Analisis Pengamanan Jaringan Pada Protokol *IPv6* Menggunakan *Multi-Layer IPSec*

Asrizal[1], Syahril Efendi[2], Zakarias Situmorang[3]

[1,2,3]*Program Studi S2 Teknik Informatika, Fakultas Ilmu Komputer dan Teknologi Informasi*
Universitas Sumatera Utara
[1]*asrizal@uinsu.ac.id*, [2]syahnyata1@gmail.com, [3]zakarias65@ust.ac.id

Abstract

Security is an important aspect in computer network operations. To support, computer network security, various security methods have been developed, both in application level security, such as Pretty Good Privacy (PGP), end-system level security, such as Socket Secure Layer (SSL), direct-link level security such as Multi Protocol Level Switching (MPLS) and IP layer security such as IP Security (IPSec). IPSec is a collection of protocols for securing networks through authentication and IP packet encryption. On the other hand, Internet Protocol Version 4 (IPv4) as a network protocol is not safe enough and is no longer able to serve the needs of new IP addresses around the world, and will soon be replaced with IPv6. Therefore, it is necessary to examine various security methods that can be developed in IPv6. In this study, the author will analyze the Multi-Layer IPSec in securing IPv6 networks.

Keywords*: IPv6, IPSec, Multi-Layer IPSec*

1. PENDAHULUAN

Keamanan merupakan aspek penting dalam operasi jaringan komputer. Untuk mendukung keamanan jaringan komputer, berbagai metode keamanan pun telah dikembangkan, baik yang bersifat *application level security* seperti *Pretty Good Privacy (PGP)* untuk pengamanan *e-mail*, *end-system level security* seperti *Socket Secure Layer (SSL), direct-link level security* seperti *Multi Protocol Level Switching (MPLS)* maupun *IP layer/subnetwork level security* seperti *IP Security (IPSec*) [1].

IPSec adalah kumpulan protokol untuk mengamankan jaringan melalui proses otentikasi dan enkripsi paket IP. Dengan *IPSec*, sebuah sistem bisa memilih protokol keamanan, algoritma kriptografi dan kunci keamanan yang akan digunakan. *IPSec* memberikan perlindungan keamanan berupa *access control, integrity protection, data authentication,* dan *confidentiality [2]*. Namun dengan penerapan *IPSec,* belum menjamin sistem aman dari serangan dan ancaman keamanan. Berbagai serangan masih mungkin terjadi seperti *denial of service* yang menyebabkan berkurangnya kualitas/kapasitas jaringan serta membatasi akses pemakai [3]. Disamping beberapa serangan lainnya seperti *eavesdropping attack* yang mengakibatkan bocornya informasi rahasia seperti *password,* maupun *data modification* yang mengakibatkan perubahan data seperti jumlah uang yang ditransfer pada sebuah transaksi perbankan dan lain sebagainya [1]. Pengiriman paket data melalui jaringan publik seperti Internet juga berpotensi mengalami gangguan keamanan seperti s*poofing* dimana pelaku bertindak seolah-olah sebagai penerima yang sah dan melakukan transaksi, maupun *sniffing* dimana pelaku dapat melihat dan memantau aktifitas pengiriman data sehingga data tidak lagi bersifat rahasia, serta *session hijacking* dimana pelaku memiliki akses penuh pada paket data dan dapat menggunakannya secara tidak sah [4].

Disisi lain, *Internet Protocol Version 4 (IPv4)* sebagai protokol jaringan walaupun telah sukses selama beberapa dekade dalam mendukung komunikasi jaringan, tidak cukup aman dan tidak mampu lagi melayani kebutuhan dan permintaan *IP address* baru diseluruh dunia yang semakin meningkat. *IPv4* akan segera digantikan oleh *IPv6* yang mendukung *IP address* yang lebih banyak serta keamanan yang lebih baik [5]. Selama beberapa dekade, *Internet Protocol Version 4 (IPv4)* merupakan protokol yang paling banyak digunakan pada jaringan internet. *IPv4* mudah diterapkan dan dapat beroperasi pada berbagai sistem operasi. Namun seiring dengan perkembangan internet dan peningkatan jumlah pengguna, diperkirakan tidak lama lagi *IPv4* akan segera habis dan tidak dapat lagi melayani pertumbuhan jaringan internet tersebut [1].

2. METODE PENELITIAN

2.1 Internet Protocol Version 6 (IPv6)

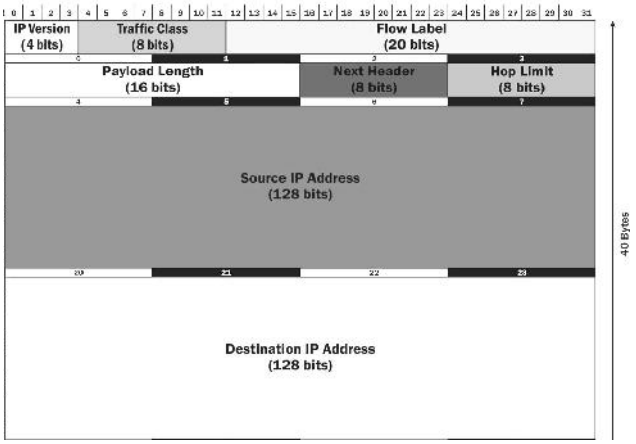
Internet Protocol Version 6 (IPv6) dikembangkan dengan beberapa peningkatan sebagai berikut:

1. *Address space* yang lebih besar guna memenuhi kebutuhan *IP address* yang semakin meningkat.
2. *Header* yang disederhanakan untuk efisiensi *routing*.
3. *Address autoconfiguration* untuk pengalamatan secara dinamis.
4. Peningkatan fleksibilitas pengalamatan *(addressing flexibility)*.
5. Dukungan terhadap alokasi sumberdaya *(resource allocation)* yang semakin baik.
6. Dukungan keamanan dengan terintegrasinya *IP Security (IPSec)* sebagai standar keamanan pada *IPv6*.

Berbeda dengan *IPv4* dimana panjang *IP address* hanya 32 bit, pada *IPv6* panjang *IP address* 128 bit atau 16 byte. Demikian juga dengan notasi yang digunakan, jika pada *IPv4* skema penomoran menggunakan notasi desimal, maka pada *IPv6* skema penomoran menggunakan notasi heksadesimal [6]. Untuk memudahkan pembacaan, *IP address* pada *IPv6* dibagi kedalam 8 blok yang masing-masing terdiri dari 4 digit. Setiap blok dipisah oleh tanda titik dua ":". Berikut contoh penulisan *IPv6 address*:

2001:0718:1c01:0016:020d:56ff:fe77:52a3

Mekanisme *IPv6 Packet Header* digambarkan pada Gambar 1.



Gambar 1. *IPv6 packet header*

2.2 IP Security (Ipsec)

IPSec merupakan protokol keamanan yang beroperasi pada *network layer* dan berfungsi menyediakan *confidentiality*, *integrity* dan *authentication* pada komunikasi jaringan Internet. Dengan model pengamanan pada *network layer* memungkinkan semua paket IP dapat dilindungi, tanpa perlu pengaturan lebih lanjut pada *application layer*. Karena skalabilitas dan dukungannya terhadap berbagai sistem yang mendukung TCP/IP, *IPSec* menjadi standar keamanan jaringan Internet [1].

Mekanisme pengamanan *IPSec* terdiri dari [3]:

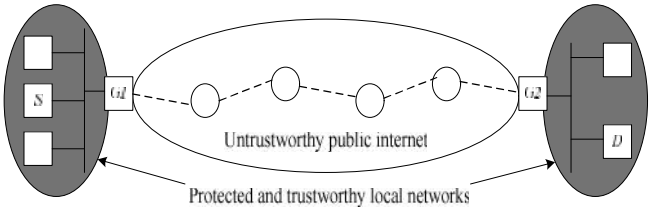
1. *Security Associations (SA).*
2. *Security Policy Database (SPD).*
3. *Security Association Database (SAD).*
4. Dua protokol keamanan: *Authentication Header (AH)* dan *Encapsulated Security Payload (ESP).*
5. Dua mode operasi: *Transport Mode* dan *Tunnel Mode*.
6. Algoritma-algoritma kriptografi yang digunakan untuk enkripsi dan dekripsi (antara lain *DES, TDES, Blowfish* dan *AES*).
7. Manajemen kunci: *Internet Key Exchange protocol (IKE)* atau pengaturan kunci secara manual.

Security Association (SA) merupakan hubungan saling terkait antara dua *end-point* yang menjelaskan bagaimana pengamanan akan dilakukan, seperti penentuan mode operasi (*tunnel mode*

atau *transport mode*), algoritma-algoritma kriptografi, dan kunci keamanan yang digunakan. *SA* juga berisi informasi tentang *IP address* tujuan [1]. *Security Policy Database (SPD)* merupakan database yang berisi kebijakan tentang tindakan apa yang akan diambil pada saat pengiriman maupun penerimaan paket. Tindakan tersebut meliputi [1]:

1. Membatalkan pengiriman paket.
2. Meneruskan pengiriman paket tanpa pengamanan.
3. Menerapkan *IPSec* untuk mengamankan proses pengiriman paket.

Mekanisme keamanan IPSec digambarkan pada Gambar 2.



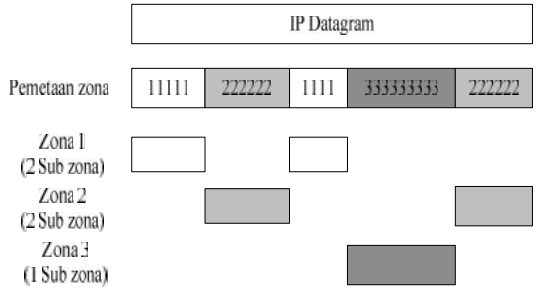
Gambar 2. *IPSec*

Berikut uraian mekanisme keamanan *IPSec* yang tertuang dalam gambar 2:

1. Jaringan lokal yang aman dan dapat dipercaya pada sumber *(S)*,
2. Jaringan Internet publik yang tidak aman,
3. Jaringan lokal yang aman dan dapat dipercaya pada tujuan *(D)*.

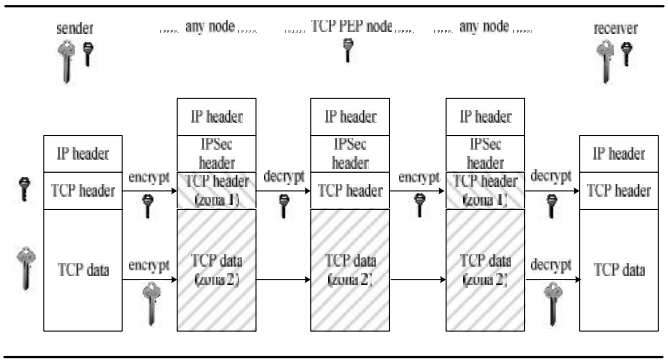
2.3 Multi-Layer IPSec

Perbedaan *IPSec* dengan *Multi-Layer IPSec* adalah bahwa pada *IPSec* proses enkripsi dan otentikasi diterapkan pada *IP datagram payload* atau *IP header* sebagai satu kesatuan, sedangkan pada *Multi-Layer IPSec*, *IP datagram* dibagi kedalam beberapa zona. Setiap zona memiliki rangkaian *security association*, kunci privat, dan pengaturan aksesnya masing-masing yang menentukan *node* mana saja yang mempunyai akes ke zona tersebut [7]. Sebuah zona adalah suatu bagian dari *IP datagram* dibawah skema perlindungan keamanan yang sama meliputi *security association*, kunci privat, dan pengaturan aksesnya masing-masing. Sebuah blok yang berdekatan dan berada dibawah zona yang sama disebut sub zona [1]. Pembagian dan pemetaan zona diilustrasikan gambar 3.



Gambar 3. Zona dan pemetaan zona pada *multi-layer IPSec*

IP datagram dibagi ke dalam 3 (tiga) zona yang dipetakan kedalam 5 (lima) sub zona dengan perincian pada zona 1 (satu) terdapat 2 (dua) sub zona, pada zona 2 (dua) terdapat 2 (dua) sub zona, dan pada zona 3 (tiga) terdapat 1 (satu) sub zona. Untuk melindungi lalu lintas jaringan dari sumber ke tujuan, *IPSec gateway* sumber akan terlebih dahulu membagi *IP datagram* ke dalam zona-zona dan menentukan *security association*, kunci privat, dan *access control* masing-masing. Pada saat *IP datagram* bergerak menuju *intermediate gateway* yang telah diotorisasi, sebagian *datagram* bisa dimodifikasi atau didekripsi/dienkripsi ulang dan sebagian lagi tidak. Ketika paket telah sampai pada *IPSec gateway* tujuan, *IPSec gateway* tujuan akan merekonstruksi ulang *datagram* kedalam bentuk aslinya [1]. Mekanisme *Multi-Layer IPSec* digambarkan pada Gambar 4.



Gambar 4. *Multi-layer IPSec*

Mekanisme *Multi-Layer IPSec* yang tertuang pda gambar 2.4 dapat dijelaskan sebagai berikut: Dalam proses pengiriman paket dari sumber ke tujuan, *IP datagram* dibagi pada 2 (dua) zona yaitu *TCP header* (zona 1) dan *TCP data* (zona 2). Bagian *TCP header* (zona 1) menggunakan skema perlindungan terpisah dengan kunci yang dibagi diantara sumber, tujuan dan *node* yang telah diotorisasi. Sedangkan bagian *TCP data* (zona 2) menggunakan perlindungan *end-to-end* dengan kunci yang dibagi hanya diantara *host* atau *security gateway* sumber dan tujuan. Dengan demikian, hanya sumber, tujuan, dan *node* yang telah diotorisasi yang mempunyai akses ke *TCP header* maupun *TCP data* [7].

2.4 Quality of Service (QoS)

Quality of Service (QoS) adalah kemampuan suatu jaringan untuk menyediakan layanan yang baik seperti yang diharapkan dengan menyediakan *bandwidth*, mengatasi *jitter* dan *delay*. *QoS* memberikan layanan yang lebih baik pada lalu lintas jaringan yang dipilih dengan berbagai teknologi yang dipakai. Parameter *QoS* adalah *latency*, *jitter*, *packet loss*, dan *throughput*. *QoS* sangat ditentukan oleh kualitas jaringan yang digunakan. *QoS* didesain untuk memastikan bahwa *end user* mendapatkan performansi yang handal dari aplikasi-aplikasi berbasis jaringan. Kemampuan *QoS* mengacu pada tingkat kecepatan penyampaian paket data dalam suatu jaringan. Faktor yang mempengaruhi kinerja jaringan komputer antara lain *packet loss*, *delay (latency)*, *jitter* dan *throughput*, yang dapat membuat efek yang cukup besar bagi banyak aplikasi [8].

QoS diukur berdasarkan parameter-parameter berikut [8]:

1. ***Throughput***, yaitu kecepatan (*rate)* transfer data efektif yang diukur dalam *bit per second (bps)*. Throughput merupakan jumlah total paket yang sukses datang yang diamati pada tujuan selama interval waktu tertentu dibagi oleh durasi interval waktu tersebut.
2. ***Delay*** merupakan total waktu yang dibutuhkan dalam pengiriman suatu paket data dari pengirim ke penerima melalui jaringan. *Delay* dapat dipengaruhi oleh jarak, media fisik yang dipakai, atau waktu proses yang lama.
3. ***Packet Loss***
   Merupakan suatu parameter yang menggambarkan kondisi yang menunjukan jumlah total paket yang hilang yang dapat terjadi karena *collision* dan *congestion* pada jaringan.

2.5 Langkah-Langkah Penyelesaian Masalah

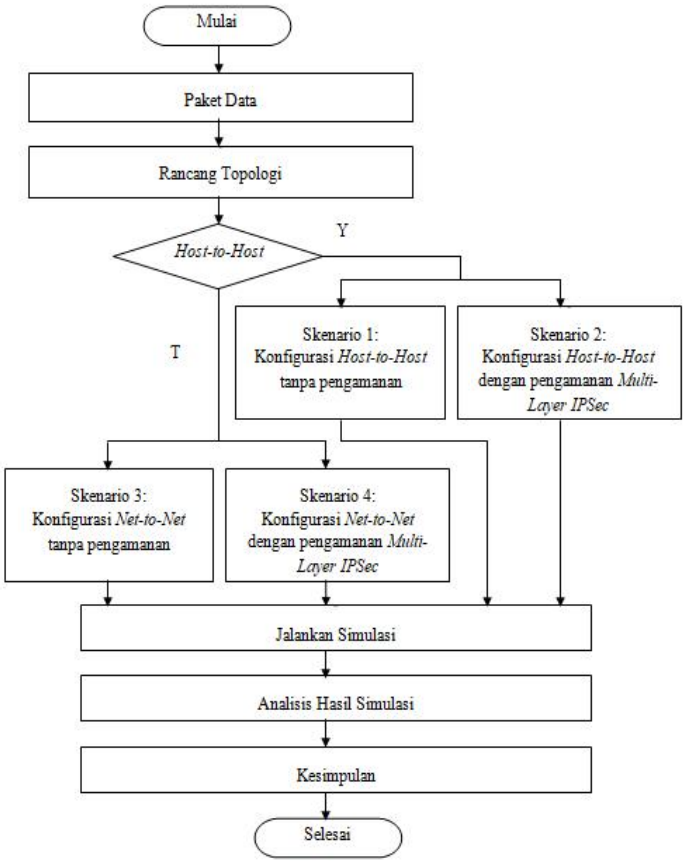
Penelitian ini bertujuan untuk mengetahui bagaimana keamanan jaringan *IPv6* dapat dicapai melalui penerapan *Multi-Layer IPSec*. Untuk mengetahui hal tersebut, peneliti merancang 2 (dua) topologi jaringan *IPv6* dalam model *host-to-host* yang terdiri dari Client-1, Client-2 dan Server, dan model *network-to-network* yang terdiri dari Client-1, Client-2, Gateway-1, Gateway-2 dan Server. Mekanisme pengujian akan dilakukan dengan melakukan pengiriman paket data dari Client-1 ke Client-2 pada masing-masing topologi. Hasil simulasi dari masing-masing topologi akan dibandingkan untuk melihat seberapa besar peningkatan keamanan yang dicapai.

Secara garis besar langkah-langkah penyelesaian masalah yang peneliti lakukan sebagai berikut:

1. Membuat rancangan topologi jaringan.
2. Melakukan konfigurasi dan set parameter jaringan untuk masing-masing skenario *host-to-host* dan *network-to-network* tanpa pengamanan *Multi-Layer IPSec* dan dengan pengamanan *Multi-Layer IPSec.*

3. Menjalankan simulasi.
4. Menganalisa hasil simulasi.
5. Menentukan kesimpulan berdasarkan analisa hasil simulasi.

Tahapan proses dan kegiatan yang dilaksanakan dalam penelitian dapat dilihat pada bagan alir Gambar 5.



Gambar 5. *Flowchart* penyelesaian masalah

2.5.1 *Multi-Layer IPSec* pada Topologi *Host-to-Host*

Pada topologi ini, peneliti menggunakan mode operasi *transport mode*, protokol keamanan *AH* pada Client-1 dan *ESP* pada Client-2, algoritma otentikasi *HMAC-MD5* pada Client-1 dan *HMAC-SHA-1* pada Client-2, algoritma enkripsi *3DES* pada Client-1 dan *DES* pada Client-2, serta *lifetime* 28.800 untuk masing-masing Client-1 dan Client-2. Untuk lebih jelasnya, konfigurasi dan setting parameter *Multi-Layer IPSec* yang dipakai pada topologi *host-to-host* dapat dilihat pada Tabel 1.

Tabel 1 Parameter *Multi-Layer IPSec* pada Topologi *Host-to-Host*

Nama	**Jenis Komponen**	***IPv6 Address***	**Mode Operasi**	**Protokol Keamanan**	**Algoritma Otentikasi**	**Algoritma Enkripsi**	***Lifetime (seconds)***
Client -1	*Workstation*	fec0::1	*Transport Mode*	*AH*	*HMAC-MD5*	3DES	28.800
Client -2	*Workstation*	fec0::2	*Transport Mode*	*ESP*	*HMAC-SHA1*	DES	28.800
Server	*Server*	fec0::10					

Selanjutnya berdasarkan Tabel 1, maka dilakukan konfigurasi dan setting parameter pada aplikasi simulasi. Untuk Client-1 dengan alamat *IPv6* fec0::1, ditentukan mode operasi yang digunakan *transport mode*, protokol keamanan *AH*, algoritma otentikasi *HMAC-MD5*, algoritma enkripsi *3DES*.

2.5.2 *Multi-Layer IPSec* pada Topologi *Net-to-Net*

Untuk pengamanan *Multi-Layer IPSec* perlu ditentukan mode operasi, protokol keamanan, algoritma otentikasi, algoritma enkripsi dan lifetime yang akan diberlakukan pada topologi. Dalam hal ini, peneliti menggunakan transport mode, sebagai mode operasi, *AH* sebagai protokol keamanan pada Client-1 dan *ESP* pada Client-2, *HMAC-MD5* sebagai algoritma otentikasi pada Client-1 dan *HMAC-SHA-1* pada Client-2, *3DES* sebagai algoritma enkripsi pada Client-1 dan *DES* pada Client-2, dan *lifetime* 28.800 untuk masing-masing Client-1 dan Client-2. Selengkapnya konfigurasi dan setting parameter *Multi-Layer IPSec* yang dipakai pada topologi *Net-to-Net* dapat dilihat pada Tabel 2.

Tabel 2. Parameter *Multi-Layer IPSec* pada Topologi *Net-to-Net*

Node	***IPv6 Address***	**Mode Operasi**	**Protokol Keamanan**	**Algoritma Otentikasi**	**Algoritma Enkripsi**	***Lifetime (seconds)***
Client-1	fec1::10	*Transport Mode*	*AH+ESP*	*HMAC-SHA1*	*3DES*	28.800
Client-2	fec2::10	*Transport Mode*	*AH*	*HMAC-MD5*	*3DES*	28.800
Gateway-1	eth0/fec1::1 eth1/fec0::1	*Transport Mode*	*AH+ESP*	*HMAC-SHA1*	*3DES*	28.800
Gateway-2	eth0/fec0::2 eth1/fec2::1	Transport Mode	AH	HMAC-MD5	3DES	28.800
Server	fec0::15					

2.5.3 Skenario Pengiriman Data

Untuk melihat performa jaringan pada masing-masing topologi ada 4 (empat) skenario yang akan dilakukan pada simulasi. Pada masing-masing skenario akan dilakukan pengiriman data dari Client-1 ke Client-2. Untuk format data yang akan dikirim dalam hal ini peneliti memilih format *database medium* sebagai sampel. Sedangkan parameter QoS yang dianalisis adalah *Traffic Sent, Traffic Received*, dan *Delay*. Selengkapnya skenario pengiriman data yang dilakukan pada masing-masing topologi dapat dilihat pada Tabel 3.

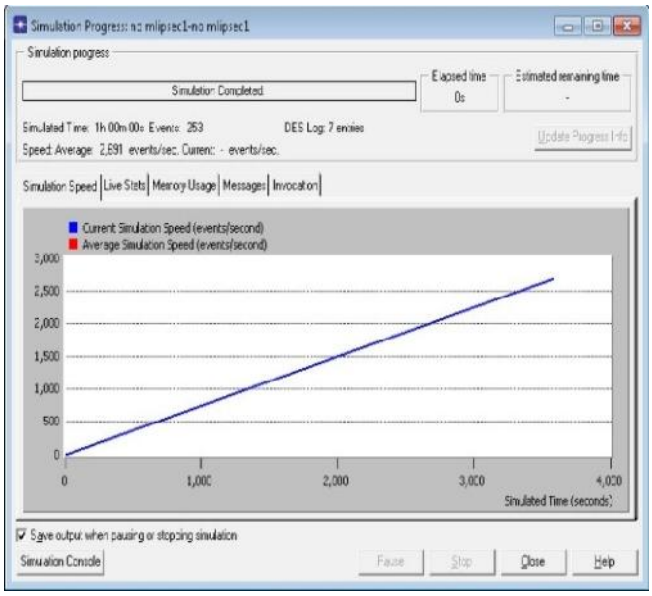
Tabel 3. Skenario Pengiriman Data

Skenario	**Topologi**	**Metode Pengamanan**	**Format Data yang dikirim**	**Parameter QoS yang diamati**
Skenario 1	*Host-to-Host*	-	*Database Medium*	*Traffic Sent, Traffic Received,Delay*
Skenario 2	*Host-to-Host*	*Multi-Layer IPSec*	*Database Medium*	*Traffic Sent, Traffic Received,Delay*
Skenario 3	*Net-to-Net*	-	*Database Medium*	*Traffic Sent, Traffic Received,Delay*
Skenario 4	*Net-to-Net*	*Multi-Layer IPSec*	*Database Medium*	*Traffic Sent, Traffic Received,Delay*

3. HASIL DAN PEMBAHASAN

3.1 Skenario 1: Pengujian Topologi Host-to-Host Tanpa *Multi-Layer IPSec*

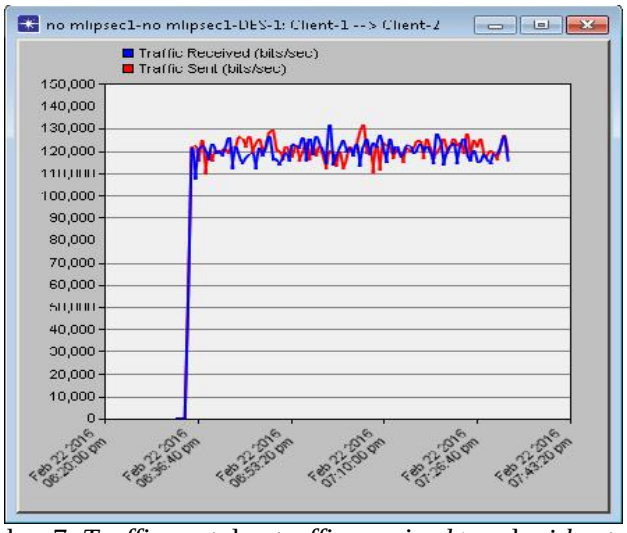
Pada topologi *host-to-host* ini pengiriman data dilakukan dari dari Client-1 dengan alamat IPv6 fec0::1 ke Client-2 IPv6 fec0::2 melalui Server IPv6 fec0::10 tanpa menggunakan *Multi-Layer IPSec*. Adapun format paket data yang digunakan adalah *database medium* sebagai sampel. Lama proses simulasi diatur selama 1 (satu) jam. Adapun hasil proses simulasi topologi *host-to-host* sebagaimana yang tertera pada Gambar 6.



Gambar 6. Proses simulasi topologi *host-to-host* tanpa *multi-layer IPSec*

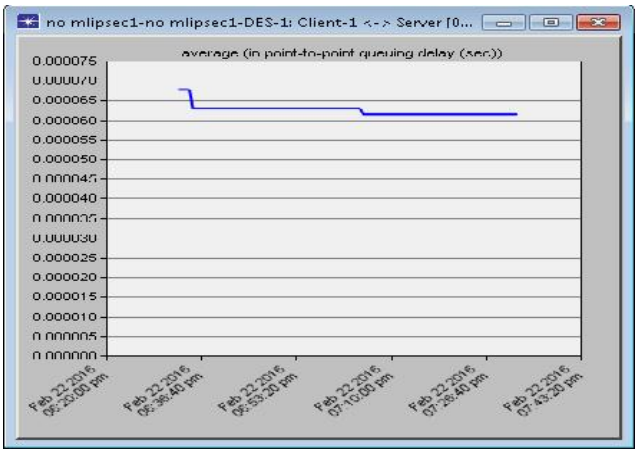
Dari gambar di atas diketahui bahwa selama 1 (satu) jam simulasi, pengiriman paket data dilakukan sebanyak 253 kali dengan rata-rata kecepatan proses 2,691 *events/sec*.

Sedangkan grafik hasil simulasi pada pengiriman paket data sebagaimana yang tertera pada gambar 7.



Gambar 7. *Traffic sent* dan *traffic received* topologi *host-to-host*

Dari grafik di atas diketahui terdapat perbedaan jumlah paket data yang dikirim dengan paket data yang diterima. Hal ini mengindikasikan adanya paket yang hilang *(packet loss)* selama proses pengiriman. Dari grafik diketahui rata-rata jumlah data yang dikirim dilihat dari titik puncak masing-masing adalah sebesar 132 *bits/sec*, sedangkan yang diterima sebesar 130 bits/sec. Terdapat perbedaan sebesar 2 *bits/sec* antara jumlah paket yang dikirim dan diterima. Maka diperoleh *packet loss* sebesar: (132-130) / 132 x 100 = 0,51 %. Angka ini masuk dalam kategori memuaskan, dimana jaringan yang termasuk dalam kategori memuaskan adalah jaringan dengan *packet loss* sebesar 3 %, kategori baik sebesar 15 %, kategori sedang 15% dan kategori jelek 25%. Sedangkan rata-rata *delay* yang dihasilkan sebagaimana yang tertera pada gambar 8 berikut, dimana diketahui *delay* pada pengiriman paket data sebesar 0,000068 detik atau 0,068 *ms*. Angka ini masuk dalam kategori memuaskan, dimana *delay* <150 ms kategori memuaskan, antara 150 s/d 300 ms kategori baik, antara 300 s/d 450 kategori sedang dan *delay* > 450 kategori jelek.



Gambar 8. *Delay* topologi *host-to-host*

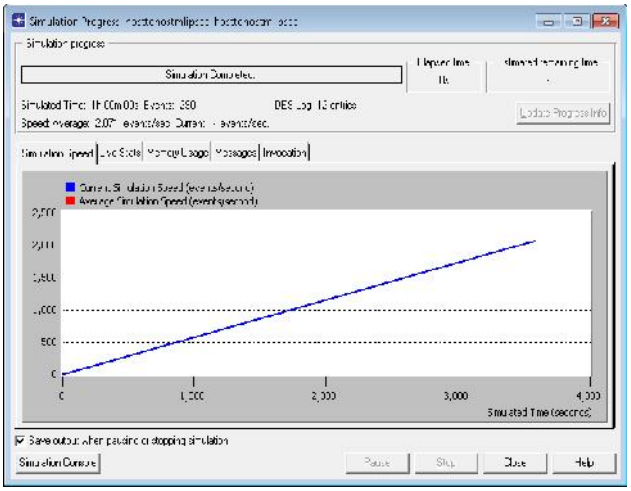
3.2 Skenario 2: Pengujian Topologi *Host-to-Host* Menggunakan *Multi-Layer IPSec*

Pada skenario ini pengiriman data dilakukan dengan menggunakan *Multi-Layer IPSec* dari Client-1 dengan alamat *IPv6* fec0::1 ke Client-2 *IPv6* fec0::2 melalui Server *IPv6* fec0::10. Adapun paramater *Multi-Layer IPSec* berupa mode operasi, protokol keamanan, algoritma enkripsi dan algoritma otentikasi serta *lifetime* yang digunakan pada skenario ini sebagaimana yang tercantum pada Tabel 4.

Tabel 4. Parameter *Multi-Layer IPSec* pada Topologi *Host-to-Host*

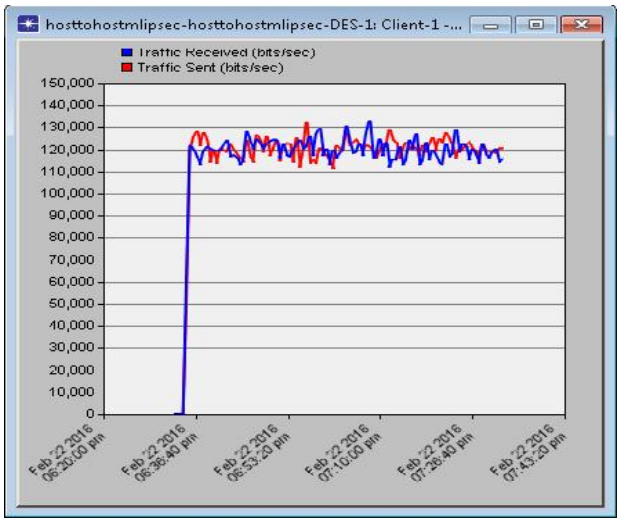
Nama	**Jenis Komponen**	***IPv6 Address***	**Mode Operasi**	**Protokol Keamanan**	**Algoritma Otentikasi**	**Algoritma Enkripsi**	***Lifetime (seconds)***
Client-1	*Workstation*	fec0::1	*Transport Mode*	*AH*	*HMAC-MD5*	3DES	28.800
Client-2	*Workstation*	fec0::2	*Transport Mode*	*ESP*	*HMAC-SHA1*	DES	28.800
Server	*Server*	fec0::10					

Simulasi dilakukan menggunakan format paket data *database medium* sebagai sampel. Lama proses simulasi diatur selama 1 (satu) jam. Dari hasil simulasi diperoleh grafik proses simulasi sebagaimana yang tertera pada Gambar 9 berikut, dimana dapat dilihat bahwa selama 1 (satu) jam simulasi, pengiriman data dilakukan sebanyak 290 kali dengan rata-rata kecepatan proses sebesar 2,071 *events/sec*.



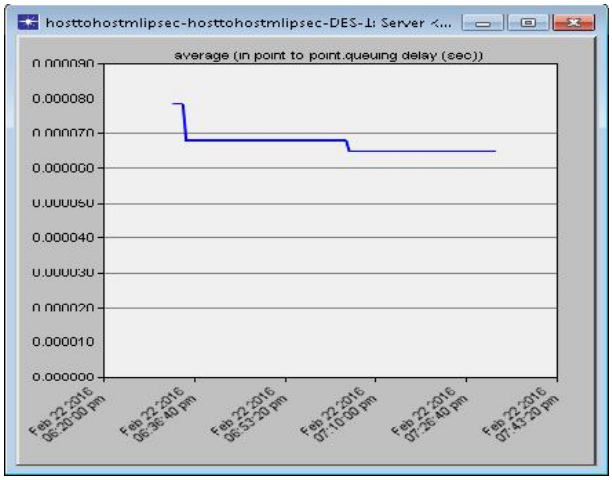
Gambar 9. Proses simulasi *host-to-host* menggunakan *multi-layer IPSec*

Adapun hasil simulasi pengiriman paket data berupa *traffic sent* dan *traffic received* pada topologi *host-to-host* ini sebagaimana yang tertera pada Gambar 10.



Gambar 10. *Traffic Sent* dan *Traffic Received* Topologi *Host-to-Host* Menggunakan *Multi-Layer IPSec*

Dari grafik di atas diketahui terdapat perbedaan jumlah paket data yang dikirim dengan paket data yang diterima. Hal ini mengindikasikan adanya paket yang hilang *(packet loss)* selama proses pengiriman. Jika dilihat dari titik puncak maka diketahui rata-rata jumlah data yang dikirim masing-masing adalah sebesar 132 *bits/sec*, sedangkan yang diterima sebesar 129 bits/sec. Terdapat perbedaan sebesar 3 *bits/sec* antara jumlah paket yang dikirim dan diterima. Maka diperoleh *packet loss* sebesar: (132-129) / 132 x 100 = 2,27 %. Angka ini masih masuk dalam kategori memuaskan. Adapun rata-rata *delay* yang dihasilkan pada topologi *host-to-host* ini dapat dilihat pada Gambar 11.

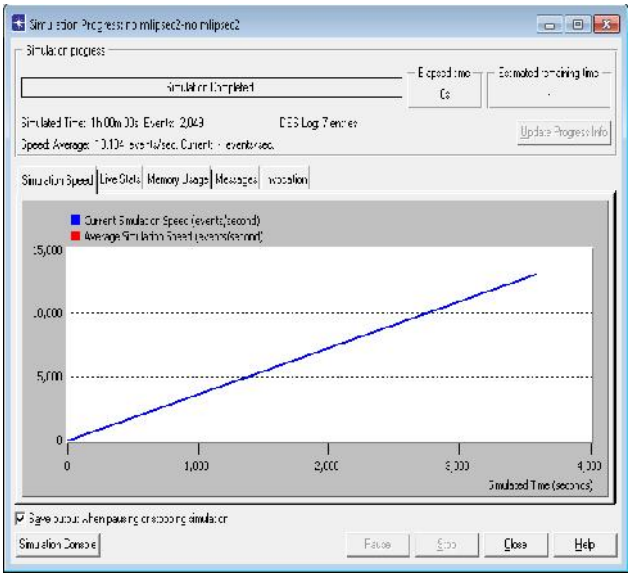


Gambar 11. *Delay* topologi *host-to-host* menggunakan *multi-layer IPSec*

Pada Gambar 11 diketahui bahwa rata-rata *delay* pada pengiriman paket data sebesar 0.000078 detik atau 0,078 ms. Jika dibandingkan dengan tanpa simulasi *host-to-host* tanpa pengamanan *Multi-Layer IPSec* maka terdapat peningkatan delay sebesar 0,000010 detik atau 0,010 *ms*.

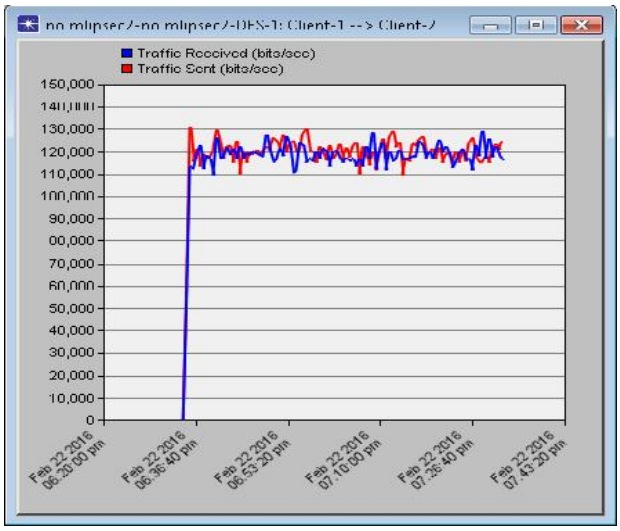
3.3 Skenario 3: Pengujian Topologi *Net-to-Net* Tanpa *Multi-Layer IPSec*

Pada skenario ini pengiriman data dilakukan dari dari Client-1 dengan alamat IPv6 fec0::10 ke Client-2 IPv6 fec2::10 melalui Gateway-1, Server dan Gateway-2. Simulasi dilakukan menggunakan format paket data *database medium* sebagai sampel. Lama proses simulasi diatur selama 1 (satu) jam. Adapun grafik proses simulasi yang dihasilkan sebagaimana yang tertera pada Gambar 12.



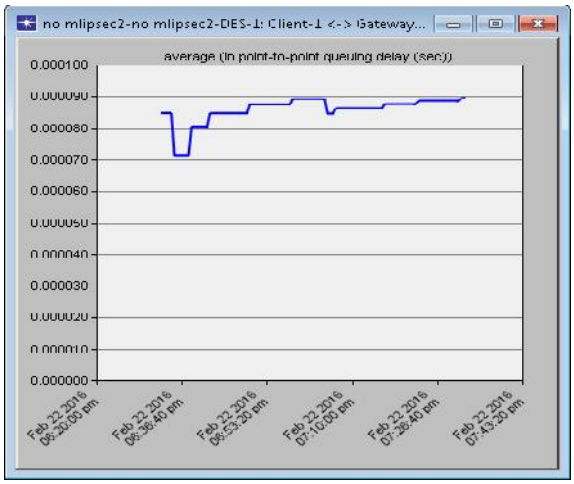
Gambar 12. Proses Simulasi Topologi *Net-to-Net*

Dari grafik di atas diketahui bahwa selama 1 (satu) jam simulasi, pengiriman data dilakukan sebanyak 2,049 kali dengan rata-rata kecepatan proses 13,134 *events/sec*. Sedangkan hasil simulasi pengiriman paket data berupa berupa *traffic sent* dan *traffic received* pada topologi *net-to net* ini sebagaimana yang tertera pada Gambar 13.



Gambar 13. *Traffic sent* dan *traffic received* pada topologi *net-to-net*

Dari grafik hasil simulasi Gambar 13, terdapat perbedaan jumlah paket data yang dikirim dengan paket data yang diterima. Hal ini mengindikasikan adanya paket yang hilang *(packet loss)* selama proses pengiriman. Jika dilihat dari titik puncak maka diketahui rata-rata jumlah data yang dikirim masing-masing adalah sebesar 130 *bits/sec*, sedangkan yang diterima sebesar 128 bits/sec. Terdapat perbedaan sebesar 2 *bits/sec* antara jumlah paket yang dikirim dan diterima. Maka diperoleh *packet loss* sebesar: (130-128) / 130 x 100 = 1,53 %. Angka ini masuk dalam kategori memuaskan. Adapun *delay* yang dihasilkan pada topologi *net-to net* ini dapat dilihat pada Gambar 14 berikut, dimana diketahui rata-rata *delay* sebesar 0,000072 atau 0,072 ms.



Gambar 14. *Delay* topologi *net-to-net*

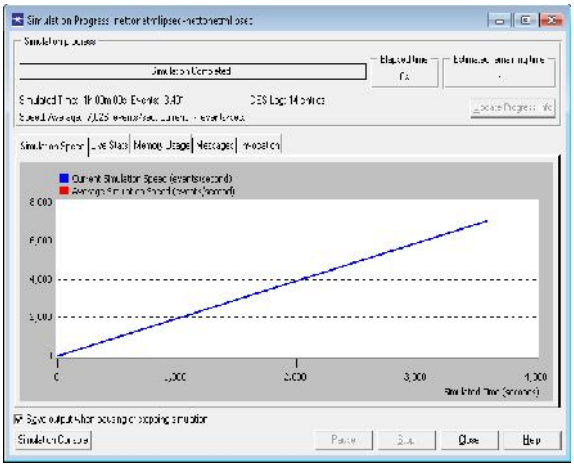
3.4 Skenario 4: Pengujian Topologi *Net-to-Net* Menggunakan *Multi-Layer IPSec*

Pada skenario ini pengiriman paket data dilakukan dari dari Client-1 dengan alamat *IPv6* fec0::10 ke Client-2 *IPv6* fec2::10 melalui Gateway-1, Server dan Gateway-2. Adapun parameter *Multi-Layer IPSec* yang digunakan berupa mode operasi, protokol keamanan, algoritma otentikasi, algoritma enkripsi dan *lifetime* yang digunakan dapat sebagaimana yang tercantum pada Tabel 5.

Tabel 5. Parameter *Multi-Layer IPSec* pada Topologi *Net-to-Net*

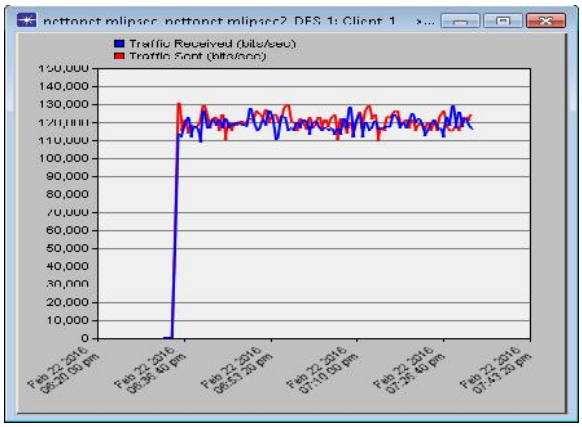
Node	***IPv6 Address***	**Mode Operasi**	**Protokol Keamanan**	**Algoritma Otentikasi**	**Algoritma Enkripsi**	***Lifetime (seconds)***
Client-1	fec1::10	*Transport Mode*	*AH+ESP*	*HMAC-SHA1*	*3DES*	28.800
Client-2	fec2::10	*Transport Mode*	*AH*	*HMAC-MD5*	*3DES*	28.800
Gateway-1	eth0/fec1::1 eth1/fec0::1	*Transport Mode*	*AH+ESP*	*HMAC-SHA1*	*3DES*	28.800
Gateway-2	eth0/fec0::2 eth1/fec2::1	Transport Mode	AH	HMAC-MD5	3DES	28.800
Server	fec0::15					

Dengan paramater yang ditentukan pada Tabel 5, maka dilakukan simulasi menggunakan format paket data *database medium* sebagai sampel. Lama proses simulasi diatur selama 1 (satu) jam. Grafik hasil proses simulasi yang dihasilkan pada topologi *net-to-net* ini dapat sebagaimana yang tertera pada Gambar 15.



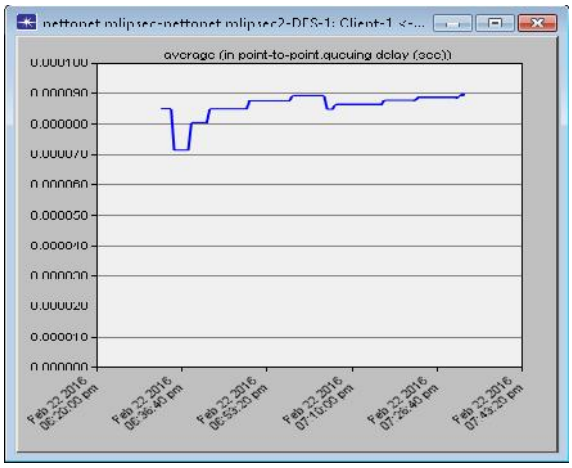
Gambar 15. Proses simulasi topologi *net-to-net* dengan *nulti-layer IPSec*

Dari grafik pada Gambar 15 diketahui bahwa selama 1 (satu) jam simulasi, pengiriman data dilakukan sebanyak 3,401 kali dengan rata-rata kecepatan proses 7,026 *events/sec*. Adapun hasil simulasi pengiriman paket data berupa *traffic sent* dan *traffic received* pada topologi *net-to-net* ini sebagaimana yang tertera pada Gambar 16 berikut.



Gambar 16. *Traffic sent* dan *traffic received* topologi *net-to-net dengan multi-layer IPSec*

Dari grafik hasil simulasi di atas terdapat perbedaan jumlah paket data yang dikirim dengan paket data yang diterima. Hal ini mengindikasikan adanya paket yang hilang *(packet loss)* selama proses pengiriman. Jika dilihat dari titik puncak maka diketahui rata-rata jumlah paket data yang dikirim adalah sebesar 130 *bits/sec*, sedangkan yang diterima sebesar 128 bits/sec. Terdapat perbedaan sebesar 2 *bits/sec* antara jumlah paket yang dikirim dan diterima. Maka, *packet loss* sebesar: (130-128) / 130 x 100 = 1,53 %. Angka ini masuk dalam kategori memuaskan. Tidak ada perbedaan nilai antara topologi *Net-to-Net* dengan atau tanpa menggunakan *Multi-Layer IPSec*. Sedangkan *delay* yang dihasilkan dapat dilihat pada Gambar 17.



Gambar 17. *Delay* topologi *net-to-net* menggunakan *multi-layer IPSec*

Dari grafik pada Gambar 17 diketahui bahwa *delay* sebesar 0,000090 atau 0,090 ms. Jika dibandingkan dengan topologi *net-to-net* tanpa pengamanan *Multi-Layer IPSec* maka ada peningkatan *delay* sebesar 0,018 *ms.*

3.5 Analisis Hasil Simulasi

Setelah dilakukan simulasi pada topologi host-to-host net-to-net dan dengan 4 (empat) skenario proses yang dilakukan maka dilakukan pembandingan hasil simulasi yang diperoleh. Hasil simulasi dari masing-masing topologi dan skenario terangkum pada Tabel 6.

Tabel 6. Hasil Pengiriman Paket Data

Skenario	Topologi	Skenario	Hasil
1	*Host-to-host*	Tanpa pengamanan	*Traffic received* ada penurunan kecepatan sebesar 2 *bits/second. Packet loss* sebesar 0,51% dan *delay* sebesar *0,078 ms.*
2	*Host-to-host*	Dengan pengamanan *Multi-Layer IPSec*	*Traffic sent* tidak ada penurunan kecepatan sedangkan *traffic received* ada penurunan kecepatan sebesar 1 *bits/second*. *Packet loss* meningkat sebesar 1,76%, dan *delay* meningkat sebesar 0,010 *ms.*
3	*Net-to-Net*	Tanpa pengamanan	*Traffic received* ada penurunan kecepatan sebesar 2 *bits/second*. *Packet loss* sebesar 1,53% *delay* sebesar 0,072 *ms*.
4	*Net-to-Net*	Dengan pengamanan *Multi-Layer IPSec*	*Traffic sent* ada penurunan kecepatan sebesar 2 *bits/second, traffic received* dan *packet loss* tetap, *delay* meningkat sebesar 0,018 *ms.*

Dari tabel di atas dapat dilihat bahwa selama 1 (satu) jam simulasi dengan format paket data *database medium* diperoleh hasil sebagai berikut:

1. Pada topologi *host-to-host* tanpa pengamanan *Multi-Layer IPSec, traffic sent* sebesar 132 *bits/second, traffic received* 130 *bits/second, packet loss* 0,51% dan delay 0,068 *ms*.
2. Pada topologi *host-to-host* menggunakan pengamanan *Multi-Layer IPSec, traffic sent* sebesar 132 *bits/second, traffic received* 129 *bits/second, packet loss* 2,27% dan delay 0,078 *ms*.
3. Pada topologi *net-to-net* tanpa pengamanan *Multi-Layer IPSec, traffic sent* sebesar 130 *bits/second, traffic received* 128 *bits/second, packet loss* 1,53% dan delay 0,072 *ms*.
4. Pada topologi *net-to-net* menggunakan pengamanan *Multi-Layer IPSec, traffic sent* sebesar 130 *bits/second, traffic received* 128 *bits/second, packet loss* 1,53% dan delay 0,090 *ms*.

Dari hasil simulasi diatas, maka diperoleh analisis hasil simulasi sebagaimana yang tertera pada Tabel 7.

Tabel 7. Analisis Hasil Simulasi

Skenario	Topologi	Skenario	Hasil
1	*Host-to-host*	Tanpa pengamanan	*Traffic received* ada penurunan kecepatan sebesar 2 *bits/second. Packet loss* sebesar 0,51% dan *delay* sebesar *0,078 ms.*
2	*Host-to-host*	Dengan pengamanan *Multi-Layer IPSec*	*Traffic sent* tidak ada penurunan kecepatan sedangkan *traffic received* ada penurunan kecepatan sebesar 1 *bits/second*. *Packet loss* meningkat sebesar 1,76%, dan *delay* meningkat sebesar 0,010 *ms.*
3	*Net-to-Net*	Tanpa pengamanan	*Traffic received* ada penurunan kecepatan sebesar 2 *bits/second*. *Packet loss* sebesar 1,53% *delay* sebesar 0,072 *ms*.
4	*Net-to-Net*	Dengan pengamanan *Multi-Layer IPSec*	*Traffic sent* ada penurunan kecepatan sebesar 2 *bits/second, traffic received* dan *packet loss* tetap, *delay* meningkat sebesar 0,018 *ms.*

4. KESIMPULAN

Berdasarkan hasil penelitian dan analisis yang telah dilakukan, maka peneliti menyimpulkan bahwa:

1. Dengan pengamanan *Multi-Layer IPSec* pada topologi *host-to-host* maupun *net-to-net* tidak terjadi penurunan kecepatan *traffic sent.*
2. Pengamanan dengan *Multi-Layer IPSec* pada topologi *host-to-host* dan *net-to-net* menyebabkan terjadinya penurunan kecepatan *traffic received* yang relatif kecil.
3. Dengan pengamanan dengan *Multi-Layer IPSec* pada topologi *host-to-host* terjadi peningkatan *packet loss* yang relatif kecil, sedangkan pada *net-to-net* tidak ada peningkatan *packet loss*.
4. Dengan pengamanan *Multi-Layer IPSec* pada topologi *host-to-host* maupun *net-to-net* terjadi peningkatan *delay* yang relatif kecil.
5. Dengan nilai *packet loss* dan *delay* yang relatif kecil, jika pengamanan dengan *Multi-Layer IPSec* diterapkan, maka *throughput* menjadi lebih baik.

BAHAN REFERENSI

[1] Kundu, A. 2010. *An Extension of Multi Layer IPSec for Supporting Dynamic QoS and Security Requirements.* Tesis. Indian Institute of Science, Bangalore.

[2] Kyburz, A. 2010. *An Automated Formal Analysis of the Security of the Internet Key Exchange (IKE) Protocol in the Presence of Compromising Adversaries.* Tesis. Department of Computer Science Swiss Federal Institute of Technology (ETH), Zurich.

[3] Faienza, A. & Amso, J. 2008. *IPsec Intrusion Detection Analysis: Using data from an Ericsson Ethernet Interface Board.* Tesis. Royal Institute of Technology (KTH), Stockholm.

[4] Syal, R. dan Malik, R. 2010. *Performance Analysis of IP Security VPN*. International Journal of Computer Applications. Vol. 8, pp. 5.

[5] Budiarto, R., Abidah, M. T., Samsudin, A. 2007. *lPv6 Transition: why a new security mechanisms model is necessary.* APAN Research Workshop, p. 313, China.

[6] Hughes, L. E. 2010. *The Second Internet: Reinventing Computer Networking with IPv6.* InfoWeapons, Cebu.

[7] Gayathri, T., Venkadajothi, S., Kalaivani, S., Divya, C., Suresh, C. G. 2009. *Mobile Multilayer IPsec protocol.* International Journal of Engineering and Technology, Vol.1(1), pp. 25.

[8] Sugeng, W., Istiyanto, J. E., Mustofa, H., Ashari, A. 2015. *The Impact of QoS Changes towards Network Performance.* International Journal of Computer Networks and Communications Security, Vol. 3, No. 2, Februari 2015.

[9] Nasution, Muhammad Irwan Padli, 2008, "Urgensi Keamanan Pada Sistem Informasi", Jurnal Iqra' Volume 02 Nomor 02.

[10] Fadhila Nisya Tanjung, Muhammad Irwan Padli Nasution, 2012, "Implementasi Pemrograman Java Untuk Alert Intrusion Detection System", pematang siantar, 31 agustus – 2 september 2012, ISBN 978-602-18749-0-5, https://www.researchgate.net/publication/307973619