ABSTRACT

Internet networks and servers have a central role in facilitating access to information, sharing data, and increasing performance efficiency in companies and individuals. Through computer networks such as LANs and WANs, there is connectivity and interaction between devices locally and globally via the internet, where servers function as the main core in providing services and managing data. However, the existence of a wider connection makes the server vulnerable to various security threats, especially from DDoS attacks. As a result, there is an interruption on the server which causes a decrease in network performance. This problem occurs because there is no implementation of a security system on the server. Therefore, the solution in this research is to apply an IDS mechanism with a Firewall to detect and prevent DDoS attacks, especially with the SYN TCP Flood and UDP Flood types. In addition, this study also conducted two evaluations of Snort performance, namely evaluation of Snort performance on parameters of detection accuracy and detection effectiveness through Snort log classification. Then evaluate the performance of Snort against the detection speed and CPU Usage parameters through the standard deviation. Both performance evaluations are carried out based on DDoS and Normal traffic scenarios. The results obtained in the log classification using the decision tree model, Snort has a good performance in terms of accuracy of 98.6%, and effectiveness of precision 99.4%, recall 98.7%, specificity 98.4%, and f1-score 99 %. The results obtained for the detection speed have a standard deviation of ±0.40 seconds and ±0.51 seconds in the DDoS scenario, while in the Normal scenario it is 0 seconds. The results obtained for CPU Usage Snort have standard deviation values of ±2.5% and ±12.3% in the DDoS scenario, while in the Normal scenario they are ±1.2% and ±1.0%.

Keywords: *Snort, Firewall, DDoS, Normal, Email.*

.