VIRTUAL PRIVATE NETWORK SOLUSI JARINGAN LUAS HEMAT UNTUK BISNIS

Huzainsyahnoor Aksad

ABSTRAK

Persaingan dunia bisnis saat ini sudah sangat-sangat ketat, terlebih dengan adanya persaingan yang mengarah pada persaingan global, produk satu Negara bisa berada pada Negara yang tidak membuat atau satu Negara membuat Negara lainpun membuat. Salah satu setrategi yang bisa dilakukan untuk menghadapi persaingan adalah dengan cara melakukan efieinsi diberbagai bidang. Salah satu yang bisa dilakukan adalah di bidang komunikasi untuk memperluas relasi.

Virtual Private Network (VPN) meruapak salah satu solusi yang dapat digunakan untuk berkomunikasi dengan murah dan aman. Karena VPN merupakan suatu komunikasi antar dua jaringan yang dibuat untuk memperluas koneksi, selain murah juga dapat membuat komunikasi menjadi lebih terjaga keamanannya.

Sistem keamanan yang dapat digunakan pada VPN adalah: Metode Tunneling, Metode Enkripsi, Metode Otentikasi User, dan Intergritas Data.

Kata Kunci : **Bisnis ,** ***VPN, Tunneling, Enkripsi***

I. Pendahuluan

1.1. Latar Belakang

Perkembangan bisnis yang sangat cepat dan meluas sekarang ini membuat suatu pelaksana bisnis harus dapat melakukan pengolahan proses bisnisnya secara cepat dan tepat, hal ini harus didukung oleh informasi yang terkini, akurat, cepat dan hemat. Namun semua pemerosesan informasi sangat dipengaruhi oleh dukungan infrastruktur komunikasi yang dimiliki oleh peleksana bisnis. Bagi pelaksana bisnis yang sudah cukup luas, terlebih yang sudah mengglobal kebutuhan akan informasi yang terkini, akurat, cepat dan hemat sangat dibutuhkan. Untuk mendapatkan informasi yang aktual, cepat, tepat dan hemat akan menjadi kunci yang vital dalam persaingan pasar yang sangat ketat.

Komputasi terdistribusi client/server, pengaksesan jarak jauh (*remote access*) dan konektifitas antar jaringan telah banyak berperan penting dalam meningkatkan produktivitas bagi pelaksana bisnis dan karyawannya dibanding sebelumnya. Pada saat yang bersamaan, pelaksana bisnis terus mencari solusi jaringan dan infrastruk-tur komunikasi data yang fleksibel untuk perkembangan bisnisnya. Era sekarang teknologi informasi tidak lagi digunakan sebagai tools atau alat bantu tetapi sudah menjadi senjata utama untuk bersaing dan mendapatkan informasi yang update/terbaru agar keputusan bisnis dapat dengan cepat diambil.

Ada banyak solusi yang bisa digunakan untuk komunikasi data pada jaringan skala luas saat ini, WAN adalah jaringan komunikasi yang meliputi area geografis yang luas dan biasanya menggunakan fasilitas dari transmisi provider, seperti perusahaan telepon atau lainya (Marilee Ford, dkk, Internetworking Technologies Handbook, 1997 : 45). Dalam

jaringan WAN sangat sensitive dengan masalah lebar pita (b*andwidth*), para penyedia jasa biasanya menentukan biaya sewa cukup besar dari layanan dan bandwidth yang digunakan.

Sebagaimana kita ketahui kegiatan bisnis terutama seorang karyawan harus bekerja walau sedang tidak dikantor, bisa saja pada saat yang mendesak seorang karyawan memerlukan akses ke file-file, e-mail dan database di kantor yang memerlukan koneksi langsung ke server. Kegiatan tersebut bisa menjadi sangat mahal dan memerlukan hardware dan dukungan teknis yang rumit. Mengirim file melalui internat mungkin menjadi sarana yang paling mudah, tetapi belum tentu file yang dikirim akan aman dari para pencuri dan pengintip rahasia suatu kegiatan bisnis. Dengan keadaan yang demikian, maka diperlukan suatu komunikasi yang aman dan murah, solusinya adalah dengan penggunaan Virtual Private Network (VPN), dimana VPN bisa terkoneksi secara local ke jaringan intranet kantor namun melalui jaringan yang bisa diakses dengan mudah seperti jaringan internet.

Sehubungan hal tersebut di atas, maka dalam makalah ini akan dijelaskan ada berapa macam tipe sebuah VPN dan metode keamanan apa saja yang digunakan VPN.

1.2. Perumusan Masalah

Sesuai dengan latar belakang yang dikemukakan di atas, maka masalah yang akan dibahas dalam penulisan ini adalah, ada berapa macam tipe sebuah VPN dan metode keamanan apa saja yang digunakan VPN.

1.3. Tujuan dan Manfaat

Penulisan ini dilakukan untuk menerangkan ada berapa macam tipe sebuah VPN dan metode keamanan apa saja yang digunakan VPN.

Manfaat yang diinginkan agar para pelaku bisnis bisa menggunakan VPN sebagai sarana untuk meningkatkan persaingan dan kinerjanya (Kamus Komputer dan Teknologi)

II. Landasan Teori

2.1. Pengertian Virtual Private Netwok (VPN)

VPN. Istilah ini merujuk pada sebuah network yang sebagian diantaranya terhubung dengan jaringan internet, namun lalu lintas data yang melalui internet dari network ini telah mengalami proses enkripsi (pengacakan). Hal ini membuat network ini secara virtual tertutup (private).

VPN dalam arti yang sederhana ialah koneksi secara logical yang menghubungkan dua node melalui public network (Herry Bayu Prasetyo.2008).

Dari pengertian tersebut VPN merupakan suatu mekanisme untuk membuat LAN/Intranet dengan melalui jaringan public (seperti internet) yang dapat dianggap untrusted, sehingga bisa memberikan data privacy, access control, data integrity, dan authentication services pada level network sehingga tidak bergantung kepada aplikasi yang menggunakan network tersebut.

Enkripsi ialah proses transformasi dari plain text/data asli ke dalam data terenkripsi yang menyembunyikan data asli.

2.2. Pengertian Bisnis

Bisnis adalah kegiatan atau usaha yang dilakukan untuk memperoleh keuntungan sesuai dengan tujuan dan target yang diinginkan dalam berbagai bidang, baik jumlah maupun waktunya. Keuntungan merupakan tujuan utama dalam dunia bisnis, terutama bagi pemilik bisnis baik keuntungan dalam jangka pendek maupun

jangka panjang. Bentuk keuntungan yang diharapkan lebih banyak dalam bentuk financial. Bidang usaha yang dapat digeluti beragam, mulai dari perdagangan, industry, pariwisata, agrobisnis atau usaha jasa-jasa lainnya.

Menurut Raymond E. Glos dalam bukunya "Business: Its Nature and Environment: An Introduction", membedakan tentang Perusahaan dan Bisnis. Perusaha-an diartikan sebagai sebuah organisasi yang memproses perubahan keahlian dan sumber daya ekonomi menjadi barang dan/atau jasa yang diperuntukkan bagi pemuas kebutuhan para pembeli, serta diharapkan akan memberikan laba kepada para pemiliknya. Bisnis diartikan sebagai seluruh kegiatan yang diorganisasikan oleh orang-orang yang berkecimpung di dalam bidang perniagaan (produsen, pedagang, konsumen, dan industri di mana perusahaan berada) dalam rangka memperbaiki standar serta kualitas hidup mereka.

Dengan kedua istilah di atas, dapat disimpulkan bahwa pengertian bisnis lebih luas daripada pengertian perusahaan karena perusahaan merupakan bagian dari bisnis.

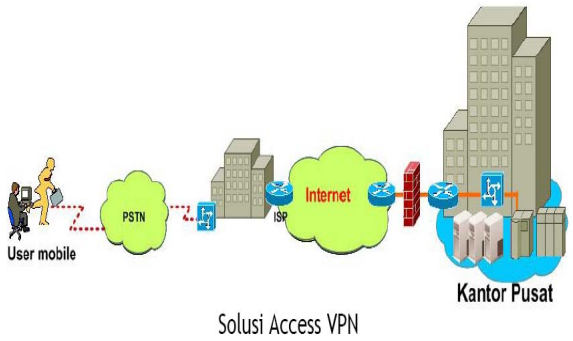
III. Metodologi Penelitian

Penulisan ini menggunakan metode studi pustaka, yakni dengan membaca buku-buku atau literatur yang mendukung penulisan ini, terutama yang berkaitan dengan Virtual Private Network (VPN), Enkripsi, dan Tunneling.

IV. Pembahasan

Ada tiga macam tipe sebuah VPN.

1. *Access VPN* : membuat koneksi jarak jauh untuk mengakses ke jaringan intranet atau ekstranet pelanggan dan pengguna bergerak dengan menggunakan infrastruktur analog, dial-up, ISDN, DSL, Mobile IP untuk membuat koneksi yang aman bagi mobile user, telecommuters dan kantor cabang.



Solusi Access VPN

Gambar 1. Solusi Akses VPN

2. *Intranet VPN* : menghubungkan kantor pusat, kantor cabang, dan remote user ke dalam jaringan internal dengan menggunakan infrastruktur koneksi yang terdedikasi.

3. *Extranet VPN* : menghubungkan dengan pihak luar seperti pelanggan, supplier, rekan bisnis, atau suatu komunitas ke dalam jaringan internal dengan menggu-nakan koneksi didacated. Koneksi ini menghubungkan jaringan internal dengan jaringan di luar perusahaan.

VPN merupakan suatu koneksi antar dua jaringan yang dibuat untuk mengkoneksikan kantor pusat, kantor cabang, telecommuters, suppliers, dan rekan bisnis lainnya, ke dalam suatu jaringan dengan menggunakan infrastruktur telekomunikasi umum dan menggunakan metode *enkripsi* tertentu sebagai media pengamanannya (Kevin, 2001). VPN merupakan sebuah jaringan private yang menghubungkan satu node jaringan ke node jaringan lainnya dengan menggunakan jaringan public seperti internet. Data yang dilewatkan akan diencopsulation (dibungkus) dan dienkripsi, supaya data tersebut terjamin kerahasiaannya.

Teknologi Enkripsi

Sebenarnya teknologi enkripsi bukan hanya milik VPN saja, namun sangat luas penggunaannya. Teknologi Enkripsi dalam VPN sangat bervariasi. Enkripsi fungsinya untuk menjaga privasi dan kerahasiaan data agar tidak dapat dengan mudah dibaca oleh pihak yang tidak berwenang. Secara garis besar teknik enkripsi terbagi atas dua jenis, yaitu :

1. Symmetric Encryption

Symmetric Encryption dikenal juga dengan nama sebutan secret key encryption. Enkripsi jenis ini banyak digunakan dalam proses enkripsi data dalam volume yang besar. Selama masa komunikasi data, perangkat jaringan yang memeiliki kemampuan enkripsi jenis ini akan mengubah data yang berupa teks murni (cleartext) menjadi berbentuk teks yang telah diacak atau istilahnya ciphertext. Teks acak ini tentu dibuat dengan menggunakan algoritma. Teks acak ini sangat tidak mudah untuk dibaca, sehingga keamanan data terjaga.

Untuk membuka data acak ini, algoritma pengacak tadi juga membuat sebuah kunci yang dapat membaca semua isi aslinya. Kunci ini dimiliki oleh si pengirim maupun si penerima data. Kunci inilah yang akan digunakan dalam proses enkripsi dan deskripsi ciphertext ini.

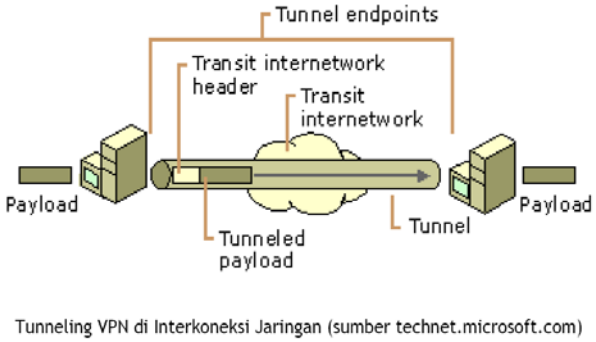
2. Asymmetric Encryption

Enkripsi jenis ini sering disebut sebagai system public key encryption. Proses enkripsi jenis ini bisa menggunakan algoritma apa saja, namun hasil enkripsi dari algoritma ini akan berfungsi sebagai pelengkap dalam mengacakkan dan penyusunan data. Dalam enkripsi jenis ini diperlukan dua buah kunci pengaman yang berbeda, namun saling berkaitan dalam proses algoritmanya. Kedua kunci pengaman ini sering disebut dengan istilah Public Key dan Private Key.

Mekanisme pembuatan public dan private key ini cukup kompleks. Biasanya key-key ini degenerate menggunakan generator yang menjalankan algoritme RSA (Ron Rivest, Adi Shanir, Leonard Adleman) atau EL Gamanl. Hasil dari generator ini biasanya adalah dua buah susunan angka acak yang sangat besar. Satu angka acak berfungsi sebagai public key dan satu lagi untuk private key. Angka-angka acak ini memang harus dibuat sebanyak dan seacak mungkin untuk memperkuat keunikan dari key-key yang digunakan.

Karena kompleknya enkripsi jenis ini, maka tidak pernah digunakan untuk mengamankan data yang sesungguhnya karena sifatnya yang selain komplek juga sangat membutuhkan proses CPU yang tinggi sehingga proses ini tidak bisa dilakukan setiap kali transaksi. Meskipun demikian, enkripsi ini akan sangat efektif dalam proses autentikasi data dan aplikasi yang melibatkan system digital signature dan key management.

Tunneling adalah salah satu metode yang digunakan untuk mentransfer data melewati infrastruktur interkoneksi jaringan dari satu jaringan ke jaringan lainnya seperti jaringan internet, data yang ditrasfer (payload) dapat berupa frames (paket) dari protocol yang lain. Tunnel menggambarkan paket data secara logika yang diencapsulations, transmisi, dan decapsulations paket (Microsoft, VPN with windows 2003 : 9).



Tunneling VPN di Interkoneksi Jaringan (sumber technet.microsoft.com)

Gambar 2. Tunneling VPN

Untuk membuat sebuah tunnel, diperlukan sebuah protocol pengatur sehingga tunnel secara logika dapat berjalan dengan baik bagaikan koneksi point-to-point sungguhan. Saat ini tersedia banyak sekali protocol pembuat tunnel yang bisa digunakan. Namum, tunneling protocol yang paling umum dan paling banyak digunakan terdiri dari tiga jenis, yaitu :

1. Layer 2 Tunneling Protocol (L2TP)
   L2TP adalah sebuah tunneling protocol yang memadukan dan mengombina-sikan dua buah tunneling protocol yang bersifat proprietary, yaitu L2F (Layer 2 Forwarding) milik Cisco Systems dengan PPTP (Point-to-Point Tunneling Protocol) milik Microsoft.
2. Generic Routing Encapsulation (GRE)
   Protocol tunneling ini memiliki kemampuan membawa lebih dari satu jenis protocol pengalamatan komunikasi. Bukan hanya paket beralamat IP saja yang dapat dibawanya, melainkan banyak paket protocol lain seperti CNLP, IPX, dan banyak lagi. Namun, semua itu dibungkus atau dienkapsulasi menjadi sebuah paket yang bersistem pengalamatan IP, kemudian paket tersebut didistribusi melalui system tunnel yang juga bekerja di atas protocol komunikasi IP.
3. IP Security Protocol (IPSec)
   IPSec adalah sebuah pilihan tunneling protocol yang sangat tepat untuk digunakan dalam VPN level korporat. IPSec merupakan protocol yang bersifat open standar yang dapat menyediakan keamanan data, keutuhan data, dan autentikasi data antara kedua peer yang berpartisipasi di dalamnya.

Penggunaan koneksi VPN dari tahun ke tahun mengalami peningkatan, karena murahnya infrastruktur yang dibutuhkan oleh VPN serta mudahnya dalam instalasi, maka koneksi ini lebih efisien dibanding menggunakan metode WAN. Jaringan VPN dikoneksikan oleh ISP lewat routernya ke router-router lain dengan menggunakan jalur internet yang telah dienkripsi antara dua titik dengan menggunakan leased line untuk hubungan jarak jauh dengan VPN, pelaksana bisnis dapat menghemat 20 sampai 40% dari biaya menggunakan WAN.

Informasi berupa sekumpulan data dalam bentuk digital merupakan aset biasanya harus dijaga kerahasiaan ataupun keutuhannya. Dengan begitu, informasi dalam bentuk digital dapat memperoleh tingkat kepercayaan setara dengan informasi dalam bentuk riil, misalnya saja setara dengan tingkat kepercayaan orang banyak terhadap kebenaran sebuah akte hukum.

Secara umum, tujuan-tujuan utama dalam penjagaan keamanan suatu informasi adalah:

- Kerahasiaan *(Confidentiality)* : untuk menjaga agar informasi tidak terbuka bagi pihak-pihak yang tidak berwenang;
- Integritas *(Integrity)* : untuk menjaga keutuhan dan keaslian data;
- Keberadaan *(Availability)* : untuk menjaga agar akses pengguna yang legal terhadap data tidak ditolak oleh sistem;
- Kelegalan penggunaan (*Legitimate use*) : untuk menjaga agar sumber-sumber daya tidak digunakan oleh pihak yang tidak berwenang.

Pada dunia elektronik, diperlukan suatu sistem yang memungkinkan penggunanya untuk mengenali dan mempercayai pengguna lain, walaupun belum pernah bertemu secara langsung. Dalam praktek, teknologi informasi digunakan untuk menjaga keamanan pada sistem informasi adalah kombinasi dari teknologi keamanan telekomunikasi dan teknologi keamanan komputer. Teknologi keamanan telekomunikasi melakukan proteksi terhadap informasi saat informasi tersebut ditransmisikan dari satu sistem ke sistem lainnya. Sedangkan teknologi keamanan komputer memproteksi informasi saat informasi tersebut berada di dalam suatu sistem komputer, misalnya saja pada saat data berada di dalam database.

Sistem keamanan di VPN dapat menggunakan beberapa metode lapisan sistem kemananan, yaitu :

1. Metode Tunnelling (*terowongan*), membuat terowongan virtual jaringan publik menggunakan protocol seperti Point to Point Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), Generic Routing Encapsulation (GRE) atau IP Sec. PPTP dan L2TP adalah layer 2 tunneling protocol, keduanya 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 ke jaringan.
2. Metode Enkripsi untuk Encapsulations (*membungkus*) paket data yang lewat di dalam tunneling, data yang dilewatkan pada pembungkusan tersebut, data disini akan dirubah dengan metode algoritma kripthography tertentu seperti DES, 3DES, atau AES.
3. Metode Otentikasi User, karena banyak user yang akan mengakses biasanya digunakan beberapa metode otentikasi user seperti Remote Access Dial In User Services (RADIUS) dan Digital Certificates.
4. Integritas Data, paket data yang dilewatkan di jaringan publik perlu penjaminan integritas data/kepercayaan data apakah terjadi perubahan atau tidak. Metode VPN menggunakan HMA C-MD5 atau HMA C-SHA1 untuk menjadi paket tidak dirubah pada pengiriman.

V. Penutup

1. Dalam rangka persaingan dunia bisnis saat ini, palaksana bisnis dituntut harus dapat selalu melakukan efisiensi dalam menggunakan perluasan komunikasi.
2. VPN adalah salah satu solusi yang dapat digunakan untuk berkomunikasi dengan aman dan murah.
3. VPN merupakan suatu komunikasi antar dua jaringan yang dibuat untuk mengkoneksikan kantor pusat, kantor cabang, telecommuters, suppliers, dan rekan bisnis lainnya.
4. Sistem keamanan di VPN bisa menggunakan : Metode Tunneling, Metode Enkripsi, Metode Otentikasi User, dan Integritas Data.

Dafatr Pustaka

Anonim, 2003, VPN With Windows 2003, Microsoft

Suprapti, Iswanti, __,*Sistem Kemanan Data dengan Metode Public Key Cryptography*

Penulis
Drs. Huzainsyahnoor Aksad
Dosen PNS Kopertis Wil. XI Kalimantan
Dpk. Pada STMIK BANJARBARU