CHAPTER I

INTRODUCTION

1.1 Background

The rapid development of information and communication technology has prompted many organizations to switch to network-based systems to increase efficiency and productivity. While digitalization brings many benefits, such as faster access and better automation, the growing reliance on digital infrastructure also presents new challenges, especially when it comes to cybersecurity. One of the threats that continues to grow and is increasingly worrying is *Distributed Denial of Service* (DDoS). This attack is carried out by flooding the *server* with a large amount of traffic, so that the system is overwhelmed and the service becomes inaccessible to legitimate users.

According to a report from Cybersecurity Ventures (2023), the number of DDoS attacks continues to increase by an average of 15% annually, and is expected to cause global losses of up to USD 10.5 trillion by 2025 [1]. Meanwhile, a report from Netscout (2024) revealed that in the first quarter of 2024 alone, the number of DDoS attacks increased by 43% compared to the same period the previous year. Attacks with HTTP Flood, SYN Flood, and UDP Flood methods are the most commonly used by cybercriminals [2]. This fact confirms that DDoS attacks are not only becoming more frequent, but also increasingly sophisticated and difficult to detect or prevent. With the increasing scale and complexity of attacks, organizations need to implement more comprehensive mitigation strategies to keep their systems secure and able to operate optimally without experiencing disruptions due to intentional spikes in traffic by hackers.

To deal with this threat, various methods have been developed to improve *High Availability* (HA) and overcome traffic spikes, one of which is by implementing *Load Balancer* [3]. *Load Balancer* in charge of distributing traffic to several *Server backend* to make sure there is no one *Servers* that are overloaded. By using *Load Balancer*, the system can maintain service availability despite high traffic spikes.

There are various methods *Load Balancing* that can be applied, one of which is *Least Connection*. This method works by directing traffic to *Servers* that have the least active connections, so that the load can be distributed more evenly [4]. Compared to the *Round Robin*, which simply divides traffic alternately without considering the

conditions of each *Servers*, *Least Connection* more adaptive in handling workload fluctuations. Research by Afiyah & Rahmika (2024) shows that this method is more effective in environments with a high number of users, where the workload on each server can vary greatly [3]. However, while Load Balancer helps to better manage traffic, it lacks mechanisms to detect or prevent DDoS attacks, making it vulnerable to attacks that overwhelm networks with excessive demand [5].

To strengthen system protection against DDoS attacks, *Load Balancer* need to be combined with an additional layer of security, such as *Intrusion Prevention System* (IPS). IPS serves as a defense system that can analyze network traffic in a *real-time* and automatically blocks suspicious activity before it reaches *Server backend* [6]. One of the widely used IPS is Suricata, which is known for its ability to conduct in-depth packet inspections (*Deep Packet Inspection*), *Rule-based detection*, as well as multi-threading support that allows the system to run at high performance [7].

The research entitled "*Development of Network Security Using a Suricata-Based Intrusion Prevention System Against Distributed Denial of Service*" by M. Tahir et al. (2024). This study discusses how Suricata can detect and treat SYN *Flood Attack* and *Ping of Death*, the two most common types of DDoS attacks [6]. The results show that Suricata is able to accurately recognize attack patterns and mitigate them before the threat reaches *Servers* Essentially, thereby increasing the protection of the system. However, this study still has limitations because it only assesses the effectiveness of Suricata as an independent social studies system, without considering how it performs if integrated with *Load Balancer*. Therefore, this study aims to examine how the combination of Load Balancer (NGINX Least Connection) and Suricata can work more optimally in protecting the system from DDoS attacks [6].

Previous studies have addressed ways to address DDoS attacks, but there are still aspects that have not been explored in depth. Romadhon & Nuha (2024) in their journal *Comparative Analysis of HAProxy and Nginx Load Balancers in Mitigating User Datagram Protocol* (UDP) *Flood Attacks* comparing the effectiveness of HAProxy and NGINX in the face of UDP attacks *Flood*. Even so, the study did not address how the combination of Load Balancer and IPS could improve protection against more complex attacks [5]. Meanwhile, Tang et al. (2024) examined the impact of HTTP Flood attacks on Apache2 and NGINX, but they did not evaluate how IPS-based solutions could help in countering such attacks [7]. On the other hand, Swetha & Dara (2018) discuss the implementation of multi-core-based IPS, but their research

does not highlight how the integration of Load Balancer and IPS can work together to deal with DDoS more effectively [8]. In addition, research conducted by Wahyu Adi Prabowo (2023) compared several systems *Intrusion Detection & Prevention Systems* (IDPS) such as Snort, Zeek, and Suricata, but did not examine how these systems would perform if implemented in a scenario *Load Balancing* [9].

From the various studies that have been conducted, no one has specifically discussed how the integration between *NGINX (*Least Connection*) Load Balancer* and Suricata IPS can improve the system's resilience to DDoS attacks. Therefore, this study aims to fill this gap by combining Load Balancer and IPS, as well as test the extent to which the combination of the two can be effective in protecting the system from DDoS threats.

This study will test the performance of the combination of Load Balancer (NGINX Least Connection) and IPS (Suricata) in the face of DDoS attacks, using Hyper-V as virtualization and Ubuntu as the operating system. Some of the key aspects to be tested include Throughput, Response Time, CPU Utilization, and Mitigation Effectiveness.

1.2 Problem Formulation

Based on the background that has been described, the formulation of the problem in this study is:

1. What kind of Suricata IPS and NGINX Load Balancer configurations provide the best balance between performance and security in the face of DDoS attacks?
2. How does the integration of Suricata IPS with NGINX *Load Balancer* using *the Least Connection* method affect *the throughput, response time, cpu utilization* of the system when facing DDoS attacks such as SYN Flood, HTTP Flood, and UDP Flood?
3. How effective is Suricata as an IPS in detecting and preventing attacks on the Load Balancer system when dealing with DDoS attacks such as SYN Flood, HTTP Flood, and UDP Flood?

1.3 Research Objectives

In accordance with the formulation of the problem, the objectives of this research are:

1. Design and implement a configuration between Suricata IPS and NGINX Load Balancer to get the best results between performance and security in the face of DDoS (SYN Flood, HTTP Flood, and UDP Flood).
2. Analyzes the effect of Suricata IPS integration with NGINX Load Balancer (Least Connection) on system throughput, response times, and cpu utilization when facing DDoS attacks (SYN Flood, HTTP Flood, and UDP Flood).
3. Measure the effectiveness of Suricata as an IPS in detecting and preventing attacks on *the Load Balancer* system when facing DDoS attacks.

1.4 Research Benefits

This study aims to develop a DDoS mitigation strategy by integrating Load Balancer (NGINX Least Connection) and IPS Suricata and measuring the effectiveness of these integrations. Specifically, this study aims to:

1. It is a reference for system developers in designing network architectures that are more efficient and resistant to cyberattacks, especially DDoS attacks.
2. Provide insights in evaluating the effectiveness of DDoS mitigation strategies, thereby enabling improvements and optimization in the implementation of Load Balancer-based and IPS-based security systems.
3. Assist network administrators in improving security and service availability by integrating NGINX Least Connection Load Balancer and Suricata IPS.

1.5 Problem Limitations

In order for this research to be more directed and focused on achieving the expected goals, there are several problem limitations set in this study:

1. This study will only test and analyze three types of DDoS attacks, namely SYN Flood, UDP Flood, and HTTP Flood. Other types of DDoS attacks, such as ICMP Flood or Smurf Attack, will not be discussed in this study.
2. The testing infrastructure will be conducted using Hyper-V virtualization, with the operating system used being Ubuntu Server on each node. Testing is only conducted in a closed environment (laboratory) and does not involve a public network or larger production scale.
3. The evaluation of the system is carried out based on four main parameters, namely: *Throughput* , *Response time*, *CPU Utilization*, the effectiveness of attack mitigation.