ABSTRAK

Perkembangan internet yang semakin hari semakin meningkat baik dari sisi teknologi maupun penggunanya membawa dampak positif maupun negatif (*cybercrime*). Berdasarkan pernyataan tersebut maka dibutuhkanlah suatu bentuk pengamanan terhadap server khususnya. Salah satu caranya adalah dengan menggunakan *Intrusion Detection Prevention System* (IDPS) dan yang akan diintegrasikan dengan firewall DMZ (*Demilitarized Zone*).

IDPS adalah proses memantau peristiwa yang terjadi dalam sistem komputer atau jaringan dan menganalisis tanda-tanda insiden yang mungkin terjadi seperti pelanggaran ataupun ancaman pelanggaran pada *computer security policies.* Pada tugas akhir ini telah dilakukan implementasi terhadap perancangan desain jaringan LAN menggunakan *firewall* DMZ yang diintegrasikan dengan IDPS yang menggunakan metode *Signatured-Based Detection.* Pada metode ini, tools yang telah digunakan berupa snort dan blockit. Setiap serangan memiliki karakter yang berbeda dengan jenis serangan yang lain, maka diharapkan dengan menerapkan rul-rule baru dalam snort dapat mengantisipasi terjadinya pelanggaran terhadap *Computer Security Poilcies.*

Dari hasil penelitian yang telah dilakukan maka topologi jaringan yang telah dibuat telah mampu mem-block setiap jenis serangan yang disesuaikan dengan skenario. Rata-rata waktu pendeteksian tiap-tiap jenis serangan adalah 0.4 detik.

Kata Kunci : *Cybercrime, IDPS, DMZ, Computer Security Policies, Firewall, Signatured-Based Detection.*