ABSTRAK

Seiring dengan kemajuan teknologi ini, keamanan data pengguna menjadi perhatian utama. Pada saat penyerangan keamanan siber, terutama serangan DDoS, hal tersebut telah meningkat secara signifikan. Jenis serangan ini memiliki potensi untuk membuat data tidak dapat diakses dalam jangka waktu tertentu. Salah satu pendekatan untuk mengatasi masalah ini adalah dengan menerapkan konsep mikrosegmentasi dalam jaringan. Mikrosegmentasi memungkinkan isolasi host dengan membagi jaringan menjadi segmen-segmen logis, seperti zona, dan mengatur akses berdasarkan konfigurasi tertentu. Penelitian ini bertujuan untuk membandingkan jaringan yang menggunakan mikrosegmentasi, dengan fokus pada peraturan kebijakan *firewall*, dan jaringan tanpa *firewall*. Dalam skenario konfigurasi dengan mikrosegmentasi, perangkat FortiGate digunakan untuk menerapkan konsep ini. Kemudian, metrik-metrik dari berbagai aspek akan dibandingkan antara jaringan yang menggunakan *firewall* FortiGate dan jaringan yang tidak memiliki *firewall*. Kedua topologi ini akan diimplementasikan dalam simulasi jaringan menggunakan GNS3. Pnegukuran yang akan dilakukan berupa Kualitas Layanan (*Quality of Service*), dan pemanfaatan sumber daya. Pengujian dilakukan dalam dua skenario berbeda: kondisi normal dan serangan DDoS dari zona eksternal, menggunakan metode ICMP *flood* dan SYN *flood*. Hasil pengujian menunjukkan bahwa penggunaan mikrosegmentasi memberikan fleksibilitas lebih besar dalam mengatur akses melalui zona-zona yang telah ditentukan, serta meningkatkan tingkat keamanan. Hal ini terlihat dari perbedaan penggunaan CPU cloud saat terjadi serangan dari zona eksternal. Pada sistem tanpa firewall, penggunaan CPU dapat mencapai 100%. Selain itu, kinerja jaringan dengan mikrosegmentasi juga menunjukkan hasil yang lebih baik dalam pengujian

Kata kunci— ***Microsegmentation***, ***FortiGate, Firewall, DDoS, Quality of Service***