View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Universitas Pasundan

Proceedings

Konferensi Nasional Sistem Informasi 2012

STIKOM BALI

23 - 25 Februari 2012

Proceeding Edition

ISBN : 9786029876802

P3M STIKOM Bali
Jl. Raya Puputan No. 86 Renon, Denpasar - Bali
Phone : +62-361-244445 | Fax : +62-361-264723
Email : info@stikom-bali.ac.id

Dipublikasikan Tahun 2012 oleh :
STMIK STIKOM Bali
Denpasar- Indonesia

ISBN : 9786029876802

Panitia tidak bertanggung jawab terhadap isi paper dari peserta

PROCEEDINGS

KONFERENSI NASIONAL SISTEM INFORMASI 2012

Ketua Editor

Evi Triandini, SP.,M.Eng

Sekretaris Editor

Luh Dwi Ari Sudawati, Amd.Kom

Anggota Editor

Candra Ahmadi, ST.,MT

I Ketut Dedy Suryawan, S.Kom

I Gusti Rai Agung Sugiarta, ST

Ni Komang Sri Julyantari, S.Kom

Ni Kadek Sumiari, S.Kom

No Makalah : 263

EKSPLORASI VIRTUAL PRIVATE NETWORK UNTUK KEAMANAN INFORMASI

Doddy Ferdiansyah[1]

[1]Jurusan Informatika, Fakultas Teknik, Universitas Pasundan
[1]doddy2112@hotmail.com

Abstrak

Virtual Private Network atau biasa disingkat menjadi *VPN* merupakan sebuah teknologi jaringan yang menggunakan teknologi '*Tunelling*' sehingga data dan informasi yang berada dalam jaringan *VPN* tersebut dapat terjaga integritasnya. Tanpa menggunakan jaringan *VPN* banyak contoh – contoh kasus hilangnya sebuah data atau informasi sudah tidak valid, seperti serangan hacker menggunakan teknik *Sniffing*. Untuk membangun sebuah Virtual Private Network yang baik harus didukung oleh sistem operasi yang baik, seperti menggunakan Server 2003 untuk sistem operasi Windows atau Red Hat untuk sistem operasi Linux. Pada penelitian ini dilakukan kajian teori tentang keamanan informasi dengan menggunakan teknologi jaringan virtual, mulai dari hardware, software dan sistem operasi yang digunakan hingga pembuatan jaringan virtual. Hasil akhir dari penelitian ini merupakan sebuah model jaringan virtual dan bagaimana sebuah informasi yang menggunakan VPN menjadi aman.

Kata kunci : *virtual private network, VPN, integritas informasi*

1. Pendahuluan

1.1. Latar Belakang

Penyebaran informasi saat ini tidak lagi menggunakan media kertas, tetapi sudah banyak menggunakan teknologi komputer dan internet. Informasi bisa didapat melalui website, e-mail, dll. Akibat dari penggunaan internet dalam penyebaran informasi, maka semakin banyak orang-orang yang berusaha untuk mendapatkan informasi yang bersifat pribadi (private), seperti isi chating, email, file perusahaan, dll.

Berbicara mengenai keamanan informasi, harus mendapat perhatian yang lebih. Apalagi keamanan terhadap data dan informasi yang bersifat rahasia dan pribadi. Salah satu cara untuk menjaga keamanan dan integritas sebuah informasi maka muncul teknologi jaringan yang dinamakan Virtual Private Network (VPN).

1.2. Identifikasi Masalah

Kemudian dapat di identifikasi bahwa permasalahan yang timbul adalah :

1. Apa saja kebutuhan untuk membangun VPN
2. Bagaimana sebuah informasi dapat terjaga keamanan dan integritasnya

Permasalahan tersebut diatas merupakan poin – poin penting untuk membangun Virtual Private Network yang baik.

1.3. Tujuan

Penggunaan teknologi VPN mempunyai tujuan sebagai berikut :

1. Sebuah model jaringan virtual yang dapat mempermudah pengaksesan suatu alat telekomunikasi (computer) dimanapun dan kapanpun
2. Menjaga keamanan dan integritas data/informasi yang dikirim atau diterima
3. Mengurangi biaya dalam membangun jaringan telekomunikasi

1.4. Metode Penelitian

Metode yang dilakukan dalam studi dan eksplorasi ini adalah sebagai berikut :

1. Studi Literatur

   Mencari dan mempelajari referensi mengenai :

   a. Konsep jaringan komputer
   b. Konsep teknologi VPN
   c. Konsep keamanan informasi

2. Analisis

   Melakukan penyelidikan atau pembelajaran lebih lanjut terhadap teknologi VPN, keamanan informasi dan tools yang dapat digunakan untuk membangun VPN

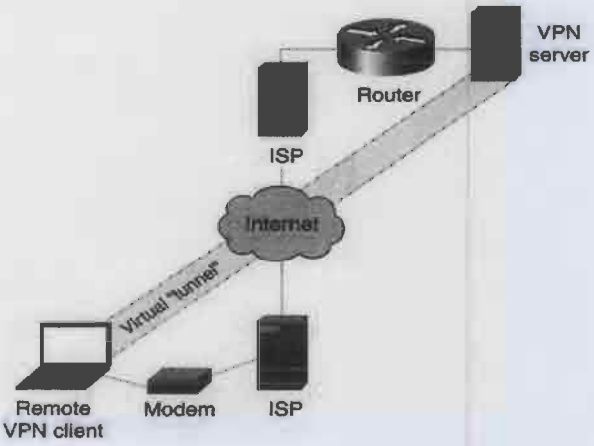
3. Perancangan

Membuat contoh sebuah server VPN yang akan diakses oleh user yang mempunyai hak untuk mengakses server tersebut.

2. Pemahaman Virtual Private Network

2.1. Pemahaman Umum

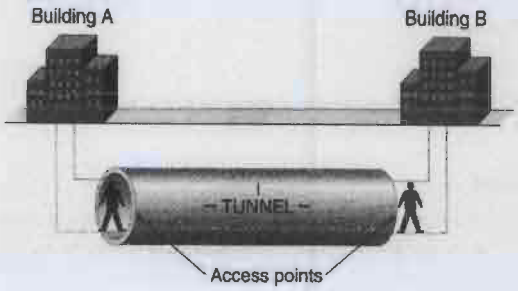
Virtual Private Network (VPN) merupakan salah satu bentuk dari teknologi jaringan masa kini dimana prinsip dasar dari VPN itu adalah membangun sebuah "*Tunneling*" atau lorong/pipa dari perangkat komunikasi satu dengan yang lainnya dengan melalui media jaringan *public* (internet). Gambar 2.1 menjelaskan tentang bagaimana infrastruktur dari VPN ini dapat terhubung.



Gambar 1. Infrastruktur VPN

Sniffer VPN dapat terjadi antara dua *end-system* atau dengan kata lain dua PC, atau bisa juga antara dua atau lebih jaringan yang berbeda. *Tunnel* dalam VPN sebenarnya hanya *logical point-to-point connection* dengan otentikasi dan enkripsi. Analoginya adalah kalau sebuah organisasi/perusahaan punya kantor di 2 gedung yang berbeda. Untuk orang/informasi bergerak dari satu kantor ke kantor lainnya, bisa melalui:

- kaki lima atau jalan umum
- menggali lubang di bawah tanah (analogi dengan VPN)



Gambar 2. Analogi VPN

2.2. Keuntungan Virtual Private Network

Ada beberapa keuntungan yang dapat diperoleh dengan menggunakan VPN :

1. Jangkauan jaringan lokal akan semakin luas, sehingga perusahaan dapat mengembangkan bisnis di daerah lain. Waktu yang dibutuhkan untuk menghubungkan jaringan lokal ke tempat lain juga semakin cepat.
2. Penggunaaan VPN dapat mereduksi biaya operasional bila dibandingkan dengan penggunaan *leased line* . VPN dapat mengurangi biaya pembuatan jaringan karena tidak membutuhkan kabel (*leased line*) yang panjang. Penggunaan kabel yang panjang akan membutuhkan biaya produksi yang sangat besar. Semakin jauh jarak yang diinginkan, semakin meningkat pula biaya produksinya. VPN menggunakan internet sebagai media komunikasinya. Perusahaan hanya membutuhkan kabel dalam jumlah yang relatif kecil untuk menghubungkan perusahaan tersebut dengan pihak ISP (*internet service provider*) terdekat.
3. VPN memberi kemudahan untuk diakses dari mana saja, karena VPN terhubung ke internet. Sehingga pegawai yang *mobile* dapat mengakses jaringan khusus perusahaan di manapun dia berada. Selama dia bisa mendapatkan akses ke internet ke ISP terdekat, pegawai tersebut tetap dapat melakukan koneksi dengan jaringan khusus perusahaan.

2.3. Kelemahan Virtual Private Network

VPN juga memiliki kelemahan yaitu :

1. VPN membutuhkan perhatian yang serius pada keamanan jaringan publik (internet). Oleh karena itu diperlukan tindakan yang tepat untuk mencegah terjadinya hal-hal yang tidak diinginkan seperti penyadapan, *hacking* dan tindakan *cyber crime* pada jaringan VPN.
2. Ketersediaan dan performansi jaringan khusus perusahaan melalui media internet sangat tergantung pada faktor-faktor yang berada di luar kendali pihak perusahaan. Kecepatan dan keandalan transmisi data melalui internet yang digunakan sebagai media komunikasi jaringan VPN tidak dapat diatur oleh pihak pengguna jaringan VPN, karena *traffic* yang terjadi di internet melibatkan semua pihak pengguna internet di seluruh dunia.
3. Perangkat pembangun teknologi jaringan VPN dari beberapa vendor yang berbeda ada kemungkinan tidak dapat digunakan secara bersama-sama karena standar yang ada untuk teknologi VPN belum memadai. Oleh karena itu fleksibilitas dalam memilih perangkat yang sesuai dengan kebutuhan dan keuangan perusahaan sangat kurang.

3. Protokol pada VPN

Virtual Privat Network (VPN) menggunakan beberapa protokol dalam berkomunikasi. Protokol – protokol yang digunakan adalah :

a. PPTP (Point-to-Point Tunneling Protocol)
   Point-to-Point Tunneling Protocol merupakan teknologi jaringan baru yang mendukung multiprotocol virtual private networks (VPN), yang memungkinkan pengguna untuk mengakses jaringan perusahaan secara lebih aman melalui Internet.
b. L2F (Layer 2 Forwarding)
   Dibuat Cisco tahun 1996. Bisa menggunakan ATM dan Frame Relay, dan tidak membutuhkan IP. L2F juga bisa menyediakan otentikasi untuk tunnel end-points.
c. L2TP (Layer 2 Tunneling Protocol)
   Dikembangkan oleh Microsoft dan Cisco. Bisa mengenkapsulasi data dalam IP, ATM, Frame Relay dan X.25.

   Keunggulan L2TP dibandingkan PPTP:
   - multiple tunnels between endpoints, sehingga bisa ada beberapa saluran yang memiliki perbedaan Quality of Service (QoS).
   - mendukung kompresi
   - bisa melakukan tunnel authentication
   - bisa bekerja pada jaringan non-IP seperti ATM dan Frame Relay.

d. IPSec
   Dalam tunneling mode, IP Sec bisa dipergunakan untuk mengenkapsulasi paket.
   IP Sec juga bisa dipergunakan untuk enkripsi dalam protokol tunneling lainnya.

4. VPN Security

Didalam suatu jaringan lokal maupun public, keamanan adalah faktor yang paling penting dalam pengiriman data atau penyampaian informasi. Berikut ini merupakan keamanan yang dapat diberikan VPN :

1. Authentication / Otentikasi
   Proses mengidentifikasi komputer *dan* manusia/user yang memulai VPN connection. Metode otentikasi dapat dilakukan dengan protokol:
   - Extensible Authentication Protocol (EAP)
   - Challenge Handshake Authentication (CHAP)
   - MS-CHAP
   - Password Authentication Protocol (PAP)
   - Shiva-PAP
2. Authorization / Otorisasi
   Menentukan apa yang boleh dan yang tidak boleh diakses seorang user.
3. Encryption / Enkripsi
   Bertugas untuk menjaga privasi dan kerahasiaan data agar tidak dapat dengan mudah dibaca oleh pihak yang tidak berhak.

Untuk memenuhi ketiga kebutuhan keamanan diatas, maka terdapat beberapa metode pengamanan data yang dapat dilakukan pada teknologi jaringan VPN antara lain dengan menggunakan *firewall*. Pengamanan bisa juga dilakukan dengan melakukan enkripsi pada data yang akan dikirim melalui intenet. Selain itu, data dapat juga dikirim menggunakan protokol khusus

yang aman untuk transmisi data melalui internet (IPSec). Alternatif lain pengendalian keamanan jaringan VPN adalah dengan menggunakan metode AAA server yang akan memeriksa autentikasi, autorisasi dan merekam segala sesuatu yang dilakukan pengguna pada suatu jaringan

5. Model Jaringan VPN Yang Telah Dibuat

Berikut ini model jaringan VPN yang telah dibuat berdasarkan analisis dan literature yang telah ada.

Gambar 3. Model Jaringan VPN

Dari hasil percobaan diatas, berikut detail dari spesifikasi yang digunakan :

- Kedua PC terhubung ke jaringan internet dan menggunakan ISP yang berbeda
- Kedua PC telah di konfigurasi untuk dapat digunakan dalam jaringan VPN
- Menggunakan protocol L2TP (Layer 2 Tunneling Protocol)

6. Kesimpulan

Setelah melakukan eksplorasi dari *Virtual Private Network* (VPN) meliputi *Hardware* dan *Software*, Kelebihan dan kekurangan, sampai dengan keamanan dari VPN itu sendiri dapat diambil beberapa kesimpulan tentang VPN :

1. Keamanan dan integritas informasi dapat terjaga karena pada model jaringan VPN menggunakan protokol L2TP.
2. Pengaksesannya dapat dilakukan dimana saja, tidak tergantung kepada ISP yang digunakan selama terdapat jaringan internet.

Daftar Pustaka:

[1] Wendy, Aris., 2005, *Membangun VPN Linux Secara Cepat*, Andy Yogyakarta.

[2] Kelompok 123P IKI-83408T MTI UI, Keamanan Jaringan Komputer, 2005

[3] Rusdy Sanny, Muhammad, *Keamanan Jaringan Virtual Private Network (VPN)*, 2003-2004