ABSTRACT

Network security is needed by the server to maintain the performance provided for users, an attack can occur anytime and anywhere. Denial of Service (DoS) attacks, these attacks disrupt the services provided by servers, hamper performance, network disruptions, reduce server performance, and damage the company's reputation. This research will implement the IDPS method using the Snort tool in detecting DoS attacks aimed at servers. This study measures the performance of IDPS Snort based on the Quality of Service (QoS) parameters provided by the server to users. The Throughput value decreases, Packet Loss increases, Delay increases, and Jitter increases when a DoS attack is executed. When Snort is active the Throughput value increases, Packet Loss decreases, Delay decreases, and Jitter decreases when a DoS attack is executed. Having Snort as IDPS can improve the quality of QoS provided by the server when an attack occurs compared to when it has not implemented *Snort*. *Snort* in this study succeeded in acting as an *Intrusion Detection Prevention System* (IDPS) so that it can detect and prevent attacks that enter the *server*.

Keywords: *Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Snort, Quality of Service (QoS)*