ANALISIS PENGARUH KEAMANAN IP SECURITY (IPSEC) PADA IMPLEMENTASI INTERKONEKSI JARINGAN IPV4 – IPV6 DILAYANAN VOIP

Anisa Sari[1], Tri Brotoharsono[2], Yudha Purwanto[3]

[1]Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom

Abstrak

VoIP (Voice over Internet Protocol) adalah suatu teknologi yang memungkinkan komunikasi suara melalui jaringan Internet. Akan tetapi, jaringan Internet memiliki celahcelah rawan terhadap aspek keamanan sehingga dibutuhkan suatu sistem keamanan yang mampu menjamin keamanan komunikasi VoIP.

Dalam tugas akhir yang berjudul "Analisis Pengaruh Keamanan IP Security (IPSec) pada Implementasi Interkoneksi Jaringan IPv4 – IPv6 dilayanan VoIP" penulis membangun jaringan yang menggunakan protokol IPSec yaitu pada interkoneksi jaringan IPv4-IPv6 menggunakan mekanisme transisi tunneling GRE pada layanan VoIP. Kemudian dilakukan uji sniffing antara cisco router gateway untuk mengetahui enkripsi paket. Selanjutnya untuk mengetahui pengaruh IPSec terhadap kualitas layanan dilakukan penelitian uji performansi jaringan.

Dari hasil pengujian dapat disimpulkan bahwa protokol sekuriti IPSec telah berhasil diimplementasikan pada interface tunnel GRE. Hal ini dapat dibuktikan dengan paket data yang dipertukarkan telah terenkripsi, sehingga sniffer tidak dapat melakukan tindakan lanjutan seperti memodifikasi paket suara maupun merelay kembali paket suara. Namun hal ini berpengaruh terhadap performansi jaringan. Yang menyebabkan penurunan performansi jaringan yang disebabkan oleh overhead. Yaitu penambahan header IPSec dan proses enkripsi terhadap paket sebelum dikirim sehingga waktu yang dibutuhkan semakin lama.

Kata Kunci : IPSec, VoIP, IPv6, IPv4, GRE, Interkoneksi, tunnelling

Abstract

VoIP (Voice over Internet Protocol) is a technology that passed voice communication through packet network infrastructure. But, packet network infrastructure also has volatile security aspects, so it is needed a security system which can keep VoIP communication security.

In this final task with titled "Security Effect Analysis of IP Security (IPSec) Implementation on IPv4-IPv6 Network Interconnection for VoIP Service" writer is building a network which use IPSec protocol on IPv4-IPv6 network interconnection use GRE tunneling transition mechanism for VoIP service. And then, she did sniffing test between Cisco router gateway to know packet encryption and quality service test to know IPSec effect to the quality service.

From the test was concluded that IPSec security protocol successfully be implemented on GRE tunnel interfaces. It is proved with encrypted data packet that changed between User. So, sniffer couldn't further action such as modified voice packet or relaying voice packet. But, this action give the effect to network quality service. It is causing decreased network performance that caused overhead, overhead is addition IPSec header. Also caused packet encryption process before packet was send so needed longer time to sent packet.

Keywords : IPSec, VoIP, IPv6, IPv4, GRE, Interkoneksi, tunnelling

BAB II
DASAR TEORI

2.1 VoIP *(Voice over Internet Protocol)*

VoIP *(Voice over Internet Protocol)* adalah suatu teknologi yang memungkinkan komunikasi suara melalui jaringan Internet. Pada mulanya Voip hanya melewatkan sinyal suara saja. Namun dengan kemampuan teknologi yang semakin canggih, bukan hanya suara tetapi video dapat dilewatkan diatas platform IP. Bahkan dengan keunggulan VoIP diantaranya yaitu lebih murah, fleksibel, *open source* sehingga mudah dikembangkan, layanan yang ditawarkan lebih banyak menjadikan VoIP sebagai alternative komunikasi masa depan menggantikan PSTN *(Public Switched Telephone Network).*

Aplikasi Voip yang telah diimplementasikan di kehidupan nyata saat ini adalah sebagai berikut:

a. PC ke PC melewati jaringan internet
b. PC ke Phone dan sebaliknya melewati jaringan internet
c. Phone ke Phone melewati jaringan Internet

Protokol yang sering digunakan dalam VoIP adalah SIP dan H.323. Kedua protokol tersebut berfungsi sebagai protokol pensinyalan, dimana SIP merupakan *text based protocol* sedangkan H.323 merupakan *Binary Based Protocol.*

2.2 *Internet Protocol version 4 (IPv4)*

IPv4 adalah sebuah jenis pengalamatan jaringan yang digunakan di dalam protokol jaringan TCP/IP yang menggunakan protokol IP versi 4. Panjang totalnya adalah 32-bit, dan secara teoritis dapat mengalamati hingga 4 miliar host computer di seluruh dunia.

2.2.1 Pengalamatan IPv4

Alamat IP versi 4 umumnya diekspresikan dalam notasi *decimal* bertitik (*dotted-decimal notation*), yang dibagi ke dalam empat buah oktet berukuran 8-bit. Karena setiap oktet berukuran 8-bit, maka nilainya berkisar antara 0 hingga 255.

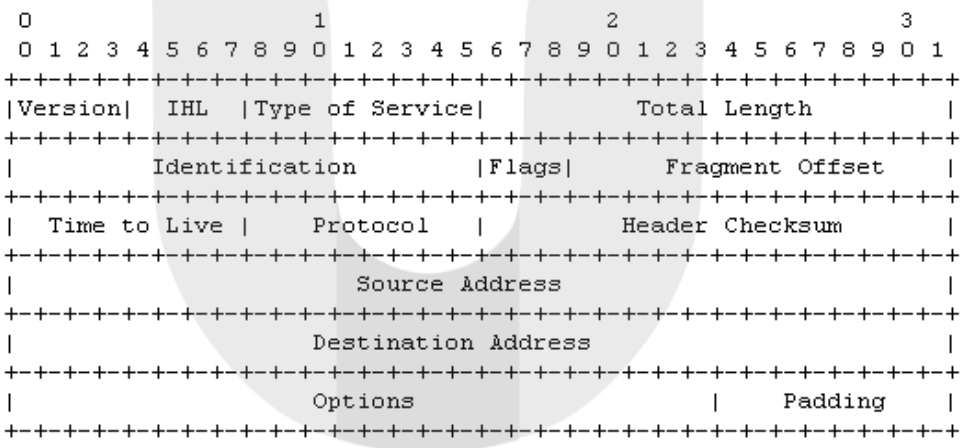
Pengalamatan IP pada *network layer* terdiri atas *net id* dan *host id. Net id* menyatakan alamat jaringan sementara *host id* menyatakan alamat unik PC pada jaringan tersebut. Dalam IPv4 mengenal pengalamatan *subnet* menggunakan notasi CIDR, yaitu informasi tambahan dalam bentuk decimal yang menyatakan jumlah bit 1 pada *subnet mask* yang digunakan. Contoh seperti pada table 2.1 berikut:

Tabel 2.1 Pengalamatan IPv4

IPv4 dalam Decimal	IPv4 dalam Biner
10.14.200.1/24	0000 1010. 0000 1110. 1100 1000. 0000 0001 *netmask* 1111 1111. 1111 1111. 1111 1111. 0000 0000 = 255.255.255.0

2.2.2 *Header* IPv4

Pada gambar 2.4. dapat dilihat format dari *header* IPv4:



Gambar 2.1 Format *Header* IPv4 [1]

Tabel 2.2 Informasi *Header* IPv4 [1]

Header	Keterangan
Version	Versi header IP
Internet Header Length	Panjang/ukuran header IP
Type of Service	Kualitas service dalam transmisi paket IP
Total Length	Total *datagram* IP, yaitu *header* IP dan muatannya.
Identification	Mengidentifikasikan sebuah paket IP tertentu yang akan difragmentasi

Flags	Berisi dua buah *flag* yang berisi apakah sebuah *datagram* IP mengalami fragmentasi atau tidak. • Bit 0 = *reserved*, diisi 0. • Bit 1 = bila 0 bisa difragmentasi, bila 1 tidak dapat difragmentasi. • Bit 1 = bila 0 fragmentasi berakhir, bila 1 ada fragmentasi lagi
Fragment offset	Digunakan untuk mengidentifikasikan *offset* di mana fragmen yang bersangkutan dimulai, dihitung dari permulaan muatan IP yang belum dipecah.
Time to Live	Waktu maksimal paket data gram harus sampai pada tujuan
Protocol	mengidentifikasikan jenis protokol lapisan yang lebih tinggi yang dikandung oleh muatan IP
Header Checksum	*Field* ini berguna hanya untuk melakukan pengecekan integritas terhadap *header* IP
Source IP Address	Alamat sumber/ pengirim datagram IP
Destination IP Address	Alamat tujuan/ tujuan datagram IP
Option	Mengkodekan pilihan-pilihan yang diminta oleh pengirim: *security label, source routing, record routing, dan time stamping*
Padding	Digunakan untuk meyakinkan bahwa *header* paket bernilai kelipatan dari 32 bit

2.3 Internet Protocol version 6 (IPv6)

Alamat IPv6 memiliki panjang 128-bit, sehingga memiliki alokasi pengalamatan sebesar 2^{128}. Total alamat yang sangat besar ini bertujuan untuk menyediakan ruang alamat yang tidak akan habis (hingga beberapa masa ke depan), dan membentuk infrastruktur routing yang disusun secara hierarkis, sehingga mengurangi kompleksitas proses routing dan tabel routing.

2.3.1 Pengalamatan IPv6

Alamat IPv6 yang terdiri dari 128 bit tidak semuanya digunakan untuk host. 64bit digunakan untuk host dan 64 bit sisanya digunakan untuk alamat prefix. Pembagian kelas pada IPv6 dilakukan berdasarkan format prefix yaitu format bit awal alamat.[2]

Pengalamatan IPv6 menggunakan 16-bit hexadesimal yang dipisahkan oleh *colon* (:) untuk merepresentasikan format pengalamatan 128-bit (x:x:x:x:x:x:x:x). Contoh 2001:1111:2222:3333:0000:0000:0000:5

Apabila pengalamatan IPv6 mengandung 16 bit yang bernilai nol saja dapat direpresentasikan dengan "::". Contohnya adalah : 2001:1111:2222:3333:0000:0000:0000:5 dapat direpresentasikan sebagai 2001:1111:2222:3333::5.

IPv6 menggunakan *bitmask* untuk keperluan *subnetting* yang direpresentasikan dengan prefix length pada teknik CIDR pada IPv4. Contoh 2001:1111:2222:3333::5/64 menyatakan bahwa 64 bit awal adalah network address.

Dalam IPv6 dikenal ada 3 tipe alamat, yaitu [3]:

- *Unicast Address*

  Yaitu *identifier* untuk suatu *single interface* yang menunjukkan alamat *interface* tersebut. Ini digunakan untuk komunikasi satu *host* ke satu *host* yang lain.

- *Anycast Address*

  Anycast address merupakan *unicast address* yang diberikan kepada beberapa *interface*. *Anycast address* hampir sama dengan alamat *unicast* yang ada pada IPv6. Perbedaanya adalah ketika router melakukan routing terhadap paket data, router akan mencarikan alamat yang terdekat dengan pengirim.

- *Multicast Address*

  Alamat ini digunakan untuk komunikasi dari satu *host* ke banyak *host*. Artinya ketika ada suatu paket yang dikirim ke *multicast address* maka paket tersebut akan dikirim ke *interface* dengan alamat *multicast* tersebut.

2.3.2 Header IPv6

Gambar 2.2 Format *Header* IPv6 [2]

Tabel 2.3 Informasi *Header* IPv6 [2]

Header	Keterangan
Version	4 bit Versi header IP
Traffic Class	Prioritas paket IPv6 jika terjadi kongesti
Flow Table	Menandai bahwa paket tersebut merupakan satu dari serangkaian paket yang memiliki urutan spesifik tertentu yang digunakan untuk menejemen QoS. *Field* ini digunakan untuk aplikasi data *real-time*
Payload Length	Menandai panjang payload paket. Jika lebih dari 65.535 byte maka *field* ini diset 0. Menggantikan *fiel Total Length* yang ada di IPv4. Jika *extension header* ada, maka perhitungan panjangnya juga ada di *field* ini.
Next Header	Menggantikan *field Protocol* yang ada pada IPv4. Menandai tambahan header pertama jika ada, jika tidak ada maka menandai *header* dari *layer* diatasnya.
Hop Limit	Menggantikan TTL pada *header* IPv4.
Source Address	Alamat IPv6 *host* asal
Destination Address	Alamat IPv6 *host* tujuan

2.4 Internet Protocol Security (IPSec)

IPSec *(IP Security)* merupakan kumpulan protokol yang dikembangkan oleh IETF *(Internet Engineering Task Force)* untuk mendukung pertukaran paket yang aman melalui IP *layer* [4]. IPSec adalah protokol *security* berbasis kriptografi yang bekerja pada layer *network*, menyediakan keamanan transmisi data [4]. IPSec dirancang untuk menyediakan keamanan berbasis kriptografi yang memiliki karakteristik *interoperable* dan berkualitas. IPSec memberikan layanan keamanan seperti *confidentiality*, *authentication,* dan *integrity.*

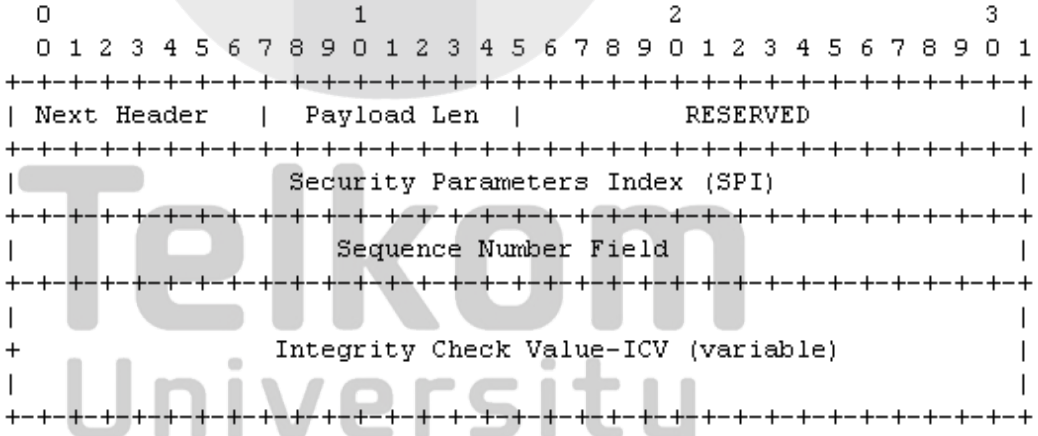
Confidentiality : Untuk menjamin kerahasiaan informasi data yang dipertukarkan agar tidak dapat dimengerti oleh pihak-pihak yang tidak berhak [4].

Integrity : Untuk menjamin bahwa data tidak berubah dalam perjalanan menuju tujuan [4].

Authentication : Untuk menjamin bahwa data yang dikirimkan memang berasal dari pengirim yang benar [4].

Secara teknis, IPSec terdiri atas dua bagian utama. Bagian pertama mendeskripsikan dua protokol untuk penambahan header pada paket yang membawa *security identifier, dan* mengenai *integrity control,* dan informasi keamanan lain, yaitu:

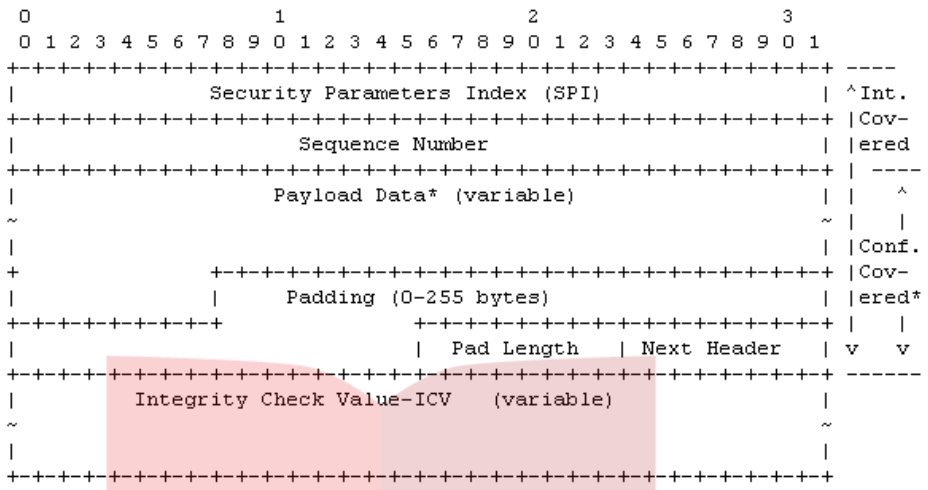
1. *Authentication Header (AH)* menyediakan data *integrity*, data *origin authentication,* dan proteksi terhadap *replay attack.*



Gambar 2.3 Format Authentication Header (AH) [5]

2. *Encapsulating Security Payload* menyediakan layanan yang disediakan oleh AH ditambah dengan *confidentiality.*

   Berikut ini adalah gambar paket *header* dari ESP:



Gambar 2.4 Format Encapsulating Security Payload (ESP) [6]

Bagian kedua berkaitan dengan protokol pembangkit dan distribusi kunci, yaitu implementasi protokol IKE *(Internet Key Exchange)* yang berfungsi dalam pembangkitan dan pertukaran *cryptographic key* secara otomatis. *Cryptographic key* digunakan dalam authentikasi node yang berkomunikasi dalam proses enkripsi dan dekripsi paket yang dikirimkan [7].

Mode IPSec terdiri dari dua, yaitu [4]:

1. Transport mode, protokol menyediakan proteksi terhadap layer diatas IP *layer*. Hal ini dilakukan dengan penambahan IPSec header diantara IP header dengan header protokol layer diatas IP yang diproteksi
2. Tunnel mode, protokol menyediakan proteksi pada paket IP sehingga sekaligus melindungi layer diatas IP layer. Hal ini dilakukan dengan mengenkapsulasi paket IP yang akan diproteksi.

Original IP Datagram

IP	UDP	Data

AH Transport Mode

IP	AH	UDP	Data

AH Tunnel Mode

New IP	AH	IP	UDP	Data

ESP Transport Mode

IP	ESP Header	UDP	Data	ESP Trailer	ESP Auth

ESP Tunnel Mode

New IP	ESP Header	IP	UDP	Data	ESP Trailer	ESP Auth

Gambar 2.5 Enkapsulasi Paket IPSec [8]

IPSec bekerja dengan tiga bagian yaitu:

1. Network-Network

2. Network-Host

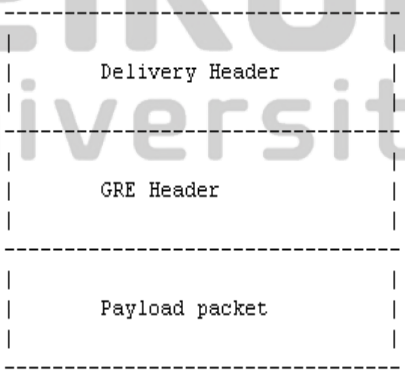
3. Host-Host

2.5 Tunnelling GRE

Tunneling adalah suatu mekanisme enkapsulasi PDU (*Packet Data unit*) dengan protokol yang lain dengan maksud untuk mengirimkan data pada *foreign network*. Tiga komponen utama dalam *tunneling* adalah :

- *Passenger Protocol*, yaitu protokol yang dienkapsulasi
- *Carrier Protocol*, yaitu protokol yang melakukan enkapsulasi
- *Transport Protocol*, yaitu protokol yang membawa (mengirim) PDU yang telah dienkapsulasi.

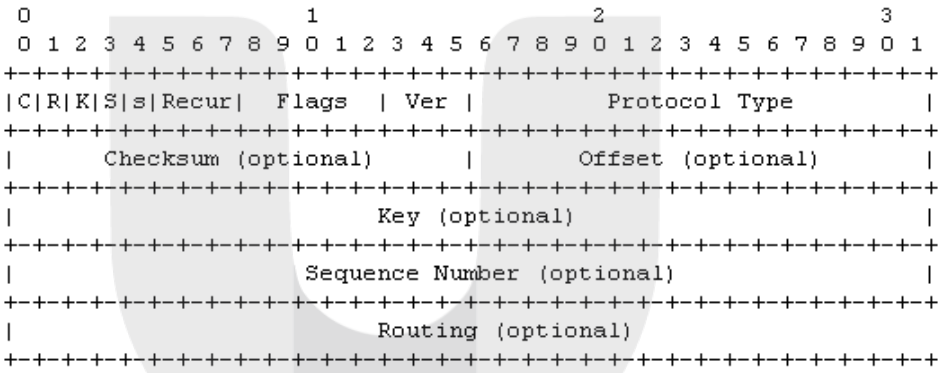
Generic Routing Encapsulation (GRE) merupakan sebuah protokol *tunneling* yang memiliki kemampuan membawa lebih dari satu jenis protokol pengalamatan komunikasi. Paket yang akan dilewatkan melalui *foreign network* dienkapsulasi menjadi sebuah paket yang bersistem pengalamatan IP kemudian paket tersebut dilewatkan melalui *tunnel*.



Gambar 2.6 Struktur dari Enkapsulasi Paket GRE [9]

Tabel 2.4 Contoh *GRE Protocol Stack*

OSI Model *Layer*	Protokol
4.*Transport*	UDP
3.*Network* (enkapsulasi GRE)	IPv6
Enkapsulasi	GRE
3.*Network*	IPv4
2.*Data link*	Ethernet
1.*Physical*	Ethernet physical layer



Gambar 2.7 Format *Header GRE* [10]

Tabel 2.5 Informasi *Header GRE* [10]

Header	Keterangan
Checksum Present (C)	Jika di-set, akan merepresentasikan dan mengandung informasi valid
Routing Present (R)	Jika di-set, maka *Offset field* akan mengandung informasi valid.
Key Present (K)	Jika di-set, maka *Key field* akan mengandung informasi valid
Sequence Number Present (S)	Jika di-set, maka *Sequence Number field* akan mengandung informasi valid

Strict Source Route (s)	Hanya disetting bila semua informasi routing terdiri dari *Strict Source Route*
Recursion Control (Recur)	Mengandung jumlah enkapsulasi tambahan yang diizinkan
Flags	*Bit-bit* ini harus bernilai 0
Version	Menunjukkan versi dari protokol GRE. Biasanya di-set 0, namun bila menggunakan PPTP, maka di-set 1
Protocol	Menunjukkan tipe protokol dari *payload* paket
Checksum	Mengandung IP *checksum* dari GRE *header* dan *payload* paket
Offset	Mengindikasikan *byte offset* dari awal *Routing Field* ke *byte* pertama dari *Source Route Entry* yang aktif untuk diuji
Key	Menunjukkan angka yang dimasukkan oleh enkapsulator
Sequence Number	Menunjukkan nomor urut paket
Routing	*Field* ini merupakan daftar dari SRE

2.6 Quality of Service (QoS)

Komunikasi saat ini dapat dilakukan melalui jaringan data / Internet. Namun bukan berarti komunikasi data tidak memiliki hambatan. Masalah rendahnya kualitas komunikasi berhubungan erat dengan permasalahan jaringan IP yaitu rendahnya *bandwith* dari jaringan itu sendiri.

QoS adalah kemampuan suatu jaringan untuk memberikan layanan yang lebih baik pada trafik data tertentu pada berbagai jenis platform teknologi. Masalah utama dari Qos adalah *delay, jitter, packetloss, dan throughput.*

2.6.1. Delay

Delay adalah waktu yang dibutuhkan data untuk menempuh jarak dari asal ke tujuan. Bermacam – macam *delay* antara lain:

a. *Inter Arrival Time* yaitu *Delay* yang terjadi antar kedatangan paket

b. *Propagation Delay* yaitu *Delay* ini terjadi karena perambatan atau perjalanan paket IP di media transmisi ke alamat tujuan.

c. *Processing Delay (Digititation and Packetitation)* yaitu *Delay* ini disebabkan sumber yang mengirimkan paket, pemrosesan paket, bergantung pada kemampuan dan beban *host*.

2.6.2. Jitter

Jitter adalah variasi delay, hal ini diakibatkan oleh variasi-variasi dalam panjang antrian, dalam waktu pengolahan data, dan juga dalam waktu penghimpunan ulang paket-paket di akhir perjalanan paket.

2.6.3. *Packetloss*

Packetloss adalah jumlah paket hilang. Hilangnya paket disebabkan oleh banyak faktor. Diantaranya yaitu, perangkat jaringan memiliki *buffer* untuk menampung data yang diterima. Jika terjadi kongesti yang cukup lama, *buffer* akan penuh, dan data baru tidak akan diterima, sehingga terjadi *packetloss*.

2.6.4. *Throughput*

Throughput adalah besar paket yang sampai dengan baik dari sumber ke tujuan dalam suatu periode waktu. *Throughput* dapat dihitung dengan membandingkan jumlah paket data yang diterima dengan baik dengan waktu pengiriman antara paket pertama dengan paket terakhir.

BAB V

KESIMPULAN DAN SARAN

5.1 KESIMPULAN

Kesimpulan yang dapat diambil dari hasil penelitian dan analisis yang telah dilakukan adalah:

1. *Protocol security IPSec* telah berhasil diimplementasikan pada *interface tunnel GRE*. Hal ini dapat dibuktikan dengan paket data yang dipertukarkan telah terenkripsi, sehingga sniffer tidak dapat melakukan tindakan lanjutan seperti memodifikasi paket data maupun merelay kembali paket suara. Penggunaan IPSec memberikan keuntungan dalam hal layanan keamanan pada saat data dipertukarkan. Akan tetapi, tentunya ada yang harus dibayarkan untuk layanan keamanan tersebut yaitu menurunnya performansi. Hal ini dikarenakan delay proses enkripsi serta penambahan header.
2. Berdasarkan hasil pengukuran pada topologi yang telah dibangun dengan batasan masalah yang telah disebutkan sebelumnya, dapat diketahui:
   a. Topologi pertama : Performansi jaringan GRE IPv6-in-IPv4 tanpa IPSec lebih baik daripada setelah diimplementasikan IPSec, dapat dibuktikan berdasar hasil pengukuran parameter QoS (tanpa background traffik) berikut

Parameter *QoS*	GRE IPv6-in-IPv4	GRE IPv6-in-IPv4 + IPSec
Delay (Average)	19.913 ms	19.90465 ms
Jitter (Average)	0.702694 ms	1.713841 ms
Packetloss (Average)	0 %	0 %
Throughput (Average)	39486.23 bps	36569.67 bps

   b. Topologi kedua : pada topologi kedua hanya berhasil membangun komunikasi VoIP pada GRE IPv4-in-IPv6, sementara IPSec tidak berhasil diimplementasikan pada interface tunnel, dikarenakan pada *Virtual Tunnel Interface IPSec* (VTI)

hanya menyediakan untuk traffik IPv6. Hal ini telah disebutkan pada salah satu *cisco guide* yang berjudul "Implementing IPSec in IPv6 Security " dengan kalimat yang menyatakan hal tersebut adalah "*The IPSec Virtual Tunnel Interface (VTI) provides site-to-site IPv6 crypto protection of IPv6 traffic"*. Sementara hasil pengukuran parameter QoS (tanpa *background traffic*) layanan VoIP pada jaringan GRE IPv4-in-IPv6 sbb:

Parameter *QoS*	GRE IPv4-in-IPv6
Delay (Average)	19.83585 ms
Jitter (Average)	0.066425 ms
Packetloss (Average)	0 %
Throughput (Average)	53604.61 bps

5.2 SARAN

Saran yang dapat penulis berikan untuk penelitian selanjutnya mengenai topik tugas akhir ini adalah:

1. Pada penelitian ini metode interkoneksi menggunakan transisi yaitu tunneling GRE. Untuk penelitian selanjutnya dapat menggunakan metode interkoneksi yang lain misal tunneling yang lain atau menggunakan metode translasi.
2. Pada penelitian ini tidak dibahas tentang user dibelakang proxy menggunakan mekanisme NAT, sehingga pada penelitian selanjutnya diharapkan dapat membahas hal tersebut.
3. Melakukan implementasi IPSec dengan kedua mode yaitu *tunnel mode* pada *core network* dan *transport mode* pada *host-gateway*.

DAFTAR PUSTAKA

[1] Rey, Marina Del. *RFC 791 Internet Protocol.* Internet Engineering Task Force, 1981

[2] S. Deering, R Hinden. *RFC 2460 Internet Protocol version 6 (IPv6) Spesification.* Internet Engineering Task Force, 1998

[3] R. Hinden, S. Deering. *RFC 4291 IP version 6 Addressing Architecture*. Internet Engineering Task Force, 2006.

[4] S. Kent, K. Seo. *RFC 4301 Security Architecture for the Internet Protocol.* Internet Engineering Task Force, 2005

[5] S. Kent. *RFC 4302 IP Authentication Header*. Internet Engineering Task Force, 2005.

[6] S. Kent, *RFC 4303 IP Encapsulating Security Payload*. Internet Engineering Task Force, 2005.

[7] D. Harkins, D. Carrel. *RFC 2409 The Internet Key Exchange (IKE).* Internet Engineering Task Force, 1998.

[8] *IPSec in VoIP Network.* Available [online]: http://www.newport-network.com, 2011.

[9] D. Farrinacci, dkk. *RFC 2784 Generic Routing Encapsulation (GRE).* Internet Engineering Task Force, 2000.

[10] S. Hanks, dkk. *RFC 1701 Generic Routing Encapsulation (GRE).* Internet Engineering Task Force,1994.