Abstrak

Software Defined Network (SDN) merupakan suatu konsep yang memungkinkan administrator untuk mengatur perangkat jaringan melalui suatu software *controller* sehingga dapat mempermudah proses konfigurasi melalui *control plane*. Akan tetapi, faktor keamanan perlu diperhatikan dalam membangun suatu jaringan. Pada dasarnya belum ada mekanisme pengecekan paket data berbahaya pada jaringan SDN. Mengamankan jaringan dapat dilakukan dengan melakukan inspeksi setiap paket data yang melalui jaringan menggunakan Intrusion Detection System (IDS). Namun, perlu dicari mengenai seberapa efektif IDS dalam mendeteksi serangan *cyber* serta dampak yang ditimbulkan dari segi performansi jaringan SDN.

Pada tugas akhir ini, telah dilakukan integrasi IDS pada jaringan SDN serta pengukuran pengaruh yang ditimbulkan dari segi performansi. Parameter performansi yang diujikan adalah *delay, throughput, jitter*, dan *packet loss ratio.* Selain itu, jaringan diuji untuk mendeteksi beberapa jenis serangan *cyber* tertentu.

Dari hasil pengujian yang telah dilakukan, jaringan SDN yang telah diintegrasikan dengan IDS memiliki kemampuan untuk mendeteksi serangan *cyber* sesuai dengan *rule* yang diterapkan sehingga tingkat keamanannya lebih tinggi. Akan tetapi, jaringan SDN setelah diintegrasikan dengan IDS secara umum mengalami penurunan pada segi performansi dibandingkan sebelum diintegrasikan dengan IDS. Hal ini dikarenakan setiap paket data yang lewat harus melewati proses pengecekan sesuai *rule* yang ada.

Kata kunci: *Software Defined Network, Intrusion Detection System*, performansi, serangan *cyber, rule*.