ABSTRACT

Konsultan Teknis Fortinet Indonesia released a data that shows that DDoS attacks in Indonesia is one of the top four worldwide with the percentage of 8,6%. The danger of this attack has shown on some particular examples that occurred throughout the world, like one particular case that happened to the biggest telecommunications company in South Korea, KT Telecom, that lost Rp7,900,000,000,- because of attacks from a group of hackers, as well as the leak of 50,000 accounts that are stolen from an IT database of WallStreet in the United States of America. Fortunately, the risk of having these cases occur on your network can be reduced by strengthen your network with Intrusion Prevention System (IPS), that will act as a main security system to monitor network traffic, detecting peculiar activities, and implementing early prevention actions on events that would cause a general failure on your network.

One of the methods that can be implemented to reduce the damage on your network's security system that is strengthened by IPS is by adding Captive Portal as a user-authentication device. Captive Portal is a network security technique that will protect your network by intercepting the traffic between clients and the web server, and forcing the clients to follow authentication procedures. The research on this Thesis will use two redundant servers that are implemented using load balancing method, with both servers are equipped with IPS as the main security system, and Captive Portal on the load balancer as user-authentication device.

The network that is strengthen by the combination of IPS and Captive Portal will be tested on its network continuity by attacking both servers with some attacking techniques, like port scanning, DoS, and DDoS. These attacks will send requests in a large number in a short period of time to put both servers into saturations, and make the most of both servers' resources. This implementation of both IPS and Captive Portal on redundant servers will hopefully increase the network's continuity up until 80%.

Key words: ***Intrusion Prevention System***, ***Captive Portal***, ***load balancing***, ***DDoS***