Virtual Private Network (VPN) Dynamic

Jawaban Keamanan untuk Intranet Pada Suatu Perusahaan

Tommy P.M. Hutapea
tommypm_hutapea@yahoo.com.au
http://tommy.wintersat.com

"Kepercayaan dalam suatu keterbukaan, Mengubah Lingkungan "

Dalam dunia internet dan intranet banyak sekali teknologi yang berkembang hingga saat ini baik itu dalam jaringan local maupun non local. Internet banyak digunakan perusahaan, kelompok pengguna bisnis, golongan maupun pribadi. Hal in dikarenakan saat ini masyaraka Indonesia umumnya sudah banyak menggunakan internet sebagai media informasi dan juga penyedia informasi. Terutama dalam dunia bisnis. Namun perlu disadari juga dunia intranet juga tidak kalah hebohnya dengan intranet khususnya bagi pelaku-pelaku bisanis dan para pengusaha yang meng-online kan bisnisnya dalam dunia internet. Salah satu teknologi yang digunakan dalam dunia intranet sendiri adalah VPN alias Virtual Private Network. Dalam pembahasan dibawah ini akan dijelaskan sejauh mana teknologi intranet yang menghandalkan VPN dalam menjawab suatu keamanan pada suatu perusahaan yang mempunyai cabang lebih dari satu dan sejauh mana kemampuan yang akan dihasilkan.

New Era Dunia Intranet

Intranet menjadi sebuah komponen penting dalam sistem informasi perusahaan saat ini. Sebuah intranet adalah sebuah jaringan internal pada perusahaan yang menggunakan teknologi internet untuk komunikasi dan pembagian informasi. Akses internet saat ini juga sudah menjadi kebutuhan rutin bagi hampir sebagian besar perusahaan Internet yang memberikan suatu fenomena tersendiri bagi perusahaan-perusahaan. Tingginya tingkat kebutuhan akan bisnis secara virtual dan elektronis serta akses internet ini mendorong kebutuhan akan *bandwidth* dan layanan yang lebih baik lagi dibandingkan yang sudah ada sekarang ini. Sehingga pelaku bisnis berusaha mencari layanan komunikasi yang handal, fleksibel, cepat, dengan harga yang murah untuk berbagai keperluan aplikasi yang mereka butuhkan.

Dalam rangka mengakomodasi grup-grup pengguna baru, yang berubah, dan yang meluas dan menyediakan pengguna-pengguna ini, informasi dalam berbagai cara , intranet dapat memberikan beberapa keuntungan, termasuk fleksibilitas, interoperabilitas, mudah digunakan, dan extendibility. Secara khusus, mereka sebaiknya menjadi terbuka dan berbasis standar (standard-based), sehingga informasi dapat dibaca oleh pengguna yang berbeda dengan aplikasi yang berbeda..

Namun demikian, keuntungan-keuntungan yang diharapkan dari intranet menuju pada sebuah tantangan penting untuk bisnis menggunakan teknologi ini adalah bagaimana mengembangkan dan menjaga kepercayaan dalam sebuah lingkungan yang telah didesain untuk akses informasi bebas dan terbuka. Internet tidak didesain dengan keamanan bisnis. Internet dahulu didesain oleh perguruan-perguruan tinggi sebagai sebuah jaringan terbuka dimana pengguna dapat akses, berbagi, dan menambah informasi semudah mungkin. Sebuah cara harus ditemukan untuk mengamankan sebuah intranet untuk bisnis tanpa melanggar sifat-sifat yang telah ada pada intranet. Sesungguhnya sebuah jawaban ideal harus menyediakan tidak saja tingkat keamanan tertinggi tetapi juga keamanan yang sedemikian rupa sehingga pengguna dapat dengan mudah meng-akses, mengubah, dan berbagi lebih banyak informasi, tidak lupa, dibawah kondisi-kondisi yang secara hati-hati dikendalikan dan dipelihara.

Internet Protocol Virtual Private Network (IP VPN) dapat memberikan solusi bagi berbagai persoalan yang ada. Karena dengan adanya IP VPN, hubungan yang dilakukan antara kantor pusat dan cabang serta partner bisnis perusahaan lebih ekonomis. Selain itu koneksi dengan IP-VPN tidak terbatas hanya pada hubungan antara kantor pusat dan cabang saja, tetapi IP-VPN juga memberikan keuntungan lebih dengan memberikan *security* hubungan untuk pengguna yang berpindah-pindah.

Gambar 1. Jaringan IP Virtual Private Network (VPN)

Apa dan Kenapa dengan VPN??

IP VPN merupakan tipe khusus dari layanan VPN yang mengirimkan layanan *Internet Protocol* (IP) privat melalui infrastruktur publik IP atau internet. Yang menjadi kunci patokan IP VPN adalah pengiriman layanan IP kepada end user. Dengan IP VPN dimungkinkan networking data secara privat dan aman melalui jaringan internet publik atau jaringan IP privat untuk komunikasi pengguna akses remote, *site-to-site*, atau *corporate-to-corporate*.

Platform Teknologi IP VPN

IP VPN berbasis jaringan publik yang berjalan di platform IP sehingga pengiriman layanan lebih bersifat *connectionless*, dalam artian data terkirim begitu saja tanpa ada proses pembentukan jalur terlebih dahulu (*connection setup*). IP bertugas untuk menangani masalah-masalah pengiriman, juga menjadi tanggung jawab IP untuk menangani masalah pengenalan datagram atau *reassembly* datagram sebagai akibat langsung proses fragmentasi.

Penggunaan jaringan publik internet dalam layanan VPN menuntut jaminan *security* yang lebih baik dibandingkan dengan layanan internet yang biasa. Sharing infrastruktur jaringan publik untuk suatu hal yang namanya privat menuntut pengamanan-pengamanan tersendiri. Dengan adanya jaminan *security* tersebut, pelanggan dapat mengirimkan dan mengakses informasi secara aman dan terlindung dari kemungkinan disusupi oleh pengakses yang tidak diinginkan.

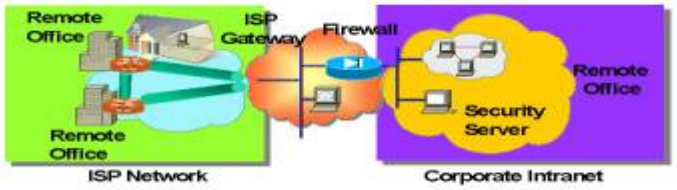
Penerapan Konfigurasi IP VPN

Casey Wilson dan Peter Doak dalam bukunya yang berjudul "*Creating and Implementing VPN*", membagi konfigurasi IP VPN yang telah diterapkan di lapangan ke dalam 3 (tiga) kategori, yaitu intranet, Extranet dan remote access ;
Dibawah ini hanya dikhususkan dalam konfigurasi intranet, sedangkan Extranet dan remote access akan dibahas dalam kesempatan yang lain.

Intranet

Intranet merupakan jaringan yang terhubung antara kantor pusat dengan kantor cabang yang tersebar di lokasi-lokasi yang terpisah dengan kantor pusat. Intranet memberikan fasilitas komunikasi dan pertukaran data serta informasi antar internal suatu perusahaan atau departemen dengan cabang yang berjauhan lokasinya.

Gambar 2. Intranet IP VPN



Kebutuhan-kebutuhan Keamanan

Dalam tantangan kepercayaan dalam sebuah lingkungan terbuka, berubah, kita akan menyelidiki kebutuhan-kebutuhan keamanan terlebih dahulu. Keamanan untuk sebuah intranet berdasarkan pada beberapa komponen hardware dan software. Teknologi dan mekanisme khusus akan bervariasi, tetapi apa yang disebut keamanan "kekuatan industri" harus selalu memenuhi lima kebutuhan dasar :

- Kerahasiaan, dengan kemampuan *scramble* atau *encrypt* pesan sepanjang jaringan yang tidak aman

- Kendali akses, menentukan siapa yang diberikan akses ke sebuah sistem atau jaringan, sebagaimana informasi apa dan seberapa banyak seseorang dapat menerima
- *Authentication*, yaitu menguji identitas dari dua perusahaan yang mengadakan transaksi
- Integritas, menjamin bahwa file atau pesan tidak berubah dalam perjalanan
- *Non-repudiation*, yaitu mencegah dua perusahaan dari menyangkal bahwa mereka telah mengirim atau menerima sebuah file

Mengakomodasi Perubahan

Sepanjang dengan keamanan "industrial-strength", sebuah intranet juga harus dapat mengakomodasi kebutuhan-kebutuhan informasi yang berubah termasuk banyak grup pengguna yang tersusun dalam banyak cara pada sebuah basis dinamis. Grup-grup pengguna mungkn termasuk pekerja-pekerja menurut departemen, jabatan, atau lokasi. Grup-grup pengguna lainnya mungkin termasuk anggota beberapa grup pada saat yang sama. Pada waktu yang sama keanggotaan dalam tiap grup berubah secara konstan sebagaimana anggota masuk atau keluar dari grup.

Sebagai tambahan, sebuah intranet harus mengakomodasi informasi dengan bentuk-bentuk berbeda, apakah halaman web, file, atau form lain. Terakhir, sebuah intranet harus mengakomodasi teknologi yang berubah dan sistem informasi kompleks yang bertambah.

Solusi : Sebuah VPN (Virtual Private Network) Dinamis

Untuk memenuhi tantangan mengembangkan dan memelihara kepercayaan dalam sebuah lingkungan yang berubah dan terbuka, TradeWave percaya bahwa strategi terbaik adalah mengimplementasikan sesuatu yang disebut Jaringan Private Virtual Dinamis (Dynamic VPN).

Secara umum, setiap VPN adalah sebuah proses dimana jaringan umum (*public network* / internet) diamankan untuk mengfungsikannya sebagaimana *private network*. Sebuah VPN tidak didefinisikan oleh rangkaian khusus atau rute. Yaitu didefinisikan oleh mekanisme keamanan dan prosedur-prosedur yang hanya mengizinkan pengguna-pengguna yang ditunjuk akses ke VPN dan informasi yang mengalir melaluinya.

VPN bukanlah hal baru. Yang membuat VPN dari *TradeWave* sesuai untuk keamanan intranet adalah kemampuan dinamisnya. Dengan dinamis, berkemampuan untuk mengakomodasi lingkungan bisnis yang terbuka dan berubah. Kemampuan ini didasarkan pada arsitektur yang unik dan set dari sifat yang terdapat pada TradeVPI, yang merupakan solusi VPN TradeWave.

Kemampuan VPN Dinamis

TradeVPI adalah sebuah himpunan aplikasi-aplikasi dan servis-servis yang berhubungan. TradeVPI memungkinkan sebuah bisnis menghasilkan dan mengeluarkan sebuah solusi VPN dinamis dengan kemampuan sebagai berikut :

- Menyediakan keamanan "industrial-strength"
- Mengakomodasi komunitas pengguna yang berubah secara dinamis
- Menyediakan kemampuan pertukaran informasi dalam berbagai bentuk form (web, file, dll)
- Mengakomodasi pengguna yang berbeda dengan berbagai macam browser, aplikasi, sistem operasi, dll
- Memungkinkan pengguna masuk ke dalam grup atau administrator memasukkan identitas dalam sebuah cara yang dikendalikan tetapi mudah
- Memelihara integritas sepanjang waktu, tanpa memperhatikan pergantian administrasi, perubahan teknologi, atau peningkatan kompleksitas sistem informasi perusahaan

Imbalan: Menggunakan Intranet untuk Bisnis

Sebuah VPN dinamis berbasis TradeVPI menawarkan bisnis, kemampuan penggunaan intranet dan teknologi internet dengan jaminan bahwa komunikasi dan transaksi akan diamankan oleh tingkat keamanan tertinggi.

Pada waktu yang sama, VPN dinamis memungkinkan bisnis mengembangkan akses informasi dan komunikasi dalam suatu cara yang dikontrol juga fleksibel. Dibandingkan dengan yang didesain terutama untuk mengunci (lock out) pengguna tertentu dengan skema keamanan terbatas atau tak fleksibel, VPN dinamis didesain untuk menyediakan tingkat tertinggi kebebasan dalam sebuah lingkungan yang aman. Sebagai contoh, sebagian besar pengguna dapat melakukan pekerjaan yang besar dengan range informasi yang besar. Karena informasi sekarang dapat tersedia dalam bentuk yang dinamis dan baik, sebuah file, data, atau dokumen perusahaan yang harus dikunci di waktu lampau, sekarang dapat diakses dalam seluruh atau sebagian oleh grup-grup pengguna yang dipilih dalam cara-cara yang ditentukan dengan tepat.

Hasilnya, VPN dinamis adalah intranet. Yang menggunakan intranet untuk menyediakan lebih banyak resource dan servis daripada sebaliknya, dengan demikian memungkinkan bisnis membuat lebih banyak penggunaan resource informasinya

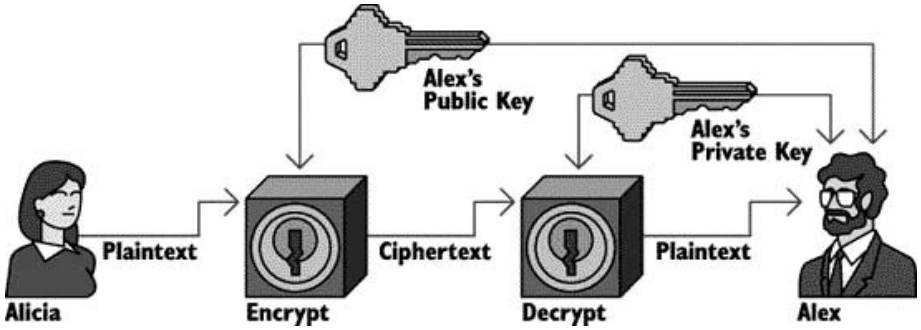
Berbicara dalam istilah bisnis, sebuah perusahaan mengimplementasi sebuah VPN dinamis dengan alasan yang sama jika mengimplementasi sebuah intranet dalam tempat pertama : fleksibel, interoperability, extendibility, mudah digunakan, dll. Sebuah VPN dinamis secara sederhana memungkinkan sebuah perusahaan menerima keuntungan intranet menjadi tingkat penuh dan sesuai. Sebaliknya, tanpa sebuah VPN dinamis, sebuah perusahaan akan tak dapat menerima keuntungan penuh dari teknologi intranet atau tak dapat menerima suatu balik modal yang sesuai dalam teknologi ini.

Metoda dan Mekanisme Keamanan

Beberapa elemen dasar dari sistem jaringan yang aman. Standard dan Mekanisme Enkripsi. Memastikan kerahasiaan pesan, enkripsi dapat ditawarkan dalam dua format yang berbeda yaitu : kunci pribadi (private key) dan kunci umum (public key). Enkripsi private-key atau symmetric-key berbasis pada sebuah kunci (atau algoritma) yang dibagi dalam dua bagian. Kunci yang sama melakukan enkrip dan dekrip pesan. Kerberos dan standar enkripsi data (DES) adalah teknologi kunci pribadi tradisional. Sebuah mekanisme private-key adalah sebuah metoda enkripsi yang telah tebukti, relatif sederhana. Masalah utama adalah dalam pembagian key : bagaimana sebuah kunci digunakan untuk keamanan dipancarkan melalui jaringan yang tidak diamankan. Kesulitan antara lain terletak pada pembangkitan, penyimpanan, dan pemancaran kunci-kunci (disebut key-management) dapat membatasi sistem private-key, khususnya melalui internet.

Pada tahun 1976, dua orang ilmuwan komputer, Whitfield Diffie dan Martin Hellman, mengembangkan sebuah teori enkripsi public-key yang menawarkan solusi masalah bagaimana mentransfer private-key. Kemudian RSA Data Security Inc., membuat sebuah algoritma yang membuat kriptografi public-key dapat dilakukan secara komersial.

Gambar 3. Enkripsi Public Key



Sebagaimana terlihat pada gambar 1, dalam sebuah solusi public-key seperti EntrustÔ dari Entrust Technologies, terdapat dua kunci (key) - sebuah private-key dan sebuah public-key yang diumumkan secara luas. Sebagai tambahan, sebuah one-time symmetric-key dibangkitkan untuk tiap transaksi. Untuk mengirim sebuah pesan pengirim, Alicia, meng-enkrip terlebih dahulu pesannya dengan menggunakan one-time symmetric-key. Kunci ini kemudian dienkripsi, menggunakan public-key dari penerima, Alex. Perlu diperhatikan bahwa sesuatu yang dienkripsi dengan public-key hanya dapat dibuka (didekrip) dengan menggunakan private-key si penerima. Ini berarti bahwa symmetric-key (yang karena itu pesan dienkrip) sekarang aman untuk transmisi lewat internet atau intranet. Ketika pesan tiba, Alex men-dekrip one-time symmetric-key dengan mennggunakan private-key kepunyaannya. Kemudian, menggunakan symmetric-key, ia men-dekrip pesan.

Keuntungan utama yang ditawarkan oleh teknologi public-key adalah bertambahnya keamanan. Walaupun lebih lambat daripada beberapa sistem private-key, enkripsi public-key secara umum lebih cocok untuk intranet untuk tiga alasan :

1. Lebih *scalable* untuk sistem yang sangat besar dengan 10 juta pengguna

2.Mempunyai alat *authentication* yang lebih fleksibel

3. Dapat mendukung tanda tangan digital

Teknologi public-key juga memungkinkan pelaksanaan non-repudiation untuk mengecek pengiriman atau penerimaan dari sebuah transaksi yang diberikan.

Sertifikat-sertifikat, Tanda Tangan Digital, dan Authentication

Dalam setiap transaksi bisnis, kedua pihak memerlukan jaminan identitas masing-masing. Kadang-kadang, authentication semudah menyediakan sebuah password. Dalam sebuah intranet, authentication dapat dilakukan dengan berbagai cara, menggunakan teknologi enkripsi yang juga digunakan untuk authentication. Teknologi ini termasuk Mekanisme Public-key Sederhana (Simple Public-key Mechanism / SPKM) yang dikembangkan Entrust Technologies, S-HTTP (Secure Hyper Text Transport Protocol) yang dikembangkan Enterprise Integration Technologies, dan SSL (Secure Sockets Layer) yang dikembangkan Netscape Communication Corporation. Tiap protokol authentication ini menggunakan algoritma RSA.

Authentication memerlukan, diantara yang lain, sebuah tanda tangan digital. Proses dimulai dengan summary matematis yang disebut "hash" yang berlaku sebagi "sidik jari" pesan. Isi pesan tak dapat diubah tanpa mengubah code hash. Kode hash ini kemudian di-enkrip dengan private-key si pengirim dan dilampirkan pada pesan tersebut. Ketika pesan telah dterima, kode hash yang dilampirkan dibandingkan dengan kode hash yang lain atau dikalkulasi summary oleh si penerima. Jika cocok, kemudian si penerima

tahu bahwa pesan tidak berubah dan integritasnya tidak berubah. Si penerima juga tahu bahwa pesan datang dari si pengirim, karena hanya si pengirim yang mempunyai private-key yang meng-enkripsi koda hash.

DSS (Digital Signal Standard) adalah sebuah standar pemerintah AS yang menyediakan jaminan integritas data dan authentication asli data. DSS juga melayani sebagaimana sebuah tanda tangan yang terikat secara legal untuk transaksi elektronik.

Kunci-kunci untuk tanda tangan digital telah di-file-kan dalam sebuah direktori public-key, terbuat dari "sertifikat-sertifikat" untuk setiap pengguna. Sertifikat-sertifikat ini seperti kartu-kartu tanda tangan dalam sebuah bank dan digunakan untuk mengecek identitas-identitas. Sebuah CA (Certification Authority) yang dipercaya, mengatur dan mendistrubusikan sertifikat-sertifikat ini, sebagai tambahan dalam untuk mendistribusikan kunci-kunci elektronik.

Daftar-daftar Kendali Akses

Acces-Control-Lists menentukan siapa yang diberikan akses ke sistem atau jaringan komputer lokal atau remote, dan juga informasi apa saja dan berapa banyak seseorang apat menerima. Sumber-sumber informasi yang berhubungan dalam jaringan dapat iorganisasikan dalam sebuah bentuk hierarki, dan Access-Control-Lists dapat juga menetapkan akses utuk pengguna-pengguna tertentu dan grup-grup pengguna tertentu.

Sebagai tambahan, mekanisme-mekanisme kendali akses dapat didistribusikan pada jaringan. Mekanisme-mekanisme tidak harus teletak pada host yang sama sebagaimana website. Ini berarti para administrator secara fisik dapat menjalankan servis-servis kendali akses pada sebuah host yang terpisah, memungkinkan banyak website menggunakan mekanisme-mekanisme kendali akses yang sama.

Threats and Control Points (Poin-poin Kendali dan Ancaman

Sekarang kita melihat beberapa elemen dasar pada keamanan jaringan. Kita melihat masalah-masalah dalam memelihara keamanan ini. Sebuah konsep kunci (key) dalam keamanan jaringan yang baik adalah gagasan dari sebuah poin kendali (control point). Sebuah poin kendali adalah suatu alat atau proses yang didesain untuk mengatasi sebuah ancaman khusus (specific threat); yang bekerja sebagaimana sebuah counter measure melawan sebuah ancaman yang ada / khusus. Sebagai contoh, sebuah kunci pintu adalah sebuah poin kendali yang dimaksudkan untuk menghalangi orang-orang yang tidak diinginkan masuk. Sebagian besar sistem keamanan berisi banyak poin kendali yang bekerja sama untuk membuat suatu paket keamanan. Dalam sebuah sistem keamanan bangunan, ada poin-poin kendali yang berbeda untuk pengeluaran badge, kode-kode keamanan, instalasi hand-scanner, kunci-kunci pintu, dan sebagainya. Keamanan dapat dikompromikan jika orang dari poin kendali sedang absen atau tidak bekerja.

Sebuah sistem keamanan jaringan dibuat berdasarkan prinsip yang sama. Seperti sistem keamanan fisik, sebuah sistem keamanan jaringan berisi sebuah himpunan poin kendali yang bekerja bersama membentuk sebuah paket keamanan yang terintegrasi.

Banyak masalah keamanan yang telah diketahui disebabkan bukan karena teknologi keamanan, tetapi karena kekuranglengkapan dalam membangun poin-poin kendali atau sebuah kegagalan dalam memelihara sebuah poin kendali dengan prosedur-prosedur dan kebijakan yang tepat.

Solusi VPN Tradisional VANS

Sebagaimana telah disebutkan di atas, VPN bukanlah hal baru. Value Added Networks (VANs), sebuah tipe VPN, telah tersedia bertahun-tahun. Sebuah VAN berdasar pada akses dial-up, leased-line, tertutup, atau khusus (private). Organisasi seperti IBM (lewat Advatis) dan General Electric Informaion Services sekarang menawarkan kemampuan EDI berdasarkan VAN. VAN menawarkan keunggulan pada transfer data cepat dan high-volume. Selain itu juga menyediakan pertukaran data ini lewat jaringan yang aman.

Pada waktu yang sama, VAN terbatas pada beberapa cara. Mereka merupakan solusi bagi owner yang membatasi pengguna pada beberpa platform software dan hardware tertentu. Selain itu juga membutuhkan koneksi dial-up atau jalur telepon dedicated, yang mungkin mahal. Sebagai tambahan, perusahaan-perusahaan harus mempunyai VAN yang sama untuk melaksanakan transaksi. Sekarang, ribuan perusahaan mempunyai VAN tetapi jumlah itu merupakan bagian kecil dari ratusan ribu perusahaan yang sekarang terhubung internet. Dua perusahaan dalam sebuah VAN juga harus menyetujui sebuah standar format EDI untuk order pembelian, catatan pengapalan, tagihan angkutan, invoice, dan form elektronik yang lain. Formating standar dapat menjadi sebuah masalah untuk satu atau kedua perusahaan jika melakukan redesain dan reorganisasi form-form yang ada.

Secara ringkas, sebuah VAN, selain terbukti merupakan platform yang aman untuk komunikasi, dapat membatasi perusahaan dalam kasus memilih rekanan bisnis dan bagaimana melakukan bisnis.

Router, Firewall, dan Router Terenkripsi

Sebuah VPN dapat berbasis pada router dan firewall. Router adalah komputer yang mengendalikan lalu lintas pada sebuah jaringan. Sebuah firewall adalah sebuah metoda yang memproteksi satu jaringan terhadap jaringan yang lain. Keduanya terletak antara jaringan internal dengan jaringan luar untuk memblok lalu lintas yang tak diinginkan. Jika pengguna mengirimka sebuah pesan, pesan tersebut mengalir melewati firewall meunju internet. Firewall akan memblok lalu lintas dari user ini jika ia tidak mempunyai izin ke internet, atau ia menggunakan protokol yang tak diizinkan.

Sebuah VPN berbasis router dan firewall dapat dibuat dalam jaringan dan lalu lintas antar jaringan. Walaupun demikian, router tak membedakan antara komunitas dan user, sehingga user pada dua jaringan harus menggunakan nama user dan password. Prosedur ini membuat sebuah logon single sangat sulit. Sebagai tambahan, nama user dan password dapat dibaca oleh orang luar, sehingga transmisi membutuhkan enkripsi.

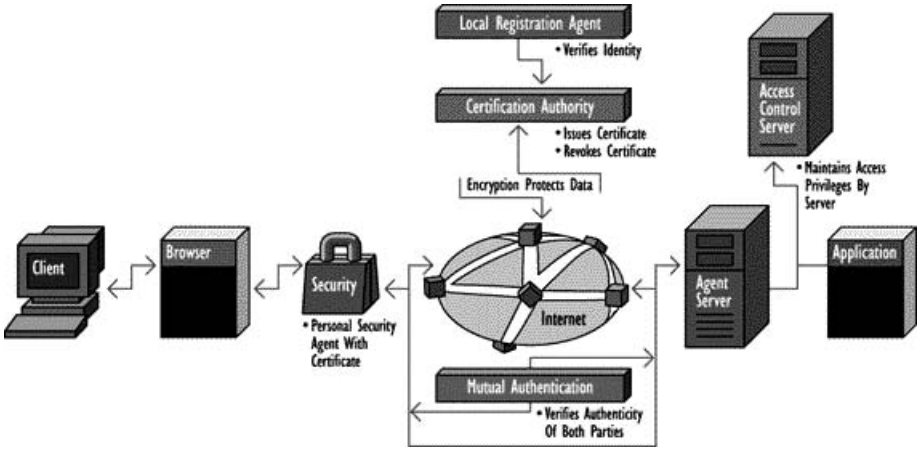
Dengan router yang terenkripsi, komunikasi dapat dilakukan antar jaringan dengan tingkat keamanan yang cukup. Sebuah sistem yang menggunakan router dan firewall tidak termasuk authentication mutual atau unilateral : seorang user tidak perlu membuktikan identitasnya di luar nama user dan password. Router juga secara khusus membagikan symmetric-key yang sama. Ini berarti keamanan dapat dikompromikan oleh seseorang dengan menggunakan key yang dicuri.

Lebih penting lagi, sebuah sistem router sangat rapuh untuk mengakomodasi grup user yang dinamis dan banyak. Tiap perubahan pada sistem sangat sulit untuk membuat dan / atau keamanan terhadap compromise.

Bagaimana TradeVPI Bekerja

VPN dinamis dari TradeWave berisi sebuah platform keamanan jaringan dan sebuah set aplikasi yang menggunakan platform keamanan tersebut. Diagram di bawah menunjukkan bagaimana bagian-bagian tersbut bekerja bersama membuat sebuah solusi VPN dinamis.

Gambar 4. Sebuah VPN Dinamis



Langkah-langkah tersebut di atas melewati bagian-bagian dari sebuah VPN dinamis dengan menggambarkan sebuah komunikasi secure HTTP (web). TradeVPI, walaupun demikian, bukan application-specific dan akan bekerja dengan aplikasi internet, sebagaimana aplikasi-aplikasi corporate-specific yang ditulis untuk menyesuaikan.

Bergabung Dengan VPN

Sebelum benar-benar menggunakan VPN, pengguna atau servis harus join pertama kali dengan registrasi CA. Sebuah corporate-employee yang dipercaya, disebut Agen Registrasi Lokal, menyetujui semua permintaan registrasi. Prosedur-prosedur keamanan yang kuat menjamin bahwa hanya user yang ditunjuk yang diregistrasi dan menerima sertifikat. CA menjamin bahwa serifikat-sertifikat yang dikembalikan diposkan dan tersedia sehingga servis dapat disangkal jika sertifikat-sertifikat ini digunakan.

Menggunakan VPN TradeWave

User dan servis mengirim dan menerima informasi secara kontinyu dalam sebuah VPN. Walaupun demikian, step-step dasar pada tiap interchange sama. Step-step berikut menggambarkan user meminta informasi dari suatu server dengan meng-klik mouse pada sebuah hyperlink.

1. User meminta (request) informasi menggunakan sebuah aplikasi desktop seperti browser internet Pertukaran informasi mulai ketika user mengirim informasi kepada user lain atau meminta informasi dari sebuah server. VPN dapat memasukkan aplikasi-aplikasi proprietary. Walaupun demikian, juga harus ditawarkan aplikasi-aplikasi yang dapat menggunakan internet, dan khususnya Worl Wide Web. Dalam hal ini user telah mengakses suatu hyperlink dalam beberapa dokumen web. Hyperlink ini, walaupun demikian, aman dan dapat diakses hanya oleh user-user yang diizinkan.
2. Aplikasi mengamankan dan mengirim pesan. Ketika client dan server mendeteksi bahwa keamanan diperlukan untuk memancarkan request dan melihat dokumen baru, mereka bekerja dalam sebuah

protocol authentication mutual. Sekali authentication terjadi, tetapi sebelum aplikasi mengirim request, dilakukan pengamanan pesan dengan meng-enkripsi-nya. Tambahan, dapat melampirkan sertifikat elektronik user atau tanda tangan. Enkripsi informasi melindungi kerahasiaan dan integritas. Tanda tangan , jika dikirmkan, akan digunakan untuk auditability. Untuk enable operability dari mekanisme-mekanisme keamanan banyak,fungsi-fungsi keamanan harus berbasis pada satndar-standar yang well-defined, seperti standar Internet Generic Security Services Application Programming Interface (GSSAPI).

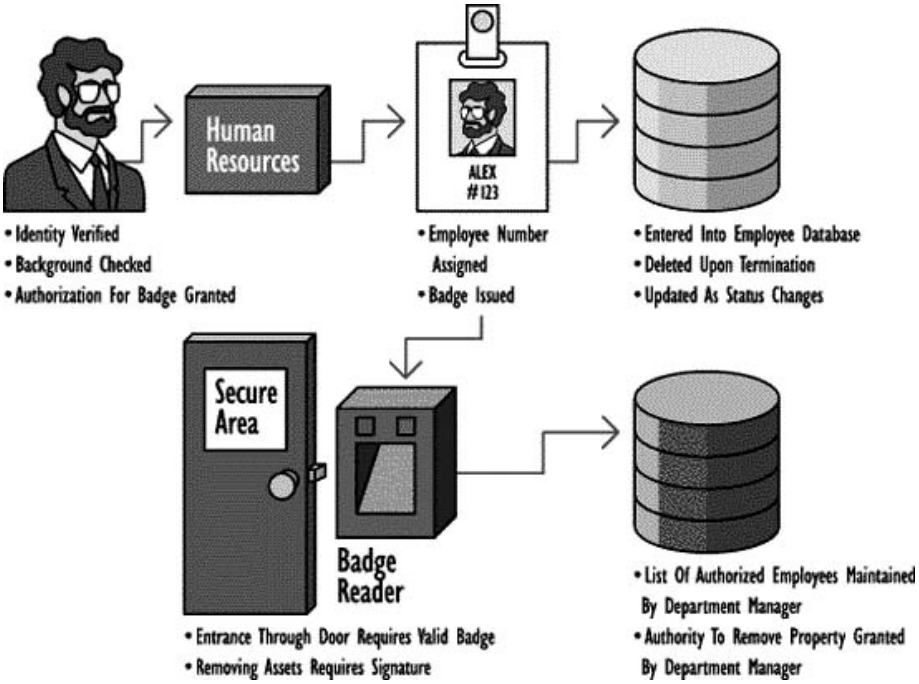
3. Pesan dipancarkan lewat Internet. Untuk request mencapai server, ia harus meninggalkan LAN, keluar ke dalam Internet, dan mencapai server pada site orang lain. Perjalanan ini mungkin melintasi satu atau lebih firewall sebelum request mencapai tujuannya. Sekali melewati firewall, request dilewatkan sepanjang jalur-jalur Internet untuk mencapai tujuan.
4. Pesan yang diterima harus lewat keamanan (security). Ketika pesan mencapai tujuan , ada kemungkinan harus melewati firewall lagi. Firewall ini akan secara hati-hati menyaring lalu lintas yang akan masuk, memastikan bahwa pesan atau obyek itu sesuai kebijakan perusahaan sebelum melewatkannya ke dalam jaringan internal. Pesan ditransfer ke server. Karena client dan server telah mengeksekusi step authentication mutual, server tahu identitas pengguna client ketika menerima request.
5. Untuk request-request, hak-hak akses user di-verify. Sebagaimana di semua jaringan perusahaan, semua user tak dapat mempunyai akses ke semua informasi perusahaan. Dalam VPN dinamis, sistem harus dapat membatasi apa yang dapat dan tidak dapat diakses oleh tiap user. Server harus menentukan apakah user mempunyai hak-hak akses untuk meminta informasi. Hal ini menggunakan suatu mekanisme kendali akses, lebih disukai suatu server terpisah. Server kendali akses membatasi akses informasi pada level dokumen. Sehingga, bahkan jika user menunjukkan sebuah sertifikat yang valid, mungkin ia akan dicegah mengakses berdasarkan kriteria (seperti kebijakan-kebijakan informasi perusahaan)
6. Informasi yang diminta, diamankan dan dikembalikan melalui Internet. Jika user mempunyai hak-hak akses pada informasi yang diminta, server informasi akan meng-enkrip informasi dan , secara optional, sertifikatnya. Kunci-kunci dikembangkan selama langkah authentication mutual digunakan meng-enkrip dan men-dekrip pesan. User sekarang mendapatkan dokumennya yang sudah diamankan.

Sebuah Analogi: sebuah Sistem Badge dan ID Pekerja

Solusi VPN TradeWave dapat dipahami sebagai ekuivalen terkomputerisasi dari sistem badge dan ID pekerja (employee). Dengan cara yang sama bahwa Human Resources atau departemen keamanan mungkin melakukan verify identitas pekerja dan melakukan assign orarng tersebut dengan sebuah nomor pekerja yang unik, sebuah VPN akan menguji identitas user dan mengeluarkan sebuah "distinguished name" yang unik yang digunakan untuk segala akses ke dan pergerakan dalam sistem. Dengan cara yang sama bahwa perusahaan terus men-track siapa saja yang mempunyai badge dan ke mana mereka dapat pergi menggunakan badge tersebut, VPN men-track, mengatur (manage), dan mengeluarkan kunci-kunci dan sertifikat-sertifikat. Sebagaimana badge-badge yang hilang dapat dikeluarkan kembali, kunci-kunci yang hilang dapat di-recovery dengan "Certification Authority".

Lebih jauh, dengan cara yang sama akses membangun atau daerah tertentu dikendalikan oleh berbagai level security clearance. VPN menngecek Access Control Lists terhadap user name dan password untuk memberi izin akses ke jaringan dan dokumen tertentu serta file. Sebagaimana pekerja meninggalkan perusahaan secara permanen akan memasukkan badge mereka, bersama kode-kode badge individual ditempatkan pada sebuah daftar user yang ditarik kembali (revoked users). Kendali akses VPN memelihara suatu daftar revoked-user dan menghalangi akses user-user ini di masa depan ke dalam sistem.

Gambar 5. Analogi Sistem Badge dan ID

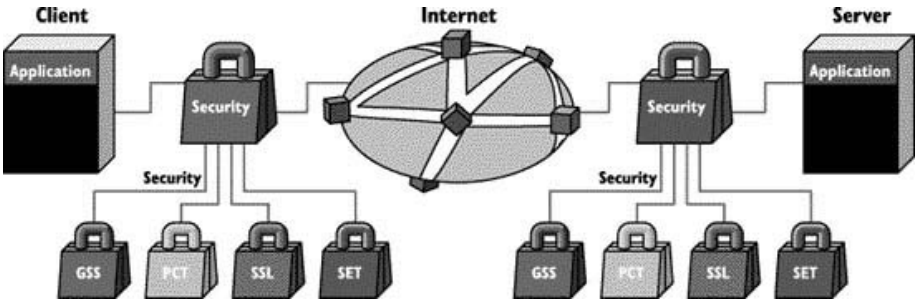


Analogi di atas tidak eksak. Sebuah PVN memotor dan mengendalikan akses informasi pada suatu basis konstan, tidak saja ketika user "enters the door". Badge-badge tidak digunakan untuk komunikasi terenkripsi, dan badge tidak menentukan atau mengendalikan tipe-tipe berbeda dari akses informasi. Walaupun demikian, analogi berguna dalam menggambarkan fakta yang dapat dihadapi VPN TradeWave dengan komunitas user yang berubah-ubah dan overlapping pada suatu basis dinamis. Analogi dapat juga mengingatkan kita bahwa enkripsi - satu dari elemen pertama yang mungkin ada dalam pikiran dalam diskusi tentang keamanan jaringan - sebenarnya hanya salah satu bagian dari solusi VPN dinamis, walaupun bagian tersebut mungkin penting. Sebuah VPN dinamis sebenarnya terdiri dari sejumlah proses kompleks termasuk kepercayaan (trust), verifikasi, manajemen, dan fungsi-fungsi lainnya - tidak saja koding den dekoding pesan.

TradeVPI Extendibilitas dan arsitektur berbasis agent

Sebuah aspek kritikal dari VPN TradeWave adalah arsitektur berbasis agen (agent-based architecture). Agent TradeWave adalah modul atau entity software stand-alone yang berkomunikasi lewat protokol standar. Karena TradeWave secara arsitektur "decoupled" agennya dari aplikasi-aplikasi lain, sebuah bisnis dapat mengubah atau meluaskan intranetnya - termasuk ekspansi melewati platform - tanpa harus merekayasa ulang sistem intranetnya. Lebih khusus lagi, arsitektur ini memungkinkan suatu bisnis memilih dan menggunakan browser apa saja, server apa saja, dan aplikasi apa saja dengan VPN dinamis.

Gambar 6. Agen Based Architecture



Agen TradeWave apat dimasukkan dengan mudah ke dalam aliran (stream) komunikasi komputer yang telah ada dengan minimalisasi gangguan pada sistem
Secara mudah menambahkan kemampuan yang tidak ada dalam sistem yang ada
Dapat di-update dengan cepat
Menggabungkan / memasukkan banyak protokol keamanan, dengan demikian mendukung sebuah sistem yang memerlukan banyak level keamanan
Arsitektur berbasis agen menyediakan sebuah solusi untuk masalah tradisional dalam sistem informasi perusahaan : konflik antara standar-standar enterprise-wide pada satu sisi dan adopsi lokal dari teknologi untuk keperluan khusus pada sisi lain. Sebuah arsitektur agent-based memungkinkan, sebagai contoh, departemen-departemen menggunakan browser-browser yang mereka inginkan tanpa mengganggu standar-standar keamanan perusahaan (enterprise-wide).

Trade Atthachés

Sebuah tambahan keuntungan dari arsitektur berbasis agent adalah kemampuan TradeVPI menggunakan berbagai module software yang disebut Trade Atthachés. Modul-modul ini dapat ditambahkan pada sistem TradeVPI untuk meningkatkan fungsionalitas dan interoperabilitas. Sebagai contoh, Trade Atthachés memungkinkan VPN meluas termasuk protokol-protokol keamanan yang berbeda tanpa mengganggu browser atau server.

Fungsi-fungsi keamanan yang baru telah tersedia dalam sistem ini. TradeVPI juga dapat mengatur beberapa Trade Atthachés keamanan secara simultan, sehingga VPN dapat mendukung platform-platform keamanan dalam waktu yang sama.

VPN Checklist

Kemampuan dan ciri-ciri yang penting dalam pengembangan sebuah solusi VPN dinamis. Kemampuan :

- Menyediakan keamanan "industrial-strength"
- Mengakomodasi komunitas user yang berubah secara dinamis
- Kemampuan bertukar informasi dalam berbagai form (web page, file, dll)
- Mengakomodasi user-user berbeda dengan browser, aplikasi, sistem operasi berbeda, dll
- Memungkinkan user bergabung dengan grup-grup atau administrator melakukan assign identitas dalam fashion yang dikendalikan tetapi sederhana
- Memelihara integritas setiap waktu, tanpa memandang pergantian administrasi, perubahan teknologi, atau peningkatan kompleksitas pada sistem informasi perusahaan

Ciri-iri khusus :

Administrasi
Update dan recovery kunci transparan

Single Sign-On

- Sebuah on-line, servis berbasis web untuk registrasi dan mengatur user dan servis-servis yang aman
- Sebuah opsi untuk membawa manajemen dan administrasi kunci in-house
- Mendukung MS mail yang aman dan cc: mail menggunakan sistem yang sama seperti yang digunakan untuk aplikasi-aplikasi web (seperti TradeAgent dengan browser atau server Microsoft atau Netscape)
- Akreditasi FIPS-PUB 140-1 dari pemerintah AS untuk software enkripsi
- Cross-certification untuk multiple Cas

Access Control

- Mekanisme kendali akses terdistribusi
- Independen aplikasi, dengan dukungan untuk sumber-sumber yang berubah yang dikendalikan akses (access controlling arbitrary resources) (dengan tambahan pada dokumen-dokumen web dan aplikasi-aplikasi CGI)
- Kendali akses berbasis authenticated-user-identities yang kuat, termasuk organizational-wildcarding
- Mendukung grup-grup user, termasuk nested-groups
- Mendukung identitas user dari banyak CA (untuk cross-certification)

Standar-standar

- mendukung tanda tangan digital DSS (DSA/SHA)
- mendukung enkripsi simetrik CAST 64-bit
- menggunakan ANSI X9.17 random number generation IETF GSSAPI-based application toolkit

Daftar Pustaka :

1. http://www.niser.org.my
2. http://www.gematel.com/Edisi30/Analisis%20Teknologi/analisis2.html
3. http://www.ipinfusion.com
4. http://www.itea.ntnu.no/sikkerhet/vpn/ - 10k
5. http://budi.insan.co.id/courses/el695/projects2002-2003/dikshie-report.pdf

Biografi dan Profil

Tommy P.M Hutapea Lahir Di Dumai, 14 September 1978. Tamat dari sekolah SMU N 1 Bukit Zin Dumai Riau Tahun 1997 dan menyelesaikan program Studi S1 Jurusan Teknik Informatika (S.Kom) Di Universitas Kristen Duta Wacana pada Tahun 2001. Saat ini menempuh Program Pasca Sarjana S2 di Di Universitas Gadjah Mada Yogyakarta pada fakultas Magister Teknologi Informasi (MTI).

Saat ini sedang bekerja pada salah satu perusahaan IT di Yogyakarta tepatnya pada PT Widya Intersat Nusantara pada bidang Jaringan Komputer dan juga sedang aktif mengajar di salah satu perguruan tinggi swasta di Yogyakarta dan sedang membimbing beberapa dosen dan mahasiswa swasta untuk bidang networking dan database. Konsentrasi Inti pada bidang Jaringan Komputer dan Network/Database Administrator dan pemograman Web (ASP), sofware House, juga aktif dalam menulis pada wahana bulanan, artikel dan dalam web pribadi yang terkoneksi pada internet dan intranet kantor.

Juga berpengalaman sebagai teknisi, lecture pada beberapa perusahan di yogyakarta (Salah Satunya PT INIXINDO) yang berhubungan dengan ilmu Komputer, Sistem Operasi (Windows NT Administrator dan Networking, Windows 2000 server dan advanced server, Novell Netware) dan Jaringan Komputer. Untuk bahasa pemograman dan database (Visual FoxPro, Delphi, ASP dan ORACLE).

Juga aktif dalam organisasi pelajar , kemahasiswaan (Koordinator LITBANG HMJTI UKDW, LITBANG Networking Universitas Kristen Duta Wacana), Litbang UKDWNetClub dan kekeluargaan (Pendiri sekaligus Ketua IMBADA UKDW Yogyakarta, Ketua OpatPusoran Yogyakarta)

Beberapa artikel pernah diterbitkan dikalangan kampus dan umun, jurnal umum, wahana ilmiah dan forum Komunikasi.

Informasi lebih lanjut mengenai penulis dapat dilihat pada :
URL http://tommy.wintersat.com
E-Mail : konsultasiit@yahoo.com.au
tommypm_hutapea@yahoo.com.au
Yahoo Messenger : tommypm_hutapea
ICQ Number : 263720662