ABSTRAK

Informasi yang bernilai sangat penting membuat informasi yang disajikan hanya boleh diakses pihak tertentu saja. Tidak menutup kemungkinan suatu jaringan disusupi oleh pihak tidak berwenang seperti *attacker*. Celah keamanan yang tersedia dimanfaatkan untuk mengambil atau mengubah informasi yang dikirimkan. Jatuhnya informasi ke *attacker* menimbulkan banyak kerugian. Banyaknya celah pada akses menghasilkan banyaknya kemungkinan serangan yang dapat dilakukan oleh penyerang. Serangan *Denial of Service* (DOS) merupakan serangan yang berfungsi untuk mengganggu target dengan melumpuhkan akses *server*. Serangan DOS yang masif disebut *Distributed* DOS. Perlu solusi yang dapat mengatur penyaringan paket data yang dilewatkan. *Proxy Server* memiliki fungsi pemilahan data *traffic* untuk meningkatkan keamanan jaringan. Penanganan serangan DDOS tidak cukup jika hanya menggunakan *proxy server* karena diperlukan proses penyaringan lebih detail terutama pada identitas paket dengan menggunakan *firewall*. Penelitian ini menguji bagaimana akses halaman *web* pada jaringan yang menghubungkan *web server*, *proxy server*, *router* dan *switch* secara *inline* pada protokol TCP terpengaruh oleh serangan DDOS yang diluncurkan dari aplikasi LOIC dengan perangkat *zombie* sebanyak 400000 saat sebelum dan sesudah implementasi sistem keamanan ini diterapkan. Parameter yang diamati adalah parameter *delay*, *packet loss*, dan *throughput* yang berdampak pada segi *availability* dari sistem keamanan yang diterapkan. Hasil parameter QOS yang didapatkan meningkat dari sebelum dan sesudah sistem keamanan diterapkan saat serangan sedang berlangsung. Nilai *delay* 2,86 s menjadi 0,0013 s, packet loss mencapai 99,79% menurun menjadi 20.24%, dan throughput mencapai 337 bps meningkat menjadi 6,33 Mbps. Serangan DDOS yang berlansgsung dapat diblokir dengan membatasi paket SYN yang dikirim dari alamat attacker.

Kata Kunci: *DDOS, Proxy Server, Firewall*