ABSTRAK

Pada aspek keamanan jaringan, perlu diketahui seberapa efektif *firewall* dapat melindungi perangkat jaringan dari serangan DDoS. Karakteristik pada suatu *firewall* memiliki fungsi yang berbeda-beda dalam melindungi sistem dari berbagai serangan luar yang dapat menyerang dan mengambil suatu data. Pada penelitian ini melakukan implementasi virtualisasi Paloalto *firewall* yang bertujuan untuk mendapatkan fungsi profil sistem pada *firewall* berdasarkan penggunana sumber daya komputasi. *Profiling* sistem *firewall* yang diteliti berdasarkan konsumsi sumber daya komputasi pada *load testing*. Pada eksperimen ini menggunakan serangan DDoS SYN *flood* pada Kali Linux sebagai *attacker*, virtualisasi Paloalto *firewall* yang melindungi *web server* pada Ubuntu Server sebagai target serangan. Pada penelitian ini dibedakan berdasarkan dua skenario pengujian yaitu berdasarkan pengujian *service* HTTP *allow* dengan pengujian *service* HTTP *block* dengan spesifikasi *memory* Paloalto pada RAM 5.5 GB dan spesifikasi RAM 8 GB. Dilakukan pengukuran berdasarkan sumber daya komputasi pada CPU, *memory* dan *session* yang berfokus pada sebelum, saat dan sesudah serangan DDoS SYN *flood*. Pola Penggunaan sumber daya komputasi cenderung linear saat terjadinya serangan DDoS SYN *flood*. Hasil eksperimen yang didapatkan pada penggunaan sumber daya komputasi tertinggi saat serangan adalah penggunaan CPU dengan rata-rata persentase sebesar 95.8%, selanjutnya peningkatan ke dua yaitu pada penggunaan memory dengan rata-rata persentase sebesar 44%, dan urutan terakhir pada session sebesar 138682. Untuk penelitian selanjutnya dapat menggunakan variasi serangan DDoS untuk mendapatkan profil yang lebih luas.

Kata Kunci: Paloalto, *Profiling*, Virtualisasi, *Testing*, Sumber Daya Komputasi.