

ABSTRAK

Perbuatan melawan hukum yang dilakukan dengan berbasis internet disebut *Cybercrime*. *Cybercrime* dapat dicegah dan ditanggulangi dengan berdasarkan aspek keamanan jaringan. Ancaman terhadap jaringan komputer lainnya yaitu *Distributed Denial of Service (DDoS)*. Salah satu melindungi sistem dari serangan DDoS yaitu dengan memproteksi menggunakan *firewall*. *Firewall* adalah sebuah sistem atau perangkat yang bisa memberikan izin keluar masuknya data atau informasi pada lalu lintas jaringan. Salah satu fungsi *firewall* adalah melindungi layanan IT. Pada penelitian ini menggunakan *virtualized Fortigate firewall* versi 7.2.0 dengan implementasi fungsi *firewall* pada *load testing* pada spesifikasi *firewall* 1,5 GB *memory* dan 2 GB *memory*. Penelitian ini berusaha mendapatkan karakter *firewall* berdasarkan sumber daya komputasi dan menggunakan dua skenario pengujian yaitu *service HTTP allow* dan *service HTTP block*. Pengujian yang dilakukan adalah DDoS SYN flood dari Kali Linux yang mengarah ke *web server* di Ubuntu *server*. Platform percobaan dilakukan dengan *virtualized firewall* Fortigate pada skala laboratorium. Percobaan yang dilakukan adalah sebelum serangan, saat serangan, setelah serangan. Hasil yang diperoleh adalah konsumsi sumber daya komputasi CPU 97,1%, *memory* 83,7%, dan *session* 148883. Untuk kelanjutan penelitian dapat berupa profil yang menggambarkan relasi antara serangan, *firewall*, dan *server*.

Kata kunci – *virtualized, Fortigate, profiling, testing, sumber daya komputasi*