ANALISIS PERBANDINGAN PROTOKOL VIRTUAL PRIVATE NETWORK (VPN) – PPTP, L2TP, IPSEC – SEBAGAI DASAR PERANCANGAN VPN PADA POLITEKNIK NEGERI SRIWIJAYA PALEMBANG

Muhammad Taufik Roseno

mtroseno@gmail.com

ABSTRAK

Virtual Private Network (VPN) merupakan salah satu solusi jaringan komputer yang menggunakan insfrastruktur jaringan publik seperti internet dengan menyediakan akses ke jaringan lokal dengan aman. VPN menawarkan penghematan dalam sisi biaya operasional dibandingkan dengan metoda privat lainnya seperti *leased line*, *frame relay* atau koneksi dial up. Politeknik Negeri Sriwijaya Palembang menggunakan fasilitas internet untuk memberikan kemudahan dalam mengakses kegiatan perkuliahan seperti jadwal absensi, jadwal mata pelajaran dan pembayaran SPP. Mempertimbangkan pentingnya keamanan komunikasi antar jaringan di Politeknik Negeri Sriwijaya maka VPN bisa menjadi salah satu alternatif pilihan untuk menyediakan jaringan yang aman. VPN menggunakan metode *tunneling* di atas jaringan publik dengan menggunakan protokol-protokol seperti *Point to Point Tunneling Protocol* (PPTP), *Layer 2 Tunneling Protocol* (L2TP) atau *IP Security* (IPSec). Ketiga protokol tersebut menyediakan tingkat keamanan dan performansi yang berbeda pada suatu jaringan yang kemudian akan dianalisis agar dapat menjadi suatu alternatif pilihan dalam menyediakan layanan akses dalam jaringan Politeknik Negeri Sriwijaya.

Kata-kunci: *Virtual Private Network, Tunneling,* PPTP, L2TP, IPSec

ABSTRACT

Virtual Private Network (VPN) is a computer networking solution that uses a public network like the Internet infrastructure by providing access to local network safely. VPN offers a cost savings in comparison to other network methods such as leased line, frame relay or dial up connection. State Polytechnic of Sriwijaya use internet facilities to provide easy access to activities such as attendance schedules, course schedules and tuition payments. Considering the importance of security of communication between the VPN network can be an alternative option to provide a secure network. VPNs use tunneling methods over public networks using protocols such as Point to Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP) or IP Security (IPSec). All three protocol provides security and performance levels vary on a network that will then be analyzed in order to become an alternative choice to provide network access services in the State Polytechnic of Sriwijaya.

Keyword: *Virtual Private Network, Tunneling,* PPTP, L2TP, IPSec

I. PENDAHULUAN

Seiring dengan berkembangnya suatu perusahaan dimana kantor-kantor cabang terletak pada banyak lokasi yang berbeda maka dibutuhkan pula suatu jenis komunikasi yang terpusat dengan tujuan untuk mempermudah pertukaran data antar cabang ataupun kemudahan para pegawai untuk mengakses informasi dimanapun mereka berada.

Untuk mewujudkan jenis komunikasi diatas diperlukan suatu jenis komunikasi data dimana seluruh data akan disimpan pada suatu server dan kemudian akan diakses oleh setiap individu yang akan membutuhkan atau client. Jenis komunikasi ini memerlukan suatu teknologi yang tidak sederhana, terutama pada teknologi hardware dan dukungan teknis yang rumit.

Beberapa tahun yang lalu, cara yang umum dipakai perusahaan untuk menghubungkan komputer pada beberapa kantor di lokasi berbeda adalah dengan menggunakan teknologi *leased line* seperti ISDN (*Integrated Service Digital Network*), *Frame Relay*, ATM. *Leased Line* menyediakan suatu jaringan privat untuk kebutuhan komunikasi antar kantor cabang dengan membentuk suatu *Wide Are Network* (WAN) untuk komunikasinya. Jenis komunikasi ini memang handal dan aman, namun memerlukan biaya yang sangat tinggi untuk menghadirkannya terutama apabila jarak antar kantor cabang juga meningkat.

Virtual Private Network (VPN) hadir sebagai salah satu solusi keamanan pada jaringan internet dimana jenis komunikasi ini dapat menyediakan suatu jaringan privat yang handal dan aman tetapi dapat berjalan pada jaringan publik seperti internet.

Politeknik Negeri Sriwijaya telah menggunakan layanan SISFOKAMPUS (Sistem Informasi Akademik Kampus) untuk menunjang kegiatan belajar mengajar di mana proses pertukaran data yang bersifat rahasia seperti proses penilaian kegiatan belajar sangat memerlukan suatu sistem keamanan yang handal.

Tujuan dari penulisan artikel ini adalah untuk mempelajari dan melakukan analisis dari ketiga protokol Virtual Private Network (VPN) yaitu PPTP, L2TP dan IPSec agar dapat menjadi bahan pertimbangan perancangan VPN pada Politeknik Negeri Sriwijaya.

Manfaat dari penulisan ini agar dapat memberikan gambaran tentang berbagai tipe protokol Virtual Private Network (VPN) sehingga didapatkan suatu perbandingan yang lengkap untuk menjadi dasar perancangan VPN di Politeknik Negeri Sriwijaya.

II. TINJAUAN PUSTAKA

Dalam melakukan analisis perbandingan protokol Virtual Private Network diperlukan beberapa materi penunjang untuk dapat memperjelas pembahasannya diantaranya jenis jaringan VPN, tunneling dan jenis protokol tunneling.

2.1 Jenis Jaringan Virtual Private Network (VPN)

Ada 3 jenis jaringan antara lain:

1. *Remote* VPN

Jenis VPN ini ditujukan pada pengguna yang ingin mengakses jaringan pusat dari tempat yang berada di luar area pusat data dimana user dapat data perusahaan kapanpun dan dimanapun berada contohnya penyelia

suatu perusahaan yang dilengkapi laptop untuk mengakses informasi di kantor pusat. Kunci dari jenis komunikasi ini adalah fleksibilitas dan biasanya bandwidth dan performance tidak menjadi isu yang begitu penting.

2. *Intranet* VPN

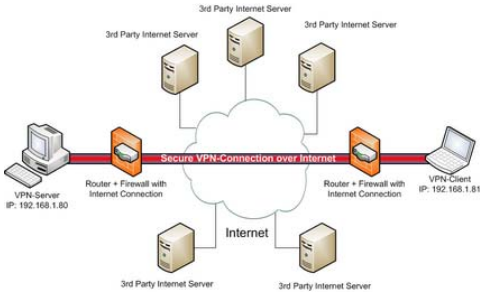
VPN jenis ini diimplementasikan pada infrastruktur jaringan diperusahaan yang memiliki beberapa lokasi gedung berbeda, biasanya digunakan untuk menghubungkan kantor kantor cabang dengan kantor pusat suatu perusahaan. Jenis VPN ini harus benar-benar aman dan memenuhi standar performansi dan kebutuhan *bandwidth* dengan persyaratan yang ketat.

3. *Extranet* VPN

Pada jenis komunikasi ini, VPN menggunakan Internet sebagai backbone utama. Biasanya VPN jenis ini ditujukan untuk skala komunikasi yang lebih luas melibatkan banyak pengguna dan kantor cabang yang tersebar.

2.2 Tunneling

Inti dari teknologi *Virtual Private Network* adalah tunneling dimana data atau paket dienkapsulasi untuk kemudian dikirim melalui media internet yang disebut tunnel. Ketika paket sampai di lokasi tujuan paket tersebut kemudian didekapsulasi untuk dikembalikan lagi kedalam format aslinya.



Gambar 1. VPN tunneling (VPN Tunnel, 2008)

2.3. Protokol Tunneling pada VPN

Untuk bisa saling berhubungan antar user pada komunikasi VPN diperlukan protokol untuk menghubungkan komunikasi tersebut. Terdapat tiga protokol yang paling populer pada jaringan *Virtual Private Network*, yaitu *Point to Point Protocol* (PPTP), *Layer Two Tunneling Protocols* (L2TP) dan *Internet Protocol Security* (IPSec).

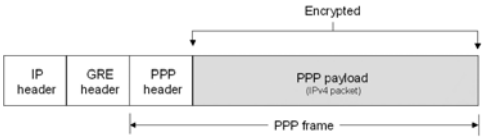
2.3.1 Point to Point Protocol (PPTP)

Dikembangkan oleh sebuah konsorsium yang terdiri dari Ascend Communications, 3Com, ECI Telematics, U.S Robotics dan Microsoft, bertujuan untuk membuat data tunneling pada jaringan internet. Protokol ini beroperasi pada layer 2 pada model OSI.

Pada proses enkapsulasi, PPTP mengenkapsulasi PPP *frames* pada IP datagrams untuk ditransmisikan pada jaringan. PPTP juga menggunakan koneksi TCP untuk mengelola *tunnel* dan GRE (Generic Routing Encapsulation).

Proses *tunneling* pada PPTP terjadi dengan cara membungkus paket informasi untuk kemudian ditransmisikan melalui jaringan internet. Pada proses ini PPTP menggunakan koneksi TCP yang dikenal sebagai PPTP *control*

connection untuk menciptakan, merawat dan mengakhiri tunnel serta *Generic Routing Encapsulation* (GRE).



Gambar 2. Struktur PPTP (Virtual Private Networking, 2005)

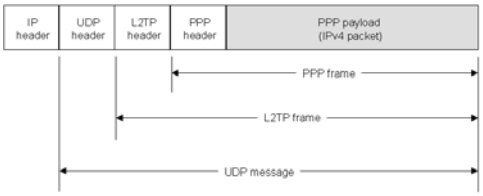
Dalam hal enkripsi, PPTP menggunakan mekanisme otentikasi yang sama dengan PPP seperti *Extensible Authentication Protocol* (EAP), *Challange Handshake Protokol* (CHAP), Shiva *Password Authentication Protocol* (SPAP) dan *Password Authentication Protocol* (PAP).

2.3.2 Layer 2 Tunneling Protocol (L2TP)

L2TP merupakan kombinasi dari PPTP milik Microsoft dan L2F (*Layer 2 Forwarding*) milik Cisco System's [1]. Protokol ini tidak menyediakan enkripsi sendiri tetapi mengandalkan enkripsi dari protokol yang dilewati pada tunnel untuk mendapatkan privasinya. Walaupun bertindak seperti *Data Link Layer Protocol* pada model OSI, L2TP sebenarnya adalah *Session Layer Protocol*.

L2TP mempunyai dua komponen utama yaitu LNS (L2TP *Network Server*) yang berfungsi untuk mengakhiri dan mengotentikasi aliran PPP dan LAC (L2TP *Access Concentrator*) yang secara fisik akan mengakhiri sebuah panggilan.

Pada dasarnya L2TP menggunakan protokol UDP untuk mengirimkan PPP frame yang telah dienkapsulasi sebagai data yang akan dikirim melalui tunnel. Sedang kan L2TP mempunyai 2 tipe *tunneling* yaitu *Compulsory Tunneling* dan *Voluntary Tunneling*



Gambar 3. Struktur L2TP (Virtual Private Networking, 2005)

2.3.1 Internet Protocol Security (IPSec)

IPSec merupakan protokol VPN yang dikembangkan oleh *Internet Engineering Task Force* (IETF) yang bertujuan untuk menyediakan framework keamanan pada layer ketiga (*Third Layer*) yaitu pada *Network Layer* sehingga dapat mengamankan data dari *layer* yang diatasnya (Gupta, 2003). Inilah alasan mengapa IPSec dikembangkan pada layer 3 daripada layer 2.

Ada beberapa sistem keamanan internet yang digunakan seperti *Secure Socket Layer* (SSL), *Transport Layer Security* (TLS) dan *Secure Shell* (SSH) yang beroperasi di atas model TCP/IP. Oleh karenanya IPSec melindungi semua aplikasi yang melewati jaringan *Internet Protocol*. Aplikasi-aplikasi tidak perlu di desain khusus untuk menggunakan IPSec tidak seperti TLS/SSL yang mengharuskan didesain khusus pada aplikasi agar dapat melindungi keamanan dari aplikasi yang dibuat.

IPSec terdiri dari 3 kombinasi protokol kunci, yaitu:

1. *Authentication Header* (AH) protokol, yang berfungsi untuk memberi header tambahan pada IP Datagram, header ini akan mengotentikasi IP Datagram yang dikirim ke penerima.

2. *Encapsulating Security Payload* (ESP) protokol, tujuan utama dari ESP adalah menyediakan kerahasiaaan pada proses otentikasi pengirim serta melakukan verifikasi integritas data selama proses transit.
3. *Internet Key Exchange* (IKE) protokol, merupakan protokol yang menyediakan kunci otentikasi sebelum sesi IPSec diimplementasikan.

III. METODE PENELITIAN

Langkah-langkah yang dilakukan dalam penulisan artikel ini dimulai dengan melakukan kajian pustaka yang berkaitan dengan Virtual Private Network (VPN), metode tunneling, protokol PPTP, L2TP dan IPSec dimana akan dievaluasi sehingga didapatkan alternatif solusi untuk dapat di implementasikan di jaringan Politeknik Negeri Sriwijaya Palembang.

IV. PEMBAHASAN

4.1. Analisa Keamanan Protokol VPN

Keamanan merupakan persyaratan yang paling dasar dalam koneksi menggunakan Virtual Private Network karena jaringan internet tidak menyediakan garansi keamanan pada koneksinya.

4.1.1 Analisa Keamanan Protokol PPTP

Protokol PPTP pada dasarnya tidak memiliki dukungan otentikasi dan enkripsi. Fungsi keamanan hanya bergantung pada protokol PPP yang dilewatkan. Pada penelitian ini digunakan Microsoft Windows yang digunakan sebagai client dimana sudah mengimplementasikan berbagai level otentikasi dan enkripsi sebagai fitur standar.

Untuk proses otentikasi Microsoft PPTP mengandalkan Microsoft Challange/Replay Handshake Protocol version 2 (MS-CHAPv2) sedangkan untuk enkripsi protokol yang digunakan adalah Microsoft Point to Point Encryption (MPPE). Namun demikian, MS-CHAPv2 masih juga rentan terhadap serangan keamanan terutama pada dictionary attack dimana *challange* dan *response* dari paket yang dikirim dapat tertangkap (George, 2004).

Bruce dkk (1999), mengemukakan bahwa walaupun Microsoft telah melakukan beberapa perubahan pada MS-CHAPv2, tetapi keamanan pada protokol PPTP tetap rentan karena sistem keamanan pada protokol ini tetap berbasis pada penggunaan *password*.

4.1.1 Analisa Keamanan Protokol L2TP

Protokol L2TP tidak menyediakan enkripsi sendiri, tetapi bergantung pada protokol enkripsi yang melaluinya diantara tunnel untuk menyediakan fungsi privasi.

L2TP mempunyai mekanisme proteksi pada tunnel yang rentan, karena L2TP mengenkapsulasi PPP oleh karena itu mekanisme keamanan yang dimiliki mewarisi fungsi keamanan dari protokol PPP termasuk enkripsi dan otentikasinya (Arora dkk, 2001). PPP memang mengotentikasi client ke LNS tetapi idak menyediakan otentikasi per paket. L2TP juga tidak menyediakan fasilitas key management walaupun otentikasi pada ujung tunnel bergantung pada distribusi password.

4.1.2 Analisa Keamanan Protokol IPSec

Pada IPSec terdapat dua protokol yang akan mengamankan lalu

lintas data yaitu *Authentication Header* (AH) yang berfungsi mengamankan alamat sumber dan tujuan pada IP Header, dan protokol *Encapsulating Security Payload* (ESP) yang bertugas melakukan enkripsi pada *data payload* agar privasi dan integritas data dapat terjaga. Pada Microsoft Windows 7 yang digunakan sebagai VPN client menggunakan algoritma AES-128 (Primary) dan 3-DES (Secondary).

Pande Putu (2007), pada penelitiannya juga mengemukakan bahwa software Cain & Abel tidak dapat merekam paket yang dikirim melalui PC Router, hal ini disebabkan adanya metode tunneling berbasis protokol IPSec pada jaringan VPN dengan algoritma 3DES 192 bit sebagai kunci enkripsinya.

4.2. Analisa Performansi Protokol VPN

Performansi merupakan salah satu tolak ukur dalam pencapaian kualitas suatu layanan jaringan komputer. Adapun parameter-parameter yang dapat diukur untuk menentukan kualiltas layanan jaringan antara lain latency, jitter dan packet loss.

4.2.1. Analisa Performansi Protokol PPTP

PPTP menggunakan UDP untuk membawa paket data dan TCP untuk membawa command control packet. Dengan menggunakan protokol TCP paket yang kembali harus dikenali terlebih dahulu untuk setiap data yang dikirim sehingga akan menghasilkan penurunan throughput jika dibandingkan dengan L2TP.

PPTP juga mengalami masalah pada jaringan yang memiliki lantency yang tinggi, hal ini juga disebabkan oleh penggunaan protokol TCP. TCP merupakan protokol yang berorientasi pada session yang berarti session akan terus terjadi antara PPTP client dan server selama proses tunneling.

Dari sisi interoperability yaitu kemampuan dari suatu sistem untuk bekerja dengan sistem lain, PPTP merupakan protokol yang spesifik pada satu vendor sehingga kemampuan interoperability sangat terbatas.

4.2.2. Analisa Performansi Protokol L2TP

Pada protokol L2TP, semua paket dienkapsulasi dengan protokol UDP sehingga utilisasi pada command & control message relatif lebih tinggi dibandingkan dengan protokol PPTP. L2TP juga memiliki kemampuan yang lebih baik dibandingkan PPTP jika berjalan pada jaringan dengan latency yang tinggi.

Sedangkan dari sisi interoperability, L2TP merupakan protokol yang mennyokong multi vendor yang berarti tidak memiliki masalah jika bekerja dengan berbagai sistem dengan vendor yang berbeda.

4.2.3 Analisa Performansi Protokol IPSec

IPSec menggunakan protokol ESP (Encapsulation Security Payload) untuk mengenkapsulasi paket yang akan di tunnel kan, dengan adanya penambahan informasi pada setiap paket yang dikirim akan meningkatkan ukuran dari paket tersebut. Hal ini akan menimbulkan penurunan pada performansi protokol IPSec. Begitu juga dengan penggunaan algoritma kriptografi dimana IPSec menggunakan 3DES dan AES untuk fungsi kriptografinya. Juga akan menambah ukuran dari paket yang dikirimkan. Dari sisi interoperabiltiy, pada umumnya protokol IPSec tidak

mendukung interoperabilitas antar vendor sehingga agak menyulitkan jiga harus bekerja dengan sistem dari vendor lain.

V. KESIMPULAN

Berikut ini beberapa kesimpulan yang diambil dari pembahasan yaitu:

1. Dari sisi keamanan, IPSec memiliki fungsi keamanan yang paling lengkap dibandingkan dengan protokol PPTP dan L2TP karena memiki protokol enkripsi dan otentikasi yang lebih baik. Sedangkan protokol PPTP dan L2TP tidak menyediakan fungsi data sendiri tetapi hanya bergantung pada protokol yang melaluinya untuk menyediakan fungsi keamanan.
2. Dari sisi performansi, PPTP dan L2TP memiliki performansi yang lebih baik dibandingkan dengan IPSec jika berjalan pada jaringan TCP/IP, sedangkan dari sisi interoperability, L2TP dapat bekerja lebih baik dengan sistem dari vendor lain dibandingkan protokol PPTP dan IPSec

DAFTAR PUSTAKA

Bruce Schneier, Mudge, David Wagner (1999), *Cryptoanalysis of Microsoft's PPTP Authentication Extensions* (MS-CHAPv2), Diakses 10 Desember 2010, dari www.schneier.com/paper-pptpv2.pdf

George Ou (2004), *PPTP VPN Authentication Protocol Proven Very Susceptible to Attack*, Diakses 10 Desember 2010, dari http://www.zdnet.com/blog/ou/ppt p-vpn-authentication-protocol-proven-very-susceptible-to-attack/21

Poonam Arora, Prem R.Vemuganti, Praveen Allani 2001 (2001), *Comparison of VPN Protocols-IPSec, PPTP, and L2TP*, Projet Report, Department of Electrical and Computer Engineering, George Mason University, Fairfax

Virtual Private Networking [image] 2005, Diakses 10 Desember 2010, dari http://technet.microsoft.com/en-us/library/bb727019.aspx

VPN Tunnel [image] 2008, 10 Desember 2010, dari http://www.tomshardware.com/reviews/secure-remote-access,1803-2.html