VIRTUAL PRIVATE *NETWORK* BERBASIS IP SECURITY DENGAN LINUX FREE SECURE WIDE AREA *NETWORK.*

Muhammad Muslich, Fatah Yasin
[1]Jurusan Teknik Arsitektur, Fakultas Teknik, Universitas Muhammadiyah Surakarta
Jl. A. Yani Tromol Pos 1 Pabelan Kartasura 57102 Telp 0271 717417
amuskan@yahoo.com

Abstrak

Tujuan penelitian adalah untuk aplikasi virtual private network berbasis pada IP Security dengan Linux free S/Wan. Mekanisme kerja virtual private network berbasis pada IP Security berisi 2 bagian. Pertama, IP Seecurity protokol terintegrasi dalam sistem operasi, kedua pembangkitan dan pendistribusian protokol key melalui Internet Key Exchange. Sistem operasi yang digunakan Debian GNU atau Linux 3.0 dan perangkat lunak atau program Free S/Wan
Hasil menunjukkan Virtual Private Network IPSec hanya memperbolehkan koneksi komputer yang secure atau komputer yang hanya memiliki sertifikat yang bisa berkoneksi. IPSec membuat paket – paket yang lewat terenkripsi oleh sebuah algoritma kriptografi
Kata Kunci : *Algorit; ESP; IKE; IP Security; VPN.*

Pendahuluan

Dunia semakin sempit, itulah yang dirasa saat ini. Terlebih kehadiran Internet dan telepon seluler (ponsel) yang memungkinkan semua aktivitas dilakukan dari jarak jauh. Mulai dari komunikasi dengan keluarga, rekan kerja sampai transaksi bisnis, dapat selesai tanpa harus bertatap maka langsung. Jaringan seluler dan jalur Internet Protokol (IP) bukan lagi teknologi asing bagi masyarakat umum.

Pada umumnya perusahaan menggunakan sistem berbasis *leased lines* atau sirkuit *frame relay* untuk menghubungkan kantor pusat dengan kantor cabang yang ada, hal tersebut tidak fleksibel mengingat saat ini sebuah perusahaan biasanya ingin cepat mempunyai jaringan komunikasi dengan rekanan bisnis yang lain atau untuk mendukung karyawan yang sedang bekerja mengerjakan proyek yang bersifat lapangan dan menuntut mobilitas.

Dilihat cara pandang jaringan, salah satu masalah jaringan internet (*IP publik*) adalah tidak mempunyai dukungan yang baik terhadap keamanan. Sedangkan dari cara pandang perusahaan, IP adalah kebutuhan dasar untuk melakukan pertukaran data antara kantor cabang atau dengan rekanan perusahaan. 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.

VPN muncul untuk mengatasi persoalan tersebut. Secara umum, VPN (*Virtual Private Network*) adalah sebuah proses dimana jaringan umum (publik *network*/internet) diamankan untuk mengfungsikannya sebagaimana *private network*. Sebuah VPN tidak didefinisikan oleh rangkaian khusus atau rute, tetapi 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 ini menjadi menarik adalah dikarenakan kemampuannya untuk mengamankan Intranet dengan kedinamisannya untuk mengakomodasi lingkungan bisnis yang selalu berubah - ubah pesat.

TCP/IP (*Transmission Control Protocol /Internet Protocol*) merupakan protokol jaringan komputer terbuka dan bisa terhubung dengan berbagai jenis perangkat keras dan lunak. Protokol TCP berada pada lapisan *transport* model OSI (*Open System Interconnection*), sedangkan IP berada pada lapisan *Network* OSI (Dony Arius, 2007).

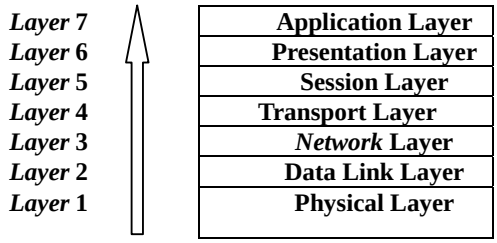
Terminologi Perangkat Jaringan

Saat merawat dan mengelola jaringan, kita akan menghadapi sejumlah istilah perangkat jaringan yang penting diketahui, antara lain : *Network Interface Card, MAC Address* dan Dua Tipe Perangkat Jaringan. Secara garis besar, perangkat jaringan dapat dikategorikan ke dalam dua tipe, yaitu *Data Communications Equipment* (DCE) dan *Data Terminal Equipment* (DTE).

Model Referensi OSI

Model referensi OSI dikembangkan oleh ISO (*International Organozation for Standardization*) sekitar tahun 1984 sebagai kerangka konseptual standar komunikasi untuk perlengkapan dan aplikasi jaringan yang diproduksi

vendor berbeda didunia. OSI menjelaskan bagaimana beragam perangkat keras dan komponen perangkat lunak dal;am komunikasi data harus berinteraksi satu sama lain. Berikut adalah model referensi OSI 7 lapisan, yang mana setiap lapisan menyediakan tipe khusus pelayanan jaringan :



Gambar 1 Tujuh *layer* OSI Model

OSI Model memiliki pembagian tugas terutama berkaitan dengan penghantaran informasi antar komputer sehingga tugas dapat lebih mudah dikelola. Tugas atau grup tugas disrahkan ke tujuh *layer* OSI dan di implementasikan secara independen. Konsep memberikan jaminan bagi setiap *layer* untuk tidak saling menginterferensi.

Tiga lapisan teratas biasa dikenal sebagai "*upper lever protokol*", sedangkan empat lapisan terbawah dikenal sebagai "*lower level protokol*". Tiap lapisan berdiri sendiri tetapi fungsi dari masing-masing lapisan bergantung dari keberhasilan operasi *layer* sebelumnya. Sebuah lapisan pengirim hanya perlu berhubungan dengan lapisan yang sama di penerima (jadi misalnya lapisan data link penerima hanya berhubungan dengan data link pengirim) selain dengan satu *layer* di atas atau dibawahnya (misalnya lapisan *network* berhubungan dengan lapisan transport diatasnya atau dengan lapisan data *link* dibawahnya).

Dasar – dasar TCP/IP

TCP/IP adalah sekumpulan protokol yang didesain untuk melakukan fungsi–fungsi komunikasi data. TCP/IP terdiri atas sekumpulan protokol yang masing–masing bertanggung jawab atas bagian–bagian tertentu dari komunikasi data. Berkat prinsip ini, tugas masing–masing protokol menjadi jelas dan sederhana. Protokol yang satu tidak perlu menegetahuui cara kerja protokol yang lain, sepanjang ia masih bisa saling mengirim dan menerima data. Berdasar penggunaan prinsip ini, TCP/IP menjadi protokol komunikasi data yang fleksibel. Protokol TCP/IP dapat diterapkan dengan mudah di setiap jenis komputer dan *interface* jaringan, karena sebagian besar isi kumpulan protokol ini tidak spesifik terhadap satu komputer atau atau peralatan jaringan tertentu. Agar TCP/IP dapat berjalan diatas interface jaringan tertentu, hanya perlu dilakukan perubahan pada protokol yang berhubungan dengan *interface* jaringan saja. Karena TCP/IP merupakan salah satu lapisan protokol OSI (*Open Sistem Interconnections*), berarti bahwa hierarki TCP/IP merujuk kepada 7 lapisan OSI tersebut.

TCP/IP didefinisikan sebagai suit *protocol* jaringan yang berperan dalam membangun *environment* jaringan global seperti Internet. *Protocol* direferensikan pula sebagai suit *protocol* **DoD** ("*dee oh dee*") atau suit *protocol Arpanet* karena TCP/IP pada dasarnya dikembangkan oleh komunitas riset *Advance Research Projects Agency (ARPA)* dari *US Departement of Defense (DoD)*.

Protokol merupakan serangkaian rule dan konvesi yang digunakan untuk menetapkan standarisasi, bahasa terstruktur untuk komunikasi. Sebagai contoh, sebuah protokol mungkin menangani pertukaran informasi diantara dua partai yang berbeda. Pada praktiknya, pertukaran data hanya dapat diselenggarakan antar komputer yang menggunakan protokol sama.

TCP (*Transmission Control Protocol*)

TCP merupakan protokol *transport* populer. TCP bekerja pada *layer* 4 (*layer* Transport) OSI *Reference Model*. Berbeda dengan UDP dan IP yang tergolong protokol "*connectionless*", TCP dikenal sebagai protokol *connection oriented*, artinya, protokol membutuhkan pembentukan koneksi terlebih dahulu (dan merawatnya) untuk menghantarkan pesan sampai terjadi proses pertukaran antarprogram aplikasi.

TCP bekerjasama dengan *Internet Protocol* (IP) untukmengirimkan data antarkomputer melintasi jaringan atau internet. Data berbentuk unit pesan. Jika IP menangani pengahantaran data,maka TCP berperan mengawasi atau menjaga track individu data (yang dikenal paket). Di sini, sebuah pesan akan dipecah menjadi beberapa bagian paket untuk efisiensi *routing*.

Ketika data yang dikirim hilang selama transit, TCP dapat mentransmisikan ulang hingga kondisi "*time out*" dicapai atau penghantaran sukses diterima.

IP (*Internet Protocol*)

IP merupakan metode yang digunakan untuk mengirim data dari satu komputer ke komputer lain melintasi jaringan. Setiap komputer (*host*) memiliki paling tidak satu *IP address* yang berguna untuk memperkenalkan dirinya ke komputer lain di Internet.

Berbeda dari TCP, IP merupakan protokol *connectionless*, yang berarti tidak ada kesepakatan koneksi terlebih

dahulu diantara *enpoint–endpoint* yang akan berkomunikasi. Setiap paket yang melintasi internet diperlakukan sebagai unit data independen, tanpa ada keterkaitan dengan unit data lainnya.

Bersama TCP, IP merupakan *jantung* protokol Internet. IP memiliki dua tanggung jawab utama, yaitu:

a. Memberikan layanan *connectionless* atas penghantaran datagram melalui *internetwork*.
b. Memberikan fragmentasi dan *reassembly* datagram untuk mendukung link data dengan ukuran *Maximum Transmission Unit* (MTU) berbeda- beda.

Layer – layer diatas *layer Network* mengambil data dan memecahnya (fragmentasi) menjadi bagian yang kecil yang disebut *packet* (paket) atau datagram. Selanjutnya, datagram secara berurutan dilepas ke *layer Network* yang merutekan mereka untuk mencapai tujuan yang tepat. Ketika semua bagian sukses mencapai tujuan, mereka dipadukan ulang (*reassembly*) oleh *layer Network* ke bentuk datagram original

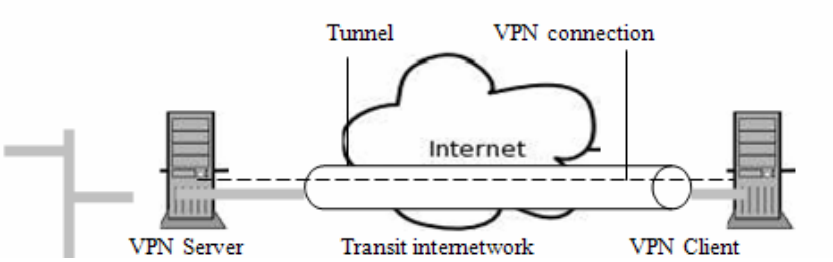
Saat mengirim atau menerima data (misalnya pesan e-mail atau halaman web), data dipecah menjadi paket – paket. Masing–masing paket akan memuat informasi *address* Internet, baik address pengirim maupun penerima. Sekumpulan protokol TCP/IP ini dimodelkan dengan empat *layer* TCP/IP.

TCP/IP terdiri atas empat lapis kumpulan protokol yang bertingkat. Keempat lapis/*layer* tersebut adalah : *Network Interface Layer*, Internet *Layer*/ *Network Layer*, Transport *Layer* /*host to host* dan *Application Layer.*

Teknologi Dasar VPN (*Virtual Private Network*)

VPN merupakan suatu cara untuk membuat jaringan bersifat *private* dan aman dengan menggunakan jaringan publik. VPN dapat mengirim data antara dua komputer yang melewati jaringan publik sehingga seolah–olah terhubung secara *point to point*. Data dienkapsulasi (dibungkus) dengan header yang berisi informasi *routing* untuk mendapatkan koneksi *point to point* sehingga data dapat melewati jaringan publik dan dapat mencapai akhir tujuan.

Sedangkan untuk mendapatkan koneksi bersifat *private*, data yang dikirimkan harus dienkripsi terlebih dahulu untuk menjaga kerahasiannya sehingga paket yang tertangkap ketika melewati jaringan publik tidak terbaca karena harus melewati proses dekripsi. Proses enkapsulasi data sering disebut *tunneling.*



Gambar 2 Koneksi VPN (*Virtual Private Network*)

Perkembangan VPN (*Virtual Private Network*)

VPN (*Virtual Private Network*) dikembangkan untuk membangun sebuah intranet dengan jangkauan yang luas melalui jaringan internet. Intranet sudah menjadi suatu komponen penting dalam suatu perusahaan dewasa ini. VPN dapat digunakan sebagai alat komunikasi oleh kantor Pusat dan kantor Cabang. Dengan dibantu perangkat lunak atau suatu alat khusus. *Virtual Private Network* atau VPN merupakan teknologi yang diterapkan pada suatu institusi atau perusahaan yang membutuhkan akses ke suatu jaringan lokal secara aman. Teknologi yang digunakan adalah internet yang kemudian diautentikasi pada server VPN untuk melakukan hubungan secara lokal terhadap server tersebut. Teknologi ini sangat tepat bagi perusahaan yang memiliki banyak cabang yang tersebar di setiap provinsi.

Sebuah VPN tidak didefinisikan oleh rangkaian khusus atau rute, namun didefinisikan oleh mekanisme keamanan dan prosedur-prosedur yang hanya mengijinkan pengguna-pengguna yang ditunjuk ke akses VPN dan informasi yang mengalir melaluinya.VPN bukanlah hal baru, yang membuat VPN ini menjadi menarik adalah dikarenakan kemampuannya untuk mengamankan Intranet dengan kedinamisannya untuk mengakomodasi lingkungan bisnis yang selalu berubah-ubah pesat.

IP VPN merupakan tipe khusus dari layanan VPN yang mengirimkan layanan Internet Protokol (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 *network*ing data secara privat dan aman melalui jaringan internet publik atau jaringan IP privat untuk komunikasi pengguna akses remote, *site-tosite*, atau *corporate-to-corporate*.

Ada empat protokol yang biasa digunakan untuk mengimplementasikan VPN di internet, yaitu:

1. *Point-to-point tunneling protocol* (PPTP)
2. *Layer-2 forwarding* (L2F)
3. *Layer-2 tunneling protocol* (L2TP)
4. *IP security protocol* (IPSec)

IPSec sudah menjadi standar dalam implementasi VPN karena cocok untuk lingkungan IP dibandingkan dengan PPTP, L2F, dan L2TP yang lebih cocok digunakan dalam multi protokol yang bukan dalam lingkungan IP

seperti NetBEUI, IPX, dan Appletalk. Selain itu enkripsi, otentifikasi, dan manajemen kunci sudah menjadi bagian yang integral dalam IPSec.

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, ***user*** dapat mengirimkan dan mengakses informasi secara aman dan terlindung dari kemungkinan disusupi oleh pengakses yang tidak diinginkan. Didalam VPN itu sendiri terdapat suatu system IPSec Tunnel yang berusaha menghubungkan antara dua *network* yang bersifat privat melalui suatu jaringan publik. Sehingga diharapkan arus informasi bersifat *secure* dan dapat dipercaya. VPN (*Virtual Private Network*) sendiri menawarkan beberapa konsep yang berhubungan dengan keamanan jaringan, diantaranya : Firewall, Authentikasi, Enkripsi dan Tunneling

IPSec (*Internet Protocol Security*)

IPSec (*IP Security*) adalah standard keamanan untuk penggunaan komunikasi berbasis Internet Protokol (IP) dengan cara enkripsi dan authentikasi semua paket IP yang lewat. IPSec menyediakan keamanan pada *level network layer*. IPSec didesain sebagai *cryptographic protocol s* yang berfungsi untuk keamanan data dan *key exchange*. Pada saat ini IPSec terdiri dari dua bagian yaitu *Encapsulating Security Payload* (ESP) yang menyediakan *authentication, data confidentiality* dan *message integrity*; *Authentication Header* (AH) menyediakan *authentication* dan *message integrity* dan tidak menyediakan *confidentiality*. Untuk sampai saat ini *key exchange protocol* sudah terdefinisikan dengan sebutan IKE (*Internet Key Exchange*) *protocol* . Untuk mengetahui implementsi dan penggunaan *protocol* IPSec yang meliputi AH. ESP, IKE, dan ISAKMP/Oakley, serta mengetahui lebih lanjut hubungan antara komponen pendukung IPSec.

IPSec merupakan kumpulan protokol, yang dikembangkan oleh IETF (*Internet Engineering Task Force*) untuk mendukung pertukaran paket yang aman melalui IP *layer.* IPSec didesain untuk menyediakan keamanan berbasis kriptografi yang memiliki karakteristik *interopable* dan berkualitas. IPSec adalah sekumpulan ekstensi dari keluarga protokol IP dan sangatlah penting untuk mengetahui bagaimana *protocol – protocol* tersebut berinteraksi satu dengan yang lainnya. IPSec menyediakan layanan kriptografi untuk keamanan transmisi data. Layanan ini termasuk *authenticity, integrity, access control, confidentiality*, dan *anti replay*. Layanan tersebut disediakan pada IP *layer* sehingga mendukung proteksi untuk IP *layer* dan *layer* lain diatasnya. Layanan IPSec mirip dengan SSL namun, IPSec melayani lapisan *network*, dan dilakukan secara transparan. Layanan tersebut dideskripsikan sebagai berikut:

a. *Confidentiality*, untuk meyakinkan bahwa sulit untuk orang lain tetapi dapat dimengerti oleh penerima yang sah bahwa data telah dikirimkan. Contoh: agar *password* tidak dapat dilihat oleh orang lain ketika *login* ke *remote server*.
b. *Integrity*, untuk menjamin bahwa data tidak berubah dalam perjalan menuju tujuan.
c. *Authenticity*, untuk menandai bahwa data yang dikirimkan memang berasal dari pengirim yang benar.
d. *Anti Replay*, untuk meyakinkan bahwa transaksi hanya dilakukan sekali, kecuali yang berwenang telah mengizinkan untuk mengulang.

Secara teknis, IPSec terdiri atas dua bagian utama. Bagian pertama mendeskripsikan dua protokol untuk penambahan *header* pada paket yang membawa *security identifier,* data mengenai *integrity control,* dan informasi keamanan lain. Bagian kedua berkaitan dengan protokol pembangkitan dan distribusi kunci. Bagian pertama IPSec adalah implementasi dua protokol keamanan yaitu :

1. AH (*Authentication header*), AH menyediakan layanan *authentication, integrity*, dan *replay protection*, namun tidak dengan *confidentiality*. AH juga melakukan pengamanan terhadap header IP.
2. ESP (*Encasulapted security payload*), ESP menyediakan layanan *authentication, integrity, replay protection*, dan *confidentiality* terhadap data. (ESP melakukan pengamanan terhadap segala sesuatu dalam paket data setelah *header*).

Implementasi IPSec

Jika membandingkan IPSec dengan internet security *protocol* lainnya, akan ditemukan perbedaan yang mendasar sesuai dengan *layer* tempat aplikasi tersebut bekerja. *Protocol* IPSec diimplementasikan kedalam *network* layer, yaitu *layer* ketiga pada model referensi OSI. *Layer* 3 (*Network layer*) akan mengerjakan layanan *network routing, flow control, segmentation / desegmentation*, dan *error control functions*.

Sedangkan *protocol* lainnya yang tersebar luas dan banyak juga digunakan seperti SSL dan TSL (Transport *Layer Security*) berjalan pada *layer* transport keatas (OSI layers 4-7). Hal ini menyebabkan IPSec lebih fleksibel dan dapat digunakan memproteksi kedua model *transport* pada *layer* diatasnya (TCP dan UDP). Tetapi hal ini juga menjadi sesuatu yang sulit diimplementasikan karena dapat meningkatkan kompleksitas dan proses yang berlebihan.

IPSec dapat diimplementasikan ke dalam *end host* atau di dalam *gateway* / *routers*. Semua itu tergantung kebutuhan dan *rule* apa yang diinginkan. Implementasi IPSec terdiri dari dua metode, yaitu :

1. Implementasi IPSec yang sudah terintegrasi dengan system operasi.
2. Implementasi IPSec dengan *vendor* (perangkat keras).

Setiap system operasi terbaru pada umumnya sudah mendukung IPSec dari yang mulai butuh *patching kernel, kompile kernel* sampai yang tinggal konfigurasi saja. Untuk IPSec yang sudah terintegrasi dengan sistem operasi akan terbentuk pada *Network* layer.

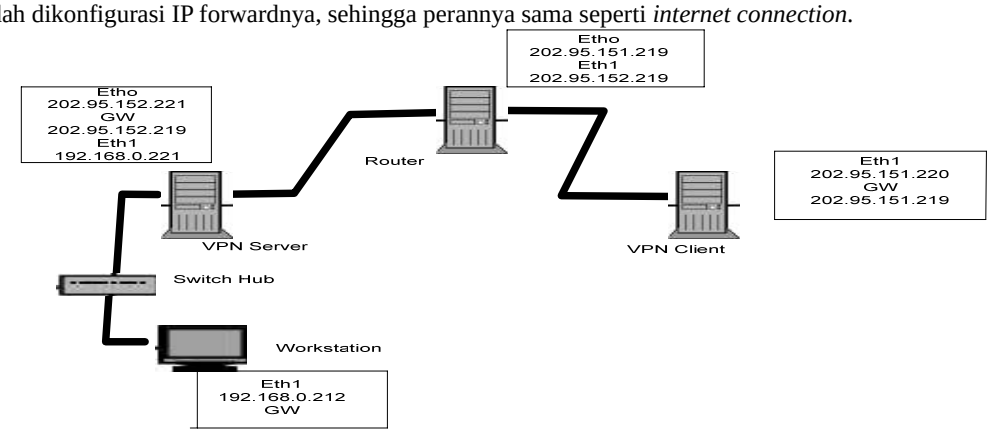
Keuntungan dari IPSec jenis tersebut adalah : terintegrasinya IPSec pada *Network* Layer, maka dengan sendirinya layanan – layanan yang berjalan pada *layer* tersebut dapat diimplementasikan dengan mudah oleh IPSec. Penerapan keamanan yang mudah per *flow* (misalkan untuk aplikasi web), dan mendukung semua mode.

Metode Penelitian

Penelitian ini membutuhkan perangkat lunak dan perangkat keras yang digunakan antara lain :

1. VPN *Server* VPN *Client*, Perangkat keras dan lunak (Pentium III 500 MHz, SDRam 256 Mb, NIC 100 Mbps, Debian Woody "Linux Kernel 2.4" dan FreeS/WAN)
2. PC *Router*, Perangkat Keras dan Lunak (Pentium III 500 Mhz, SDRam 128 Mb, NIC 100 Mbps dan MikrotikRouters OS 2.9.27)
3. *Client Windows*, Perangkat Keras dan Lunak (Pentium IV 1,8 Ghz, DDR 512 Mb, NIC 100 Mbps, Switch Hub 4 *port* dan Windows XP Professional Service Pack 2I.3 Peralatan yang dipakai)

Implementasi VPN pada penelitian ini dilakukan pada jaringan lokal. Sistem yang dibangun tidak diimplementasikan secara langsung dengan *internet connection*. Sebagai gantinya digunakan sebuah PC Router yang sudah dikonfigurasi IP forwardnya, sehingga perannya sama seperti *internet connection*.



Gambar 3 Koneksi VPN

Bagian pertama adalah implementasi protokol IPSec yang terintegrasi dalam sistem operasi. Oleh karena itu, pada implementasinya harus dipastikan bahwa opsi IPSec telah berada pada kernel dari suatu sistem operasi. Untuk IPSec yang sudah terintegrasi dengan sistem operasi akan terbentuk pada *network layer* dalam model OSI. Dengan terintegrasinya IPSec pada *network* layer, maka dengan sendirinya layanan – layanan yang berjalan pada *network layer* tersebut dapat diimplementasikan dengan mudah oleh IPSec. Penelitian ini IPSec diimplementasikan pada sistem operasi Debian GNU/Linux 3.0 dengan kernel linux 2.4.18.

Bagian kedua berkaitan dengan protokol pembangkitan dan distribusi kunci yang diimplementasikan dengan *key management* melalui mekanisme IKE (*Internet Key Exchange*). Sebelum pertukaran data secara aman terjadi, perjanjian komputer secara benar harus dilakukan. Untuk itu IETF (*Internet Engineering Task Force*) membuat standar metode perjanjian tersebut dengan nama IKE (*Internet Key Exchange*).

Hasil dan Pembahasan

Pengujian Koneksi VPN

Pengujian ini, ada dua skenario koneksi yang akan dilakukan :

1. Koneksi *host to host*, yaitu koneksi antara VPN Server dengan VPN Client.
2. Koneksi *roadwarrior – net*, yaitu koneksi jaringan dibelakang VPN Server dengan jaringan dibelakang VPN Client yang menggunakan sistem operasi Windows XP.

Analisa Jaringan

Menganalisa jaringan VPN ini, penulis menggunakan dua *tool monitoring* jaringan, yaitu : *ping* dan *tcpdump*.

Status Konfigurasi *Host to Host*

Sebelum menjalankan koneksi vpn, terlebih dahulu lihat status konfigurasi pada masing – masing titik vpn dengan ipsec barf.

1. Status Konfigurasi VPN *Server*.
   Ketikkan perintah *# ipsec barf*
   Jun 18 21:10:26 vpn-server ipsec__plutorun: Starting Pluto subsystem...
   Jun 18 21:10:27 vpn-server Pluto[243]: Starting Pluto (FreeS/WAN Version 1.96)
   Jun 18 21:10:27 vpn-server Pluto[243]: including X.509 patch (Version 0.9.9)
   Jun 18 21:10:27 vpn-server Pluto[243]: Changing to directory '/etc/ipsec.d/cacerts'
   Jun 18 21:10:27 vpn-server Pluto[243]: loaded cacert file 'cacert.pem' (1688 bytes)
   Jun 18 21:10:27 vpn-server Pluto[243]: Changing to directory '/etc/ipsec.d/crls'
   Jun 18 21:10:27 vpn-server Pluto[243]: loaded crl file 'crl.pem' (711 bytes)
   Jun 18 21:10:27 vpn-server Pluto[243]: loaded my X.509 cert file '/etc/x509cert.der' (892 bytes)
   Jun 18 21:10:27 vpn-server Pluto[243]: | from whack: got --esp=3des
   Jun 18 21:10:27 vpn-server Pluto[243]: loaded host cert file '/etc/ipsec.d/vpn.moch-muslich.com.pem' (5120 bytes)
   Jun 18 21:10:28 vpn-server Pluto[243]: loaded host cert file '/etc/ipsec.d/client.moch-muslich.com.pem' (5120 bytes)
   Jun 18 21:10:28 vpn-server Pluto[243]: added connection description "roadwarrior"
   Jun 18 21:10:28 vpn-server Pluto[243]: | from whack: got --esp=3des
   Jun 18 21:10:28 vpn-server Pluto[243]: loaded host cert file '/etc/ipsec.d/vpn.moch-muslich.com.pem' (5120 bytes)
   Jun 18 21:10:28 vpn-server Pluto[243]: loaded host cert file '/etc/ipsec.d/client.moch-muslich.com.pem' (5120 bytes)
   Jun 18 21:10:28 vpn-server Pluto[243]: added connection description "roadwarrior-net"
   Jun 18 21:10:28 vpn-server Pluto[243]: listening for IKE messages
   Jun 18 21:10:28 vpn-server Pluto[243]: adding interface ipsec0/eth0 202.95.151.200
   Jun 18 21:10:28 vpn-server Pluto[243]: loading secrets from "/etc/ipsec.secrets"
   Jun 18 21:10:28 vpn-server Pluto[243]: loaded private key file '/etc/ipsec.d/private/vpn.moch-muslich.com.key' (1744 bytes)
   + _____ date
   + date
   Wed Jun 18 21:28:47 WIT 2008
2. Status Konfigurasi VPN Client.
   Sama seperti VPN Server, ketikkan perintah *# ipsec barf*
   Jun 18 21:10:26 vpn-client ipsec__plutorun: Starting Pluto subsystem...
   Jun 18 21:10:27 vpn-client Pluto[243]: Starting Pluto (FreeS/WAN Version 1.96)
   Jun 18 21:10:27 vpn-client Pluto[243]: including X.509 patch (Version 0.9.9)
   Jun 18 21:10:27 vpn-client Pluto[243]: Changing to directory '/etc/ipsec.d/cacerts'
   Jun 18 21:10:27 vpn-client Pluto[243]: loaded cacert file 'cacert.pem' (1688 bytes)
   Jun 18 21:10:27 vpn-client Pluto[243]: Changing to directory '/etc/ipsec.d/crls'
   Jun 18 21:10:27 vpn-client Pluto[243]: loaded crl file 'crl.pem' (711 bytes)
   Jun 18 21:10:27 vpn-client Pluto[243]: loaded my X.509 cert file '/etc/x509cert.der' (892 bytes)
   Jun 18 21:10:27 vpn-client Pluto[243]: | from whack: got --esp=3des
   Jun 18 21:10:27 vpn-client Pluto[243]: loaded host cert file '/etc/ipsec.d/vpn.moch-muslich.com.pem' (5120 bytes)
   Jun 18 21:10:28 vpn-client Pluto[243]: loaded host cert file '/etc/ipsec.d/client.moch-muslich.com.pem' (5120 bytes)
   Jun 18 21:10:28 vpn-client Pluto[243]: added connection description "roadwarrior"
   Jun 18 21:10:28 vpn-client Pluto[243]: | from whack: got --esp=3des
   Jun 18 21:10:28 vpn-client Pluto[243]: loaded host cert file '/etc/ipsec.d/vpn.moch-muslich.com.pem' (5120 bytes)
   Jun 18 21:10:28 vpn-client Pluto[243]: loaded host cert file '/etc/ipsec.d/client.moch-muslich.com.pem' (5120 bytes)
   Jun 18 21:10:28 vpn-client Pluto[243]: added connection description "roadwarrior-net"
   Jun 18 21:10:28 vpn-client Pluto[243]: listening for IKE messages
   Jun 18 21:10:28 vpn-client Pluto[243]: adding interface ipsec0/eth0 202.95.151.200
   Jun 18 21:10:28 vpn-client Pluto[243]: loading secrets from "/etc/ipsec.secrets"
   Jun 18 21:10:28 vpn-clientPluto[243]: loaded private key file '/etc/ipsec.d/private/vpn.moch-muslich.com.key' (1744 bytes)
   + _____ date
   + date

Wed Jun 18 21:38:47 WIT 2008

Koneksi *Host to Host*

Sebelum memulai koneksi, aktifkan IPSec *daemon* di masing masing *host* vpn server dan vpn client. Ketikkan perintah :

 # /etc/init.d/ipsec restart
Ipsec_setup: Stopping FreeS/WAN IPsec…
IPSEC EVENT: KLIPS device ipsec0 shut down.
Ipsec_setup: Starting Frees/WAN IPsec 1.96…

Jika tidak ada pesan *error*, maka koneksi *host to host* VPN Server dengan VPN Client diaktifkan dengan perintah :

 # ipsec auto –up roadwarrior
104 "roadwarrior" #1: STATE_MAIN_I1: initiate
106 "roadwarrior" #1: STATE_MAIN_I2: sent MI2, expecting MR2
108 "roadwarrior" #1: STATE_MAIN_I3: sent MI3, expecting MR3
004 "roadwarrior" #1: STATE_MAIN_I4: ISAKMP SA established
112 "roadwarrior" #2: STATE_QUICK_I1: initiate
004 "roadwarrior" #2: STATE_QUICK_I2: sent Q12, IPsec SA established

IPsec SA established menunjukkan bahwa koneksi antara dua *host* diperbolehkan.

Test Koneksi *Host to Host*

Tcpdump digunakan untuk mengetes enkripsi paket vpn dengan cara melihat paket - paket yang lewat. *Ping* paket icmp dari vpn server ke vpn client. Jalankan tcpdump pada vpn client, kemudian lihat *output*nya.

16:11:13.584499 202.95.151.200>202.95.151.100:ESP(spi=0x127077cd,seq=0x4e)
16:11:14.584064 202.95.151.100>202.95.151.200:ESP(spi=0xc6156b29,seq=0x4f)
16:11:14.584464 202.95.151.200>202.95.151.100:ESP(spi=0x127077cd,seq=0x4f)
16:11:15.584065 202.95.151.100>202.95.152.200:ESP(spi=0xc6156b29,seq=0x50)

Hasil output vpn server, ESP (*Encapsulation Security Payload*) menunjukkan bahwa paket telah terbungkus oleh suatu algoritma enkripsi.

Matikan koneksi dengan menghentikan IPSec pada vpn server maupun vpn client.

 # /etc/init.d/ipsec stop

Ping ulang dari jaringan lokal di belakang vpn server di belakang vpn client kemudian lihat tampilan *output* pada vpn server.

17:34:15.234904 202.95.152.221>202.95.151.220:icmp echo reply
17:34:16.234624 202.95.151.220>202.95.152.221:icmp echo request (DF)
17:34:16.234846 202.95.152.221>202.95.151.220:icmp echo reply
17:34:17.234629 202.95.151.220>202.95.152.221:icmp echo request (DF)

Hasil *output* menunjukkan bahwa paket tidak terenkripsi dengan *IPSec*.

Aktifasi Koneksi Roadwarrior-Net

Menggunakan bantuan script Marcus Mueller, kolaborasi IPSec pada FreeSWAN dengan Windows XP sudah tidak menjadi masalah. *Script* tersebut bekerja dengan cara. Menjalankan *syntax - syntax* pada. *ipsecpol.exe* dan *ipseccmd.exe***.** Untuk Windows XP, aktifasi koneksi dilakukan dengan mengetikkan ipsec pada folder c:\ipsec.

Test koneksi

Setelah mengetikkan *ipsec* maka akan *verbose* (ditampilkan) parameter koneksi tersebut. Koneksi dibuat *auto start* dan langsung terkoneksi jika client mulai mengirim paket ke *server*.

Tes koneksi yang paling mudah dilakukan dengan cara mengirim paket ICMP ke jaringan di belakang vpn client.

C:\ipsec>ping 192.168.1.2 –t
Pinging 192.168.0.2 with 32 bytes of data:
Negotiating IP Security
Negotiating IP Security
Negotiating IP Security
Negotiating IP Security
Negotiating IP Security
Reply from 192.168.1.2:bytes=32 time=410ms TTL=127
Reply from 192.168.1.2:bytes=32 time=410ms TTL=127
Reply from 192.168.1.2:bytes=32 time=410ms TTL=127
Reply from 192.168.1.2:bytes=32 time=410ms TTL=127
Reply from 192.168.1.2:bytes=32 time=410ms TTL=127
Reply from 192.168.1.2:bytes=32 time=410ms TTL=127
Reply from 192.168.1.2:bytes=32 time=410ms TTL=127

Reply from 192.168.1.2:bytes=32 time=410ms TTL=127
Reply from 192.168.1.2:bytes=32 time=410ms TTL=127
Reply from 192.168.1.2:bytes=32 time=410ms TTL=127
Ping statistics for 192.168.1.1:
Packets:Sent=16, Received=10, Lost=6(37%loss)
Approximate round trip times in milli-seconds:
Minimun=347ms, Maximum=2930ms, verage=661ms

Tcpdump

Jalankan tcpdump pada vpn server, kemudian lihat *outputnya*.

 # tcpdump
16:11:13.584499 202.95.151.200>202.95.151.100:ESP(spi=0x127077cd,seq=0x4e)
16:11:14.584064 202.95.151.100>202.95.150.200:ESP(spi=0xc6156b29,seq=0x4f)
16:11:14.584464 202.95.151.200>202.95.151.100:ESP(spi=0x127077cd,seq=0x4f)
16:11:15.584065 202.95.151.100>202.95.151.200:ESP(spi=0xc6156b29,seq=0x50)

Dari hasil *output* vpn server, ESP (*Encapsulation Security Payload*) menunjukkan bahwa paket telah terbungkus oleh suatu algoritma enkripsi. Matikan koneksi dengan menghentikan IPSec pada vpn *server* maupun vpn *client*.

 # /etc/init.d/ipsec stop

Ping ulang dari jaringan lokal di belakang vpn *server* di belakang vpn *client* kemudian lihat tampilan *output* pada vpn *server*.

17:34:15.234904 202.95.152.221>202.95.151.220:icmp echo reply
17:34:16.234624 202.95.151.220>202.95.152.221:icmp echo request (DF)
17:34:16.234846 202.95.152.221>202.95.151.220:icmp echo reply
17:34:17.234629 202.95.151.220>202.95.152.221:icmp echo request (DF)

Hasil *output* menunjukkan bahwa paket tidak terenkripsi dengan *IPSec*.

Kesimpulan

VPN IPSec hanya memperbolehkan koneksi yang *secure* dalam artian komputer yang memiliki sertifikat saja yang bisa saling berkoneksi. IPSec membuat paket – paket yang lewat terenkripsi oleh sebuah algoritma kriptografi.

Daftar Pustaka

Andry Syah Putra, (2000), "*Jaringan Berbasis Linux*", Andi Offset

Aris Wendy, Ahmad SS Ramadhana,(2005), "*Membangun VPN Linux Secara Cepat"*, Andi Publisher

Betha Sidik, (2004), "*Unix dan Linux, Panduan Bekerja dalam Lingkungan Unix dan Linux*", Informatika, Bandung

Nate Carlson, "Configuring An IPSec Tunnel Beetwen Openswan And Windows 2000/XP", *www.natecarlson.com/linux/ipsec-x509.php*

Onno W. Purbo, Adnan Basamalah, Ismail Fahmi, dan Achmad Husni Thamrin, (1998), "*TCP/IP; Standar, Desain, dan Implementasi*,", Elex Media Komputindo, Jakarta

Rahmat Rafiudin, (2006), "*IP Routing dan Firewall dalam Linux*", Andi Offset

Ridwan Danjaya, SE, S.Kom, (2004), "*Membangun Jaringan Komputer dengan Linux*", Usaha Nasional Surabaya