ABSTRACT

Based on the rapid development of technology, which has positive and negative impacts, one of the negative impacts is data leakage, called cybercrime. This is very dangerous and causes huge losses. In addition, the most commonly found cybercrimes are malware threats, phishing, DDoS, and others. In this study, the implementation of the Paloalto firewall is carried out by configuring the firewall, as is the attack testing stage using malware such as Eicar, ransomware, Trojans, Dos, and web filtering. The results of this test aim to prevent the risk of data loss, material loss, and the paralysis of public services. And to be efficient and effective in scanning for a variety of attacks without affecting network performance. The implications of the results found are expected to solve the problem at hand perfectly. NGFW performs prevention by blocking access to malware that enters its network traffic. This research also implements NGFW, where firewall configuration is carried out, namely by creating a rule policy on the firewall. In this study, an evaluation of network performance was carried out after the implementation of NGFW and firewall configuration. The results show that the use of NGFW and rule policies on firewalls can improve network security efficiently and effectively. It is hoped that these results can overcome the paralysis of public services due to malware attacks and improve network performance.

Keywords: Cybercrime; Next Generation Firewall; Malware; Paloalto; Testing