ABSTRACT

NIL USAWATUL HASANAH, VPN SERVER IMPLEMENTATION USING L2TP PROTOCOL(LAYER 2 TUNNELING PROTOCOL) AND IPSEC AS NETWORK SECURITY AT THE CENTRAL STATISTICAL AGENCY OF WEST SUMATRA PROVINCE

One way to maintain and improve the quality of service and security on the network of a central statistical agency is to add a VPN feature. With the increasing number of internet users, but not accompanied by the presence of skilled human resources or network administrators, the threat of cybercrime has emerged. Administrators who always monitor traffic by accessing routers and access points to determine network conditions. There are times when the Administrator is on a public network and cannot access the router and access point devices because the public IP obtained is dynamic (random). To overcome this problem, this is done through the Network Development Life Cycle (NDLC) method by combining the L2TP and IPSec VPN protocol systems on Mikrotik. VPN is a private and secure network that uses a public network such as the internet. One of the basic security measures for VPN technology is Internet Protocol Security (IPSec). IPSec is a protocol used to secure datagram transmission on TCP/IP based networks. (L2TP) is a tunneling protocol that can be used and supports VPN. L2TP is also a normal tunnel from one router to another router or from a client to a host gateway through an ISP's Network Access Server (NAS). This research aims to design and implement a Virtual Private Network (VPN) network system by utilizing public networks. where this system provides advanced security improvements to the internet network using IPSec.

Keywords:VPN,Mikrotik,L2TP,IPS

ABSTRAK

NIL USWATUL HASANAH,IMPLEMENTASI VPN SERVER MENGGUNAKAN PROTOKOL L2TP(LAYER 2 TUNNELING PRTOCOL)DAN IPSEC KEAMANAN JARINGAN PADA BADAN PUSATS TATISTIK PROVI NSI SUMATRA BARAT

Salah satu cara untuk menjaga dan meningkatkan kualitas layanan dan keamanan pada jaringan suatu badan pusat *statistic*adalah dengan menambahkan fitur VPN. Dengan meningkatnya jumlah pengguna *internet*, namun tidak diimbangi dengan keberadaan sumber daya manusia atau *Administrato*r jaringan yang terampil, ancaman kejahatan dunia maya pun bermunculan. *Administrator* yang selalu memonitoring jalanya lalu lintas dengan mengakses router dan *access point* untuk mengetahui kondisi jaringan. ada kalanya ketika *Administrator* berada pada jaringan publik maka tidak dapat mengakses router dan perangkat *access point* dikarenakan IP publik yang didapatkan bersifat *Dynamic* (acak). Untuk mengatasi permasalahan tersebut dilakukan melalui metode *Network Development Life Cycle* (NDLC) dengan mengabungkan sistem protokol VPN L2TP dan IPSec yang ada pada Mikrotik. VPN merupakan sebuah jaringan private dan aman dengan menggunakan jaringan publik seperti internet. Salah satu basis pengamanan teknologi VPN adalah Internet *Protocol Security* (IPSec). IPSec merupakan protokol yang digunakan untuk mengamankan transmisi datagram pada jaringan berbasis TCP/IP. (L2TP) merupakan salah satu *tunneling protocol* yang dapat digunakan dan mendukung VPN. L2TP juga merupakan terowongan normal dari satu router ke router lain atau dari klien ke gateway host melalui Server Akses Jaringan (NAS) ISP. Penelitian ini bertujuan untuk merancang dan mengimplementasikan sistem jaringan *Virtual Private Network* (VPN) dengan memanfaatkan jaringan publik. dimana sistem ini memberikan peningkatan keamanan tahap lanjut pada jaringan internet dengan menggunakan IPSec.

Kata Kunci: VPN, Mikrotik, L2TP, IPSec