

Tinjauan Mekanisme dan Aplikasi IPSEC
(*IP Security Protocol*)
Studi Kasus VPN (*Virtual Private Netwok*)

R M Dikshie F *

*dikshie@ppk.itb.ac.id

1 Pendahuluan

Berkembangnya internet dengan pesat membuat semua orang didunia dapat saling berkomunikasi satu dengan yang lainnya dengan mudah dan cepat. Pada awalnya keamanan bukan tujuan dari desain TCP/IP. Baru sesudah tahun 1995 dimana internet menjadi konsumsi umum dan lalu lintas perdagangan melalui internet orang mulai menyadari arti penting keamanan jaringan internet. Bagi pengguna internet yang memerlukan privasi dalam berkomunikasi tentunya ada masalah-masalah yang muncul dalam situasi sehari-hari, misalnya sebuah perusahaan yang akan mengirimkan dokumen penting kepada kantor cabang melalui internet memerlukan situasi dimana jalur yang dilalui aman dari observasi dari pihak lain, modifikasi paket data oleh pihak lain atau *spoofing*.

Salah satu solusi dari permasalahan diatas adalah menggunakan IPSEC. IPSEC adalah sebuah standar yang dibuat oleh *Internet Engineering Task Force* (IETF) yang berguna untuk mengamankan transmisi data dalam jalur komunikasi data yang tidak terproteksi dengan aman seperti internet.

2 Deskripsi

IPSEC bekerja pada lapisan *network*, memproteksi dan mengotentifikasi komunikasi paket IP antara *host* dan berfungsi baik pada lalulintas IPv6 maupun IPv4. IPSEC ini sebenarnya adalah fitur yang dimiliki oleh IPv6 namun oleh beberapa *developer* diaplikasikan kedalam IPv4.

IPSEC mempunyai 4 buah elemen, yaitu :

1. AH (*authentication header*)
2. ESP (*encapsulating security payload*)
3. IPcomp (*IP payload compression*)
4. IKE (*internet key exchange*)

Secara umum layanan yang diberikan IPSEC adalah :

1. *Data Confidentiality*, pengirim data dapat mengenkripsi paket data sebelum dilakukan transmit data.

2. *Data Integrity*, penerima dapat mengotentifikasi paket yang dikirimkan oleh pengirim untuk meyakinkan bahwa data tidak dibajak selama transmisi.
3. *Data Origin Authentication*, penerima dapat mengotentifikasi asal dari paket IPSEC yang dikirimkan.
4. *Anti Replay*, penerima dapat mendeteksi dan menolak paket yang telah dibajak.

Hasil akhir dari tugas akhir mata kuliah EL-695 Keamanan Sistem Informasi ini adalah sebuah tinjauan mekanisme cara kerja dari IPSEC dan penggunaan dalam dunia internet dalam hal ini penulis akan menggunakan VPN (*Virtual Private Network*) sebagai studi kasus.