ABSTRAK

Peranan tekno*log*i informasi dikehidupan sehari-hari semakin meningkat. Hal ini membawa dampak positif berupa pengolahan data dan automasi yang cepat dan efektif. Sedangkan dampak negatifnya adalah privasi dan keamanan data yang harus dapat dikontrol. Disinilah peranan penting *network security*. Terdapat bermacam-macam jenis serangan, pada penelitian ini DDoS adalah serangan yang disimulasikan ke dalam jaringan. Serangan ini berupa TCP SYN *Flood* yang berasal dari luar dan dalam jaringan. Maka dari itu, perlu adanya pembagian zona dan hak akses di dalam jaringan untuk mencegahnya. *Microsegmentation* adalah salah satu penerapan yang sesuai dan juga ditujukan untuk melakukan mitigasi dari serangan DDoS. Penelitian ini dilakukan dengan menerapkan metode *Zone Based Firewall* ke dalam Cisco *Router* yang dijalankan di GNS3 sebagai *Network* Simulator. Pengujian dilakukan dengan membandingkan topo*log*i non-segmentasi dan segmentasi dengan dua skenario berbeda. Hasil dari pengujian yang dilakukan menunjukkan bahwa penelitian ini berhasil membagi zona dan hak akses di dalam jaringan dan memitigasi serangan DDoS pada topo*log*i *Segmentation*. Namun, penerapan *Zone Based Firewall* juga mengakibatkan perubahan di Qualityof Service dikarenakan penggunaan resource dari *firewall* yang lebih besar.

Kata kunci— ***Microsegmentation, Zone Based Firewall, DDoS, Quality of Service.***