ABSTRACT

The increasing use of web pages causes web servers to be vulnerable to various attacks that interfere with web server performance. One of the attacks on web servers is data flooding which disrupts access from users to the web because web server performance is hampered. A network security system is needed that implements an Intrusion Prevention System (IPS) to prevent data flooding attacks. There are several softwares that can implement IPS methods such as Snort and Suricata. This study analyzed the performance of IPS Snort and Suricata in preventing data flooding attacks based on web server service QoS parameters. Comparison of the performance of Snort and Suricata was seen through 4 test scenarios. In the first scenario the system did not experience data flooding attacks to measure the normal performance of the web server. In the second scenario the system experienced a data flooding attack without IPS. In the third and fourth scenarios the system experienced a data flooding attack by applying IPS Snort and Suricata alternately. Based on this test, the value of the QoS parameter (delay, packet loss, throughput, RTT) was obtained. The results of QoS parameter measurements in scenario 1 were throughput 1,898 Mbps, packet loss 0.029%, delay 3.409 ms, and RTT 0.028 s. In scenario 2, throughput was 0,0007 Mbps, packet loss was 64.854 %, delay was 3475.518 ms, RTT was 14.642 s. In scenario 3, throughput was 0,725 Mbps, packet loss was 0.018%, delay was 7.885 ms, and RTT is 0.064 s. In scenario 4, throughput was 0,748 Mbps, packet loss was 0.017%, delay was 7.669 ms, and RTT was 0.062 s.

***Keywords** : Web server, Data flooding, IPS, Snort, Suricata*