ANALISI DAN IMPLEMENTASI REMOTE ACCESS VPN DENGAN MENGGUNAKAN L2TP COMPULSORY TUNNELING VIA RADIUS

Novenny Dwina Astri Purba[1], Tri Brotoharsono[2], Vera Suryani[3]

[1]Teknik Informatika, Fakultas Teknik Informatika, Universitas Telkom

Abstrak

Kerahasiaan data pada jaringan internet merupakan salah satu hal penting yang harus dipertimbangkan. Dengan VPN (virtual private network) memungkinkan sebuah teknologi komunikasi dapat terkoneksi pada jaringan public dan menggunakannya untuk dapat bergabung dengan jaringan local.Dengan menggunakan jaringan publik ini,user dapat mengakses fitur-fitur yang ada pada jaringan lokalnya,mendapatkan hak dan pengaturan yang sama bagaikan secara fisik kita berada dimana jaringan local itu berada.Data yang dilewatkan akan diencapsulation (dibungkus) dan dienkripsi agar data tersebut terjamin kerahasiaannya.

Salah satu teknologi virtual private network yang digunakan adalah remote-access VPN . Remote-access VPN memberikan keuntungan di mana memungkinan user secara mobile dapat mengakses data di mana saja selama user tersebut dapat berhubungan dengan remote-access VPN server. Remote-access VPN dibangun dengan menggunakan Layer 2 Tunneling Protocol (L2TP) sebagai implementasi dari VPN dan RADIUS untuk sistem management user yang mencakup authentication-authorization-accounting (AAA).

Dengan penggabungan teknologi Remote access VPN dengan L2TP dan Radius yang mencakup authentication-authorization-accounting (AAA).diharapkan menjadikan VPN menjadi lebih mudah pengimplementasian dan memberikan tingkat keamanan data yang lebih baik .

Kata Kunci : Virtual Private Networks, Remote Access,Layer 2 Tunneling Protokol, Authentication-Authorization,Accounting (AAA),enkripsi

Abstract

Confidentiality of data is one of the important thingson the Internet. With a VPN (virtual private network) allows a communication technology can be connected to public networks and using it to join the local network.Using a public network, the user can access the available features on its local network, get the rights and the same settings as we are physically located where the local network is located. The missed data will beencapsulated (wrapped) and is encrypted so that data confidential.

One of the virtual private network technology used is the remote-access VPN. Remote-access VPN provides benefits which allow a mobile user can access data anywhere over the user can be associated with a remote-access VPN server. Remote-access VPN built using Layer 2 Tunneling Protocol (L2TP) as the implementation of the VPN and RADIUS for user management system that includes the authentication-authorization-accounting (AAA).

With the incorporation of technology Remote access VPN with L2TP and Radius authentication-authorization covering-accounting (AAA). Expected to make the VPN becomes easier implementation and provides a level of data security better.

Keywords : Virtual Private Networks, Remote Access,Layer 2 Tunneling Protokol, Authentication-Authorization,Accounting (AAA),enkripsi

BAB I

Pendahuluan

1.1 Latar Belakang

Dewasa ini pertumbuhan jumlah user internet semakin meningkat. Hal ini dikarenakan perkembangan teknologi internet dan tingkat kebutuhan manusia untuk melakukan pertukaran informasi juga meningkat. Dan penggunaan internet memudahkan user untuk mengakses data. Karena pertumbuhan pengguna internet yang semakin meningkat,dibutuhkan keamanan data yang baik untuk dapat mengirim data tanpa merubah keutuhan data yang dipertukarkan di internet. Untuk memungkinkan terjaminnya keamanan data tersebut dibangun satu jaringan *private* di atas jaringan public yang ada. Jaringan private yang digunakan untuk mengatasi masalah keamanan data tersebut adalah *Virtual Private Network* (VPN).

VPN (*Virtual Private Network*) merupakan koneksi antar dua jaringan dengan menggunakan infrastruktur telekomunikasi umum dan menggunakan metode enkripsi tertentu sebagai media pengamannya.Atau dengan kata lain VPN adalah jaringan *private* yang dibangun di atas jaringan public seperti internet yang menghubungkan satu jaringan ke jaringan lainnya.Implementasi VPN menggunakan *remote access* untuk memudahkan user dapat mengakses data dimanapun selama user masih terhubung dengan *Remote access* VPN server.Pada implementasi keamanan data pada VPN ini digunakan metode *tunneling.* Metode tunneling melakukan proses enkapsulasi ,transmisi dan decapsulasi paket yang di komunikasikan. Metode tunneling menggunakan *Point To Point Protocol(*PPTP) dan *Layer 2 Tunneling Protocol(* L2TP), *IP Sec.* PPTP dan L2TP merupakan layer 2 tunneling protocol, dimana kedua protocol tersebut melakukan pembungkusan payload pada frame *Point to Point Protocol* (PPP) untuk dilewatkan pada jaringan. IP Sec berada pada layer 3 yang menggunakan packet,yang akan melakukan pembungkusan IP Header sebelum dikirim pada jaringan.

Pada implementasi L2TP diperlukan keamanan data yang dikirimkan oleh user kepada server dan juga sebagai manajemen untuk computer untuk menghubungkan dan menggunakan layanan jaringan. Manajemen komputer disini berupa Authentication, Authorization, dan Accounting (AAA). Salah satu protokol yang mendukung AAA ini adalah protokol RADIUS(*Remote Access Dial-in User Service*), sehingga protokol radius ini digunakan untuk manajemen komputer pada L2TP tunneling ini. RADIUS atau *Remote Authentication Dial-In User Service* merupakan sebuah protocol yang memungkinkan perusahaan untuk melakukan *Authentication* (pembuktian keaslian), *Authorize* (otoritas/pemberian hak) dan *Accounting* (akuntansi) (AAA) untuk me-*remote* para pengguna atau user yang ingin mengakses suatu sistem atau layanan dari pusat server jaringan komputer. Dengan adanya protocol RADIUS ini dapat terbentuk suatu manajemen akses yang terkontrol pada jaringan yang besar.

1.2 Rumusan Masalah

Dari latar belakang masalah di atas, dapat diambil *point-point* penting yang akan menjadi perumusan masalah yang melatarbelakangi Tugas Akhir ini. Point-point tersebut adalah sebagai berikut :

1. Bagaimana mengimplementasikan Remote Access VPN dengan Menggunakan L2TP Compulsory Tunneling via RADIUS di dalam jaringan Internet.
2. Bagaimana performansi jaringan setelah menggunakan L2TP Compulsory Tunneling via RADIUS.
3. Bagaimana proses Authentifikasi,Accounting,Authorize pada tunneling L2TP menggunakan RADIUS

Batasan masalah dalam tugas akhir ini adalah

1. Implementasi ini dilakukan dalam skala laboratorium dengan jaringan yang kecil dengan menggunakan minimal 3 komputer.
2. Parameter pengujian adalah Authentifikasi,Accounting,dan Authorize pada Radius. Sedangkan untuk keamanan data,pengujian dilakukan dengan menggunakan tools untuk menangkap data sensitive (username, password) dari paket-paket data yang dipertukarkan dari client ke L2TP server.

3. Sistem operasi yang digunakan untuk L2TP server adalah FreeBSD 9, dan untuk client menggunakan Microsoft Windows XP SP 2.
4. Tidak membahas IPSec secara spesifik

Hipotesa awal dari tugas ini adalah penggunaan RADIUS sebagai protokol Authentifikasi,Accounting,Authorize memungkinkan paket data dari user ke server bisa sampai dan memudahkan proses tunneling VPN dengan menggunakan tunneling L2TP.

1.3 Tujuan

Tujuan dari dibuatnya tugas akhir ini adalah sebagai berikut :

1. Mengimplementasikan Remote Access VPN dengan Menggunakan L2TP Compulsory Tunneling via RADIUS di dalam jaringan.
2. Menguji Authentication,Accounting,Authorize pada RADIUS dengan parameter pengujian pada RADIUS

1.4 Metodologi Penyelesaian Masalah

Dalam tugas akhir ini, metodologi penyelesaian masalah untuk buku ini adalah sebagai berikut :

a. Studi Literatur
   Pada tahap ini dilakukan pendalaman materi tentang VPN, L2TP, RADIUS, dan teori-teori yang mendukung tugas akhir ini.
b. Perancangan Sistem dan Jaringan
   Dalam tahap ini, dilakukan perancangan sistem dan jaringan yang sesuai dengan topik tugas akhir ini. Sistem nantinya akan terdiri dari L2TP server dengan RADIUS server dan database server.
c. Implementasi Sistem
   Dalam tahap ini, dilakukan implementasi dari perancangan system dan jaringan yang telah dibuat.

d. Pengujian

Dalam tahap ini dilakukan beberapa tahap pengujian. Tahap pengujian tersebut adalah sebagai berikut :

1) Pengujian L2TP dengan protocol RADIUS untuk *management user*. Untuk Implementasi RADIUS menggunakan *FreeRadius* dan *MySQL* sebagai database dan L2TP server menggunakan *MPD5*.
2) Pengujian Authentifikasi,Accounting,Authorize pada RADIUS dengan parameter pengujian pada RADIUS

e. Analisa dan Kesimpulan

Tahap ini dilakukan analisis dari scenario pengujian yang dilakukan selama percobaan pada point nomor 4, dan kemudian di dapat kesimpulan dari tugas akhir ini.

1.5 Sistematika Penulisan

Sistematika penulisan buku proyek akhir ini adalah sebagai berikut :

BAB I PENDAHULUAN
Bab ini berisi latar belakang masalah, perumusan masalah, tujuan, batasan masalah, dan metode penyelesaian yang dilakukan.

BAB II LANDASAN TEORI
Bab ini memuat berbagai teori yang mendukung terlaksananya pengembangan aplikasi ini, khususnya teori yang mendukung dalam pembuatan sistem.

BAB III PERANCANGAN SISTEM DAN JARINGAN
Bab ini berisi tentang analisis kebutuhan dari sistem untuk mengetahui kekurangan dan kelemahan sistem yang ada pada saat ini sehingga dapat ditentukan kebutuhan yang diperlukan dalam pembuatan aplikasi ini agar pengembangan aplikasi ini dapat lebih baik.

BAB IV IMPLEMENTASI DAN TESTING
Bab ini berisi tentang pengimplementasian rancangan pada tahap sebelumnya dan melakukan pengujian terhadap aplikasi yang telah dibuat.

BAB V PENUTUP
Bab ini berisi kesimpulan atas hasil kerja yang telah dilakukan beserta rekomendasi dan saran untuk pengembangan dan perbaikan selanjutnya.

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil yang telah dilakukan, maka dapat diambil kesimpulan:

1. Berdasarkan hasil konfigurasi L2TP dengan Radius diperoleh hasil bahwa simulasi Remote Acces VPN bisa dikonfigurasikan pada tunneling L2TP dengan Radius dan menjamin keamanan data untuk setiap proses Radiusnya,baik Authentifikasi,Authorize dan Accounting karena adanya proses enkripsi data. Pada saat pengujian keamanan data, dilakukan proses sniffing pada saat client log ini di web student, pada proses sniffingnya password sudah dienkripsi sehingga tidak dapat dibaca.
2. Proses AAA dapat berjalan dengan baik pada pengujian sistem. Authentifikasi dapat dilakukan dengan baik,dan setiap data log-in yang dimasukkan tidak sesuai dengan data yang ada di database server tidak akan lolos pada proses Authentifikasi. Pada Proses Authorize sendiri setiap klien diberikan hak untuk akses dengan adanya penamaan IP-address untuk setiap klien yang berbeda. Pada proses Accounting, pengujian berhasil mencatat setiap kegiatan klien berupa billing dari setiap byte dan paket data yang diberikan oleh sistem kepada klien dan yang telah diterima oleh klien dari sistem. Data billing tersebut sudah berhasil di simpan di Radius server. Proses update pada Accounting juga telah berhasil diuji. Set update disetting selama 10 detik, dan update datanya berjalan kira-kira setiap 10 detik.

5.2 Saran

Berikut ini saran yang dapat diberikan untuk pengembangan aplikasi ini lebih lanjut agar aplikasi ini menjadi lebih baik :

1. Implementasi proses *Authentication-Authorization-Accounting* (AAA) L2TP dengan *protocol* TACACS+. Selain RADIUS sebagai *protocol* implementasi AAA, ada *protocol* lain yang dapat digunakan yaitu *Terminal Access Controller Access-Control System* (TACACS+). Radius menggunakan protokol UDP dalam proses transmisi datanya,sedangkan TACACS+ menggunakan protokol TCP. Pada RADIUS proses Authentifikasi dan Authorize berlangsung secara bersamaan,sedangkan pada TACACS+ berlangsung terpisah untuk proses AAA yang menyebabkan tingkat keamanan data lebih aman.
2. Analisa keamanan data dalam L2TP dengan menggunakan IPSec. IPSec dapat dikombinasikan dengan L2TP dengan cara mengenkapsulasi paket L2TP dengan Penambahan header IPSec.

Daftar Pustaka

[1] Aboba, B., Zorn, G., *"Implementation of L2TP Compulsory Tunneling via RADIUS"* , RFC 2809, April 2000.

[2] Rigney, C., Willens, S., Rubens, A., Simpson, W., *"Remote Authentication Dial In User Service (RADIUS)", RFC 2865*, June 2008.

[3] Dreyfus,Emmanuel, "*Remote user access VPN with IPsec* ",October 2005

[4] Postel, J., "User Data Protocol", STD 6, RFC 768, August 1980.

[5] B. Aboba(2005).*Guidance for AAA Managemen* ,[online].Tersedia: http://tools.ietf.org/html/draft-housley-aaa-key-mgmt-01

[6] *Layer 2 Tunnel Protocol*,[online] (http://www.cisco.com/en/US/docs/ios/12_0t/12_0t1/feature/guide/l2tpT.htm,diakses tanggal 23 Desember 2009)

[7] *Configuring QoS for L2TP Interfaces*,[online] (http://www.juniper.net/techpubs/software/erx/junose61/swconfig-policy-qos/html/qos-config14.html ,diakses tanggal 27 desember 2009)

[8] *RADIUS* (http://wiki.wireshark.org,diakses tanggal 5 desember 2009)

[9] Kusuma, Ineke., *Perancangan Sistem VPN dengan menggunakan PPTP dan L2TP*, [online] (http://digilib.its.ac.id,diakses tanggal 25 desember 2009)

[10] *Virtual Private Network*,[online] (http://www.scribd.com/doc/24070594/VPN-Jurnal,diakses tanggal 28 Desember 2009)