# ABSTRAK

*Peran teknologi informasi dalam kehidupan sehari-hari semakin meningkat, terutama sejak munculnya internet. Ini telah membuat mengirim dan memproses data lebih cepat dan lebih dapat diandalkan. Namun, ini telah menimbulkan kekhawatiran tentang seberapa aman data pengguna sebenarnya. Akhir-akhir ini, jumlah serangan keamanan siber meningkat, terutama dengan serangan DDoS. Serangan ini dapat membuat data tidak dapat diakses untuk beberapa waktu. Salah satu cara untuk mengurangi ini adalah dengan menerapkan mikrosegmentasi ke jaringan. Mikrosegmentasi mencapai untuk mengisolasi host jaringan dari satu sama lain menggunakan segmen logis seperti zona dan menerapkan aturan berdasarkan konfigurasi. Penelitian ini akan meneliti perbandingan jaringan ter-mikrosegmentasi dengan non-mikrosegmentasi. Dalam konfigurasi ter-mikrosegmentasi, akan digunakan FortiGate Next-Generation Firewall untuk mengimplementasikan mikrosegmentasi, kemudian akan dibandingkan berbagai metrik dengan jaringan non-mikrosegmentasi, yang menjalankan firewall tradisional, dengan kedua topologi divirtualisasikan di GNS3 Network Simulator. Metrik ini mencakup fungsionalitas, statistik keamanan, Kualitas Layanan, dan pemanfaatan sumber daya. Metrik akan diuji dalam tiga skenario berbeda: keadaan normal, serangan DDoS dari luar, dan DDoS dari dalam. Metode yang akan digunakan untuk serangan tersebut adalah ICMP flood. Hasil dari pengujian yang dilakukan menunjukkan bahwa mikrosegmentasi memberikan fungsionalitas yang lebih fleksibel dengan penggunaan zone dan rule pada zone tersebut, dan keamanan juga lebih baik, dengan perbedaan server CPU utilization maksimum sebesar 22% saat serangan insider berlangsung, dimana dalam sistem tanpa mikrosegmentasi angka tersebut mencapai 100%. Performa jaringan mikrosegmentasi juga lebih baik, dengan peningkatan mencapai 415% lebih baik.*

*Kata Kunci*−***Microsegmentation, Next-Generation Firewall, DDoS***