

ABSTRAK

Virtual data center merupakan salah satu teknologi yang bertujuan untuk mengurangi jumlah fisik *data center* dengan cara membuat mesin *virtual* dalam 1 *server* fisik. Untuk membuat mesin *virtual* dalam 1 *server* fisik diperlukan sebuah *hypervisor*. Dengan terciptanya *virtual data center* maka teknologi *cloud computing* akan dapat diimplementasikan. Salah satu *platform cloud computing* yang dapat mengelola *resource* dari *data center* adalah *openstack*. Ancaman dari teknologi *cloud computing* adalah dengan adanya *ip public* yang sangat rentan dengan serangan *dos(denial of service)* diantaranya adalah *syn flood attack*. Telah terdapat sistem keamanan untuk mendeteksi *syn flood attack* namun sistem keamanan yang ada masih dipasang pada sisi server dan hanya dipasang pada satu poin. Hal tersebut tentu akan menghabiskan *resource* dari sebuah server dan perangkat jaringan. Untuk mencegah hal tersebut akan dibangun sebuah mesin *virtual* di dalam jaringan *virtual data center* yang akan berfungsi sebagai *router* dan *firewall* dengan memanfaatkan teknologi *openvswitch* yang mendukung teknologi *SDN(Software Defined Network)* dengan menggunakan protokol *openflow* dan *sflow*. Dengan memanfaatkan *sflow-RT* yang merupakan *sflow collector* sebagai pendeteksi serangan dan *opendaylight* yang merupakan *openflow controller* sebagai pemitigasi serangan maka serangan *syn flood attack* akan dapat dicegah sebelum memasuki mesin *virtual data center* dari *openstack*.

Kata kunci: *Virtual data center, Openstack, SDN(Software Defined Network), Sflow, Openflow, Openvswitch, Sflow-RT, Opendaylight*