ABSTRACT

Software Defined Network (SDN) *is a network architecture which make control plane and data plane being separated. In* SDN *control plane is located in an entity called controller and data plane is located in every network device like router or switch. In* SDN *controller act as a brain in the network, allow a network administrator to design, implement or configure network just from controller. Because of that,* SDN *has more flexibility and controllablity than a conventional network. Beside that pros, there is* SDN *has an issue especially in it's security. Because of that, this Final Project will implementing the Intrusion Prevention System* (IPS) *based on Snort*.

This Final Project work by integrating Snort's alert with Ryu's rest_firewall module to do blocking at packet detected as an attack. After that, will do an attack simlation to see the capability of IPS *to mitigation to the attack.*

From the simulation we can see that a network with SDN *architecture which already integrating the Snort's alert and Ryu's rest_firewall module could detect attack from* ICMP *flood attack and Ping of Death. And, the block.sh and unblock.sh script could block the malicious packet not going into the network.*

Keywords: *Software Defined Network* (SDN), *Ryu Controller*, *Intrusion Prevention System* (IPS), ICMP *Flood*, *Ping of Death*