ABSTRACT

The topic of the thesis is about comparison study of Floodlight Static Flow Pusher and Firewall on Software Defined Networking (SDN) which used as flow management tools for handle Distributed Denial of Services (DDoS) Attack. This attack typically sends a huge number of packets to the victim that drives the SDN Controller to stall state and make the entire connected network become inaccessible.

There are many detection methods for DDoS attack offered by researchers, but they commonly use same mitigation method, which is filter type mitigation using flow management tools that divided into two modules, Access Control List (ACL) module with proactive way and Firewall module which is pushing rules on the reactive way. The best detection method becomes dull when combined with poor mitigation method, so this thesis will try to study the difference of ACL and Firewall in terms of performance for handle DDoS attack and ensure the availability of SDN network that depends on the controller state.

The research scheme uses Floodlight as SDN Controller, Mininet for network model simulator, and all flow streams are monitored by custom sFlow-RT. The performance of ACL and Firewall determines by their DDoS attack block capability on various attack rate. This performance consists of three metrics, reaction time, downtime, and recovery time.

As the result, Firewall has better performance than ACL, even on maximum attack rate. ACL performance will be comparable with Firewall on lower packet rate (lower than 600pps) so, Firewall mitigation scheme is more suitable for handle burst packet from DDoS attack than ACL.

Keywords: Proactive, Reactive, ACL, Firewall, Floodlight, SDN, DDoS