ABSTRAK

Intrusion Prevention System (IPS) merupakan sebuah *tools* yang digunakan untuk mendeteksi dan mencegah masuknya paket berbahaya ke dalam sistem yang dikirimkan dari sebuah *host*. Pada jaringan SDN, IPS dapat dihubungkan dengan *switch* yang akan menjadi *firewall*. Adapun IDS yang dapat digunakan pada arsitektur SDN ini salah satunya adalah Snort. Namun, IDS Snort ini sendiri memiliki sebuah kelemahan, yang dimana durasi blokir yang ditentukan akan selalu sama. Oleh karena itu, dibutuhkan suatu sistem yang dapat membantu IDS Snort agar menjadi adaptif. Sistem ini bertujuan agar waktu blokir yang diberikan berbanding lurus dengan frekuensi serangan yang datang.

Pada penelitian ini, penulis merancang suatu sistem yang dapat merubah IDS Snort menjadi *adaptive* IPS. Adapun logika yang digunakan untuk membangun sistem ini adalah logika fuzzy, yaitu logika yang menggunakan sistem keanggotaan. Sistem keanggotaan ini yang akan menentukan, apakah frekuensi paket yang datang tersebut dikategorikan sebagai serangan yang sering atau tidak, yang kemudian hasil penentuan tersebut yang akan menentukan apakah waktu blokir untuk *host* sumber akan terus bertambah atau tidak, apabila dalam masa blokir ternyata *host* sumber masih melakukan serangan, maka waktu blokir untuk *host* terebut akan terus bertambah. Sistem fuzzy yang dibuat diuji dengan beberapa serangan, yaitu serangan *Host Discovery* dan serangan *Distributed Denial of Service*(DDoS).

Hasil yang diperoleh dari penelitian Tugas Akhir ini adalah, sistem fuzzy yang telah dirancang dapat menjadikan IDS Snort menjadi *adaptive* IPS, yang dimana IPS ini dapat beradaptasi dengan frekuensi serangan yang datang, serta waktu blokir yang diberikan berbanding lurus dengan frekuensi serangan. Selain itu juga, serangan *Host Discovery* dan serangan DDoS yang digunakan untuk pengujian ini dapat diblokir oleh sistem yang telah dirancang.

Kata Kunci: IPS, IDS, logika fuzzy, SDN, Snort, *Host Discovery*, DDoS.