BAB II

LANDASAN TEORI

UNIT PELAKSANA TEKNIS PERPUSTAKAAN UNIKOM

2.I Informasi

Sumber dari informasi adalah data. Data merupakan bentuk jamak dari bentuk tunggal data-item. Data adalah kenyataan yang menggambarkan suatu kejadian-kejadian dalam satu kesatuan yang nyata. Kejadian adalah sesuatu yang terjadi pada waktu tertentu.

Informasi adalah data yang telah diolah menjadi suatu bentuk yang penting bagi penerima dan mempunyai nilai nyata yang dapat digunakaan untuk pengambilan keputusan untuk masa sekarang maupun masa datang. Informasi merupakan proses lebih lanjut dari data dan mempunyai nilai tambah.

Kualitas dari informasi tergantung dari beberapa hal, yaitu:

a. *Lengkap*, artinya informasi yang diterima pemakai tidak boleh terpotong – terpotong.
b. *Akurat*, artinya informasi harus terbebas dari kesalahan-kesalahan dan tidak bias atau menyesatkan atau dengan kata lain didefinisikan sebagai perbandingan dari informasi yang benar dengan jumlah seluruh informasi yang dihasilkan pada satu proses pengolahan data tertentu. .
c. *Relevan*, artinya informasi tersebut mempunyai manfaat bagi pemakainya.
d. *Tepat Waktu*, artinya informasi yang datang kepada penerima tidak boleh terlambat, informasi yang sudah usang tidak akan berguna lagi. Informasi merupakan landasan bagi pengambilan keputusan maka jika

terjadi keterlambatan dapat berakibat fatal bagi perusahaan atau organisasi itu sendiri.

Dewasa ini mahalnya nilai informasi disebabkan harus cepatnya informasi tersebut didapat, sehingga diperlukan teknologi-teknologi untuk mendapatkan mengolah dan mengirimkannnya.

2.2 Jaringan Komputer

Jaringan komputer adalah sebuah kumpulan komputer, printer dan peralatan lainnya yang terhubung dalam satu kesatuan. Informasi dan data bergerak melalui kabel-kabel atau tanpa kabel sehingga memungkinkan pengguna jaringan komputer dapat saling bertukar dokumen dan data, mencetak pada printer yang sama dan bersama-sama menggunakan hardware/software yang terhubung dengan jaringan.

Setiap komputer, printer atau periferal yang terhubung dengan jaringan disebut **node**. Sebuah jaringan komputer dapat memiliki dua, puluhan, ribuan atau bahkan jutaan node.

Adapun ciri-ciri jaringan komputer adalah :

1. Berbagi perangkat keras (hardware).
2. Berbagi perangkat lunak (software).
3. Berbagi saluran komunikasi (internet).
4. Berbagi data dengan mudah.
5. Memudahkan komunikasi antar pemakai jaringan.

2.2.1 Local Area Network (LAN)

Local Area Network (LAN), merupakan jaringan milik pribadi didalam sebuah gedung atau kampus yang berukuran sampai beberapa kilometer. LAN

seringkali digunakan untuk menghubungkan komputer-komputer pribadi dan *workstation* dalam kantor suatu perusahaan atau pabrik-pabrik untuk memakai bersama sumberdaya *(resouce*, misalnya printer) dan saling bertukar informasi.

Secara garis besar terdapat dua tipe jaringan atau LAN, yaitu jaringan *Peer to Peer* dan jaringan *Client-Server*. Pada jaringan peer to peer, setiap komputer yang terhubung ke jaringan dapat bertindak baik sebagai *workstation* maupun *server*. Sedangkan pada jaringan *Client-Server*, hanya satu komputer yang bertugas sebagai *server* dan komputer lain berperan sebagai *workstation*.

2.2.2 Metropolitan Area Network (MAN)

Metropolitan Area Network (MAN), pada dasarnya merupakan versi LAN yang berukuran lebih besar dan biasanya menggunakan teknologi yang sama dengan LAN.

MAN dapat mencakup kantor-kantor perusahaan yang letaknya berdekatan atau juga sebuah kota dan dapat dimanfaatkan untuk keperluan pribadi (swasta) atau umum. MAN mampu menunjang data dan suara, bahkan dapat berhubungan dengan jaringan televisi kabel.

2.2.3 Wide Area Network (WAN)

Wide Area Network (WAN), jangkauannya mencakup daerah geografis yang luas, seringkali mencakup sebuah negara bahkan benua. WAN terdiri dari kumpulan mesin-mesin yang bertujuan untuk menjalankan program-program (aplikasi) pemakai.

2.2.4 Internet

Sebenarnya terdapat banyak jaringan didunia ini, seringkali menggunakan perangkat keras dan perangkat lunak yang berbeda-beda . Orang yang terhubung

ke jaringan sering berharap untuk bisa berkomunikasi dengan orang lain yang terhubung ke jaringan lainnya. Keinginan seperti ini memerlukan hubungan antar jaringan yang seringkali tidak kompatibel dan berbeda. Biasanya untuk melakukan hal ini diperlukan sebuah mesin yang disebut ***gateway*** guna melakukan hubungan dan melaksanakan terjemahan yang diperlukan, baik perangkat keras maupun perangkat lunaknya.

Internet merupakan gabungan komunikasi antar jaringan komputer, yang menggunakan satelit sebagai sarana penghubungnya sehingga membuat sistem informasi dapat berkomunikasi secara global. *Internet* adalah sekumpulan jaringan yang berlokasi tersebar di seluruh dunia yang saling terhubung membentuk satu jaringan besar komputer, sehingga sesama pemakai komputer dapat saling menukar data, pesan, dan informasi dengan pemakai komputer lainnya.

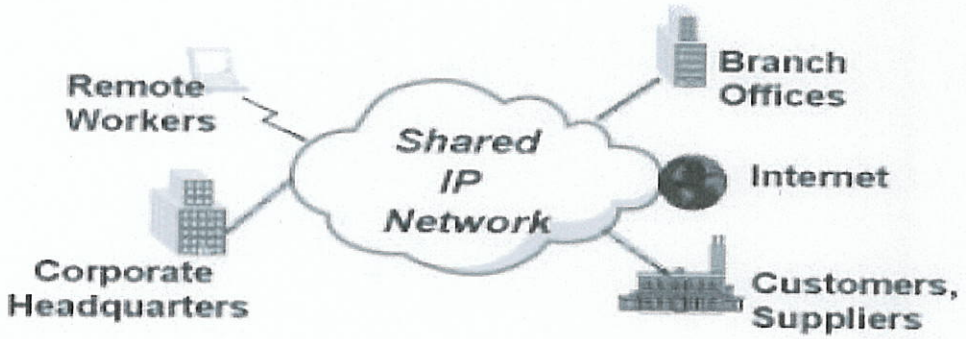
2.3 Virtual Private Network

Virtual Private Network (VP) adalah jaringan data privat yang menggunakan infrastruktur telekomunikasi umum, seperti jaringan Internet publik, dengan memanfaatkan *protokol tunneling* dan sekuriti demi keamanan data. VPN merupakan pilihan yang ekonomis bagi suatu perusahaan yang ingin memiliki jaringan privat sendiri. Pada VPN, data dikirimkan dalam bentuk *terenkripsi*, sehingga kecil kemungkinannya untuk disadap oleh pihak lain. Protokol standar bagi enkripsi ini adalah *Point-to-Point Tunneling Protocol (PPTP).*

Virtual private network (VPN) 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 dimana pun 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 diatas tersebut dapat dilakukan dengan menggunakan *leased line*. Namun biaya yang dibutuhkan untuk membangun infrastuktur 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 (mis. internet).



Gambar 2.1 Topologi jaringan VPN

2.3.1 Jenis implementasi 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 remote access, intranet, Extranet

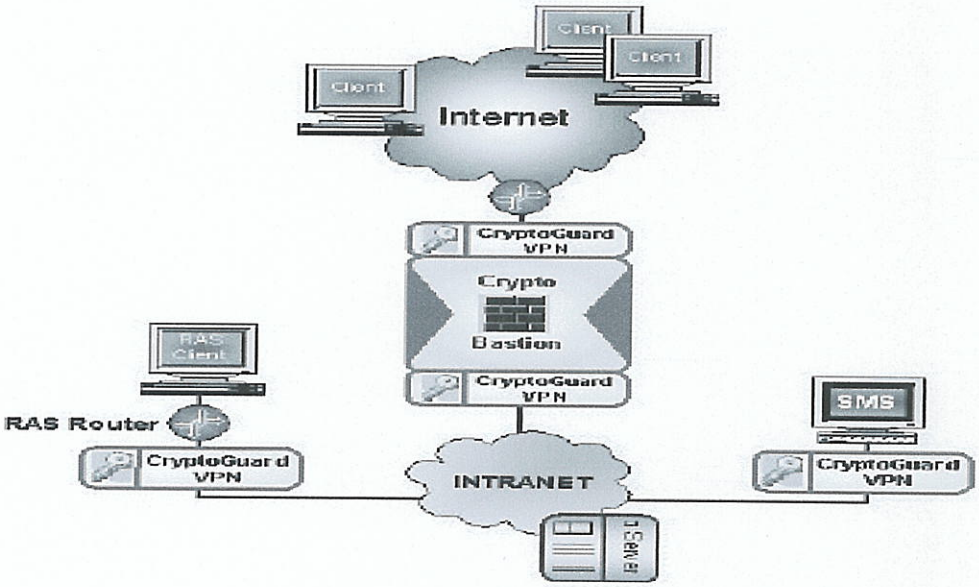
a. Remote Access VPN

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), untuk PT Himalaya ini bekerja sama dengan ***QuasarNet***, sebagai pihak ketiga yang menyediakan jasa layanan VPN. 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.yaitu berupa *RAS /Remote Access.*

Keuntungan-keuntungan dari perpindahan ke Access VPN antara lain adalah pengurangan biaya perusahaan akibat pengeluaran yang berhubungan dengan modem dan terminal server equipment, penggunaan pulsa lokal sehingga mengurangi penggunaan hubungan interlokal. Selain itu, Access VPN mempunyai tingkat skabilitas yang tinggi dan kemudahan dalam pengorganisasian jaringan jika ada penambahan pengguna baru, sehingga perusahaan bisa lebih

berkonsentrasi pada core bisnis dan bisa mengurangi beban pemeliharaan jaringan. Telecommuter, divisi sales, perwakilan atau kantor cabang, dan karyawan yang bertugas di luar adalah para pengguna Access VPN.



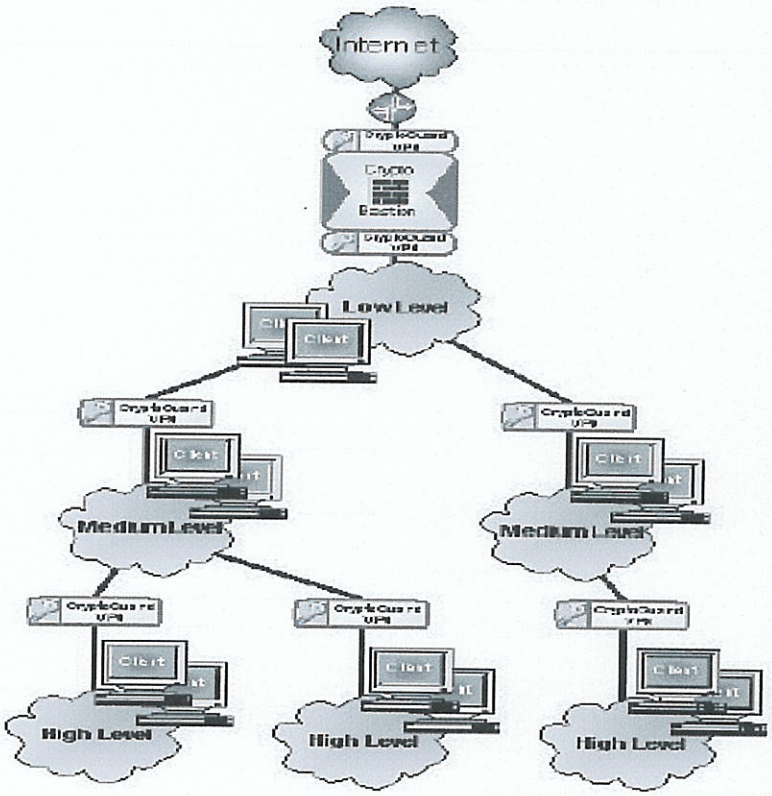
Gambar 2.2 Remote Access

b. 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.

Intranet VPN

Intranet VPN menghubungkan kantor pusat dan seluruh kantor cabang melalui infrastruktur jaringan publik menggunakan *IP security (IPSec)* atau *Generic Route Encryption (GRE)* untuk memberikan keamanan pada tunnel yang dipakai. Dengan menggabungkan service dari provider seperti mekanisme *Quality of Service (QoS)*, manajemen bandwidth *Weighted Fair Queuing (WFQ)* dan penggunaan *Commited Access Rate (CAR)* di router peusahaan, akan memberikan penggunaan bandwidth WAN yang efisien dan throughput yang bisa dipercaya. Keuntungan dari Intranet VPN adalah pengurangan biaya bandwidth di WAN, kemudahan penggabungan kantor cabang baru dan adanya link redundancy WAN pada service provider.

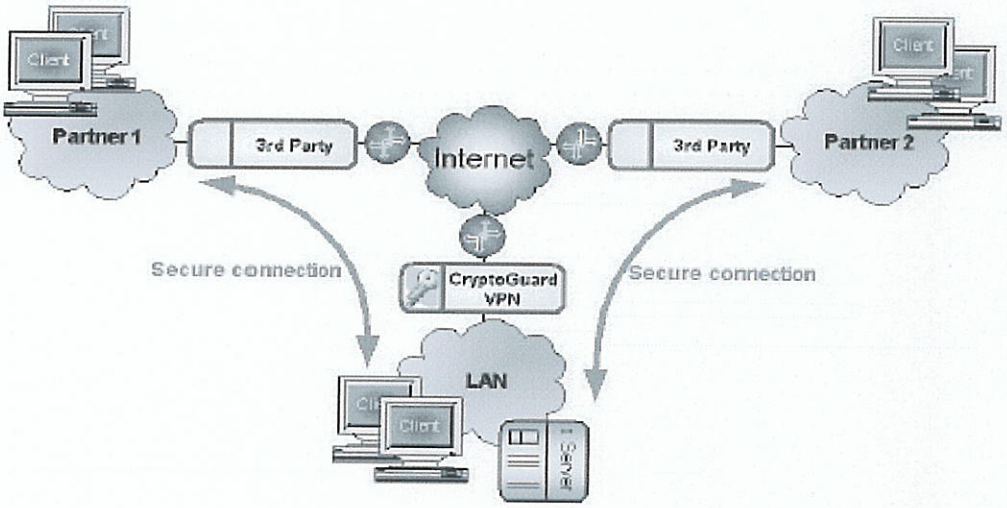


Gambar 2.3 Intranet VPN

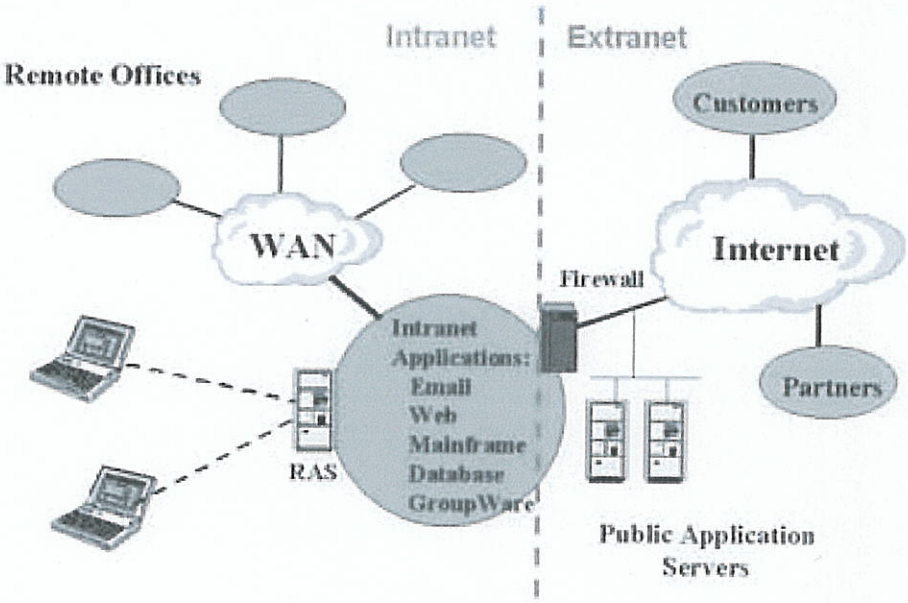
UNIT PELAKSANA TEKNIS PERPUSTAKAAN UNIKOM

Extranet VPN

Menghubungkan ke perusahaan partner dan supplier membutuhkan biaya yang tinggi dan tingkat kesulitan yang tinggi pula. Selain itu, dibutuhkan sering terjadi masalah dengan kompatibilitas device yang digunakan tiap perusahaan. Extranet VPN menghubungkan pelanggan, supplier dan partner melalui jaringan telekomunikasi publik dengan menggunakan saluran khusus. Pelayanan yang disediakan sama dengan pelayanan jika menggunakan jaringan pribadi, sehingga pengguna seperti menggunakan intranet dari perusahaan tersebut. Extranet menggunakan arsitektur dan protokol yang sama dengan yang digunakan pada Access VPN dan Intranet VPN.



Gambar 2.4 Ekstranet VPN



Gambar 2.5 Implementasi VPN

2.4 Protokol

Jaringan Intenet 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. VPN muncul untuk mengatasi persoalan tersebut. Sebuah jaringan perusahaan yang menggunakan infrastruktur IP untuk berhubungan dengan kantor cabangnya dengan cara pengalamatan

secara *private* dengan melakukan pengamanan terhadap transmisi paket data.

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

Point-to-point tunneling protocol (PPTP)

Layer-2 forwarding (L2F)

Layer-2 tunneling protocol (L2TP)

IP security protocol (IPSec)

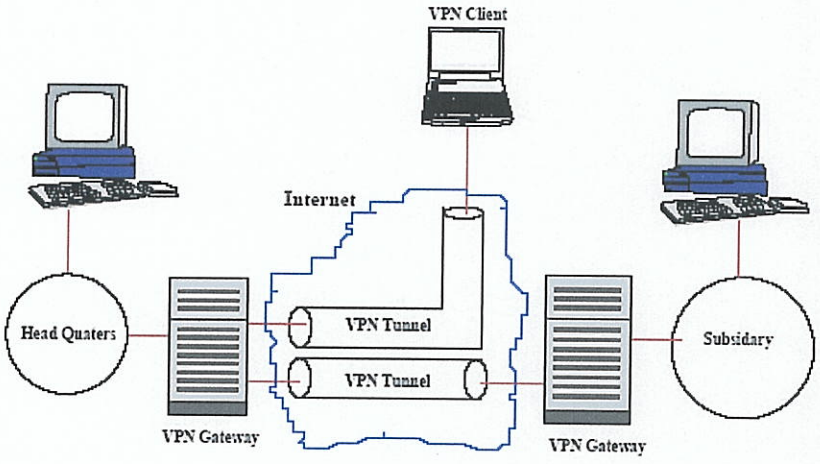
Saat akan membuat sebuah koneksi VPN, software pada ujung di bagian mengontak gateway VPN, sebagai contoh mungkin adalah router Ethernet di perusahaan. Gateway biasanya memverifikasi apakah seorang yang akan pemakai yang terotorisasi dengan mengecek password Anda. Kemudian *software VPN* akan membuatkan sebuah tunnel dan menambahkan sebuah *header* pada paket data yang dimengerti oleh jaringan Internet. Saat paket mencapai endpoint dari *gateway*, *gateway* akan menarik kembali header Internet tersebut, dan mengarahkan paket tersebut ke tujuan akhirnya. VPN menggunakan salah satu dari tiga teknologi tunneling yang ada: PPTP, L2TP dan standar terbaru, Internet Protocol Security (biasa disingkat menjadi IPSec).

Bila tunnel membuatkan jaringan, enkripsi akan menciptakan privasi/keamanan di dalamnya, dengan mengacak data yang lewat sehingga hanya pihak yang memiliki kunci digital saja yang dapat membacanya. PPTP dan L2TP dapat memverifikasi sebuah identifikasi pengguna dan mengacak data menggunakan kriptografi dasar, yaitu mengacak dan menenkripsikan seluruh file secara bersamaan. Untuk situasi dan kalangan bisnis tertentu, metoda pengamanan tersebut masih mencukupi. Untuk perusahaan yang memerlukan tingkat keamanan super-ketat mungkin lebih baik menggunakan *protokol IPSec*, yang memiliki proses tingkat lanjut, memverifikasi dan mengenkripsi setiap paket data untuk dapat mencapai privasi tingkat maksimum.

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.

Koneksi *host-to-network*, biasanya digunakan oleh seseorang yang menginginkan akses aman terhadap sumberdaya suatu perusahaan. Prinsipnya sama dengan koneksi *network-to-network* hanya saja salah satu sisi *gateway* digantikan oleh *client*.



Gambar 2.6 Network-to-Network dan Host-to-Network

2.5 Keamananan dengan IPSec

IPSec merupakan singkatan dari *IP security*. IPSec merupakan suatu protokol yang digunakan untuk melakukan pertukaran paket pada layer IP secara aman. IPSec menyediakan dua jenis mode enkripsi, yaitu mode transport dan mode tunnel. Mode transport akan mengkripsi bagian data (*payload*) masing-masing paket tanpa mengubah *header* paket tersebut. Algoritma yang digunakan untuk mengenkripsi data adalah algoritma kriptografi simetris. IPSec mode ini

menggunakan sub-protokol yang disebut sebagai *encapsulated security payload* (ESP).

Pada mode tunnel, data dan *header* paket yang akan dikirim dilakukan komputasi menggunakan teknik *checksum kriptografi* dan mengubah bagian *header* paket IP menggunakan fungsi *hasing* yang aman. Paket ini akan ditambahkan *header* baru yang mengandung nilai *hash* agar informasi yang ada pada paket biasa diautentikasi di bagian penerima. Mode ini seolah-olah membuat "terowongan" khusus pada jaringan publik yang hanya dapat diakses oleh orang-orang tertentu.

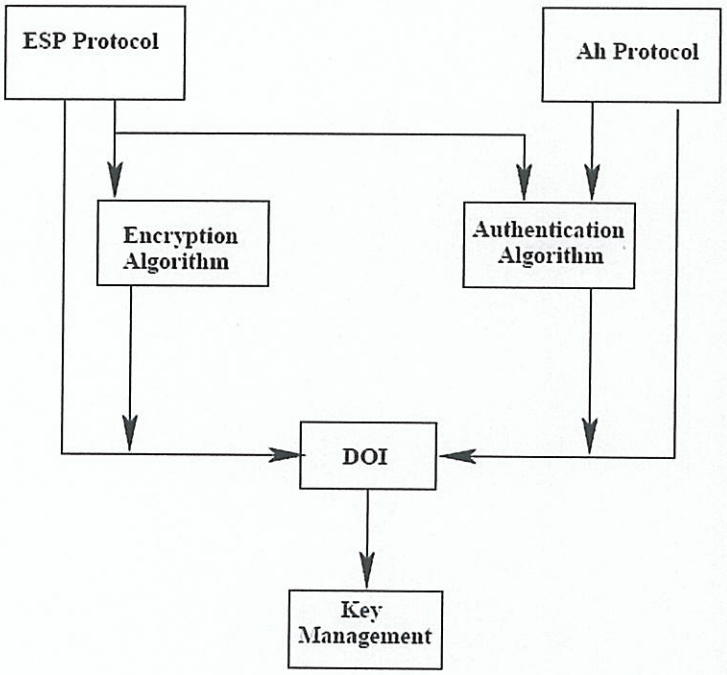
Protokol yang berjalan dibelakang IPSec adalah:

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).

Berdasarkan fungsi, IPSec diaplikasikan berdasarkan titik akhir dimana IPSec melakukan enkasulapsi. Pembagian berdasarkan fungsi tersebut adalah:

- *Transport mode*. *Transport mode* digunakan untuk mengenkripsi dan mengotentifikasi (*optional* data IP (*transport layer*).
- *Tunnel mode*. *Tunnel mode* mengenkripsi seluruh paket IP.

Transport mode biasanya digunakan untuk komunikasi *peer-to-peer* antara *nodes*dan *tunnel mode* biasanya digunakan untuk mengamankan komunikasi *gateway*dengan yang lainnya. Untuk VPN digunakan *tunnel mode*.



Gambar 2.7 Arsitektur IPSec

Key Management Secara bersama protokol IPSec AH dan ESP menyediakan privasi, integritas, dan otentifikasi dari paket IP, namun hal tersebut belum lengkap. IETF juga telah menyediakan protokol yang melayani negosiasi antar protokol IPSec, algoritma, dan kunci dalam komunikasi tersebut, verifikasi identitas, dan mengatur pertukaran kunci.

Cara kerja IPSec dapat dibagi dalam lima tahap, yaitu:

- _Memutuskan menggunakan IPSec antara dua titik akhir di internet
- _Mengkonfigurasi dua buah *gateway* antara titik akhir untuk mendukung IPSec

- _ Inisialisasi *tunnel* IPSec antara dua *gateway*
- _ Negosiasi dari parameter IPSec/IKE antara dua *gateway*
- _ Mulai melewatkan data