Intisari

Di dunia informatika, teknologi komunikasi yang saat ini berkembang memungkinkan untuk melewatkan trafik suara melalui jaringan komputer adalah *Voice over Internet Protocol* (VoIP). VoIP merupakan teknologi yang memilki kemampuan melakukan panggilan suara, video, data yang dijalankan diatas infrastruktur jaringan *packet network.* Masalah keamanan menjadi kebutuhan yang mendasar karena VoIP dikirimkan melewati jaringan publik yang bersifat tidak aman, dimana *Real-time Transport Protocol* (RTP) sebagai protokol pembawa suara yang umum digunakan pada VoIP rawan akan serangan *sniffer* dengan melihat isi dari *RTP payload*, sehingga paket *RTP* dapat ditangkap, direkontruksi dan di playback, sehingga cara untuk membangun keamanannya yaitu dengan menggunakan VPN Tunneling *Point To Point Protocol* (PTPP) dan *Layer 2 Tunniling Protocol/Internet Protokol Security* (L2TP/IPSec) yang merupakan keamanan dengan membuat terowongan *virtual* diatas jaringan public, data akan dienkapsulasi dan dienkripsi agar terjamin kerahasiaanya. Penelitian ini bertujuan untuk membangun suatu jaringan komunikasi beserta keamanannya. Metode penelitian menggunakan *Experimental Research* merupakan penelitian yang dilakukan untuk mengetahui akibat yang ditimbulkan dari suatu perlakuan yang diberikan secara sengaja oleh peneliti. Hasil penelitian menunjukkan bahwa tanpa keamanan percakapan pada VoIP dapat di sniffer dengan merekam pembicaraan yang berlangsung melalui VoIP *calls* pada *tools wireshark backtrack* dan setelah adanya keamanan VPN tunneling PPTP dan L2TP/IPsec *sniffer* tidak dapat menangkap informasi sehingga kerahasiaan dapat terjaga, selain itu analisis terhadap performance VoIP setelah menggunkan PPTP dan L2TP/IPSec sangat baik karena banyak panggilan yang success dilihat dari SIP *statistics*

Kata Kunci : *VoIP, RTP, VPN Tunneling PPTP dan L2TP/IPSec*