ABSTRACT

Security is a very important part of Information Technology (IT) which has been used in various fields. Especially in the current era where we are required to be able to use all technology to support activities. Utilization of IT can facilitate operations so as to improve service quality. But on the other hand, if security is not maintained, it will have an impact on service availability.

Software Defined Network is a network architecture that allows the network to be controlled centrally by separating the Control Plane and Data Plane making it easier from the operator's side to manage the network consistently, therefore SDN is believed to be able to replace the existing network which tends to be rigid. But despite the capabilities of the SDN, SDN security is still a major concern.

In this final project, the design of an Snort and IPTables based IPS system that is integrated with the Honeypot system in the Software Defined Network network architecture will be carried out. IPS will detect attacks based on the applied rules and if there is an attack then IPS will give an alert to the Controller which then the Controller will check the database and divert the attack traffic to the Honeypot

In this final project, the author analyzes accuracy, detection speed and Quality of Service in the form of comparison of Throughput and Packet Loss between the time the attack occurs and when the attack is successfully transferred. The results of this final project show that the accuracy rate is 99.87%, the average detection speed for Port Scanning, Ping of Death, ICMP Flood and TCP SYN Flood attacks are 1.207 s, 1.045 s, 1.047 s, and 1.101 s. While the QoS measurement shows that after the attack is transferred, there is an increase in the Throughput value and a decrease in the Packet Loss value.

Keywords: *Cyber Security, Software Defined Network, Intrusion Prevention System*