Abstract

Distributed Denial of Service (DDoS) is a type of attack that can exhaust server resources. This attack results in a decrease in server quality so that it cannot be accessed by authorized users. Servers that are commonly victimized by this attack belong to companies from various sectors. PT Datacomm Diangraha provides solutions to these problems. As PT Datacomm Diangraha will do to Company X, which is to implement an Intrusion Prevention System (IPS) device as Anti-DDoS on its customers according to the customer's needs. This paper will test IPS devices in preventing DDoS attacks such as TCP Flood, UDP Flood, and ICMP Flood. The test is conducted by connecting the attacker and victim to the IPS device in the local network. The analysis will be done by comparing the network traffic and throughput of the victim when the attack is carried out when protected by IPS, no protection, and when traffic is normal. Experiments were conducted by performing a one-minute attack. The results of the experiments show that the traffic when protected by an IPS is similar to that during normal traffic. In addition, tests were conducted to prevent XSS malware to prove that IPS can prevent other attacks besides DDoS. From the test results, it was found that IPS can prevent DDoS attacks with 100% accuracy. The throughput data obtained when a DDoS attack occurs without IPS protection is 260978.9 - 1080732.32 bps. Throughput data when a DDoS attack occurs with IPS protection of 42.55 - 49.95 bps, which shows similarity in value with throughput during normal traffic which is 43.43 bps.

Keywords: DDoS; IPS; Anti-DDoS; malware; XSS