

**TINJAUAN MEKANISME DAN APLIKASI  
IPSEC: STUDI KASUS VPN**

R M Dikshie Fauzie

# Daftar Isi

<b>1 Pengantar</b>	<b>3</b>
<b>2 Pendahuluan</b>	<b>4</b>
<b>3 IPSec</b>	<b>6</b>
3.1 <i>IPSec Modes</i> . . . . .	7
3.2 <i>Key Management</i> . . . . .	9
3.3 Cara Kerja IPSec . . . . .	10
<b>4 Evaluasi IPSec</b>	<b>13</b>
4.1 Umum . . . . .	13
4.2 Penanganan Data . . . . .	13
<b>5 Rangkuman dan Kesimpulan</b>	<b>15</b>

# Daftar Gambar

2.1	<i>Private Network Menggunakan Leased Lines</i> . . . . .	4
2.2	<i>Private Network Menggunakan Public Internet</i> . . . . .	5
3.1	<i>Network-to-Network dan Host-to-Network</i> . . . . .	7
3.2	Arsitektur IPSec . . . . .	8
3.3	Paket IP Sebelum Memasukkan AH . . . . .	8
3.4	<i>Transport Mode</i> dan AH . . . . .	9
3.5	<i>Tunnel Mode</i> dan AH . . . . .	9
3.6	Paket IP Sebelum Memasukkan ESP . . . . .	9
3.7	<i>Transport Mode</i> dan EPS . . . . .	9
3.8	<i>Tunnel Mode</i> dan EPS . . . . .	9
3.9	Hubungan IPSec antara Bob dan Alice . . . . .	11

# **Bab 1**

## **Pengantar**

Makalah ini dibuat dalam rangka memenuhi tugas mata kuliah EL-695 Keamanan Sistem Informasi.

R M Dikshie Fauzie  
23201093  
Magister Teknologi Informasi  
Program Pasca Sarjana  
Institut Teknologi Bandung  
dikshie at ppk.itb.ac.id

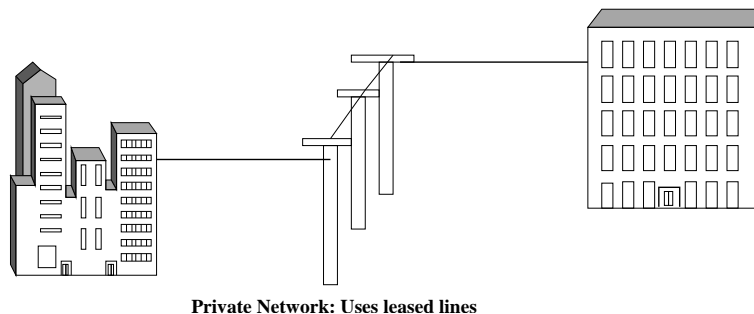
## Bab 2

# Pendahuluan

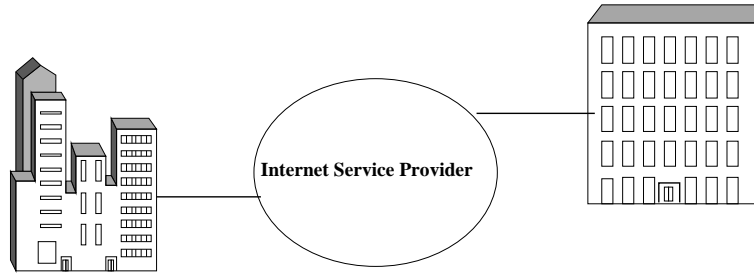
Kebutuhan bisnis dimasa sekarang didukung dengan variasi jaringan komunikasi yang luas. Para karyawan di perusahaan mengakses sumberdaya perusahaan untuk mendukung pekerjaan mereka melalui jaringan komunikasi yang perusahaan mereka miliki. Belum lagi rekanan bisnis perusahaan yang turut mengakses sumberdaya perusahaan dengan jaringan yang lain dalam rangka kerja sama membagi informasi bisnis, perencanaan bisnis bersama, dan lain sebagainya.

Pada umumnya perusahaan menggunakan berbasis *leased lines* atau sirkit *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.

VPN menggunakan jaringan internet yang sudah tersedia untuk menjawab persoalan jaringan perusahaan seperti yang dideskripsikan seperti diatas. Dibandingkan jaringan *leased lines* atau *frame relay*, VPN menggunakan infrastruktur yang sudah ada di internet untuk melakukan pertukaran data antara kantor pusat sebuah perusahaan dan kantor cabangnya. Deskripsi singkat mengenai VPN dapat dilihat pada gambar 2.1 dan 2.2.



Gambar 2.1: *Private Network Menggunakan Leased Lines*



Gambar 2.2: *Private Network Menggunakan Public Internet*

Dari cara pandang jaringan, salah satu masalah jaringan internet (*IP public*) 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. VPN muncul untuk mengatasi persoalan tersebut. Sebuah jaringan perusahaan yang menggunakan infrastruktur IP untuk berhubungan dengan kantor cabangnya dengan cara pengalaman secara *private* dengan melakukan pengamanan terhadap transmisi paket data [5].

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)*

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.

## Bab 3

# IPSec

IPSec adalah sekumpulan ekstensi dari keluarga protokol IP. IPSec menyediakan layanan kriptografi untuk keamanan transmisi data. Layanan ini termasuk *authenticity*, *integrity*, *access control*, *confidentiality*, dan *anti replay*. Layanan IPSec mirip dengan SSL namun, IPSec melayani lapisan *network*, dan dilakukan secara transparan. Layanan tersebut dideskripsikan sebagai berikut:

- *Confidentiality*, untuk meyakinkan bahwa sulit untuk orang lain tetapi dapat dimengerti oleh penerima yang sah bahwa data telah dikirimkan. Contoh: Kita tidak ingin tahu seseorang dapat melihat password ketika login ke *remote server*.
- *Integrity*, untuk menjamin bahwa data tidak berubah dalam perjalanan menuju tujuan.
- *Authenticity*, untuk menandai bahwa data yang dikirimkan memang berasal dari pengirim yang benar.
- *Anti Replay*, untuk meyakinkan bahwa transaksi hanya dilakukan sekali, kecuali yang berwenang telah mengizinkan untuk mengulang.

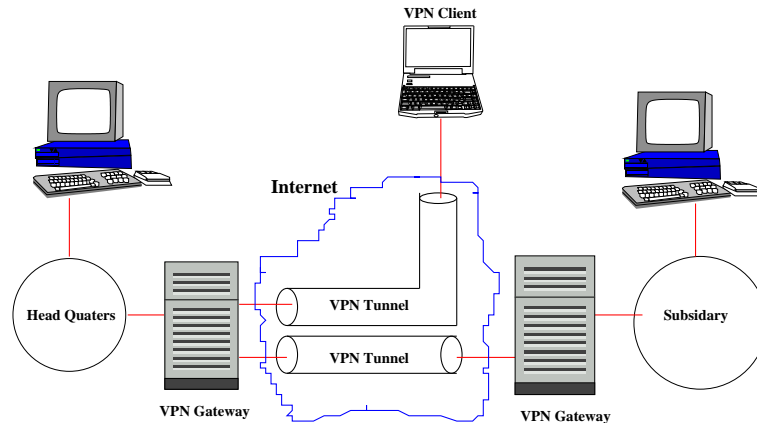
IPSec bekerja dengan tiga jalan, yaitu:

1. *Network-to-network*
2. *Host-to-network*
3. *host-to-host*

Contoh koneksi *network-to-network*, misalnya sebuah perusahaan yang mempunyai banyak kantor cabang dan ingin berbagi data dengan aman, maka tiap cabang cukup menyediakan sebuah *gateway* dan kemudian data dikirimkan melalui infrastruktur jaringan internet yang telah ada. Semua lalu lintas data antara *gateway* disebut *virtual tunnel*. Kedua *tunnel* tersebut memverifikasi otentifikasi pengirim

dan penerima dan mengenkripsi semua lalu lintas. Namun lalu lintas didalam sisi *gateway* tidak diamankan karena diasumsikan bahwa LAN merupakan segment jaringan yang dapat dipercaya.

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 3.1: *Network-to-Network* dan *Host-to-Network*

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 (*Encapsulated security payload*), ESP menyediakan layanan *authentication*, *integrity*, *replay protection*, dan *confidentiality* terhadap data (ESP melakukan pengamanan terhadap segala sesuatu dalam paket data setelah header).

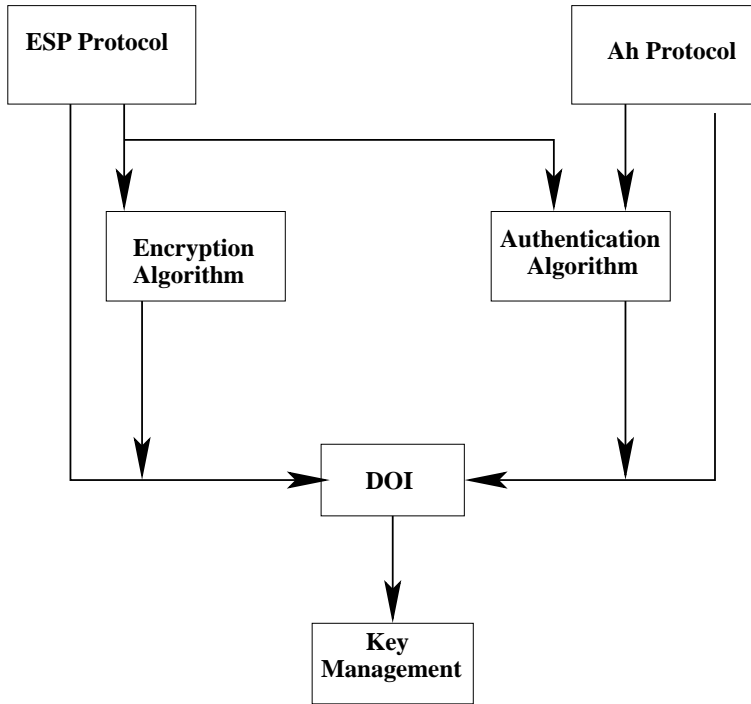
Secara umum arsitektur IPSec dapat dilihat pada gambar 3.2.

Pengamanan hubungan dalam IPSec didefinisikan dalam istilah *security associations* (SA). Tiap SA mendefinisikan satu hubungan data secara unidirectional. Ada tiga *fields* dalam SA yaitu *destination IP address*, *security parameter index*, dan *security protocol*.

### 3.1 *IPSec Modes*

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

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



Gambar 3.2: Arsitektur IPsec

- *Tunnel mode*. *Tunnel mode* mengenkripsi seluruh paket IP.

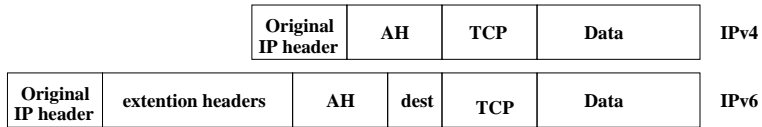
*Transport mode* biasanya digunakan untuk komunikasi *peer-to-peer* antara *nodes* dan *tunnel mode* biasanya digunakan untuk mengamankan komunikasi *gateway* dengan yang lainnya. Untuk VPN digunakan *tunnel mode*.

Implementasi AH pada IPv4 dan IPv6 diperlihatkan pada gambar:

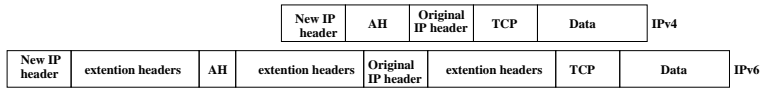
	Original IP header	TCP	Data	IPv4
Original IP header	extention headers	TCP	Data	IPv6

Gambar 3.3: Paket IP Sebelum Memasukkan AH

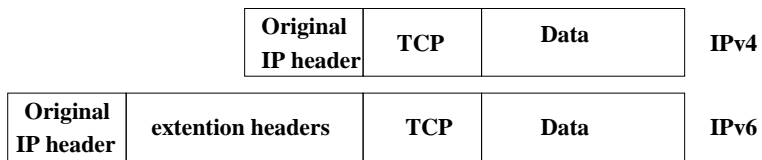
Implementasi ESP pada IPv4 dan IPv6 diperlihatkan pada gambar:



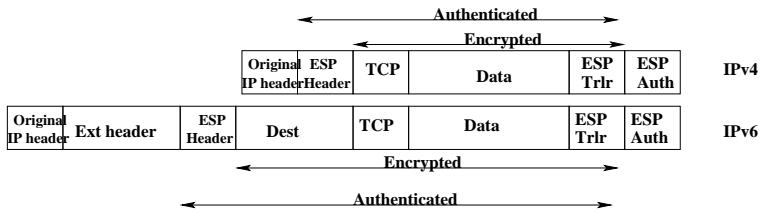
Gambar 3.4: *Transport Mode* dan AH



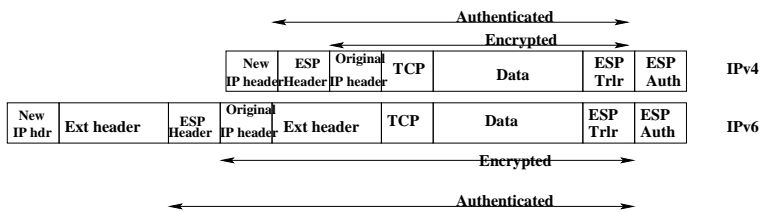
Gambar 3.5: *Tunnel Mode* dan AH



Gambar 3.6: Paket IP Sebelum Memasukkan ESP



Gambar 3.7: *Transport Mode* dan EPS



Gambar 3.8: *Tunnel Mode* dan EPS

### 3.2 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 me-

nyediakan protokol yang melayani negosiasi antar protokol IPSec, algoritma, dan kunci dalam komunikasi tersebut, verifikasi identitas, dan mengatur pertukaran kunci.

ISAKMP(*the internet security association and key management protocol*)/*Oakley key exchange protocol* secara otomatis mengatasi pertukaran kunci rahasia antara pengirim dan penerima. Protokol tersebut memadukan ISAKMP dengan metode Oakley. ISAKMP biasa disebut juga IKE (*internet key exchange*).

ISAKMP didasarkan atas model pembangkitan kunci Diffie-Hellman, dimana dua entitas saling berbagi informasi sebelum yakin identitas entitas yang lainnya. Dengan Diffie-Hellman, dua entitas membangkitkan nilai *public* mereka, yang kemudian mereka kirim ke entitas yang lain. Dua entitas berkomunikasi melalui UDP. Tiap entitas mengambil kunci *public* yang telah diterima dan mengkombinasikannya dengan kunci *private*. Hasilnya seharusnya sama untuk kedua entitas, namun tidak ada satu pun yang dapat membangkitkan nilai yang sama.

Meskipun ISAKMP adalah metode pertukaran kunci secara otomatis, ISAKMP tidak mengizinkan tingkat kepercayaan apapun dalam kunci untuk dikendalikan. Dengan ISAKMP, SPI (32 bit yang berisi informasi protokol keamanan untuk sebuah paket) dapat berubah dalam jangka waktu tertentu.

ISAKMP mendukung tiga metode pertukaran kunci yaitu: *main mode*, *aggressive mode*, dan *quick mode*. *Main mode* membangun yang dikenal sebagai fasa pertama dari ISAKMP SA. SA atau *security association*, adalah metode untuk menyimpan semua detail mengenai kunci dan algoritma dalam tiap sesi IPSec. SA mencakup informasi yang sangat luas, termasuk algoritma otentifikasi AH dan kunci, algoritma enkripsi ESP dan kunci, berapa sering kunci harus diganti, bagaimana komunikasi diotentifikasi, dan informasi tentang umur SA.

*Main mode* membangun sebuah mekanisme yang digunakan untuk komunikasi diwaktu mendatang. Pada *main mode* persetujuan dalam otentifikasi, algoritma, dan kunci dilakukan. *Main mode* membutuhkan tiga tahap pertukaran antara pengirim dan penerima. Langkah pertama, dua entitas setuju dalam menggunakan algoritma dan hash untuk komunikasi. Langkah kedua, bertukar kunci *public* menggunakan model pertukaran Diffie-Hellman dan kemudian membuktikan identitas mereka kepada yang lain. Langkah terakhir, penerima dan pengirim saling memverifikasi identitas.

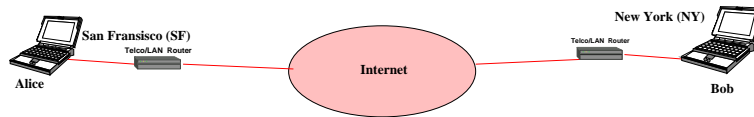
Pada *aggressive mode* sama dengan *main mode* hanya saja jumlah langkah yang dilakukan dua langkah saja, dan yang terakhir pada *quick mode* dimana dapat digunakan setelah SA ISAKMP telah dibuat menggunakan *main mode* atau *aggressive mode* untuk membuat material baru untuk membangkitkan kunci. Ini dikenal sebagai fasa pertukaran kedua. Dalam *quick mode*, semua paket telah dienkripsi, jadi langkah ini lebih mudah dari *main mode* dan *aggressive mode*.

### 3.3 Cara Kerja IPSec

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

Untuk lebih jelasnya berikut ini diberikan contoh langkah demi langkah IPSec antara Bob yang berada di kota New York dan Alice yang berada di kota San Francisco (Gambar 3.9).



Gambar 3.9: Hubungan IPSec antara Bob dan Alice

Langkah-langkah hubungan tersebut diuraikan sebagai berikut:

- SF mengkonfigurasi IPSec dengan NY
- NY mengkonfigurasi IPSec dengan SF
- Alice mengirimkan data kepada Bob
- SF mengenali bahwa data tersebut harus diamankan
- SF memulai IKE dengan *peer* di NY
- SF menawarkan algoritma enkripsi, algoritma hash (untuk otentifikasi), metode otentifikasi, Diffie-Hellman, protokol ESP atau AH
- NY setuju dengan tawaran SF lalu meresponnya dengan mengirimkan persetujuan kepada SF
- SF membangkitkan bilangan acak, '*nonce*', dan mengirimkannya bersama kunci *public* ke NY
- NY menggunakan kunci *public* SF untuk mendekrip *nonce* yang telah dienkripsi dan kemudian memverifikasinya ke SF
- SF menggunakan kunci *private* untuk menandatangani *nonce* dan mengirimkannya kembali ke NY
- NY menggunakan kunci *private* untuk menandatangani *nonce* dan mengirimkannya kembali ke SF

- SF menggunakan kunci *public* untuk mendekrip *nonce* yang dienkrip kemudian memverifikasi ke NY
- NY menggunakan kunci *public* SF untuk mendekrip *nonce* yang dienkrip kemudian memverifikasi ke SF
- SF memulai *quick mode negotiation* dengan NY dengan membangkitkan dan mengirimkan *security parameter index* (SPI)
- NY memverifikasi bahwa SPI belum digunakan olehnya dan mengkonfirmasi bahwa SF dapat menggunakan SPI tersebut, sambil NY juga mengirimkan SPI miliknya sendiri ke SF.
- SF mengkonfirmasi SPI milik NY dan mengirimkan alamat dari *host* Alice yang akan menggunakan IPSec SA
- NY mengkonfirmasi ke SF bahwa dapat mendukung IPSec untuk Alice dan sekaligus mengirimkan alamat *host* Bob ke NY
- SF mengkonfirmasi ke NY bahwa dapat mendukung IPSec untuk Bob dan mengirimkan atribut IPSec (umur SA dan algoritma enkripsi ke NY)
- NY memverifikasi bahwa atribut IPSec yang dikirimkan SF dan membangun pasangan SA IPSec (*inbound dan outbound*) untuk Bob untuk berbicara kepada Alice
- SF menerima konfirmasi atribut IPSec NY dan membangun pasangan SA IPSec (*inbound dan outbound*) untuk Alice untuk berbicara kepada Bob
- Tunnel terbentuk

## Bab 4

# Evaluasi IPSec

Pada saat ini IPSec merupakan solusi praktis terbaik untuk keamanan transmisi paket IP [4]. Namun ada beberapa kritik yang dapat ditunjukkan kepada IPSec.

### 4.1 Umum

Secara umum IPSec mempunyai kompleksitas yang cukup besar. IPSec terlalu banyak memiliki *options* dan terlalu banyak memiliki fleksibilitas [4]. 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"** [3].

### 4.2 Penanganan Data

Inti dari IPSec terdiri atas fungsi-fungsi yang menyediakan layanan otentifikasi dan *confidentiality* untuk paket IP. Ini yang digunakan contohnya untuk memba-

ngun VPN diatas jaringan internet yang tidak dapat dipercaya untuk mengamankan transmisi paket data.

IPSec mempunyai dua macam operasi yaitu *transport* dan *tunnel*. Ada dua protokol yang digunakan yaitu AH dan ESP. AH menyediakan layanan otentifikasi dan ESP menyediakan layanan otentifikasi, enkripsi, dan keduanya. Hal ini membuat masalah kompleksitas. Misalkan dua mesin yang yang ingin melakukan otentifikasi sebuah paket ada mempunyai empat cara berbeda yaitu: transport dengan AH, tunnel dengan AH, transport dengan ESP, dan transport dengan ESP.

Beberapa saran yang diajukan oleh Ferguson dan Schneier [4] adalah menghapus *transport mode* karena dapat mengurangi kebutuhan untuk memisahkan mesin dalam satu jaringan kedalam dua kategori yaitu *hosts* dan *gateway*, dan secara umum *hosts* dalam satu jaringan masih dapat dianggap sebagai *trusted machines* sehingga *transport mode* jarang digunakan. Dalam kenyataan sehari-hari sebuah perusahaan dalam berkomunikasi dengan kantor cabang atau rekan bisnis mereka lebih banyak menggunakan VPN, artinya *tunnel mode* lebih sering digunakan dalam kehidupan sehari-hari.

Ferguson dan Scheneier [4] juga mengusulkan agar protokol AH tidak perlu digunakan, karena protokol ESP selalu dapat menyediakan layanan otentifikasi dan enkripsi. Dalam semua kasus, enkripsi tanpa otentifikasi adalah hal yang sia-sia, karena itu Ferguson dan Scheneier [4] juga mengusulkan agar memodifikasi protokol ESP agar selalu menyediakan layanan otentifikasi, namun layanan enkripsi menjadi *optional*.

## Bab 5

# Rangkuman dan Kesimpulan

Pada makalah 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 secara de facto 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 [4].

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:

- Untuk VPN sebaiknya menggunakan *tunnel mode* dengan protokol ESP dan melakukan enkripsi, dan menggunakan pertukaran kunci secara otomatis untuk pengamanan maksimum pada transmisi data.
- 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.

# Bibliografi

- [1] Anonymous, *Virtual Private Networks (VPNs) Tutorial*, The International Engineering Consortium, <http://www.iec.org>
- [2] Anonymous, *Introduction to IPSec VPN's*, Cisco Systems, Inc., 1998
- [3] Anonymous, *Using IPSec: OpenBSD FAQ*, <http://www.openbsd.org/faq/faq13.html>
- [4] Ferguson, N., and Schneier, B., *A Cryptographic Evaluation of IPSec*, Counterpane Internet Security, 2000.
- [5] Scandariato, R., and Risso, F., *Advanced VPN Support on FreeBSD Systems*, BSDCon Europe, Netherland, 2002.
- [6] Stallings, W., *Cryptography and Network Security, third edition*, Prentice Hall, 2002.