Implementasi dan Analisis SSL VPN
Sebagai Solusi Keamanan Jaringan

[1] Khairul Luqman, [2] Budhi Kristianto
Fakultas Teknologi Informasi
Universitas Kristen Satya Wacana
Jl. Diponegoro 52-60, Salatiga 50771, Indonesia
Email: [1] khairul.luqman@ymail.com, [2] budhik@yahoo.com

Abstract

The progress of internet makes easy to access in everywhere. The impact can cause a good like the information can be achieved so quickly, and bad cause that causes security problem like stealing data (account information). There are many solution to accomplish, likes encrypt data, use digital signature and setup firewall. Also used leased lines, it's secure but the leases are expensive. Another solution is making Virtual Private Network. VPN creates network inside network, called tunnel. There are a lot of implementation of VPN. PPTP (Point-to-Point Protocol) is dial-up standard feature to the internet provider then build point-to-point tunnel. L2TP (Layer Two tunneling Protocol), it's called Layer 2 Forwarding, developed by adding excess of PPTP. IPsec (IP Security), standard solution that have a good level security but too difficult to implement. Last, SSL VPN, be known as Transport Layer Security (TLS). Because it's open source and only needs web browser and internet connection. So, SSL VPN is the answer for the network security. SSL changes a transport protocol like UDP to secure communication through tunnel. SSL VPN uses private keys, certificate, username and password for authentication. This paper describes how to implement and analyse SSL VPN. Setup a server and client to communicate using OpenVPN, it's VPN based application that support SSL/TLS encryption. Client can browse securly because the data will encrypted through tunnel and can't be seen by others. SSL VPN makes an information data secure.
Keywords: *Security Network, Virtual Private Network, Secure Socket Layer*

Abstrak

Perkembangan internet yang pesat membuatnya dapat diakses di mana saja yang dapat berdampak baik, seperti kecepatan dalam memperoleh data dan buruk yang menyebabkan masalah keamanan, misal pencurian data. Ada beberapa metode untuk mengatasi masalah ini, seperti mengenkripsi data, menggunakan tandatangan digital dan *firewall*. Juga *leased lines,* aman tetapi harga sewanya mahal. Solusi lain adalah menggunakan *Virtual Private Network.* VPN membuat jaringan di dalam jaringan atau disebut *tunnel.* Implementasi VPN diantaranya adalah PPTP *(Point-to-Point Protocol)*. Fitur standar dengan *dial-up* ke penyedia internet kemudian dibangun *point-to-point tunnel* melalui jaringan telepon. L2TP (*Layer Two Tunneling Protocol)*, awalnya *Layer 2 Forwarding*, dikembangkan dengan menambahkan kelebihan-kelebihan PPTP. IPsec (IP *Security)*, solusi yang sudah distandarisasi dan mempunyai tingkat keamanan yang cukup baik tapi implementasinya cukup rumit. Terakhir SSL VPN atau *Transport Layer Security* (TLS), karena bersifat *open source* dan hanya membutuhkan fasilitas layanan seperti *web browser* dan koneksi internet, maka VPN berbasis SSL ini menjawab solusi untuk keamanan jaringan. SSL mengubah suatu protokol *transport* seperti UDP menjadi sebuah saluran komunikasi aman melalui *tunnel.* SSL VPN menggunakan *private keys, certificate, username* dan *password* untuk melakukan autentikasi. Tugas akhir ini menjelaskan bagaimana implementasi dan analisis VPN berbasis SSL. Mengkonfigurasi *server* dan *client* dengan menggunakan OpenVPN yang merupakan aplikasi VPN yang mendukung enkripsi SSL/TLS. *Client* dapat *browsing* secara aman karena data akan dienkripsi melalui *tunnel* yang tidak diketahui pihak lain. SSL VPN dapat menjaga informasi data secara aman.
Kata Kunci: *Security Network, Virtual Private Network, Secure Socket Layer*

---

[1] Mahasiswa Fakultas Teknologi Informasi Jurusan Teknik Informatika, Universitas Kristen Satya Wacana Salatiga.
[2] Staff Pengajar Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana Salatiga.