ABSTRAK

Jaringan *internet* dan *server* memiliki peran sentral dalam mempermudah akses informasi, berbagi data, dan meningkatkan efisiensi kinerja di perusahaan maupun individu. Melalui jaringan komputer seperti LAN dan WAN, terjadi konektivitas dan interaksi antara perangkat secara lokal maupun global via *internet*, di mana *server* berfungsi sebagai inti utama dalam menyediakan layanan dan mengelola data. Namun, dengan adanya koneksi yang lebih luas menjadikan *server* rentan terhadap berbagai ancaman keamanan, terutama dari serangan DDoS. Akibatnya, terjadi gangguan pada *server* yang menyebabkan penurunan kinerja jaringan. Permasalahan tersebut terjadi karena belum ada penerapan sistem keamanan pada *server*. Oleh sebab itu, solusi pada penelitian ini adalah menerapkan mekanisme IDS bersama *Firewall* untuk mendeteksi dan mencegah serangan DDoS terutama dengan jenis SYN TCP *Flood* dan UDP *Flood*. Selain itu, penelitian ini juga melakukan dua evalusi kinerja Snort yaitu evaluasi kinerja Snort terhadap parameter akurasi deteksi dan efektivitas deteksi melalui klasifikasi *log* Snort. Kemudian evaluasi kinerja Snort terhadap parameter kecepatan deteksi dan CPU *Usage* melalui standar deviasi. Kedua evaluasi kinerja dilakukan berdasarkan skenario lalu lintas DDoS dan Normal. Hasil yang diperoleh pada klasifikasi *log* dengan model *decision tree*, Snort memiliki kinerja yang baik dalam tingkat *accuracy* sebesar 98,6%, dan efektivitas *precision* 99,4%, *recall* 98,7%, *specificity* 98,4%, serta *f1-score* 99%. Hasil yang diperoleh pada kecepatan deteksi memiliki standar deviasi ±0,40 detik dan ±0,51 detik pada skenario DDoS, sedangkan pada skenario Normal 0 detik. Hasil yang diperoleh pada CPU *Usage* Snort memiliki nilai standar deviasi ±2,5% dan ±12,3% pada skenario DDoS, sedangkan pada skenario Normal ±1,2% dan ±1,0%.

Kata Kunci: Snort, Firewall, DDoS, Normal, Email.