

ABSTRACT

IT Telkom Jakarta as an educational institute views that optimizing the use of the website is a priority, plus IT Telkom Jakarta has several business processes that rely on digital data, including academic data stored on one server. Seeing the importance of the website, it is necessary to increase security for this website. Moreover, the IT Telkom Jakarta website can be accessed by many users via a wired or wireless fidelity (Wifi)-based Local Area Network (LAN). Therefore, maintaining security on the web is needed to overcome users who carry out attacks and protect the web from various information threats. To maintain security against these security attacks, a system equipped with a firewall and an Instruction Detection System (IDS) is needed. The IDS used is OPNsense, where in this OPNsense there is Suricata. Suricata is one solution related to security problems. Suricata is an open source Intrusion Detection and Prevention System (IDPS) which is the next generation of IDS/IPS. The result of the implementation of OPNsense Suricata is that Suricata can prevent attacks by blocking attacks. Where when scanning and testing DDOS, the OPNsense system will record attacks, send attack notifications and block attacks.

Keywords: OPNsense, DDOS, Suricata, Website, IDS, Firewall.