ABSTRACT

The role of information technology in everyday life is increasing, especially since the advent of internet. It has made transferring and processing data faster and more reliable. However, this has caused concerns with how secure user data really is. Lately, the number cybersecurity attacks has been rising, particularly with DDoS attacks. These attacks can make data inaccessible for some time. One way to mitigate this is by implementing microsegmentation to networks. Microsegmentation achieves to isolate network hosts from each other using logical segments such as zones and applies rules based on the configuration. This study will research on comparing a microsegmented network with a non-microsegmented one. In our microsegmented configuration, we will use a FortiGate Next-Generation Firewall to implement microsegmentation, then we will compare various metrics with the non-microsegmented network, that runs a traditional firewall, with both topologies being virtualized in GNS3 Network Simulator. These metrics include functionality, security statistics, Quality of Service, and resource utilization. The metrics will be tested in three different scenarios: normal traffic, DDoS attack from the outside, and DDoS from the inside. The results of the tests carried out show that microsegmentation provides more flexible functionality with the use of zones and rules in that zone, and security is also better, with a maximum server CPU utilization difference of 22% during insider attacks, where in systems without microsegmentation this figure reaches 100%. The performance of the microsegmented network is also better, with an increase of up to 415%.

Keywords−***Microsegmentation, Next-Generation Firewall, DDoS***