Abstract

SDN or Software Defined Network is a network architecture where there is a separation between the control plane and the forwading plane. SDN has an advantage with the separation between control plane and forwarding plane to make network control can be done through network programming. But, despite the advantages SDN with the centralized network, the potential threat of security will increase as an attacker will only target the control plane. The author wants to implement IPS on the SDN. IPS is the system that focus for identifying and blocking networks access that are considered malicious by the system. IPS application that used in this study is Snort. In order for Snort to be able to block the network access, the Snort must be run in IPS mode. To integrate Snort into an SDN network there are some challenges, such as: Snort runs in passive mode (IDS), so IPS will not to block access and log file from Snort has different format. On this final project, the authors will build Snort become IPS mode into SDN network architecture and do some modification on log file for the same format.

Keywords : *Attacker*, IPS, *log file*, SDN, Snort, Ryu.