ABSTRAK

Data center pada rumah sakit merupakan salah satu fasilitas yang menempatkan sistem komputer seperti sistem komunikasi dan penyimpanan data pada jaringan. Keterkaitan satu dengan lainnya memudahkan akses khususnya untuk client. Akses layanan jaringan menggunakan suatu sistem merupakan suatu permasalahan yang dapat muncul terutama pada bagian keamanan sistem tersebut. Adapun masalah yang mucul terkait keamanan jaringan meliputi aspek *confidentiality, integrity* dan *availability* (CIA). Ketiga aspek tersebut menjadi topik utama mengingat sistem yang terintegrasi berbagai layanan sehingga apabila terjadi suatu kebocoran data atau terganggunya kinerja server maka akan sangat mengganggu layanan yang diberikan pada client.

Mengatasi permasalahan diatas, sistem keamanan menggunakan VPN Server yang berbasis IPsec sebagai otentikasi jaringan. VPN (*Virtual Private Network*) merupakan suatu teknologi yang memungkinkan seseorang terkoneksi dengan jaringan lokal dengan memanfaatkan koneksi jaringan publik sehingga orang tersebut seperti terkoneksi dengan jaringan lokal secara langsung. Tools yang digunakan pada sistem keamanan jaringan yaitu menggunakan Ubuntu Server 12.04 LTS sebagai sistem operasi, VPN Server berbasis IPsec yang menggunakan protokol Openswan sebagai sistem autentikasi jaringan.

Hasil akhir dari pembangunan jaringan ini yaitu pada pengujian sistem VPN Server yang berbasis IPsec dapat berjalan dengan baik sesuai permasalahan di sistem keamanan pada jaringan. Pengujian dilakukan seperti serangan sniffing menggunakan Wireshark, kemudian VPN Server dapat mengatasi masalah penangkapan data tersebut, dan akhirnya username beserta password tidak dapat dimiliki oleh pelaku serangan.

Kata Kunci: VPN, IP *Security*, *Tunneling*, *Openswan, Sniffing, Keamanan Jaringan*

ABSTRACT

Data center at the hospital is one facility that puts computer systems and communication systems such as data storage on the network. Relation to one another with easy access especially for the client. Access network services using a system is a problem that can arise, especially on the security of the system. The issues that arise related to network security inclued aspects of confidentially, integrity and availability (CIA). These three aspects are the main topic given the system from by a variety of integrated services, so if there is a leak or disruption of performance of the server, it would greatly disrupt the servies provided to the client.

The way to solve the above problems, the system security using IPsec-based VPN server as network authentication. VPN (Virtual Private Network) is a technology that allows one to connect to a local network by using a network connection such as public so people connected to the local network directly. Tools used in the network security system using Ubuntu 12:04 LTS Server as the operating system, IPsec-based VPN server that uses protocol OpenSWAN as a network authentication system.

The end result of the construction of this network is in testing systems-based IPsec VPN Server can run properly according issues in security systems on the network. Tests carried out such an attack sniffing using Wireshark, then VPN Server can solve the problem of data capture, and eventually username and password can not be owned by the perpetrators of the attacks.

Keywords: VPN, IP *Security*, *Tunneling*, *Openswan, Sniffing, Network security*