CHAPTER V
CONCLUSION

5.1 Conclusion

Based on the results of the implementation and testing that has been carried out, several conclusions can be obtained as follows.

1. *The integration of Suricata's Intrusion Prevention System* (IPS) with NGINX Load Balancer using the Least Connection method was successfully implemented in an Ubuntu Server-based virtualization environment. The system consists of an IPS Suricata, an NGINX Load Balancer, as well as two backend servers that can operate according to the designed topology.
2. SYN Flood, UDP Flood, and HTTP Flood attacks without IPS mechanisms cause a decrease in system performance characterized by decreased *throughput* and *slow response times*. *Throughput* decreased to 3153.53 req/s on SYN Flood, 4463.19 req/s on UDP Flood, and 2588.32 req/s on HTTP Flood. Meanwhile, *the response time* slowed down to 158,553 ms, 112,028 ms, and 193,175 ms respectively.
3. The implementation of Suricata as *an Intrusion Prevention System* (IPS) is able to detect and block attack traffic in all test scenarios. In the SYN Flood test, Suricata managed to drop 2,263,680 packets. Meanwhile, in the UDP Flood and HTTP Flood tests, Suricata managed to record *65,035 and 9,169* drop events, respectively.
4. The application of Suricata IPS is able to increase *throughput* in all attack scenarios. In SYN Flood attacks *throughput* increased by 27.98%, in UDP Flood increased by 21.27%, and in HTTP Flood increased by 44.11%. In addition, *the response time* is faster by 72.32% for SYN Flood, 77.84% for UDP Flood, and 72.02% for HTTP Flood compared to conditions without IPS.
5. Based on the results of the CPU Utilization test, most of the processing load shifted to the IPS *virtual machine* with CPU usage of 32.68% in SYN Flood testing, 20.11% in UDP Flood, and 35.04% in HTTP Flood. Meanwhile, CPU usage on the Load Balancer and both backend servers remains close to baseline conditions, so service availability can be maintained as long as the system receives a DDoS attack.

5.2 Suggestions

Based on the results of the research that has been conducted, there are several suggestions that can be used for further research development, which are as follows.

1. Further research can be tested with more types of DDoS attacks, such as HTTP Flood and SYN Flood with active IPS mechanisms so that the effectiveness of mitigation on different types of attacks can be analyzed more thoroughly.
2. Further research can use higher hardware specifications so that the testing process can be carried out with a greater traffic load and produce more diverse data.
3. The development of Suricata rules can be done by utilizing built-in rules and more specific rules so that attack detection and prevention capabilities can be improved.
4. Further research can combine Suricata with other security mechanisms, such as firewalls, Web Application Firewalls (WAF), and different load balancing algorithms to obtain a better level of security and service availability.
5. Subsequent research can use more than one attacker and a larger number of clients so that the test scenario can be closer to the actual network conditions.