ABSTRAK

Berdasarkan Perkembangan teknologi yang begitu pesat memiliki dampak yang positif dan negatif, salah satu dampak negatifnya adalah adanya kebocoran data yang disebut dengan kejahatan siber. Hal tersebut sangatlah berbahaya dan menimbulkan kerugian yang begitu besar. Selain itu juga, kejahatan siber yang paling sering ditemukan adalah seperti ancaman malware, phishing, DDoS, dan lainnya.

Pada penelitian ini melakukan implementasi Paloalto firewall dengan melakukan konfigurasi pada firewall dan juga tahap pengujian serangannya dengan menggunakan malware seperti Eicar, ransomware, Trojan, Dos, dan juga adanya web filtering. Hasil pengujian ini bertujuan untuk mencegah risiko kehilangan data, kerugian material, lumpuhnya layanan publik. Dan agar efisien dan efektif dalam melakukan scanning dari variasi serangan tanpa mempengaruhi performa jaringan. Implikasi hasil yang ditemukan diharapkan dapat menyelesaikan masalah yang dihadapi dengan sempurna.

NGFW melakukan pencegahan dengan memblokir akses malware yang masuk pada traffic jaringannya. Pada penelitian ini juga melakukan implementasi NGFW di mana dilakukan konfigurasi firewall yaitu dengan pembuatan rule policy pada firewall tersebut. Pada penelitian ini, dilakukan evaluasi terhadap performa jaringan setelah implementasi NGFW dan konfigurasi firewall. Hasilnya menunjukkan bahwa penggunaan NGFW dan rule policy pada firewall dapat meningkatkan keamanan jaringan dengan efisien dan efektif. Diharapkan hasil ini dapat mengatasi lumpuhnya layanan publik akibat serangan malware serta memperbaiki performa jaringan.

Kata Kunci: Kejahatan Siber; Next Generation Firewall; Malware; Paloalto; Testing