ABSTRACT

On the security aspect, it is necessary to know how effectively a firewall can protect network devices from DDoS attacks. The characteristics of a firewall have different functions in protecting the system from various external attacks that can attack and retrieve data. In this research, the implementation of Paloalto firewall virtualization aims to obtain the system profile function on the firewall based on the use of computing resources. Profiling of the firewall system of this experiment based on the consumption of computing resources in load testing. This experiment used a DDoS SYN flood attack on Kali Linux as an attacker and a virtualization Paloalto firewall that protects a web server on Ubuntu Server as an attack target. This research distinguished based on two test scenarios, namely based on testing the service HTTP allow and service HTTP block with Paloalto memory specifications at RAM 5.5 GB and RAM 8 GB specifications. Measurements were made based on computing resources on CPU, memory, and a session focused on before, during, and after DDoS SYN flood attacks. The pattern of usage of computing resources tends to be linear when a DDoS SYN flood attack occurs. The experimental results obtained on the highest use of computing resources during the attack were CPU usage with an average percentage of 95.8% and the second increase was in memory usage with an average percentage of 44%, and the session usage was 138682. For further research, it can use variations of DDoS attacks to get a wider profile.

Keywords*: Computing Resources, Paloalto, Profiling, Virtualization, Testing*