

Intisari

PT. Telkom Indonesia Unit Kandatel Sleman WITEL Yogyakarta bergerak dibidang jasa telekomunikasi menggunakan *Website* GISTA untuk melakukan pendataan aset produksi, pendataan pelanggan dan pengambilan keputusan. Namun, saat ini *Website* GISTA hanya bisa digunakan dengan menggunakan *server* lokal, padahal *website* tersebut akan sangat berguna jika dapat diakses saat karyawan melakukan survei di lapangan. Hal ini dikarenakan belum adanya sistem keamanan jaringan yang diterapkan pada *Website* GISTA jika diakses melalui jaringan publik. Solusi atas permasalahan diatas adalah dengan melakukan penelitian berupa perancangan dan implementasi *Virtual Private Network* (VPN) menggunakan aplikasi *SoftEther* VPN yang dapat memberikan keamanan dalam mengakses *Website* GISTA saat diakses melalui jaringan publik sehingga tidak dapat diketahui oleh pihak luar.

Penelitian ini dilakukan berdasarkan kebutuhan karyawan PT. Telkom Indonesia Unit Kandatel Sleman WITEL Yogyakarta yang diperoleh melalui wawancara dan survei. Berdasarkan langkah-langkah tersebut, kemudian dilakukan implementasi jaringan, pengujian dan evaluasi VPN yang kemudian dianalisis dan dibahas dalam penelitian ini. Pengujian dilakukan dengan melakukan percobaan *packet loss*, *round trip time* dan *sharing data*. Sedangkan evaluasi dilakukan dengan dua cara, yaitu melakukan serangan ke VPN *Server* dengan menggunakan metode *Denial of Service* dan *sniffing* dengan menggunakan aplikasi *Wireshark*.

Hasil pengujian menunjukkan bahwa jaringan VPN yang telah dibuat dapat menghubungkan VPN *Server* ke VPN *Client* dan antar VPN *Client*, aktivitas-aktivitas yang dilakukan melalui jaringan publik yang dilakukan oleh VPN *Client* tidak dapat diketahui oleh pihak luar karena telah terenkapsulasi dan terenkripsi, serta antar VPN *Client* sudah bisa saling berbagi data. Hasil evaluasi terhadap serangan yang dilakukan menunjukkan bahwa VPN *Server* mengalami sedikit gangguan saat diakses oleh VPN *Client*, namun tetap dapat berjalan normal. Sedangkan untuk proses *sniffing*, jaringan VPN telah terenkapsulasi karena aplikasi *Wireshark* tidak berhasil melacak aktivitas yang dilakukan oleh VPN *Client*.

Kata kunci : VPN, *SoftEther* VPN, *Website* GISTA, keamanan, *web server*

Abstract

PT. Telkom Indonesia Kandatel Unit Yogyakarta Sleman Witel is a company working in the field of telecommunication services using the GISTA Website to perform data collection production assets, customer data and new asset development planning in the migration process of cable network to fiber optic network. Currently GISTA Website can only be used by using a local server, despite the website usefulness if it can be accessed when employees conduct field survey. This is due to lack of network security system applied to the GISTA Website for access through a public network. The solution to the above problems can be found by conducting research in the form of design and implementation of Virtual Private Network (VPN) using SoftEther VPN application that can provide access security in GISTA Website when accessed through public network so it won't be known by outsiders.

This study was conducted based on the needs of employees of PT. Telkom Indonesia Kandatel Unit Yogyakarta SlemanWitel obtained through interviews and surveys. Based on these measures, the research proceeded with network implementation, testing and evaluation of VPN which is then analyzed and discussed in this study. The Tests was carried out by doing packet loss, round trip time and sharing data experimentation. While the evaluation was done in two ways, attacking the VPN Server by using Denial of Service and sniffing by using Wireshark application.

The results showed that the implemented VPN network could connect the VPN server to the VPN Client as well as made inter VPN Client connection, the VPN Client activities carried out through the public network could not be known by outsiders because it has been encapsulated and encrypted, and VPN Clients were able to share data among them. Evaluation result of the carried out attacks showed that the VPN server encountered small interference when accessed by the VPN Client, but still able to run normally. As for the sniffing process, VPN network has been successfully encapsulated as Wireshark application was not able to trace the activities undertaken by the VPN Client.

Keywords : *VPN, SoftEther VPN, Website GISTA, security, web server*