ABSTRAK

Serangan *Distributed Denial of Service* (*DDoS*) *SYN Flood* merupakan ancaman serius terhadap jaringan berbasis *Software Defined Networking* (*SDN*). Penelitian ini menganalisis dampak serangan menggunakan *hping3* terhadap performa jaringan dengan pendekatan *Supply Chain Management Network* (*SCMN*). *Topologi* eksperimen melibatkan *SDN controller*, *Open vSwitch*, *web server*, *router PFSense*, serta dua jaringan tambahan sebagai *client* dan *attacker*. Sistem keamanan dirancang dengan mengintegrasikan *IDPS* berbasis *Snort v2*, serta pemfilteran trafik menggunakan *iptables* dan *ipset*. Evaluasi performa dilakukan berdasarkan parameter *Quality of Service* (*QoS*), yaitu *throughput*, *packet loss*, *delay*, dan *jitter*. Hasil menunjukkan bahwa *IDPS* menurunkan *throughput* saat serangan dari 1095,10 bit/s menjadi 455,45 bit/s, serta pada kondisi minimal dari 3,33 bit/s menjadi 1,34 bit/s. *Packet loss* tercatat 0% pada tiga skenario, kecuali pada *Non IDPS Flooding* sebesar 0,00075295%. *Delay* tertinggi terjadi pada *IDPS* Minimal yaitu 381,72 ms dan terendah pada *Non IDPS* Minimal 145,35 ms. *Jitter* tertinggi terdapat pada *IDPS Flooding* 1084,73 ms, diikuti *IDPS* Minimal 379,21 ms. Temuan ini menunjukkan efektivitas *IDPS* dalam mitigasi serangan, meski berdampak pada *delay* dan *jitter*. Sistem terbukti menjaga kestabilan jaringan dan mempertahankan *QoS* selama serangan berlangsung.

Kata Kunci: *DDoS, SYN Flood, SDN, Snort v2, IDPS, Iptables,Iipset, Quality of Service,* Keamanan Jaringan.