ABSTRACT

Current technological developments have grown rapidly, especially in the use of computer networks, but these developments also have an impact on the security of a network. Therefore, today's computer network security system is very important in maintaining the confidentiality and integrity of data to guard against intruders who try to change or even damage data owned by a network. The Intrusion Detection and Prevention System (IDPS) is a solution that can be used to assist administrators in monitoring and analyzing as well as blocking malicious packets on a network. In its implementation, there are several types of tools that can be used to support the performance of the Intrusion Detection and Prevention System (IDPS). In this study, we will analyze the performance of the IDPS method using Snort in detecting and blocking UDP flooding and SYN flooding attacks. To test the performance of the IDPS system with snort, an attack test was carried out and used Quality of Service (QoS) test parameters, namely throughput, delay, Jitter, and packet loss. Based on the results of the study, Snort succeeded in increasing the throughput value when UDP flooding and SYN flooding attacks entered the server, so that connectivity in the network providing services was getting better. Furthermore, snort is able to reduce the delay value so that the time spent sending data is faster than before snort was active. In terms of Jitter, it causes the value of the range between delays to decrease, so that the quality of data transmission when the client accesses the web server increases from before.

Keywords: network security, Intrusion Detection and Prevention System, Quality of Service (QoS), UDP flooding, SYN flooding.