ABSTRAK

Serangan *Distributed Denial of Service* (DDoS) seperti *ICMP Flood* dan *SYN Flood* merupakan tantangan dalam menjaga ketersediaan dan kestabilan jaringan. *Software-Defined Network* (SDN) melakukan kontrol jaringan terpusat dan fleksibel, namun belum dilengkapi mekanisme keamanan untuk mendeteksi dan memblokir serangan secara otomatis. Untuk mengatasinya, diperlukan integrasi dengan sistem yang memantau trafik dan melakukan mitigasi ketika ancaman terdeteksi. Penelitian ini merancang sistem keamanan jaringan dengan mengintegrasikan SDN menggunakan *OpenDayLight* sebagai *controller*, *Suricata* sebagai sistem deteksi dan mitigasi, serta *OpenvSwitch* untuk pengelolaan trafik. Sistem diuji dan dievaluasi menggunakan parameter QoS meliputi *throughput, packet loss, delay* dan *jitter*. Hasil menunjukkan sistem berhasil mendeteksi dan memitigasi serangan DDoS otomatis. Pada serangan *ICMP Flood*, *throughput* turun dari 234.254 bit/s menjadi 117.743 bit/s, *delay* meningkat dari 1.746 ms menjadi 4.904 ms, *jitter* dari 1.158 ms menjadi 3.298 ms, dan *packet loss* tetap 0%. Pada serangan *SYN Flood*, *throughput* turun dari 410.315 bit/s menjadi 165.172 bit/s, *delay* dari 1.159 ms menjadi 3.298 ms, *jitter* dari 1.158 ms menjadi 3.298 ms, dan *packet loss* dari 0,00262% menjadi 0%. Sistem terbukti menjaga kestabilan jaringan dan mempertahankan QoS selama serangan berlangsung.

Kata Kunci : SDN, *IDPS, DDoS*, *Quality of Service, Keamanan Jaringan*