ABSTRACT

Data security in order to maintain privacy of communications made by every user of public services has become a priority for the service providers. Unfortunately, security is still limited to the access server, not on the network that the user through towards the server. Therefore, VPN will be one of solutions to handle data security problem in the network.

Virtual Private Network (VPN) offers the concept of data security by establishing a private communication tunnels in a public network, such as the Internet. One of VPN network implementation is using the Secure Socket Layer protocol (SSL) to implement a layered security key to keep the communication private.

SSL encryption in VPN technology can keep the data packet during the delivery process. The test results show that SSL based VPN can maintain data security from the threat of sniffing and disclosure attack. In contrast to native IPv4 network and GRE based VPN that the data security performance are still vulnerable to security threats. In addition, by looking at the QoS performance in video streaming service, SSL based VPN has the worst performance when compared to native IPv4 and GRE based VPN.

Key words : VPN, SSL, security, sniffing, disclosure attack, QoS, GRE