## *ABSTRACT*

*Actions against the law that are carried out on an internet-based basis are called Cybercrime. Cybercrime can be prevented and overcome based on network security aspects. Another threat to computer networks is Distributed Denial of Service (DDoS). One way to protect the system from DDoS attacks is to protect it using a firewall. A firewall is a system or device that can allow entry and exit of data or information on network traffic. One of the functions of a firewall is to protect IT services. In this study using a virtualized Fortigate firewall version 7.2.0 with the implementation of the firewall function in load testing on the firewall specifications of 1.5 GB memory and 2 GB memory. This study tries to get the firewall character based on computing resources and uses two test scenarios, namely the HTTP allow service and the HTTP block service. The test carried out is a DDoS SYN flood from Kali Linux which leads to a web server on the Ubuntu server. The experimental platform was carried out with Fortigate's virtualized firewall on a laboratory scale. The experiments carried out were before the attack, during the attack, after the attack. The results obtained are the consumption of CPU computing resources 97.1%, memory 83.7%, and session 148883. For further research, it can be in the form of profiles that describe the relationship between attacks, firewalls, and servers.*



*Keywords –* ***Virtualized Fortigate, profiling, testing, computing resources***