ABSTRACT

Computer network have been become integral part of telecommunication today. Many companies use computer networks to be able to communicate and exchange data with the company's branches, partners and their employees who were there in the field. At the beginning company use a channel based on leased lines or frame relay circuit to connect the central office and the branch office. This is not efficient and flexible at this time because the cost which must be issued a quite expensive to rent a leased lines channel and the access can only done within that closed network, so it’s difficult for mobile user.

Virtual Private Network become appropriate solution to solve the problem. VPN allows to build a communication network through the public network, viewed seems to communicate in a private network. Security assured with the use of data encryption and authentication. This final project discuss the implementation of L2TP/IPSec VPN, which is defined in RFC 3193 standard, a VPN technology which is a combination of L2TP and IPSec, securing the L2TP packet over IPSec tunnel. Implementation is done by building a VPN server and Radius server that integrated to handle user authentication. Analysis is done to measure the time needed for the tunnel setup and performance when using file transfer protocol.

From the measurement results, obtained L2TP/IPSec tunnel setup delay pre shared key for an average of 2,123 seconds and 2,162 seconds for the certificate. On the use of a VPN will be added to the header of at least 104 bytes and a maximum of 356 bytes compared to the normal delivery of only 40 bytes. Adding headers and delay processing of authentication and encryption cause a decrease in performance in terms of delay, packet loss and throughput. The use of AES give a better performance than 3DES, whereas a good performance obtained HMAC-MD5 at low background traffic and HMAC-SHA-1 at high background traffic.

Keywords: VPN, L2TP, IPSec, L2TP/IPSec, Radius