ABSTRACT

As the Internet growth, service providers have to think about the increase of internet users. A server has limited capabilities to handle multiple users at once. One technique to overcome this problem is by adding more servers. By adding more servers, current services are still running while the configuration process is still on their way. So, the services would not be shut down.

However, adding more servers might cause a problem if they are not well handled. This process must be done in a short time and transparent to users. To handle this problem, we can use Linux Virtual Server (LVS).

LVS as a clustered server form could be attacked by Distributed Denial of Services (DDoS), an attack that causes the servers deny their legitimate user requests. To minimize the effect of this attack, we put honeypot among the existing backend servers.

Honeypot is a "fake" server that act like a real server. So, attacker will think that their attack is successful. But in fact it is not, in addition, the attacker’s location can be located to prevent another attack. Based on the test results, the proposed system could mitigate DDoS attack effect on LVS. Besides, the proposed system performs better than using iptables if client request rate is low.

Keywords: LVS, Honeypot, DDoS, Packet Redirection