# ABSTRAK

Keamanan jaringan adalah salah satu aspek penting dalam dunia internet. Suatu jaringan internal perusahaan membutuhkan keamanan khusus yang dapat menjaga data-data penting dari serangan *hacker*, salah satu caranya adalah memasang *firewall*. *Demilitarized Zone* (DMZ) merupakan salah satu teknik *firewall* yang mengamankan *server* internal dari serangan *hacker* yang berasal dari internet namun tetap mengizinkan akses menuju *server* pada jaringan DMZ. Secara umum DMZ dibangun dengan tiga konsep, yaitu NAT, PAT, dan *Access List*. NAT *(Network Address Translation)* digunakan untuk mentranslasi alamat asli ke alamat internal. PAT *(Port Addressable Translation)* berfungsi untuk manajamen *port*. *Access List* berfungsi sebagai pengatur atau pengontrol lalu lintas dalam jaringan.

Konsep dasar DMZ merupakan *three legs firewall* yang berarti *device* dengan tiga *interfaces* yang menghubungkankan jaringan internet, internal, dan jaringan khusus untuk *server*. *Server* pada DMZ dapat bekerja pada seluruh jaringan baik intranet maupun internet. Akses seperti *Web Server*, DNS, DHCP, *Proxy* dan lain sebagainya tetap dapat dijalankan. *Hacker* atau *cracker* hanya dapat melakukan serangan ke jaringan DMZ, dan tidak dapat mengakses *host* di jaringan internal. *Firewall* DMZ dapat diintegrasikan dengan *IPS* agar dapat melindungi sistem ketika terjadi serangan.

Sistem keamanan yang merupakan integrasi dari DMZ dan IPS diuji menggunakan beberapa parameter yaitu QoS *(Quality of Service)* dan CIA *(Confidentiality, Integrity, and Access List)*. Hasil pengujian QoS menunjukkan perubahan yang tidak significant, perubahan nilai *throughput* sebesar 0.5% dan *delay* sebesar 6.5%. Hasil pengujian CIA menunjukkan IPS mampu menangani serangan DoS, *exploit*, dan *port scanning*.



Kata Kunci : *Firewall,* DMZ, NAT, PAT, *Access List,* IPS