BAB 9 – SECURITY

Banyak orang berpikir bahwa IPv6 lebih aman dari IPv4. Aspek keamanan IPv6 didesain sebagai pengganti ipv4. tetapi IPv6 juga memiliki atribut yang lebih baik dibandingkan dengan IPv4. Pada bab ini akan menjelaskan perbedaan antara IPv6 dan IPv4 berkaitan dengan keamanan (yang baik dan yang buruk), serta menjelaskan bagaimana perangkat keamanan standar seperti filter paket untuk IPv6. Keamanan IPV6 ini menggunakan IPsec. IPsec adalah teknologi yang menyediakan untuk keamanan transmisi data..

PERBEDAAN DARI IPV4

Banyak perubahan antara IPv4 dan IPv6 memiliki implikasi keamanan. Hal ini terutama berlaku untuk penggunaan yang lebih luas dari ICMP, ruang alamat yang lebih besar dan alamat link-lokal.

MEMANFAATKAN BATAS HOP

Pada IPv4, perlu dilakukan penyaringan pesan redirect ICMP pada link ke seluruh Internet, penyerang dapat mencoba untuk membingungkan host dengan mengirimkan pesan redirect yang dipalsukan. Dalam IPv6, masalah ini bisa saja jauh lebih buruk, seperti di IPv6, penggunaan ICMP sangat diperluas. Namun, para penulis RFC 1970 pada tahun 1996 dan penggantinya RFC 2461 pada tahun 1998 datang dengan trik cerdas untuk menolak pesan ICMPv6 yang dikirim oleh penyerang remote. Semua ICMPv6 jenis lain yang hanya digunakan pada subnet tunggal memiliki Batas Hop mereka yang diatur oleh ke 255 sistem berasal. Hal ini memungkinkan sistem penerima untuk menentukan apakah paket yang dikirim oleh sistem pada subnet yang sama atau dengan sistem remote. Jika pengirim dan penerima berbagi subnet, paket tidak dapat melalui setiap router, sehingga Batas Hop tetap harus 255 pada penerima. Jika penyerang mengirimkan paket dengan Batas Hop dari 255, penerima akan melihat nilai yang lebih rendah. Mengatur Hop Limit awal yang lebih rendah dari 255 jelas tidak akan ada gunanya, dan Batas Hop tinggi tidak mungkin karena 255 adalah nilai tertinggi yang sesuai dalam bidang 8-bit.