ABSTRACT

VPN (Virtual Private Network) is a way to create a private and secure network by using public network such as the Internet. Public networks which are used today are vulnerable for security threats such as theft of data, and gives a great loss if the data stolen is an important data business transactions of an enterprise. Therefore, it required a network that is inaccessible to the public. First , data must be encapsulated and then encrypted so it can't be read when passing through public network because they have to pass through the decryption process.

There are three types of VPN, consist of trusted, secure, and hybrid VPN [18]. Secure VPN is a combination of tunneling and encryption technology. The use of encryption in VPN technology make a VPN can't be read by unauthorized users because they have to pass through the decryption process first.

Implementation of IPSec (Internet Protocol Security) and GRE (Generic Routing Encapsulation) based VPN is a type of VPN that is often used to build a private and secure network

The purposes are how to implement IPSec-based VPN and GRE-based VPN, to analyze the effect of sniffing, disclosure attack and SYN attack based on network vulnerabillities especially on data confidentiality ,authentication and availability. In addition, to analyze the effect of cryptographic technologies on QoS parameters (delay and throughput).

Keywords : Security, VPN, IPSec, GRE , *Sniffing, Disclosure attack, SYN attack Delay, Throughput*