Abstrak

SDN atau *Software Defined* Network adalah arsitektur jaringan dimana adanya pemisahan antara *control plane* dan *forwading plane*. Jaringan SDN memiliki keunggulan dengan adanya pemisahan antara *control plane* dan *forwarding plane* membuat kontrol jaringan dapat dilakukan melalui pemrograman jaringan. Tetapi, disamping keunggulan yang ada, dengan tersentralisasinya jaringan tersebut, maka potensi ancaman keamanan akan meningkat. Sistem yang diusulkan yaitu dengan menerapkan IPS (*Intrusion Prevention System*) pada jaringan SDN. *Intrusion Prevention System* adalah sistem yang fokus untuk mengidentifikasi dan melakukan blokir jaringan yang dianggap jahat oleh sistem. Aplikasi IPS yang digunakan dalam penelitian ini adalah Snort. Agar Snort mampu melakukan blokir akses, maka Snort harus dijalankan dalam mode IPS. Untuk mengintegrasikan *Snort* ke dalam jaringan SDN terdapat beberapa tantangan yang dihadapi, seperti : Snort berjalan dalam mode *passive* (IDS) sehingga tidak melakukan blokir akses dan format *log file* dari Snort yang berbeda-beda. Pada tugas akhir sistem yang dibangun dengan mengkonfigurasi Snort mejadi mode IPS kedalam arsitektur jaringan SDN dan adanya modifikasi pada *log file* untuk penyeragaman format.

Kata Kunci: *Attacker*, IPS, *log file*, SDN, Snort, Ryu.