ABSTRACT

As this technology advances, user data security becomes a major concern. In times of cyber security attacks, especially DDoS attacks, this has increased significantly. This type of attack has the potential to make data inaccessible for a certain period of time. One approach to overcome this problem is to apply the concept of microsegmentation in networks. Microsegmentation enables host isolation by dividing the network into logical segments, such as zones, and organizing access based on specific configurations. This research aims to compare networks that use microsegmentation, with a focus on firewall policy regulations, and networks without firewalls. In configuration scenarios with microsegmentation, FortiGate devices are used to implement this concept. Then, metrics from various aspects will be compared between networks that use the FortiGate firewall and networks that do not have a firewall. These two topologies will be implemented in a network simulation using GNS3. The measurements that will be carried out will be in the form of Quality of Service and resource utilization. Testing was carried out in two different scenarios: normal conditions and DDoS attacks from external zones, using the ICMP flood and SYN flood methods. Test results show that the use of microsegmentation provides greater flexibility in organizing access through predetermined zones, as well as increasing the level of security. This can be seen from the difference in cloud CPU usage when an attack occurs from an external zone. On systems without a firewall, CPU usage can reach 100%. In addition, network performance with microsegmentation also shows better results in testing

Keywords—***Microsegmentation, FortiGate, Firewall, DDoS, Quality of Service***