ABSTRAK

SDN merupakan suatu teknologi yang memisahkan antara *control plane* dan *data plane*. *Control plane* berfungsi untuk mengkonfigurasi perangkat jaringan menggunakan *controller* SDN sedangkan *data plane* berfungsi meneruskan paket informasi.. *Controller* merupakan kendali utama untuk jaringan dan bersifat tersentralisasi , jika bagian ini berhasil diserang maka seluruh jaringan dapat diambil alih. Jika sumber daya SDN diserang dengan teknik *Denial Of Service* SYN *Flood*ing akan menghabiskan sumber daya jaringan sehingga menyebabkan *controller* SDN tidak dapat melayani permintaan pengguna jaringan SDN. Salah satu upaya mengatasi hal itu sistem keamanan IPS digunakan karena dapat mencegah serangan DoS dengan menggunakan aplikasi snort untuk memblokir serangan secara *real time*. Pengujian yang dilakukan menguji kinerja parameter QoS dengan serangan DoS SYN *Flood* menggunakan aplikasi hping3 berupa *Throughput*, *Latency*, CPU *Load* dan penggunaan memori sebelum dan sesudah implementasi sistem keamanan IPS dengan skenario pengujian sebelum serangan, saat serangan dan saat blokir. Didapatkan hasil pada penelitian ini pada hasil QoS *throughput* sebelum serangan memiliki rata-rata 22,536 Gb/s, saat serangan 14,163 Gb/s,saat blokir 14,926 Gb/s. Pada hasil QoS *Latency* sebelum serangan 0,10643& ms, rata-rata saat serangan 0,11893 ms, saat blokir memiliki rata-rata 0,0461 ms. Pada hasil QoS CPU *Load* sebelum serangan 26,92%, saat serangan 100,416%,saat blokir 99,093%. Pada hasil QoS memori sebelum serangan 4,08%, saat serangan 0,1%, saat blokir 18%. Dan Kesimpulan bahwa Implementasi penggunaan IPS terbukti efektif dapat mendeteksi dan memblokir serangan *Denial Of Service* sehingga meningkatkan kualitas sistem keamanan pada jaringan SDN.

Kata Kunci : *SDN, Denial Of Service , Throughput, Latency,* IPS.