SIMULASI SECURITY JARINGAN PADA VIRTUAL PRIVATE NETWORK

TUGAS AKHIR

Oleh

BAMBANG WAHYU BUDIONO

BP. 05092001

PROGRAM STUDI TEKNIK KOMPUTER

JURUSAN TEKNOLOGI INFORMASI

POLITEKNIK UNIVERSITAS ANDALAS

PADANG

2008

Abstrak

Teknologi *Virtual private network* cocok digunakan untuk perusahaan-perusahaan yang mempunyai beberapa cabang dan menginginkan pemusatan data. *Virtual private network* [VPN] merupakan cara untuk membuat suatu jaringan bersifat private dan aman dengan menggunakan jaringan public. Adanya VPN dapat mengirim data antara dua komputer yang melewati jaringan public sehingga seolah-olah terhubung secara point to point. Disaat kantor induk terhadap kantor cabang melakukan transaksi, yang didalamnya terdapat data rahasia perusahaan. Dihawatirkan adanya pihak yang tidak bertanggung jawab merusak atau mengambil data tersebut. Baik itu Hacker maupun virus yang ditanamkan dalam jaringan tersebut.

Dengan konsep keamanan yang bersifat *authentication, authorization* dan *enkripsi* didalamnya. Data yang dilewatkan telah dienkripsi melalui *IPSec* [IP Security] sebagai pemicunya yang merupakan perangkat lunak. ISP [*Internet Servis Provider*] merupakan media penghantar yang akan menghubungkannya. Penerapan VPN menghemat biaya tanggungan terhadap ISP dan dapat diterapkan sesuai jaringan yang telah ada.

Kata kunci: **Virtual Private Network, Point to Point, Authentication, Authorization, Enkripsi, Internet Servis Provider**

BAB I

PENDAHULUAN

1.1 Latar Belakang Permasalahan

Teknologi jaringan komputer dan internet saat ini telah merasuk ke seluruh segi kehidupan. Sangat sulit pada saat ini untuk menemukan bidang yang belum tersentuh oleh teknologi jaringan komputer. Salah satu bidang yang sangat pesat perkembangannya dalam penerapan teknologi jaringan komputer adalah bidang Industri. Dibeberapa industri besar pelaku bisnis menginginkan data tersaji dengan cepat di atas meja tanpa memikirkan cara-cara menyajikan data tersebut.

Teknologi *virtual private network* cocok digunakan oleh perusahaan yang mempunyai beberapa cabang dan menginginkan pemusatan data. Teknologi *virtual private network* [VPN] merupakan cara membuat jaringan bersifat private dan aman dengan menggunakan jaringan publik. Dengan adanya VPN dapat mengirim data antara dua komputer yang melewati jaringan publik sehingga seolah terhubung secara point to point. Data diengkapsulasi [dibungkus] dengan header sehingga sampai ke tujuan. Dengan adanya koneksi bersifat private, data yang dikirimkan dienkripsi terlebih dahulu untuk menjaga kerahasiaannya sehingga paket tertangkap ketika melewati jaringan publik tidak terbaca karena melewati proses deskripsi. Sebuah keamanan jaringan dibutuhkan sekali untuk menjaga privasi dan otentikasi sebuah Instansi.

Berbagai cara orang yang ingin memasuki sebuah jaringan orang lain, sehingga setelah telah memasukinya dapat melakukan apa saja sesukanya. Hal ini yang tidak diinginkan, dalam hal ini dapat menjatuhkan citra Instansi dan dapat

merusak asset berharga Instansi tersebut. Sehingga dibutuhkannya jaringan yang aman dan *Dedicated* [rahasia], dan karyawan dan pihak Instansi bisa bekerja dengan aman dan cepat. Berdasarkan hal diatas, maka penulis mencoba untuk membahas permasalahan tersebut dalam bentuk tugas Akhir dengan judul **" Implementasi Security Jaringan Pada Virtual Private Network"**.

1.2 Perumusan Masalah

Jaringan VPN ini tidak banyak kendala yang ditemukan seperti telas dijelaskan sebelumnya, maka didapat rumusan permasalahan sebagai berikut:

1. Seefektif apakah jika jaringan ini diterapkan pada Instansi terkait ?
2. Berapa besar keuntungan menghemat biaya tanggungan terhadap ISP ?
3. Bagaimana penerapan dan konfigurasi sistem Jaringan VPN ?
4. Apakah dengan dibangun jaringan VPN ini dapat memudahkan dan membuat nyaman bagi pengguna layanan ini ?
5. Bagaimana bentuk pengamanannya setelah jaringan ini diterapkan ?

1.3 Batasan Masalah

Agar permasalahan menjadi lebih terarah dan sistematis sesuai dengan sasaran yang ingin dicapai, maka batasan-batasan pada tugas akhir ini adalah:

1. Merancang bentuk konfigurasi VPN yang akan dibangun.
2. Penggunaan *Operating Sistem* [OS] sebagai perangkat lunaknya yang bersifat open source dan memberikan layanan VPN .
3. Perancangan diterapkan sesuai standarisasi penerapan perangkatnya dan sesuai dengan perangkat jaringan yang telah dimiliki.

Bab V

PENUTUP

5.1 Kesimpulan

Setelah membangun layanan keamanan VPN maka disimpulkan:

1. Memverifikasi data, dari klient dan servernya serta paket yang difilter. Paket yang di transfer melalui IPSec di filter dengan mengenkapsulasi pada header data yang dilewatkan lalu dikirim ketujuannya. Dalam VPN dibutuhkan sinkronisasi antara sisi Klient dan Server menggunakan CA (*chertifikat authentication*), *key menagement* pada IPSec yang digenerate sebagai kunci masuk atau login untuk meminta terhadap server.

2. Enkripsi yang dipakai 3DES (*triple data enchrytion standar*) merupakan enkripsi handal dan cepat dalam mengenkripsi, dengan kombinasi bit data sampai 168 dengan tiga kali pengulangan, sistem enkripsi data sehingga datanya benar-benar terjaga.

3. Untuk keamannya sebaiknya menutup semua Port yang tidak dipakai dan membuka port yang dibutuhkan VPN saja. Port number dipakai untuk melayani komunikasi yang berbeda dalam jaringan pada saat bersamaan.

4. Kemudahan membangun VPN dikarena mudah disesuaikan dengan bentuk jaringan yang telah ada.

5. VPN yang dibagun masih menggunakan jaringan lokal, serta linux yang dipakai masih berbasis GUI.

Daftar Pustaka

Chris Brenton, Cameron Hunt. Network Security. Elex Media Komputindo. Jakarta: 2008

Cisco Networking Academy Program, CCNA 1 and 2 Companion Guide Third Edition

Computer Security Institute, **1999 CSI/FBI Computer Crime and Security Survey**, CSI, Winter 1999. http://www.gocsi.com

http://romisatriawahono.net, Subnetting Siapa Takut ?

http://fedora.redhat.com/docs/selinux-apache-fc3/

https://sourceforge.net/docman/display_doc.php?docid=21959[amp]group_id=21266

IR. Hendra Wijaya, Belajar Sendiri Cicsco Router, Elex Media Komputindo, 2004

Lawrie Brown, ***Lecture Notes for Use with Network and Internetwork Security by William Stallings***, on-line document. http://www1.shore.net/~ws/Security-Notes/index.html

Onno W. Purbo, ***Keamanan Jaringan Internet***, Elex Media Komputindo, Jakarta,2000

Robby Wirza. Pembuatan VPN Database Pemesanan Tiket Pesawat Terbang. Padang : TA, 2006