ABSTRACK

SDN is a technology that separates the control plane and the data plane. The control plane functions to configure network devices using the SDN controller while the data plane functions to forward information packets. The controller is the main control for the network and is centralized, if this section is successfully attacked then the entire network can be taken over. If SDN resources are attacked with Denial Of Service, SYN Flooding will consume network resources, causing the SDN controller to be unable to serve SDN network user requests. One of the efforts to overcome this problem is to use an IPS security system because it can prevent DoS attacks by using the snort application to block attacks in real time. The tests carried out tested the performance of QoS parameters with a DoS SYN Flood attack using the hping3 application in the form of Throughput, Latency, CPU Load and memory usage before and after the implementation of the IPS security system with test scenarios before the attack, during the attack and during blocking. The results obtained in this study on the results of QoS throughput before the attack had an average of 22.536 Gb/s, during an attack 14,163 Gb/s, when blocking 14.926 Gb/s. In the results of QoS Latency before the attack was 0.10643& ms, the average during the attack was 0.11893 ms, when blocking had an average of 0.0461 ms. In the QoS CPU Load results before the attack 26.92%, during the attack 100.416%, when blocking 99.093%. In memory QoS results before attack 4.08%, during attack 0.1%, when blocking 18%. And the conclusion is that the implementation of using IPS has proven to be effective in detecting and blocking Denial Of Service attacks so as to improve the quality of the security system on the SDN network.

Keywords: Software-Defined Network , Denial Of Service, Throughput, bandwidth,Latency, Intrusion Prevention System..