ABSTRAK

Software Defined Network (SDN) adalah arsitektur jaringan yang memisahkan antara *control plane* dan *data plane*. Dalam SDN, *control plane* berada pada pada sebuah entitas yang biasa disebut *controller* sedangkan *data plane* berada di masing-masing perangkat *networking* pada arsitektur tersebut. *Controller* pada SDN berfungsi sebagai otak di dalam arsitektur SDN yang memungkinkan untuk mendisain, mengimplementasikan atau pun mengelola sebuah jaringan dilakukan secara sentral sehingga membuat SDN memiliki fleksibilitas dan kemampuan mengontrol jaringan yang lebih tinggi dibandingkan arsitektur jaringan konvensional. Dibalik keuntungan-keuntungan yang sudah disebutkan, kerentanan terhadap serangan masih menjadi perhatian khusus untuk mengadaptasi teknologi ini. Untuk itu, pada Tugas Akhir ini akan dilakukan penerapan *Intrusion Prevention System* (IPS) berbasis *Snort* pada arsitektur SDN yang menggunakan *Ryu Controller*.

Penerapan IPS pada Tugas Akhir ini dilakukan dengan cara mengintegrasikan *alert* dari perangkat lunak bernama *Snort* dengan modul *rest_firewall* yang terdapat pada *Ryu Controller*. Setelah dilakukan penerapan IPS akan dilakukan simulasi serangan untuk mengetahui kemampuan sistem dalam melakukan mitigasi terhadap serangan.

Dari simulasi yang telah dilakukan, pada arsitektur SDN yang sudah diterapkan IPS di dalamnya dapat mendeteksi paket serangan yang dikirim secara *flood* (ICMP *Flood*) ataupun serangan yang dilakukan ukuran paket yang dikirim (*Ping of Death*) ataupun serangan yang mengkombinasikan kedua serangan tersebut. Ditambah *script bash* yang terdiri dari block.sh dan ublock.sh terbukti dapat melakukan blokir atau mitigasi terhadap serangan.

Kata Kunci: *Software Defined Network* (SDN), *Ryu Controller*, *Intrusion Prevention System* (IPS), ICMP *Flood*, *Ping of Death*