ABSTRACT

Software Defined Network is a network architecture that separates the functions of controlling and forwarding function of a network device, essentially is network centralization. However, the concept of a centralized network has a weakness in terms of security control plane. In this Final Project aims to apply and analyze the influence of security mechanisms in terms of performance using Intrusion Prevention System (IPS) which has advantages in the presence of packet blocking mechanism as a preventive function.

In this study, integration of IPS on the SDN network has been conducted and testing and measuring the effects caused in terms of network performance. The parameters used are QoS including delay, jitter, throughput, and packet loss ratio. In addition, testing is also done to measure the limits of IPS Snort when handling attacks in large quantities.

From the tests that have been done, SDN Network integrated with IPS is able to block the attack packets sent simultaneously with the service pack of video stream and VoIP. SDN network integrated with IPS seen from the results of QoS parameter performance testing tend to be more stable, because it is able to block the attack packets to minimize the decrease in performance due to the incoming packet attacks when the delivery of service packets. In addition, the ability of IPS in analyzing incoming packets decreased when the number of attack packets entered 9,000 packets / s.

Keywords: Software Defined Network (SDN), Intrusion Prevention System (IPS), Snort, Performance, Ryu.