ABSTRAK

Software Defined Network (SDN) sebuah paradigma baru dalam sebuah jaringan. Berbeda dengan jaringan konvensional yang fungsi *forwarding* dan kontrol berada pada satu perangkat. Jaringan SDN mempunyai fungsi *forwarding* dan kontrol dipisah sehingga berada di perangkat yang berbeda. Keamanan jaringan SDN, ada beberapa faktor yang mempengaruhi keamanan pengguna, terdapat beberapa ancaman yang dapat menyerang bagian *control plane* dan *data plane*. untuk mengatasi ancaman tersebut digunakan metode *Intrusion Detection System* (IDS), *Intrusion Preventation System* (IPS) dan *Deep Packet Inspection* (DPI). Namun IDS dan IPS masih ditemukan kekurangan dari segi performansi jaringan. Masalah tersebut dapat diselesaikan dengan menggunakan metode *Deep Packet Inspection* (DPI). DPI memungkinkan administrator jaringan dalam memonitoring dan menganalisis traffic jaringan secara *real time*. Penelitian ini dilakukan implementasi metode DPI pada jaringan yang diuji dengan teknik serangan DOS SYN *flood* secara *direct attack*. Solusi untuk mengatasi serangan maka DPI memerlukan *controller* untuk memblokir serangan dan *tools* ntopng DPI yang mendeteksi serangan pada jaringan SDN. Ntopng juga mengatasi masalah *false positive* dengan membagi tingkatan serangan yang terdeteksi di SDN. Penelitian ini didapatkan hasil *Throughput* sebelum serangan 5,962 Mbits/sec menjadi 0 Mbits/sec dan *latency* sebelum serangan 0,0754 second dan pada saat serangan meningkat menjadi 0,875 second. penurunan *Throughput* dan meningkatnya *latency* ini disebabkan karena adanya serangan DoS yang mengakibatkan komunikasi antar host tidak dapat berjalan.

Kata Kunci : SDN, *Deep Packet Inspection, Denial of service, Latency, Throughput*