ABSTRACT

Development of the internet that are getting increasing both in terms of technology and its users have a positive impact and negative (cybercrime). Based on these statements then required some form of security for server particulary. One solution is by using the Intrusion Detection and Prevention System (IDPS) and will be integrated with the DMZ (Demilitarized Zone) firewall.

IDPS is the process of monitoring the events in a computer system or network and analyzing the signs of an incident that may occur as a violation or threat on computer security policies. in this thesis author has been successfully design an implementation of a LAN network using a firewall DMZ, integrated with IDPS using Signatured-Based Detection method. The tools that used in this method are snort and blockit. Each attach has a different character with another type, it is expected that by applying a new rule in snort can anticipate the occurrence of violations of the Computer Security Poilcies.

From the research that has been done, the network topology that has been made has been able to block any kind of attack which adjusted to the scenario. The average time of detection of each type of attack is 0.4 seconds.

Key words : *Cybercrime, IDPS, DMZ, Computer Security Policies, Firewall, Signatured-Based Detection.*