solutions. However, there are still some issues associated with this technology, such as the problem of false positive results, excessive computational overhead, and evasion tactics used by attackers. To overcome these problems, a comparative study of different IDS and IPS solutions should be performed, since both approaches have certain advantages and disadvantages. Thus, although the IDS approach does not affect network performance significantly, the IPS solutions can prevent potential threats from occurring. The purpose of this paper is to conduct a comparative analysis of intrusion detection and intrusion prevention systems in terms of effectiveness, functionality, performance, and application within a variety of network types. Since the security of networks is crucial for any organization, it is necessary to analyze and compare the approaches used to achieve the maximum degree of safety. For example, while the first method may require lower computational resources, IPS solutions can provide users with more reliable results. This research paper explores the issue of the comparison of the IDS and IPS solutions within network security. In particular, its objective is to discuss the mechanisms of these technologies, their strengths, weaknesses, and effectiveness in practice. To conduct a comparative study, the author will use tools, including the Cisco Packet Tracer software.

- *Problem Statement*

Currently, there are a large number of constantly developing and evolving risks for network information security. In particular, there are risks associated with the presence of viruses, Trojans, spyware, ransomware, intrusion into the network or unauthorized access, denial of service or DoS attacks, and many others. At the same time, the use of various computer network structures is becoming increasingly common and important for the operation of any organization and the functioning of all types of services available on the Internet. Accordingly, in today's network security architecture, there is a constant need for protecting the network from cyber threats in real time and being able to respond immediately. Two major network security products that provide network security by detecting cyber attacks and malicious activities in the network are called Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS). At the same time, IDS implies monitoring traffic passing through the network, analyzing data, identifying suspicious activities, and sending notifications accordingly. IPS provides a similar process of identifying potential threats but takes preventive action. Nevertheless, these systems, despite similar goals, have quite different technical features regarding operational principles, speed and efficiency, possible performance impact, deployment, and others. This, in turn, creates certain problems for organizations or system administrators trying to choose the appropriate solution to network security issues. Nevertheless, there is currently a significant need for comparative analysis of the advantages, disadvantages, and characteristics of these solutions, which can help make decisions more efficiently.

II. LITERATURE REVIEW

With the rapid development of computer networks and the internet, numerous security threats such as hacking, data breaches, and various types of cyberattacks have become more prevalent. Generally, intrusions can be described as activities that aim to breach the confidentiality, integrity, and availability of computer systems (Liao et al., 2013; Scarfone & Mell, 2007). Due to these emerging threats, IDS and IPS have been widely utilized as necessary tools for detecting and defending against possible attacks. IDS is defined as any technology designed to detect any potential malicious activity or policy violations in network or computing systems (Abbas et al., 2023). It constantly monitors the network and produces alerts whenever there is an anomaly in its activities. On the other hand, IPS enhances IDS by not only identifying the threat but also preventing it by blocking malicious packets or killing harmful connections (Abbas et al., 2023; Stavroulakis & Stamp, 2010). Nowadays, the significance of IDS and IPS has increased significantly due to the increasing reliance on computer networks and infrastructure. Modern cyber threats, such as DDoS attacks and malware infections, have made it necessary for organizations to implement IDS and IPS tools (Garcia-Teodoro et al., 2009; Modi et al., 2013). Throughout the history of intrusion detection, several milestones have been reached. For instance, Denning (1987) presented the first systematic approach for detecting anomalies in computer systems. Since then, IDS has gone through many advancements and now consists of two major types: signature-based and anomaly-based (Garcia-Teodoro et al., 2009). Nevertheless, each type of IDS comes with several limitations. For example, signature-based IDS cannot detect new or zero-day attacks while anomaly-based IDS frequently generate high levels of false positives. According to modern research, one of the most promising trends in IDS development is machine learning (Abdulganiyu et al., 2023). At the same time, the use of machine learning in IDS presents significant challenges related to computational complexity and high requirements regarding accuracy (Sommer & Paxson, 2010; Axelsson, 2000). The evolution of IDS corresponds to the increase in the number and complexity of cyber attacks. As cyber threats become more advanced, IDS should evolve correspondingly in order to be able to respond adequately (Patcha & Park, 2007). An IDS usually includes

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26may1407

three major elements: sensors, analyzers, and user interfaces (Bace & Mell, 2001). Sensors collect data from network traffic or hosts, analyzers analyze the collected information, and user interfaces show alerts to the administrators of the system. IDS may include two types of components: Network-based IDS (NIDS) and Host-based IDS (HIDS) (Patcha & Park, 2007). While NIDS monitor the network traffic as a whole, HIDS collect information about individual devices. Moreover, the effectiveness of IDS relies not only on adequate configuration but also on appropriate data analysis methods and successful integration with other parts of the security system (Northcutt, 2005; Mukherjee, 1994). At the same time, IDS components should be updated and protected since they are targeted frequently by hackers (IEEE Access Review, 2021). The concept of IPS was developed based on IDS; however, IPS differs significantly from IDS by including real-time responses to detected activities. Unlike IDS, IPS blocks malicious traffic immediately instead of detecting and reporting the intrusion only (Scarfone & Mell, 2007). In other words, it acts not as a detector but as a protective device. Moreover, IPS operates in-line; thus, all data have to pass through it (Behl & Behl, 2017). Incorporation of this method improves security in the network as it prevents cyber attacks from occurring within the network. Nonetheless, since it is inline, it might delay communication and affect performance negatively (Modi et al., 2013). According to research, IPS is very efficient in detecting and preventing attacks that have been detected earlier. However, it is not efficient in detecting new types of attacks and cyber activities (Modi et al., 2013; Sommer & Paxson, 2010). Moreover, there is a possibility of legitimate data being blocked because of the inappropriate configuration of the IPS system. Nonetheless, it plays an integral role in modern security architectures because of its capability to offer instant protection from cyber attacks (Debar et al., 1999). Some notable differences between IDS and IPS systems include their function and mode of operation. IDS only detects cyber threats passively and does not interfere with any traffic on the network, while IPS operates inline and prevents attacks actively in addition to detection (Abbas et al., 2023; Scarfone & Mell, 2007). The difference influences several characteristics of both devices regarding their effectiveness and performance in detecting and preventing cyber attacks. While IDS is not intrusive and does not compromise the performance of the network, it does not provide immediate protection from attacks (Garcia-Teodoro et al., 2009). However, IPS offers adequate protection from cyber attacks actively. Nevertheless, it interferes with network performance and affects network throughput (Modi et al., 2013). Organizations can choose between IDS, IPS, or both based on their needs and requirements (Axelsson, 2000; Patcha & Park, 2007). IDS/IPS systems use signature-based, anomaly-based, and hybrid detection techniques (Liao et al., 2013). Signature-based detection technique is very efficient in detecting known threats. However, it cannot detect new attacks (Garcia-Teodoro et al., 2009). Conversely, the anomaly-based detection technique can detect new types of attacks. However, it generates many false positives. Hybrid systems attempt to integrate the best qualities of the two systems to attain more accuracy and reliability (Abdulganiyu et al., 2023). The introduction of machine learning and deep learning has enhanced detection capabilities, enabling systems to evolve and adapt to new threats. Nevertheless, the success of these approaches greatly relies on the quality of data used during training and configuring the systems (Ngueajio et al., 2022). The effectiveness of intrusion detection and prevention systems (IDS and IPS) can be measured through parameters such as detection rate, false positive rate, response time, and throughput of the network (Axelsson, 2000). According to some findings, IPS detects more attacks than IDS because of being proactive and affects network performance significantly less than IDS (Modi et al., 2013). False alarms are still a critical issue for both systems that influence reliability (Sommer & Paxson, 2010). Reliable data and testing should be used to make proper performance evaluation. Contemporary researches put emphasis on the role of high-quality datasets and proper assessment frameworks in the evaluation process (Rahman & Hasan, 2025). IDS and IPS are crucial tools for detecting malicious traffic on computer networks but there are a number of challenges associated with the utilization of such solutions. These are limited scalability, a high rate of false positives, growing sophistication of cyber attacks, etc. (Garcia-Teodoro et al., 2009). Advanced detection algorithms usually demand powerful computational resources to work correctly. The widespread use of encryption makes it hard for IDS/IPS to detect malicious traffic as well. In addition, there are numerous techniques that can be utilized by attackers to circumvent detection mechanisms successfully (Ptacek & Newsham, 1998). It proves once again that constant improvements are required in order to deal with new challenges efficiently. Current trends in IDS and IPS are characterized by attempts to integrate artificial intelligence and machine learning techniques (Ngueajio et al., 2022). The application of deep learning algorithms has increased the precision in detecting complex patterns in attacks. Nevertheless, they need substantial data and computing power (Abdulganiyu et al., 2023). In addition, cloud-based IDS and IPS have become common due to their scalability and versatility. Moreover, the application of the MITRE ATT&CK framework has led to enhanced detection and prevention of advanced persistent threats (Rahman & Hasan, 2025). Hybrid security systems that integrate IDS, IPS, and firewall technology have emerged as the most commonly used approach for safeguarding computer networks. Based on the literature review, IDS and IPS have proved to be essential aspects of the contemporary network security architecture. While IDS contributes to network visibility and monitoring, the IPS provides an opportunity for proactively preventing threats to the system. However, there is still a significant gap in the comparative study of IDS and IPS.Most of the studies only conduct theoretical analysis and lack empirical justification (Abdulganiyu et al., 2023). Hence, a simulation-based research design is required in order to validate the claims made by the researchers. Simulation is one of the best research methodologies that can be applied to assess the performance of IDS and IPS. The present study will fill this research gap by comparing IDS and IPS through simulation-based research.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26may1407

III. APPROACH

The methodology adopted in this research will be anchored on the establishment of a simulated environment using Cisco Packet Tracer to undertake a comparative analysis between the functioning of IDS and IPS in network security. In this simulated environment, it will be expected to have an actual LAN that can be used to simulate the functioning of IDS and IPS systems in order to make valid inferences from the experiments conducted. In this regard, a network environment will be designed using Cisco Packet Tracer to emulate the functioning of a computer network in a real life scenario. In this stage, a realistic LAN will be constructed which incorporates various connected devices such as personal computers and servers to establish a realistic network setting. Communication within the network is established by interconnecting personal computers and servers with each other via switches and routers. This stage sets the tone for carrying out experiments in the established LAN. Once a functional LAN is designed, the configuration of IDS and IPS are carried out. IDS system configuration involves establishing this security system in monitoring mode whereby it will monitor all the transactions in the LAN in order to generate alert on any detected malicious activity in the LAN. Contrary to the IDS configuration, IPS is configured in inline mode. This means that it will be set up to inspect network activities and prevent attacks by blocking malicious transactions in real time. With these security systems configured, the next step will involve carrying out simulated attacks on the established LAN and assessing how these IDS and IPS respond. The simulated attacks that can be carried out may include ping flood attack to create denial-of-service, unauthorized access attack and port scanning activities among others. After the simulation processes, the data obtained from the simulations is gathered based on the performance criteria of the detection rate, response time, and the rate at which false alarms were triggered by both the systems. This gives an insight into how efficient the IDS and IPS systems are in the similar scenario. Finally, after gathering the data, there will be a comparison of the performance of the two systems. Comparison is performed through tabular representations and graphs that show the performance difference of the two types of systems.

IV. RESULTS AND DISCUSSION

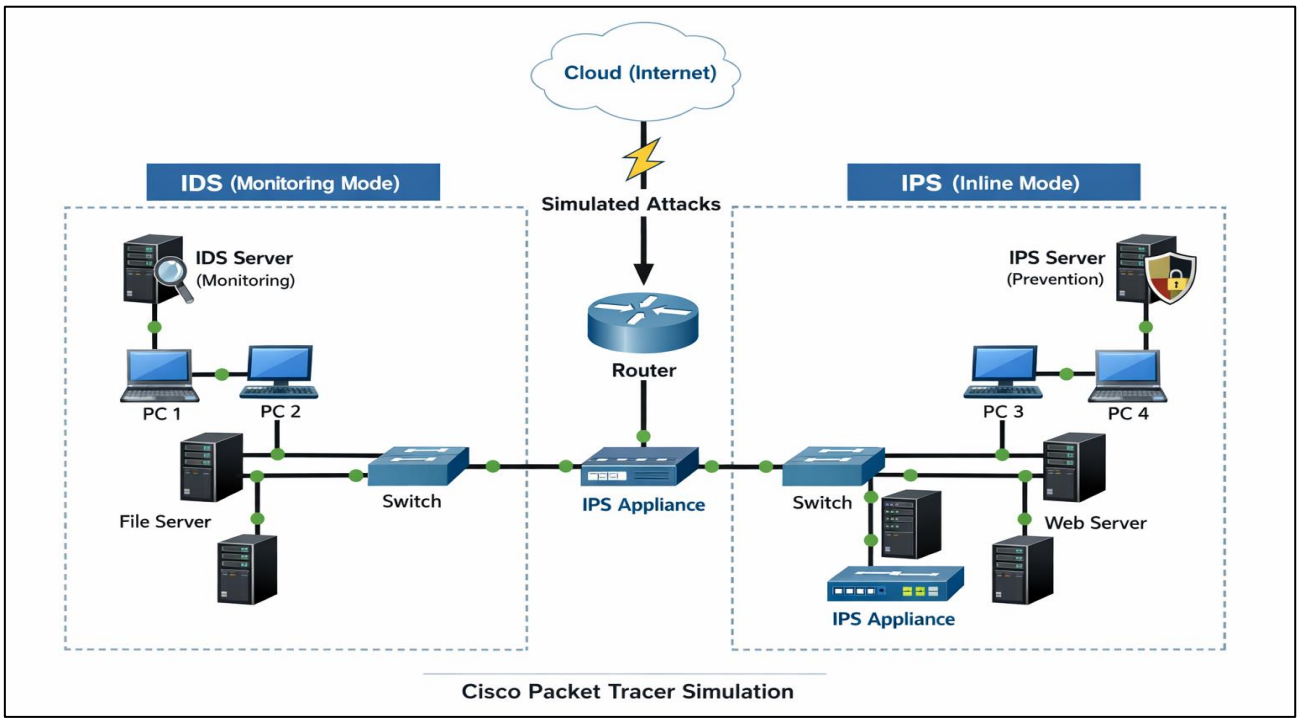

Fig 1: Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) Simulation.

The simulation environment used Cisco Packet Tracer to enable practical demonstration of the differences between intrusion detection systems and prevention systems by setting up a modern network with different topologies, representing different modes of operation, namely IDS monitoring and IPS inline, that are joined through a common router acting as a gateway to an internet cloud. The attacks are created through the internet and sent from the cloud to the network, through the router, so that the effects of IDS and IPS can be seen in similar situations. In IDS, network topology is designed to support passive monitoring in the network. IDS network includes two client machines, file server, switch, and IDS itself. IDS machine is located in a way that it monitors the network traffic and processes it, but does not participate in the actual transmission process. As packets travel between devices, they are collected and analyzed by IDS and suspicious activity, such as attacks and malware traffic, is identified. Whenever IDS detects a threat in the form of an attack, it raises alarms to notify the administrators of its presence. No action is taken by IDS to counteract and stop the attack. Therefore, IDS only performs monitoring and detection of threats, and does not prevent them, thus causing

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26may1407

fewer disruptions in the normal functioning of the network. IDS system may be prone to errors in monitoring and detecting attacks, leading to increased occurrence of false positives that will require further investigation to validate. On the other hand, IPS network topology is set up using an inline design. Similar to IDS, IPS network comprises of two client machines, web server, switch, and IPS appliance. Unlike IDS, IPS appliance acts as an inline device, meaning that all network traffic travels through it, no matter whether it is leaving or entering the network. As the packets enter the IPS, they are examined in real-time for any presence of malicious content or activity. Once an attack is detected, the IPS automatically blocks the packets or drops the connection that initiated the attack. As a result, threats are prevented from entering the network infrastructure, enhancing the level of protection offered by the IPS. Nonetheless, packet inspection causes additional overheads, thus leading to lower network throughput and higher latency. Attacks generated from the internet cloud are used in the simulation for the two cases of intrusion detection systems. These attacks include denial of service attempts, unauthorized access, and port scanning activities among others. The same number of attacks are launched against the IDS and IPS systems for fairness purposes. Analysis of the simulation reveals that the IPS is more effective and efficient in identifying and responding to attacks than the IDS. This happens because the IPS automatically terminates any malicious packets that are detected while the IDS only produces alerts. Therefore, the IDS has lower response times due to delayed reactions. It is evident that there is a trade-off between network performance and security when deploying an IDS or IPS. The IDS ensures maximum network performance since it does not disrupt the traffic flow. Nevertheless, the IDS cannot prevent attacks because it lacks automatic response mechanisms. Conversely, the IPS has lower network performance since it interferes with the traffic flow. However, it enhances network protection by terminating attacks automatically. Moreover, the IPS has more accurate responses than the IDS because it filters the data packets using stringent standards. IDS can allow traffic carrying malware to travel through the network and even affect the internal devices before raising alarms. In the case of the IPS, the traffic containing the malware is stopped at the IPS device, and consequently, it will not affect the web server and client machines. In conclusion, there are significant differences in how these two devices work as shown by this simulation. It can be observed that IDS can help monitor network activity and detect possible attacks. However, it cannot stop any threats since its purpose is to identify malicious activities. On the other hand, although IPS can provide better security, it adds extra burden and costs to the network. Based on the findings, the best option is to integrate IDS and IPS together to create a better system that takes advantage of both devices' strengths.

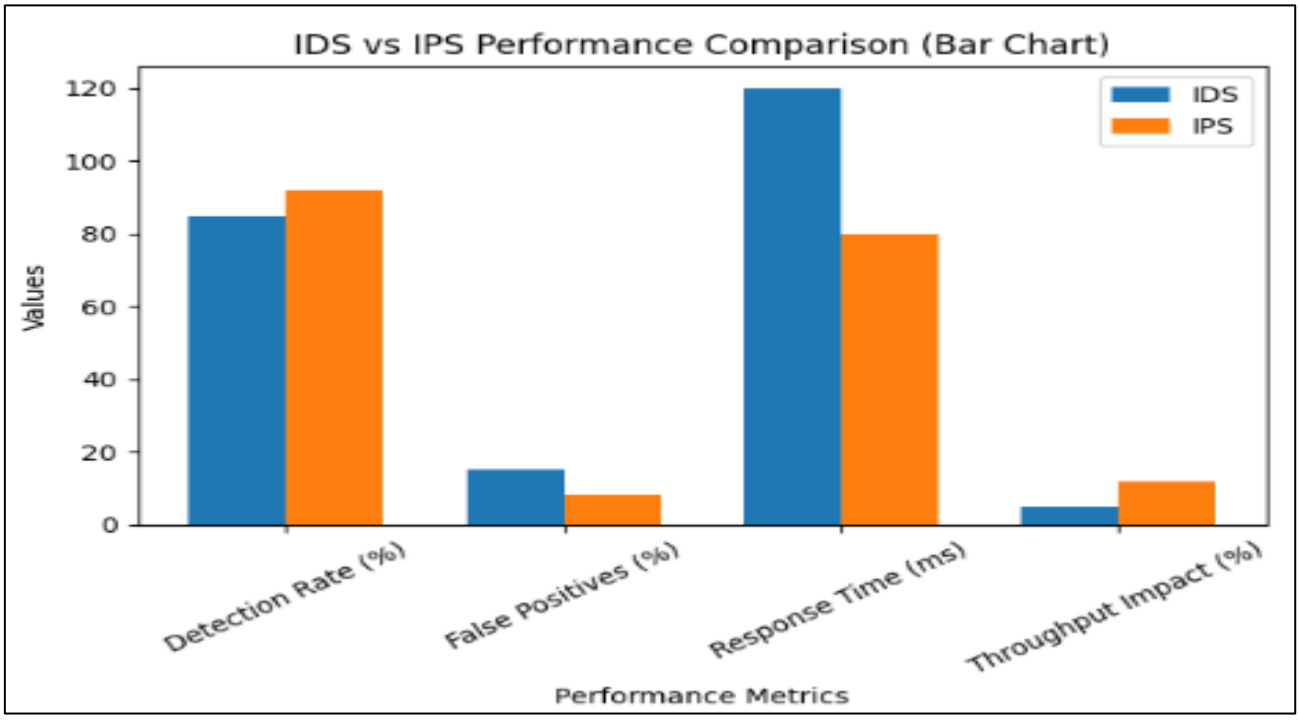

Fig 2: IDS vs IPS Performance Comparison (Bar Chart).

The bar graph above depicts a comparison between IDS and IPS in terms of some critical performance characteristics. From the graph, it can be seen that IPS has better detection capabilities and fewer errors than IDS, which implies better accuracy. Furthermore, IPS is faster because it operates inline. On the other hand, IDS has a lower impact on throughput, meaning that it is not as resource-consuming as IPS.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26may1407

Table 1 Comparative Interpretation of IDS and IPS Simulation Results Table

Performance Metric	Intrusion Detection System (IDS)	Intrusion Prevention System (IPS)	Interpretation / Explanation
Detection Rate (%)	85%	92%	IPS performs better because it not only detects but also actively blocks threats in real-time, whereas IDS only identifies and alerts.
False Positives (%)	15%	8%	IDS generates more false alarms since it passively monitors traffic, while IPS applies stricter filtering mechanisms, reducing incorrect alerts.
Response Time (ms)	120 ms	80 ms	IPS is faster because it operates inline and reacts immediately to threats, while IDS takes longer due to its monitoring and alert-based approach.
Throughput Impact (%)	5%	12%	IDS has negligible impact on network performance because it does not affect the traffic flow, while IPS has higher overhead because of its real-time examination and blocking.

The results from the comparison show that IPS is better in terms of detection and response because of its proactive method of securing the system; however, the cost of increased overhead in the network cannot be overlooked. On the other hand, IDS offers an optimal solution in monitoring, with reduced overhead, yet it is prone to having more false positives and delayed responses.

V. CONCLUSION

This research compares two intrusion detection systems with intrusion prevention systems in the modern network security environment using simulated networks created with Cisco Packet Tracer software. The methodology included design of an ideal local area network, implementation of both IDS and IPS in monitoring and inline modes respectively, and subsequent exposure of both systems to similar types of cyber attacks. Metrics used in evaluating the performance of IDS and IPS include detection rate, false positive cases, response rate, and the extent of network performance impact as a result of attacks. According to the simulation outcome, IDS plays an integral role in identifying cyber activities but has limited capabilities to actively prevent such attacks from causing harm. IDS was found to be efficient in detecting malicious activities with minimum network performance impact, which can be attributed to the fact that this system operates in passive mode. As such, this approach to network security allows for delays during response times, which leads to high rates of false positives since it takes longer for IDS to respond to malicious activities detected within a network system. IPS was found to deliver better security performance because it actively blocks malicious activities within an internal network by filtering and inspecting the packets of information received before being directed inside a network. This characteristic of IPS improves detection rates and reduces the rates of false positives, which can cause disruptions in normal network operations. Although IPS performs better than IDS in protecting internal network security, this system consumes more computing resources due to inline operation, thus, causing some performance losses on a network. The comparative study reveals that there is a clear trade-off between performance and security aspects when dealing with modern intruders. Both IDS and IPS have their strengths and weaknesses depending on the type of network environment. However, an effective solution would be a combination system that integrates the two security measures by merging the ability of IDS to detect attacks with the preventive measure of IPS.

REFERENCES

[1]. Amoroso, E. (2012). *Cyber attacks: Protecting national infrastructure*. Butterworth-Heinemann.

[2]. Anderson, J. P. (1980). Computer security threat monitoring and surveillance. *Technical Report, James P. Anderson Co.*

[3]. Axelsson, S. (2000). Intrusion detection systems: A survey. *Technical Report, Chalmers University of Technology*.

[4]. Bace, R., & Mell, P. (2001). *Intrusion detection systems*. National Institute of Standards and Technology (NIST).

[5]. Behl, A., & Behl, K. (2017). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.

[6]. Debar, H., Dacier, M., & Wespi, A. (1999). Towards a taxonomy for intrusion-detection systems. *Computer Networks, 31*(8), 805–822.

[7]. Denning, D. E. (1987). An intrusion-detection model. *IEEE Transactions on Software Engineering, SE-13*(2), 222–232.

[8]. 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.

[9]. Julisch, K. (2003). Clustering intrusion detection alarms to support root cause analysis. *ACM Transactions on Information and System Security, 6*(4), 443–471.

[10]. Kumar, S., & Spafford, E. H. (1994). A pattern matching model for misuse intrusion detection. *Proceedings of the National Computer Security Conference*.

[11]. Lee, W., & Stolfo, S. J. (1998). Data mining approaches for intrusion detection. *Proceedings of the 7th USENIX Security Symposium*.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26may1407

[12]. Liao, H. J., Lin, C. H. R., Lin, Y. C., & Tung, K. Y. (2013). Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications, 36*(1), 16–24.
[13]. Modi, C., Patel, D., Borisaniya, B., Patel, A., & Rajarajan, M. (2013). A survey of intrusion detection techniques in cloud. *Journal of Network and Computer Applications, 36*(1), 42–57.
[14]. Mukherjee, B., Heberlein, L. T., & Levitt, K. N. (1994). Network intrusion detection. *IEEE Network, 8*(3), 26–41.
[15]. Northcutt, S. (2005). *Network intrusion detection*. New Riders.
[16]. Paxson, V. (1999). Bro: A system for detecting network intruders in real-time. *Computer Networks, 31*(23–24), 2435–2463.
[17]. Patcha, A., & Park, J. M. (2007). An overview of anomaly detection techniques: Existing solutions and latest technological trends. *Computer Networks, 51*(12), 3448–3470.
[18]. Ptacek, T. H., & Newsham, T. N. (1998). *Insertion, evasion, and denial of service: Eluding network intrusion detection*. Secure Networks Inc.
[19]. Roesch, M. (1999). Snort: Lightweight intrusion detection for networks. *Proceedings of LISA '99*.
[20]. Scarfone, K., & Mell, P. (2007). *Guide to intrusion detection and prevention systems (IDPS)*. National Institute of Standards and Technology (NIST).
[21]. Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. *IEEE Symposium on Security and Privacy*.
[22]. Stallings, W. (2018). *Network security essentials: Applications and standards* (6th ed.). Pearson.
[23]. Tanenbaum, A. S. (2011). *Computer networks* (5th ed.). Pearson.
[24]. Wagner, D., & Soto, P. (2002). Mimicry attacks on host-based intrusion detection systems. *Proceedings of the ACM Conference on Computer and Communications Security*.
[25]. Whitman, M. E., & Mattord, H. J. (2016). *Principles of information security* (5th ed.). Cengage Learning.