## ABSTRACT

*With the internet, a company will find it easier to complete work and access imported data via the internet, there is a need for a network security system. Therefore, it is an experiment using a network security system based on a Virtual Private Network (VPN) on a proxy. The type of VPN used is OpenVPN, where the application works to create an encrypted point-to-point tunnel connection. OpenVPN uses private keys, certificates, or usernames and passwords to authenticate when establishing a connection. The VPN used by the researcher is a VPN with the SSTP (Source Socket Tunneling Protocol) method. This research was conducted to find out how to design a network security system using SSTP and to find out whether the system using the SSTP method is able to encrypt data properly. To prove the level of security, the author uses the Wireshark application and tries to carry out attacks using Attacking Denial of Services (DoS). From the results of the study, it can be seen that using HTTPS will minimize the theft of data from other parties because the certificate has its own identification such as an organization, and so on.*



*Keywords: Virtual Private Network (VPN), Source Socket Tunneling Protocol (SSTP), Wireshark, Attacking Denial of Services (DoS).*