ABSTRACT

Valuable information is very important to make information may only accessible by certain parties. Doesn't rule out network ifiltrated by unauthorized parties such as attacker. Available security loopholes used to retrieve or change sent information. Fall of information to attacker caused many losses. Gaps in access results bring possibilities of attacks that can be launched to disrupt targets by disabling server access. Denial of Service (DOS) attack is attack that serve to disrupt target by disabling access of sending and receiving data. Massive DOS attack called a Distributed DOS. Therefore, solution needed to manage data access such as filtering passed data packets. Proxy Server has functions of sort data traffic to improve network security. Handling DDOS attacks is not enough if only using proxy server because it requires more detailed filtering process, especially on identity of passed data packets by using firewall. This research examines how web pages access that connect web server, proxy server, router, and switch inline on TCP affected by DDOS attacks launched by LOIC applications with 400000 zombie devices before and after implementation of delay, packet loss, and throughput which have impact on applied availability of security system. QOS parameter results obtained increase from before and after security sistem applied when attack is ongoing. Delay time decreased from 2.86 s to 0.0013 s, packet loss from 99.79% decreased to 20.24%, and reached throughput from 337 bps increased to 6.33 Mbps. Launched DDOS Attack also can be blocked by blocking SYN packets sent from attacker's address.

***Keywords**: DDOS, Proxy Server, Firewall*