

TUGAS AKHIR
KEAMANAN JARINGAN KOMPUTER
IMPLEMENTASI IPSEC PADA VPN



Oleh

BAMBANG ARDIYANSYAH 0805 3111 017

JURUSAN TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA

2008

IMPLEMENTASI IPSEC PADA VPN (VIRTUAL PRIVATE NETWORK)

I. Pendahuluan

1. Latar belakang

Internet telah sangat mengurangi batasan jarak dan waktu. Kini, seorang karyawan yang sedang berada jauh dari kantornya tidak perlu lagi untuk kembali ke kantor untuk sekedar mengambil data yang tersimpan pada database kantor. Dengan mengkoneksikan database kantor pada internet, karyawan tersebut yang juga terkoneksi dengan internet dapat *download* data tersebut langsung dari komputernya. Apabila karyawan tersebut dapat *download* data dari database kantor tersebut, maka memungkinkan orang lain juga dapat *download* juga. Oleh karena itu, dibuatlah berbagai macam cara agar orang yang tidak dikehendaki tidak dapat *download*, merubah ataupun menghapus data penting tersebut.

Virtual Private Network (VPN) sendiri merupakan sebuah teknologi komunikasi yang memungkinkan adanya koneksi dari dan ke jaringan publik serta menggunakannya bagaikan menggunakan jaringan lokal dan juga bahkan bergabung dengan jaringan lokal itu sendiri. Dengan menggunakan jaringan publik ini, maka *user* dapat mengakses fitur-fitur yang ada di dalam jaringan lokalnya, mendapatkan hak dan pengaturan yang sama bagaikan secara fisik kita berada di tempat dimana jaringan lokal itu berada. Hal yang perlu diingat adalah sebuah *private network* haruslah berada dalam kondisi diutamakan dan terjaga kerahasiaannya. Keamanan data dan ketertutupan transfer data dari akses ilegal serta skalabilitas jaringan menjadi standar utama dalam Virtual Private Network ini.

Virtual private network (VPN) ini juga berkembang pada saat perusahaan besar memperluas jaringan bisnisnya, namun mereka tetap dapat menghubungkan jaringan lokal (*private*) antar kantor cabang dengan perusahaan mitra kerjanya yang berada di tempat yang jauh. Perusahaan juga ingin memberikan fasilitas kepada pegawainya (yang memiliki hak akses) yang ingin terhubung ke jaringan lokal milik perusahaan di manapun mereka berada. Perusahaan tersebut perlu suatu jaringan lokal yang jangkauannya luas, tidak bisa diakses oleh sembarang orang, tetapi hanya orang yang memiliki hak akses saja yang dapat terhubung ke jaringan lokal tersebut.

Implementasi jaringan tersebut dapat dilakukan dengan menggunakan *leased line*. Namun biaya yang dibutuhkan untuk membangun infrastruktur jaringan yang luas menggunakan *leased line* sangat besar. Di sisi lain perusahaan ingin mengoptimalkan biaya untuk membangun jaringan mereka yang luas. Oleh karena itu VPN dapat digunakan sebagai teknologi alternatif untuk menghubungkan jaringan lokal yang luas dengan biaya yang relatif kecil, karena transmisi data teknologi VPN menggunakan media jaringan publik yang sudah

ada yaitu internet. Pada VPN sendiri terdapat beberapa protokol yang dapat digunakan, antara lain PPTP, L2TP, IPSec, SOCKS, CIPE. Protokol PPTP merupakan protokol awal yang dibangun oleh Microsoft. Selain menjadi dasar dari pengembangan protokol VPN selanjutnya, PPTP juga terdapat pada berbagai versi Windows, diberikan sejak Windows 95 dirilis. VPN dengan Protokol tersebut juga menawarkan solusi biaya yang murah.

2. Tujuan Penelitian

Adapun tujuan dari penelitian sebagai berikut :

1. Mengetahui dan mengerti VPN serta teknologi pendukung VPN itu sendiri
2. Mengetahui cara kerja dari VPN
3. Mengetahui cara kerja IPsec pada VPN

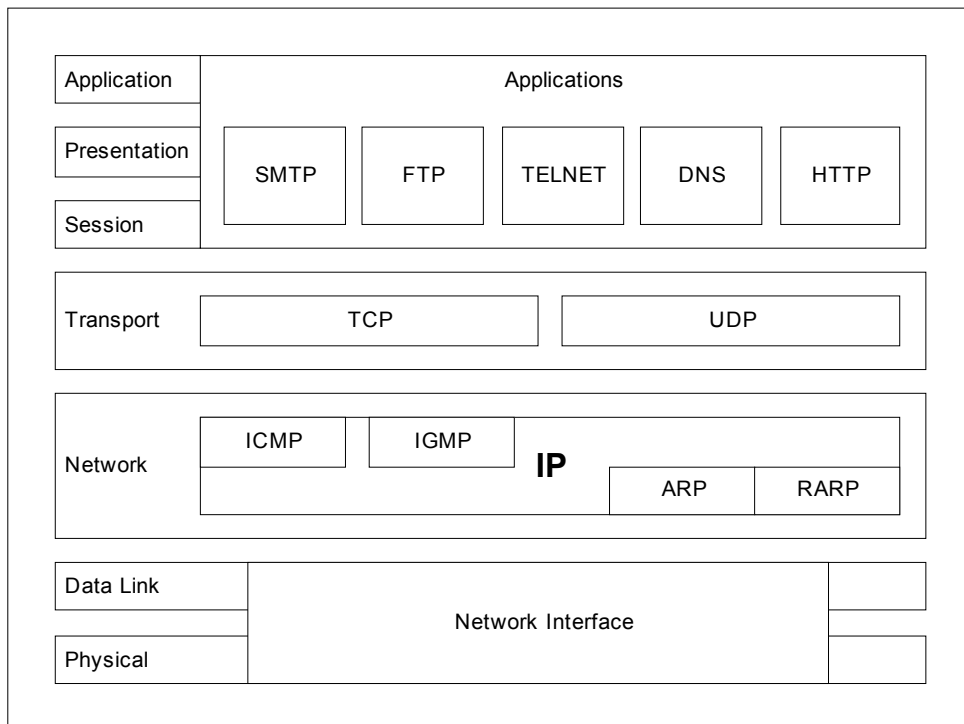
3. Metode Penelitian

Data dan informasi yang diperkukan diperoleh adalah dengan cara **studi pustaka**, yaitu dengan mengadakan pengumpulan data teoritis dari buku-buku yang mendukung penyusunan Tugas Khusus ini, serta berbagai artikel yang diperoleh dari internet.

II. Landasan Teori

TCP/IP

TCP/IP dikembangkan mengacu pada model *Open System Interconnection* (OSI), dimana, *layer-layer* yang terdapat pada TCP tidak persis sama dengan *layer-layer* yang terdapat pada model OSI. Terdapat empat *layer* pada TCP/IP, yaitu: *network interface*, *network*, *transport* dan *application*. Tiga *layer* pertama pada TCP/IP menyediakan *physical standards*, *network interface*, *internetworking*, dan fungsi *transport*, yang mengacu pada empat *layer* pertama pada model OSI. Tiga *layer* teratas dari model OSI direpresentasikan di model TCP/IP sebagai satu *layer*, yaitu *application layer*.



Gambar 1 TCP/IP dan OSI model

1. Internet Protocol Version 4 (IPv4)

IP merupakan suatu mekanisme transmisi yang digunakan oleh protokol-protokol TCP/IP, dimana IP bersifat *unreliable*, *connectionless* dan *datagram delivery service*.

Unreliable berarti bahwa protokol IP tidak menjamin datagram (Paket yang terdapat di dalam IP *layer*) yang dikirim pasti sampai ke tempat tujuan. Protokol IP hanya berusaha sebaik-baiknya agar paket yang dikirim tersebut sampai ke tujuan. Jika dalam perjalanan, paket tersebut

mengalami gangguan seperti jalur putus, kongesti pada *router* atau target *host down*, protokol IP hanya bisa menginformasikan kepada pengirim paket melalui protokol ICMP bahwa terjadi masalah dalam pengiriman paket IP. Jika diinginkan keandalan yang lebih baik, keandalan itu harus disediakan oleh protokol yang berada di atas IP *layer* misalnya TCP dan aplikasi pengguna.

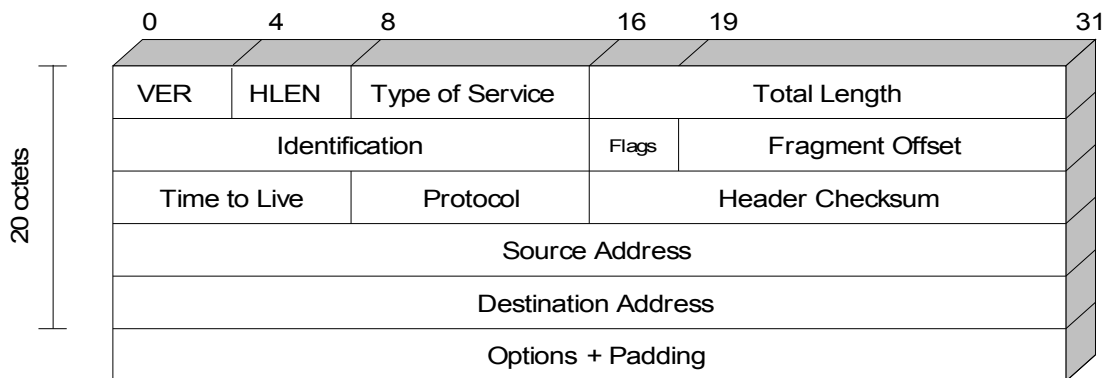
Connectionless berarti bahwa dalam mengirim paket dari tempat asal ke tujuan, baik pihak pengirim dan penerima paket IP sama sekali tidak mengadakan perjanjian terlebih dahulu (*handshake*).

Datagram delivery service berarti bahwa setiap paket yang dikirimkan tidak tergantung pada paket data yang lain. Akibatnya jalur yang ditempuh oleh masing-masing paket data bisa jadi berbeda satu dengan yang lainnya.

Pada saat ini secara umum internet masih menggunakan IP *version 4*, dimana pemakaiannya sudah semakin terbatas mengingat jumlah pengguna internet yang berkembang dengan cepat. Hal ini disebabkan oleh panjang alamat yang dimiliki IPv4 yaitu 32 bit. Pada gambar 2 di bawah ini ditunjukkan format *header* dari IPv4

Informasi yang terdapat pada *header* IP :

- *Version* (VER), berisi tentang versi protokol IP yang dipakai.
- *Header Length* (HLEN), berisi panjang *header* IP bernilai 32 bit.



Gambar 2 IPv4 Header

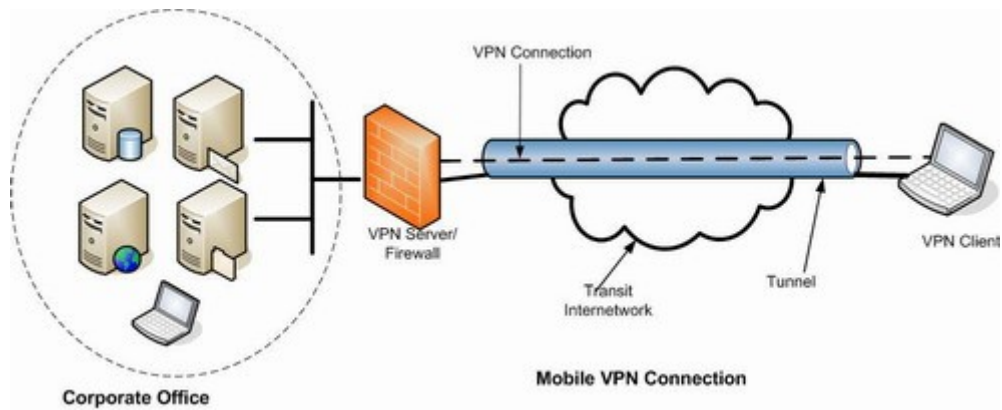
- *Type of Service* (TOS), berisi kualitas *service* cara penanganan paket IP.
- *Total Length of Datagram*, total panjang datagram IP dalam ukuran *byte*.
- *Identification*, *Flags*, dan *Fragment Offset*, berisi tentang data yang berhubungan dengan fragmentasi paket.

- *Time to Live (TTL)*, berisi jumlah *router/hop* maksimal yang boleh dilewati paket IP. Setiap kali paket IP melewati *router*, isi *field* akan dikurangi satu. Jika TTL telah habis dan paket belum sampai ke tujuan, paket akan dibuang dan *router* terakhir akan mengirimkan paket ICMP *time exceeded*.
- *Protocol*, berisi angka yang mengidentifikasi protokol *layer* atas, yang menggunakan isi data dari paket IP ini.
- *Header Checksum*, berisi nilai *checksum* yang dihitung dari seluruh *field* dari *header* paket IP. Sebelum dikirimkan, protokol IP terlebih dahulu menghitung *checksum* dari *header* paket IP tersebut untuk nantinya dihitung kembali di sisi penerima. Jika terjadi perbedaan maka paket dianggap rusak dan dibuang.
- *Source IP Address*, alamat asal/sumber.
- *Destination IP Address*, alamat tujuan.
- *Option*, mengkodekan pilihan-pilihan yang diminta oleh pengirim seperti *security label*, *source routing*, *record routing*, dan *time stamping*.
- *Padding*, digunakan untuk meyakinkan bahwa *header* paket bernilai kelipatan dari 32 bit.

Virtual Private Network

Virtual Private Network (VPN) adalah sebuah teknologi komunikasi yang memungkinkan untuk dapat terkoneksi ke jaringan publik dan menggunakannya untuk dapat bergabung dengan jaringan lokal. Dengan cara tersebut maka akan didapatkan hak dan pengaturan yang sama seperti halnya berada di dalam kantor atau LAN itu sendiri, walaupun sebenarnya menggunakan jaringan milik publik.

VPN dapat terjadi antara dua *end-system* atau dua komputer atau antara dua atau lebih jaringan yang berbeda. VPN dapat dibentuk dengan menggunakan teknologi *tunneling* dan enkripsi. Koneksi VPN juga dapat terjadi pada semua layer pada protokol OSI, sehingga komunikasi menggunakan VPN dapat digunakan untuk berbagai keperluan. Dengan demikian, VPN juga dapat dikategorikan sebagai infrastruktur WAN alternatif untuk mendapatkan koneksi *point-to-point* pribadi antara pengirim dan penerima. Dan dapat dilakukan dengan menggunakan media apa saja, tanpa perlu media *leased line* atau *frame relay*.



Gambar 3 Ilustrasi VPN

Fungsi Utama Teknologi VPN

Teknologi VPN menyediakan tiga fungsi utama untuk penggunaannya. Ketiga fungsi utama tersebut antara lain sebagai berikut.

Confidentially (Kerahasiaan)

Dengan digunakannya jaringan *publik* yang rawan pencurian data, maka teknologi VPN menggunakan sistem kerja dengan cara mengenkripsi semua data yang lewat melaluinya. Dengan adanya teknologi enkripsi tersebut, maka kerahasiaan data dapat lebih terjaga. Walaupun ada pihak yang dapat menyadap data yang melewati internet bahkan jalur VPN itu sendiri, namun belum tentu dapat membaca data tersebut, karena data tersebut telah teracak. Dengan menerapkan sistem enkripsi ini, tidak ada satupun orang yang dapat mengakses dan membaca isi jaringan data dengan mudah.

Data Integrity (Keutuhan data)

Ketika melewati jaringan internet, sebenarnya data telah berjalan sangat jauh melintasi berbagai negara. Pada saat perjalanan tersebut, berbagai gangguan dapat terjadi terhadap isinya, baik hilang, rusak, ataupun dimanipulasi oleh orang yang tidak seharusnya. Pada VPN terdapat teknologi yang dapat menjaga keutuhan data mulai dari data dikirim hingga data sampai di tempat tujuan.

Origin Authentication (Autentikasi sumber)

Teknologi VPN memiliki kemampuan untuk melakukan autentikasi terhadap sumber-sumber pengirim data yang akan diterimanya. VPN akan melakukan pemeriksaan terhadap semua data yang masuk dan mengambil informasi dari sumber datanya. Kemudian, alamat sumber data tersebut akan disetujui apabila proses autentikasinya berhasil. Dengan demikian, VPN menjamin semua data yang dikirim dan diterima berasal dari sumber yang seharusnya. Tidak ada data yang dipalsukan atau dikirim oleh pihak-pihak lain.

Non-repudiation

Yaitu mencegah dua perusahaan dari menyangkal bahwa mereka telah mengirim atau menerima sebuah file mengkomodasi Perubahan.

Kendali akses

Menentukan siapa yang diberikan akses ke sebuah sistem atau jaringan, sebagaimana informasi apa dan seberapa banyak seseorang dapat menerima.

Perangkat VPN

Pada dasarnya, semua perangkat komputer yang dilengkapi dengan fasilitas pengalamatan IP dan diinstal dengan aplikasi pembuat *tunnel* dan algoritma enkripsi dan dekripsi, dapat dibangun komunikasi VPN di dalamnya. Komunikasi VPN dengan *tunneling* dan enkripsi ini dapat dibangun antara sebuah *router* dengan *router* yang lain, antara sebuah *router* dengan beberapa *router*, antara PC dengan *server* VPN *concentrator*, antara *router* atau PC dengan *firewall* berkemampuan VPN, dan masih banyak lagi.

Teknologi Tunneling

Teknologi *tunneling* merupakan teknologi yang bertugas untuk menangani dan menyediakan koneksi *point-to-point* dari sumber ke tujuannya. Disebut *tunnel* karena koneksi *point-to-point* tersebut sebenarnya terbentuk dengan melintasi jaringan umum, namun koneksi tersebut tidak mempedulikan paket-paket data milik orang lain yang sama-sama melintasi jaringan umum tersebut, tetapi koneksi tersebut hanya melayani transportasi data dari pembuatnya. Hal ini sama dengan seperti penggunaan jalur *busway* yang pada dasarnya menggunakan jalan raya, tetapi dia membuat jalur sendiri untuk dapat dilalui bus khusus.

Koneksi *point-to-point* ini sesungguhnya tidak benar-benar ada, namun data yang dihantarkannya terlihat seperti benar-benar melewati koneksi pribadi yang bersifat *point-to-point*.

Teknologi ini dapat dibuat di atas jaringan dengan pengaturan *IP Addressing* dan *IP Routing* yang sudah matang. Maksudnya, antara sumber *tunnel* dengan tujuan *tunnel* telah dapat saling berkomunikasi melalui jaringan dengan pengalamatan IP. Apabila komunikasi antara sumber dan tujuan dari *tunnel* tidak dapat berjalan dengan baik, maka *tunnel* tersebut tidak akan terbentuk dan VPN pun tidak dapat dibangun.

Apabila *tunnel* tersebut telah terbentuk, maka koneksi *point-to-point* palsu tersebut dapat langsung digunakan untuk mengirim dan menerima data. Namun, di dalam teknologi VPN, *tunnel* tidak dibiarkan begitu saja tanpa diberikan sistem keamanan tambahan. *Tunnel* dilengkapi dengan sebuah sistem enkripsi untuk menjaga data-data yang melewati *tunnel* tersebut. Proses enkripsi inilah yang menjadikan teknologi VPN menjadi aman dan bersifat pribadi.

Teknologi Enkripsi

Teknologi enkripsi menjamin data yang berlalu-lalang di dalam *tunnel* tidak dapat dibaca dengan mudah oleh orang lain yang bukan merupakan komputer tujuannya. Semakin banyak data yang lewat di dalam *tunnel* yang terbuka di jaringan publik, maka teknologi enkripsi ini semakin dibutuhkan. Enkripsi akan mengubah informasi yang ada dalam *tunnel* tersebut menjadi sebuah *ciphertext* atau teks yang dikacaukan dan tidak ada artinya sama sekali apabila dibaca secara langsung. Untuk dapat membuatnya kembali memiliki arti atau dapat dibaca, maka dibutuhkan proses dekripsi. Proses dekripsi terjadi pada ujung-ujung dari hubungan VPN. Pada kedua ujung ini telah menyepakati sebuah algoritma yang akan digunakan untuk melakukan proses enkripsi dan dekripsinya. Dengan demikian, data yang dikirim aman sampai tempat tujuan, karena orang lain di luar *tunnel* tidak memiliki algoritma untuk membuka data tersebut.

Jenis implementasi VPN

Remote Access VPN

Pada umumnya implementasi VPN terdiri dari 2 macam. Pertama adalah *remote access* VPN, dan yang kedua adalah *site-to-site* VPN. *Remote access* yang biasa juga disebut *virtual private dial-up network* (VPDN), menghubungkan antara pengguna yang *mobile* dengan *local area network* (LAN).

Jenis VPN ini digunakan oleh pegawai perusahaan yang ingin terhubung ke jaringan khusus perusahaannya dari berbagai lokasi yang jauh (*remote*) dari perusahaannya. Biasanya perusahaan yang ingin membuat jaringan VPN tipe ini akan bekerjasama dengan *enterprise service provider* (ESP). ESP akan memberikan suatu *network access server* (NAS) bagi perusahaan tersebut. ESP juga akan menyediakan *software* klien untuk komputer-komputer yang digunakan pegawai perusahaan tersebut.

Untuk mengakses jaringan lokal perusahaan, pegawai tersebut harus terhubung ke NAS dengan men-*dial* nomor telepon yang sudah ditentukan. Kemudian dengan menggunakan *software* klien, pegawai tersebut dapat terhubung ke jaringan lokal perusahaan.

Perusahaan yang memiliki pegawai yang ada di lapangan dalam jumlah besar dapat menggunakan *remote access* VPN untuk membangun WAN. VPN tipe ini akan memberikan keamanan, dengan mengenkripsi koneksi antara jaringan lokal perusahaan dengan pegawainya yang ada di lapangan. Pihak ketiga yang melakukan enkripsi ini adalah ISP.

Site-to-site VPN

Jenis implementasi VPN yang kedua adalah *site-to-site* VPN. Implementasi jenis ini menghubungkan antara 2 kantor atau lebih yang letaknya berjauhan, baik kantor yang dimiliki

perusahaan itu sendiri maupun kantor perusahaan mitra kerjanya. VPN yang digunakan untuk menghubungkan suatu perusahaan dengan perusahaan lain (misalnya mitra kerja, *supplier* atau pelanggan) disebut **ekstranet**. Sedangkan bila VPN digunakan untuk menghubungkan kantor pusat dengan kantor cabang, implementasi ini termasuk jenis **intranet site-to-site** VPN.

Ada empat buah protocol yang biasa dan sering digunakan dalam pengimplementasian VPN(Virtual Private Network).

1. *Ipssec (Ip Security Protocol)*
2. *Layer-2 Forwarding*
3. *Layer-2 Tunneling Protocol (L2TP)*
4. *Point to Point Tunneling Protocol*

IPSEC

IPsec merupakan suatu set ekstensi protokol dari *Internet Protocol (IP)* yang dikeluarkan oleh *Internet Engineering Task Force (IETF)*. IPsec didesain untuk menyediakan interoperabilitas, kualitas yang baik, sekuriti berbasis kriptografi untuk IPv4 dan IPv6. layanan yang disediakan meliputi kontrol akses, integritas hubungan, otentifikasi data asal, proteksi jawaban lawan, kerahasiaan (enkripsi), dan pembatasan aliran lalu lintas kerahasiaan. Layanan-layanan ini tersedia dalam IP layer, memberi perlindungan pada IP dan layer protokol berikutnya. *IP Security* menyediakan sederet layanan untuk mengamankan komunikasi antar komputer dalam jaringan. Selain itu juga menambah integritas dan kerahasiaan, penerima jawaban optional (penyortiran jawaban) dan otentifikasi data asal (melalui manajemen kunci SA), *IP Security* juga menyediakan kontrol akses untuk lalu lintas yang melaluinya. Tujuan-tujuan ini dipertemukan dengan dipertemukan melalui penggunaan dua protokol pengamanan lalu lintas yaitu *AH (Authentication Header)* dan *ESP (Encapsulating Security Payload)* dan dengan penggunaan prosedur dan protokol manajemen kunci kriptografi. Jika mekanisme ini diimplementasikan sebaiknya tidak merugikan pengguna, host dan komponen internet lainnya yang tidak mengganggu mekanisme ini untuk melindungi lalu lintas data mereka. Mekanisme ini harus fleksibel dalam menggunakan algoritma keamanan, maksudnya yaitu modul ini dapat menggunakan algoritma sesuai dengan pilihan tanpa mempengaruhi komponen implementasi lainnya. Penggunaan algoritma defaultnya harus dapat memfasilitasi interoperabilitas dalam internet pada umumnya. Penggunaan algoritma ini dalam hubungannya dengan proteksi lalu lintas (*IPSec traffic protection*) dan protokol manajemen kunci (key management protocols), bertujuan memperbolehkan sistem dan pengembang aplikasi untuk meningkatkan kualitas yang tinggi, internet layer, teknologi keamanan berbasis kriptografi.

IPSec protokol yang dikombinasikan dengan algoritma *default*-nya didesain untuk menyediakan keamanan lalu lintas internet yang baik. Bagaimanapun juga keamanan yang diberikan oleh protokol ini sebenarnya bergantung pada kualitas dari implementasi, yang mana implementasi ini diluar lingkup dari standarisasi ini. Selain itu keamanan sistem komputer atau jaringan adalah fungsi dari banyak faktor, meliputi individu, fisik, prosedur, sumber kecurigaan dan praktek keamanan komputer dalam dunia nyata. IPSec hanya salah satu komponen dari arsitektur sistem keamanan. Keamanan yang didapat dari pemakaian IPSec bergantung pada lingkungan operasi dimana implementasi IPSec dijalankan. Sebagai contoh kerusakan dalam keamanan sistem operasi.

IPsec merupakan suatu set ekstensi protokol dari *Internet Protocol* (IP) yang dikeluarkan oleh *Internet Engineering Task Force* (IETF). Istilah dari IPsec mengacu pada suatu set dari mekanisme yang didesain untuk mengamankan trafik pada level IP atau pada *network layer*. Teknologi dari IPsec ini didasari oleh teknologi modern dari kriptografi, dimana layanan keamanan yang disediakan antara lain yaitu[4]:

Confidentiality : Untuk menjamin kerahasiaan dimana sulit bagi pihak yang tidak berwenang untuk dapat melihat atau mengerti kecuali oleh penerima yang sah bahwa data telah dikirimkan.

Integrity : Untuk menjamin bahwa data tidak berubah dalam perjalanan menuju tujuan.

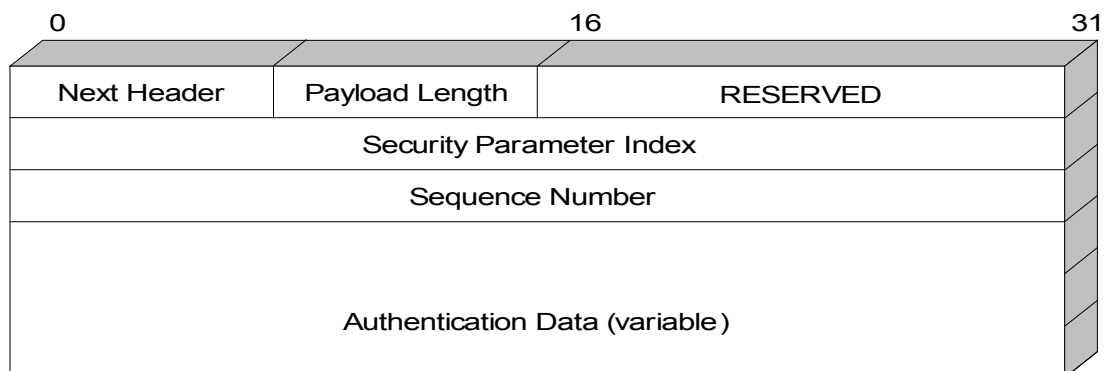
Authenticity : Untuk menjamin bahwa data yang dikirimkan memang berasal dari pengirim yang benar.

Anti Reply : Untuk menjamin bahwa transaksi hanya dilakukan sekali, kecuali yang berwenang telah mengizinkan untuk mengulang transaksi.

Terdapat dua protokol yang berjalan di belakang Ipsec, yaitu:

- *Authentication Header* (AH), menyediakan layanan *authentication, integrity, replay protection* pengamanan pada *header* IP, namun tidak menyediakan layanan *confidentiality*[5].

Berikut ini adalah gambar paket *header* dari AH.

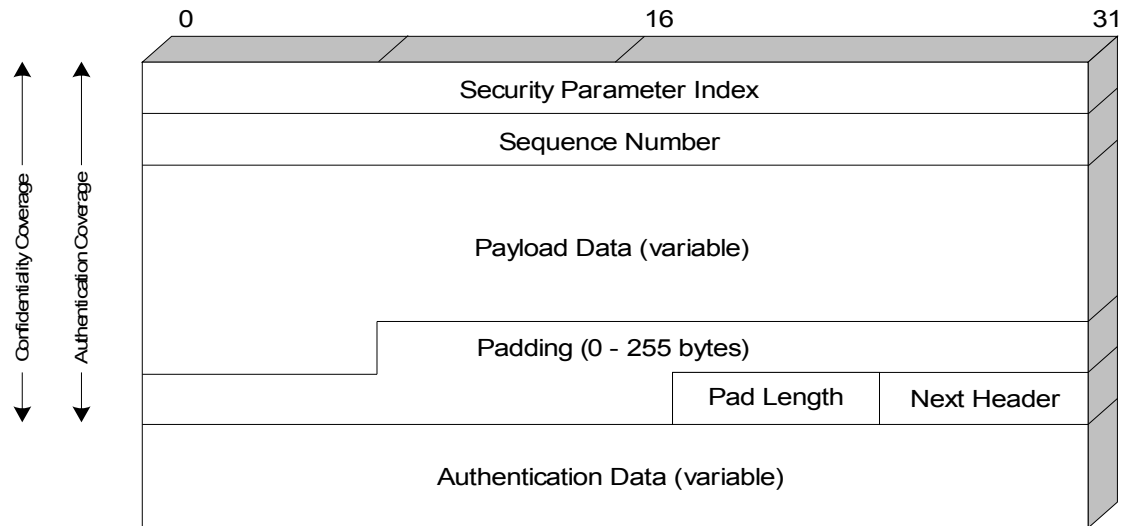


Authentication Header (AH) Packet Header

- *Encapsulating Security Payload* (ESP), menyediakan layanan *Authentication, integrity, replays*

protection dan *confidentiality* terhadap data (ESP melakukan pengamanan data terhadap segala sesuatu dalam paket data setelah *header*)[6].

Berikut ini adalah gambar paket *header* dari ESP.



Gambar 4 Encapsulating Security Payload (ESP) Packet Header

1. Arsitektur IPsec

Perkembangan arsitektur IPsec mengacu pada pokok persoalan yang terdapat pada RFC. Terdapat tujuh bagian utama pada gambar 5 yang dapat digunakan untuk mendefinisikan keseluruhan arsitektur dari IPsec.

- **Architecture**

Mencakup konsep secara umum, definisi, kebutuhan keamanan, dan mekanisme yang mendefinisikan teknologi dari IPsec.

- **Encapsulating Security Payload (ESP)**

Menyediakan layanan kerahasiaan data dengan enkripsi, enkapsulasi, dan secara opsional yaitu autentikasi.

- **Authentication Header (AH)**

Menyediakan mekanisme untuk autentikasi data sumber dan layanan *connectionless data integrity* untuk paket IP.

- **Encryption Algorithm**

Menyediakan bermacam-macam algoritma enkripsi yang digunakan oleh ESP.

- **Authentication Algorithm**

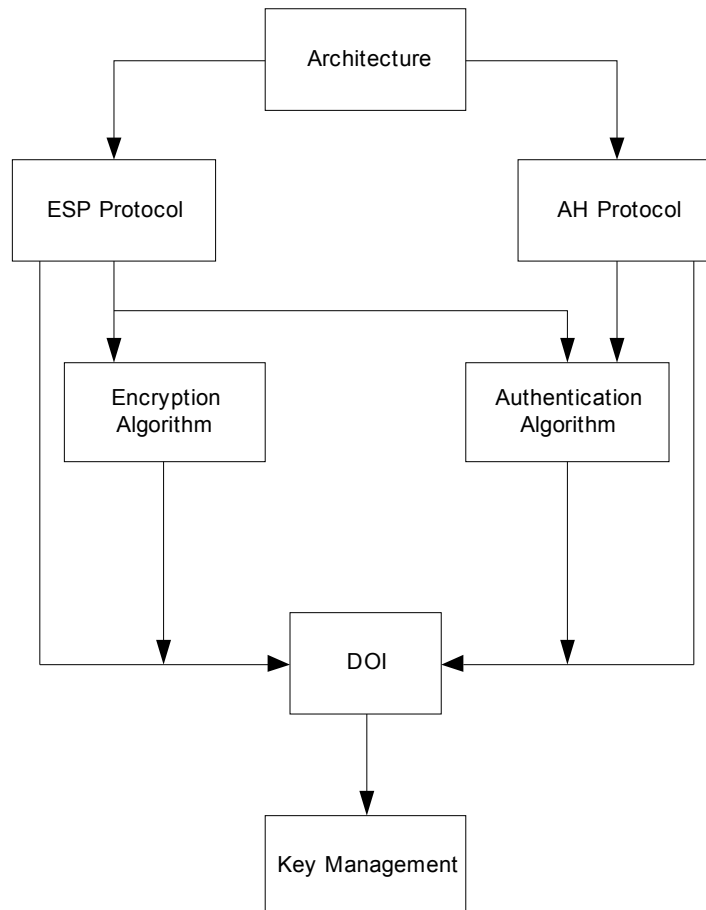
Menyediakan algoritma autentikasi yang digunakan oleh AH dan secara opsional digunakan pula oleh ESP.

- **Domain of Interpretation (DOI)**

Mendefinisikan format *payload*, pertukaran tipe dan konvensi untuk penamaan terhadap informasi keamanan yang relevan. DOI juga mengandung nilai-nilai yang dibutuhkan untuk menghubungkan bagian satu dengan yang lainnya.

- **Key Management**

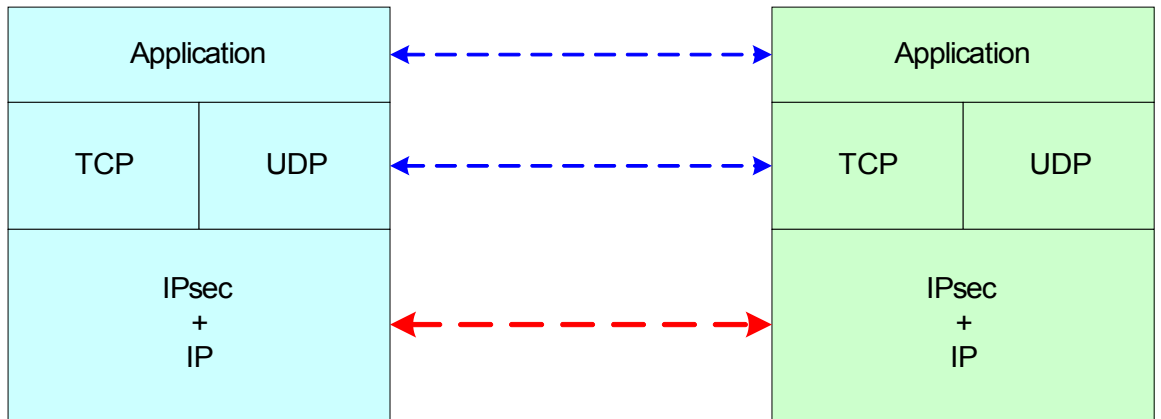
Mengandung dokumen yang menggambarkan bermacam-macam skema dari manajemen pertukaran kunci.



Gambar 5 Secure IP Documentation Overview

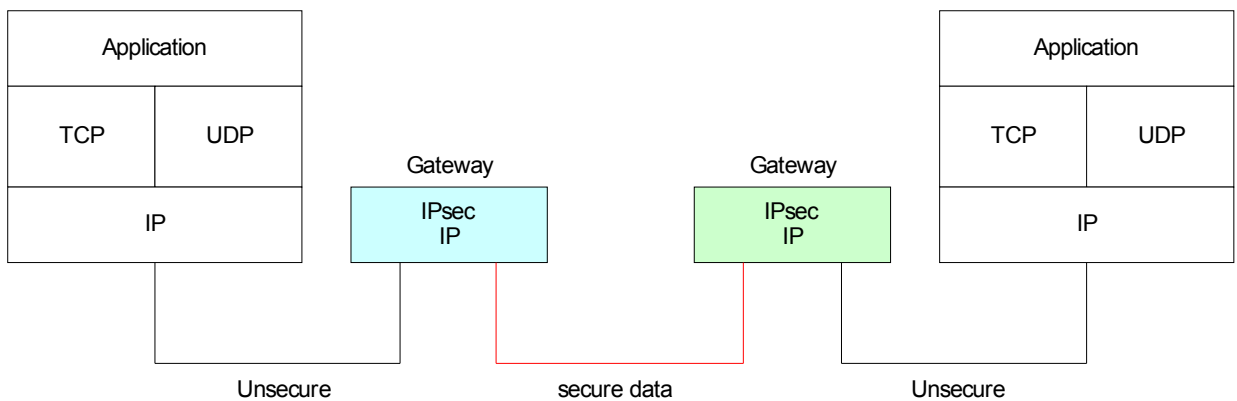
2. IPsec Modes

Terdapat dua mode dalam implementasi dari IPsec. Mode pertama yang digunakan yaitu *transport mode*. Secara umum mode ini digunakan untuk komunikasi *end-to-end* antar dua *host*. Contohnya komunikasi *client-server*.



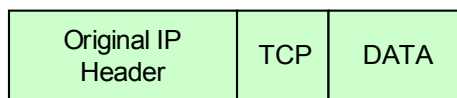
Gambar 6 *Transport Mode IPsec*

Mode implementasi kedua dari IPsec yaitu *tunnel mode*. *Tunnel mode* menyediakan proteksi untuk keseluruhan paket IP. Seperti terlihat pada Gambar 7, dimana *gateway* mengenkapsulasi keseluruhan paket, termasuk *original header* dari IP, kemudian menambahkan *header IP* baru pada paket data, lalu mengirimkannya ke jaringan publik menuju *gateway* yang kedua, dimana informasi akan di dekripsi dan bentuk asli informasi akan sampai ke penerima.

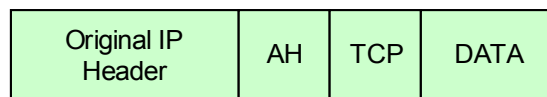


Gambar 7 *Tunnel Mode Ipsec*

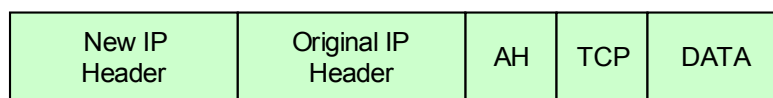
Implementasi AH pada IP diperlihatkan pada gambar di bawah ini:



Gambar 8 Paket IP sebelum diimplementasikan AH

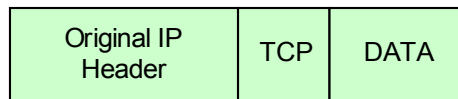


Gambar 9 *Transport Mode dan AH*

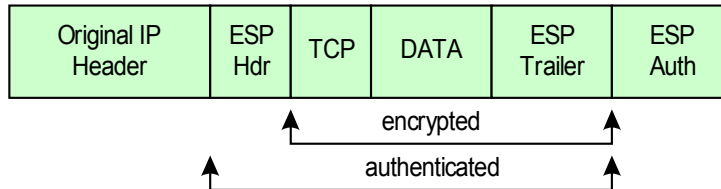


Gambar 10 *Tunnel Mode dan AH*

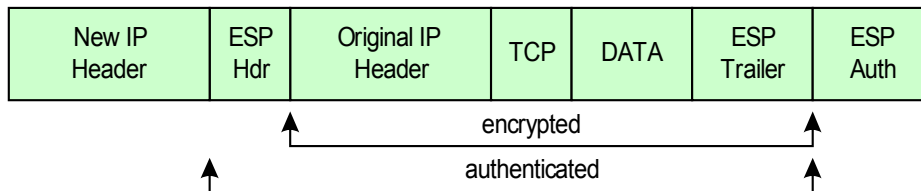
Implementasi ESP pada IP diperlihatkan pada gambar di bawah ini[6]:



Gambar 11 Paket IP sebelum diimplementasikan ESP



Gambar 12 *Transport Mode* dan ESP



Gambar 13 *Tunnel Mode* dan ESP

Security Association

Bagian ini akan menjelaskan kebutuhan manajemen untuk implementasi Ipv6 dan implementasi Ipv4 yang mengimplementasikan AH, ESP atau keduanya. Konsep “Security Association” adalah pokok dari IPsec. Semua implementasi dari AH dan ESP harus mendukung konsep Security Association seperti yang dijelaskan dibawah. Bagia terakhir menguraikan berbagai aspek manajemen Security Association, mendefinisikan manajemen kebijakan SA yang diperlukan, proses lalulintas, dan teknik manajemen SA.

Definisi dan ruang lingkup

Security Association adalah suatu hubungan simplex yang menghasilkan layanan keamanan lalulintas yang dibawahnya. Layanan keamanan ini dihasilkan oleh SA dengan penggunaan AH atau ESP tapi bukan penggunaan keduanya. Jika proteksi AH dan ESP diterapkan dalam aliran lalulintas, kemudian dua tau lebih SA di-create untuk menghasilkan proteksi dalam aliran lalulintas. Untuk mengamankan komunikasi dua arah antara dua Host, atau antara dua security gateway maka dibutuhkan dua SA (satu di masing-masing arah).

Security Association secara unik dikenali dari tiga komponen yaitu Security Parameter Index (SPI), alamat tujuan IP dan protokol keamanan (AH atau ESH). Nilai SPI mencakup nilai

1 sampai 255 yang ditetapkan oleh IANA (Internet Assigned Number Authority) untuk penggunaan dimasa yang akan datang. Nilai SPI nol (0) ditetapkan untuk penggunaan implementasi khusus lokal dan tidak dikirim lewat kabel. Sebagai contoh implementasi manajemen kunci mempunyai nilai SPI nol yang berarti tidak ada Security Association selama periode ketika implementasi IPSec telah meminta bahwa entitas manajemen kunci tersebut menetapkan SA baru, tetapi SA belum masih belum ditetapkan. Pada prinsipnya, alamat tujuan merupakan unicast address, IP broadcast address atau multicast group address. Bagaimanapun mekanisme manajemen SA IPSec saat ini hanya didefinisikan untuk SA unicast. Oleh karena itu, untuk diskusi pemaparan selanjutnya SA dideskripsikan utamanya untuk komunikasi point-to-point, meskipun konsepnya dapat diaplikasikan untuk kasus komunikasi point-to-multipoint.

Seperti telah dituliskan dibagian sebelumnya didefinisikan dua tipe SA yaitu mode transport dan mode tunnel. SA mode transport adalah SA antara dua Host. Dalam kasus dimana link security ingin digunakan antara dua sistem intermediate sepanjang path mode transport juga dapat digunakan antara dua security gateway. Dalam kasus terbaru mode transport juga digunakan untuk mensupport IP-in-IP atau GRE tunneling melalui SA mode transport. Catatan bahwa fungsi kontrol akses merupakan bagian yang penting dari IPSec secara signifikan dibatasi dalam konteks ini. Sehingga penggunaan mode transport harus dievaluasi secara hati-hati sebelum digunakan. Dalam Ipv4, header protokol keamanan mode transport terlihat setelah header IP dan beberapa pilihan lain dan sebelum protokol layer yang lebih tinggi (seperti TCP atau UDP) dalam Ipv6, header protokol keamanan terlihat setelah header base IP dan ekstensionnya, tetapi mungkin juga terlihat sebelum atau sesudah pilihan tujuan dan sebelum protokol layer yang lebih tinggi. Dalam kasus ESP SA mode transport menyediakan layanan keamanan hanya untuk protokol layer yang lebih tinggi darinya, tidak untuk IP header atau ekstension header yang mendahului ESP header. Dalam kasus untuk AH, proteksi juga ditambahkan ke bagian yang dipilih dari IP header, bagian yang dipilih dari ekstension header dan option pilihan (yang terdapat pada header Ipv4, Hop-by-Hop ekstension header Ipv6, atau ekstension header tujuan pada Ipv6).

SA mode tunnel sebenarnya adalah SA yang diaplikasikan di IP tunnel. Dengan hanya sepasang pengecualian, kapan saja ujung manapun dari SA adalah Security gateway, SA harus mode tunnel. SA diantara dua security gateway pada dasarnya adalah SA mode tunnel seperti SA antara Host dan Security Gateway. Catatan bahwa dalam kasus dimana lalu lintas ditujukan untuk security gateway seperti SNMP commands, security gateway berlaku sebagai Host dan mode transport diperbolehkan. Tapi dalam kasus tersebut security gateway tidak berlaku sebagai gateway. Seperti tertulis diatas security gateway mungkin mendukung mode transport untuk menyediakan link (Hubungan) keamanan. Dua Host dapat menyusun sebuah mode tunnel antara mereka. Kebutuhan untuk transit traffic SA meliputi security gateway untuk menjadi SA

tunnel mengacu ke kebutuhan untuk menghindari problem potensial dengan memperhatikan fragmentasi dan penyusunan ulang dari paket IPSec dan dalam keadaan dimana path yang banyak (melalui security gateway yang berbeda) menuju ke tujuan yang sama dibelakang security gateway.

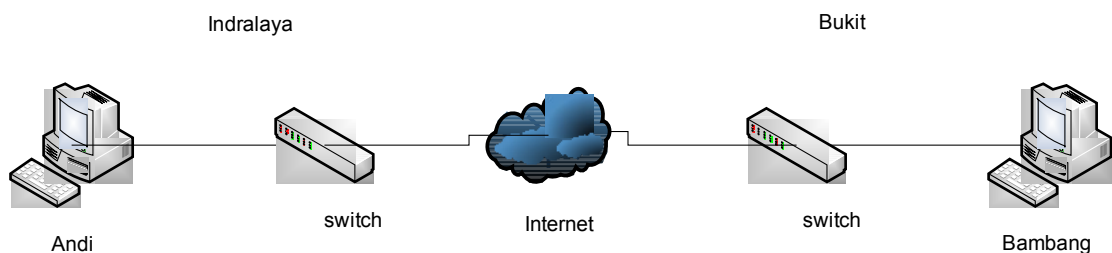
Untuk SA mode tunnel ada header IP luar yang menspesifikasikan pemrosesan tujuan IPSec ditambah dengan header IP dalam yang menunjukkan tujuan terakhir dari paket tersebut. Header protokol keamana terlihat setelah header IP luar dan sebelum header IP dalam. Jika AH diterapkan dalam mode tunnel bagian header IP luar diperoleh proteksi seperti halnya paket IP yang disalurkan (semua header IP dalam diproteksi seperti halnya layer protokol yang lebih tinggi). Jika ESP diterapkan proteksi dikerjakan hanya pada paket yang disalurkan tidak pada header luar.

III. PEMBAHASAN

Cara kerja IPsec dapat dibagi dalam lima tahap, yaitu:

1. Memutuskan menggunakan IPsec antara dua titik akhir di internet
2. Mengkonfigurasi dua buah *gateway* antara titik akhir untuk mendukung IPsec
3. Inisialisasi *tunnel* IPsec antara dua *gateway*
4. Negosiasi dari parameter IPsec/IKE antara dua *gateway*
5. Mulai melewati data

Untuk lebih jelasnya berikut ini diberikan contoh langkah demi langkah IPsec antara Bambang yang berada di kota Bukit dan Andi yang berada di kota Indralaya



Gambar 14 Hubungan IPsec Andi dan Bambang

Langkah-langkah hubungan tersebut diuraikan sebagai berikut:

1. Indralaya mengkonfigurasi IPsec dengan BUKIT
2. BUKIT mengkonfigurasi IPsec dengan INDRALAYA
3. Andi mengirimkan data kepada Bambang
4. INDRALAYA mengenali bahwa data tersebut harus diamankan
5. INDRALAYA memulai IKE dengan *peer* di BUKIT
6. INDRALAYA menawarkan algoritma enkripsi, algoritma hash (untuk otentifikasi), metode
7. INDRALAYA membangkitkan bilangan acak, '*nonce*', dan mengirimkannya bersama kunci *public* ke BUKIT
8. BUKIT menggunakan kunci *public* INDRALAYA untuk mendekrip *nonce* yang telah dienkrip dan kemudian memverifikasi Bukita ke INDRALAYA
9. INDRALAYA menggunakan kunci *private* untuk menandatangani *nonce* dan mengirimkannya

kembali ke BUKIT

10. BUKIT menggunakan kunci *private* untuk menandatangani *nonce* dan mengirimkannya kembali ke INDRALAYA
11. INDRALAYA menggunakan kunci *public* untuk mendekrip *nonce* yang dienkrip kemudian memverifikasi ke BUKIT
12. BUKIT menggunakan kunci *public* INDRALAYA untuk mendekrip *nonce* yang dienkrip kemudian memverifikasi ke INDRALAYA
13. INDRALAYA memulai *quick mode negotiation* dengan BUKIT dengan membangkitkan dan mengirimkan *security parameter index* (SPI) → sudah dijelaskan pada landasan teori
14. BUKIT memverifikasi bahwa SPI belum digunakan olehnya dan mengkonfirmasi bahwa INDRALAYA dapat menggunakan SPI tersebut, sambil BUKIT juga mengirimkan SPI miliknya sendiri ke INDRALAYA.
15. INDRALAYA mengkonfirmasi SPI milik BUKIT dan mengirimkan alamat dari *host* Andi yang akan menggunakan IPsec SA
16. BUKIT mengkonfirmasi ke INDRALAYA bahwa dapat mendukung IPsec untuk Andi dan sekaligus mengirimkan alamat *host* Bambang ke BUKIT
17. INDRALAYA mengkonfirmasi ke BUKIT bahwa dapat mendukung IPsec untuk Bambang dan mengirimkan atribut IPsec (umur SA dan algoritma enkripsi ke BUKIT)
18. BUKIT memverifikasi bahwa atribut IPsec yang dikirimkan INDRALAYA dan membangun pasangan SA IPsec (*inbound dan outbound*) untuk Bambang untuk berbicara kepada Andi
19. INDRALAYA menerima konfirmasi atribut IPsec BUKIT dan membangun pasangan SA
20. IPsec (*inbound dan outbound*) untuk Andi untuk berbicara kepada Bambang
21. Tunnel terbentuk

Secara umum IPsec mempunyai kompleksitas yang cukup besar. IPsec terlalu banyak memiliki *options* dan terlalu banyak memiliki fleksibilitas . Ada cukup banyak cara untuk melakukan hal yang sama dalam IPsec, sebagai akibat dari para *developer* IPsec yang mencoba mendukung berbagai macam situasi dengan *options* yang berbeda-beda. Akibat kompleksitas tersebut muncul potensi kelemahan dan menyulitkan analisis keamanan terhadap IPsec.

Hal kedua yang perlu mendapat perhatian adalah dokumentasi. Dokumentasi IPsec sangat sulit dimengerti. Tidak ada pendahuluan, pembaca harus sedikit demi sedikit secara perlahan memahami dokumentasi IPsec. Salah satu contoh dokumentasi IPsec yang sulit dimengerti adalah spesifikasi ISAKMP.

Dokumentasi IPsec tidak menyebutkan tujuan secara eksplisit. Tanpa tujuan yang eksplisit tidak ada standar analisis yang tepat untuk keamanan data melalui IPsec. Kekurangan spesifikasi IPsec juga menyulitkan pengguna untuk menggunakan IPsec, ada banyak *prerequisites* yang tidak disebutkan secara eksplisit dalam dokumentasi IPsec. Seorang desainer jaringan yang mencoba menggunakan

IPsec tanpa mengetahui dengan jelas dokumentasi serta *prerequisites* yang tidak utuh akan menghasilkan fungsi IPsec yang tidak optimal atau dengan kata lain tidak mencapai tujuan keamanan yang diharapkan. Perlu diingat bahwa **"Hampir aman sama dengan tidak aman"**

V. KESIMPULAN

Pada tulisan ini telah dibahas sebelumnya mengenai VPN, IPSec, cara kerja IPSec, *key management*, dan evaluasi terhadap IPSec. Dari yang sudah dibahas sebelumnya ada beberapa fakta penting yaitu IPSec sebagai dasar untuk VPN, selama ini memang menjadi standar untuk pengamanan transmisi data, Sementara itu fakta yang lain menunjukkan bahwa ada beberapa kelemahan IPSec yaitu berkaitan dengan masalah kompleksitas, yang dikhawatirkan akan menyebabkan ambiguitas, kontradiksi, inefisiensi, dan sumber kelemahan.

Secara umum ada empat komponen dalam VPN internet: jaringan internet, *security gateways*, *security policy*, dan *key management*. Jaringan internet menyediakan infrastruktur komunikasi data untuk VPN. *Security gateways* berdiri antara jaringan *public* dan *private*, mencegah intrusi yang tidak berhak kedalam jaringan *private*. *Security gateways* juga menyediakan layanan *tunneling* dan enkripsi data sebelum ditransmisikan ke jaringan *public*. Secara detail *security gateway* untuk VPN meliputi kategori: router, firewall, hardware khusus VPN yang terintegrasi, dan perangkat lunak VPN.

Kesimpulan yang dapat ditarik dari makalah ini adalah:

1. Untuk VPN sebaiknya menggunakan *tunnel mode* dengan protokol ESP dan melakukan enkripsi, dan menggunakan pertukaran kunci secara otomatis untuk pengamanan maksimum pada transmisi data.
2. Bagi perusahaan yang ingin mengaplikasikan IPSec (VPN) perlu merumuskan terlebih dahulu dengan jelas mengenai fungsi dan tujuan keamanan transmisi data yang ingin dicapai, agar pemilihan perangkat keras, perangkat lunak, dan spesifikasi IPSec yang ada dapat memenuhi kriteria yang diinginkan perusahaan tersebut.

DAFTAR PUSTAKA

1. <http://www.ipsec-howto.org/ipsec-howto>
2. www.cert.or.id/~budi/courses/
3. <http://linto.jmn.net.id>
4. www.budi.insan.co.id/courses/ec7010/dikmenjur/
5. Thomas, Tom. 2005. Network Security First step. Penerbit Andi, Yogyakarta.
6. Thomas, Tom. 2005. Computer Networking First-step, Computer Networking First-step. Penerbit Andi, Yogyakarta.