IMPLEMENTASI DAN ANALISIS SISTEM KEAMANAN IP SECURITY (IPSEC) DI DALAM MULTI PROTOCOL LABEL SWITCHING-VIRTUAL PRIVATE NETWORK (MPLS-VPN) PADA LAYANAN BERBASIS IP MULTIMEDIA SUBSYSTEM (IMS)

IMPLEMENTATION AND ANALYSIS SECURITY SYSTEM OF IP SECURITY (IPSEC) IN MULTI PROTOCOL LABEL SWITCHING-VIRTUAL PRIVATE NETWORK (MPLS-VPN) SERVICE BASED ON IP MULTIMEDIA SUBSYSTEM (IMS)

Reza Arlan[1], Rendy Munadi[2], Nur Andini[3]

[1,2,3]Program Studi S1 Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom

rezaarlan@students.telkomuniversity.ac.id[1], rendymunadi@telkomuniversity.ac.id[2], nurandini@telkomuniversity.ac.id[3]

Abstrak

Permasalahan kemanan jaringan selalu dikembangkan sejalan dengan perkembangan teknologi informasi. *IP Security (IPsec)* merupakan metode enkripsi untuk melindungi kerahasiaan, dan keutuhan data pengguna layanan di jaringan public. *Multi Protocol Label Switching – Virtual Private Network (MPLS-VPN)* yang banyak digunakan belum sepenuhnya aman, hal ini dikarenakan *MPLS-VPN* hanya membentuk saluran yang terpisah dari saluran lainnya pada jaringan internet sedangkan data yang dilewati belum terenkripsi. *IPSec* pada *MPLS-VPN* merupakan solusi yang sangat tepat untuk meningkatkan kemanan pada layanan berbasis *IP Multimedia Subsystem (IMS)* Dari hasil pengujian upaya *network scanning* dari luar *core* ke dalam *core MPLS-VPN* tidak berhasil, hal ini karena propagasi paket di dalam *core* menggunakan metode *virtual routing and forwarding (vrf)* dan ditambahkannya *route distinguisher (rd)* pada MPLS-VPN. Dari upaya *sniffing* trafik voice dan chat di dalam *core MPLS-VPN* didapatkan bahwa paket-paket dapat di-*capture* dan dibuka isinya, namun dengan *IPSec tunnel* komunikasi *client* tidak dapat dibuka karena sudah dienkripsi oleh protokol *ESP*. Penyisipan paket *MPLS* dapat dilakukan menggunakan *tools loki* dari, namun dengan adanya *IPSec tunnel* penyisipan paket tidak dapat dilakukan. Sistem keamanan *MPLS-VPN* dan *IPSec Tunnel* tidak menjamin dari serangan *Denial of Service (DoS)*, dari pengujian didapat *packet loss* mencapai kisaran 30 persen yang artinya masih dibawah standar ITU-T G.104 yang memiliki ambang batas maksimal 20 persen.

Kata kunci: Keamanan jaringan, *IP Security, MPLS-VPN, IP Multimedia Subsystem*

Abstract

Network security issues have always been developed in line with the development of information technology. IP Security (IPsec) is a method of encryption to protect the confidentiality and integrity of user data services in public networks. Multi Protocol Label Switching - Virtual Private Network (MPLS-VPN) are widely used yet fully secure, this is because MPLS-VPN only form a separate channel from the other channels on the internet while the network through which data is not encrypted. IPSec on MPLS-VPN is the perfect solution to improve the security on the service based on IP Multimedia Subsystem (IMS) From the experiment obtained that network scanning to get an overview of the topology of the outer core into the core MPLS-VPN does not work, it is because of the propagation of the package is in the core using a label to establish Label Switching Path (LSP) through the process of virtual routing and forwarding (VRF) and added a route distinguisher (rd) at MPLS-VPN. Sniffing voice and chat communications in MPLS-VPN core found that the packets can be captured and the contents of the communication can be opened, but with IPSec tunnel the content of the packets cannot be opened because the packet has been encrypted using ESP protocol. Insertion package and modifications MPLS paths can be done using the tools loki in MPLS-VPN core, but with IPSec tunnel the insertion of packets towards client can not be done. The security system MPLS-VPN and IPSec Tunnel not guarantee from Denial of Service (DoS) attack, obtained from the testing of packet loss in the range of 30 percent which means it is still under the ITU-T G.104 standard which has the maximum threshold of 20 percent.

Keywords : ***Network Security, IP Security, IP Multimedia Subsystem***

1. Pendahuluan

Keamanan jaringan teknologi informasi dan komunikasi saat ini memiliki definisi yang berbeda-beda. Kata "aman" dapat diartikan sangat berbeda antara satu pengguna dengan pengguna lainnya. Bagi pengguna layanan berjualan *online* keamanan website yang menjajakan dagangan sangatlah penting karena jika sampai website terganggu maka kepuasan pelanggan pun akan berkurang karena ketersediaan (*availability*) konten dagangan dalam web tidak boleh sampai hilang walaupun hanya beberapa saat. Berbeda halnya untuk militer dan Bank, kerahasiaan *(confidentiality)*, keutuhan data *(integrity)*, dan keaslian *(authentication)* dari data merupakan hal utama. *Multi Protocol Label Switching-Virtual Private Network (MPLS-VPN)* pada dasarnya sudah menyediakan keamanan berupa pembentukan jalur tersendiri untuk pengguna VPN, namun ditinjau dari kerahasiaan, keaslian dan keutuhan masih dipertanyakan karena data tidak dienkripsi. Dalam hal kerahasiaan, keaslian dan keutuhan data *IP Security (IPSec) Tunnel* merupakan solusi yang paling tepat untuk menjawab kebutuhan kemanan tersebut.

.

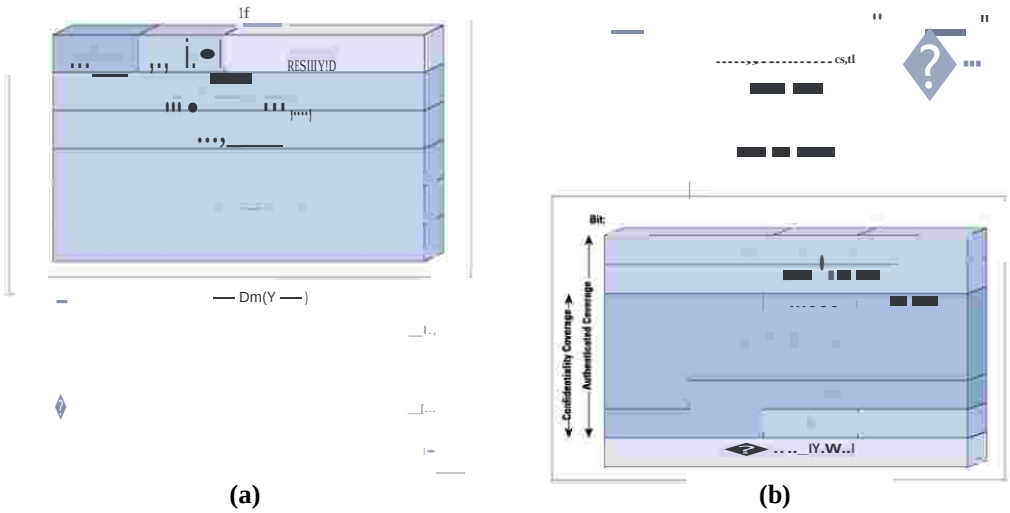
2. Dasar Teori

A. *IP Security (IPSec)* [2]

IP Security merupakan standar yang didefinisikan oleh RFCs 2401 untuk memastikan kemanan dan privasi dalam komunikasi menggunakan protocol IP. Standar *IPSec* menyediakan kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan autentikasi perangkat (*authentication*). *IPSec Tunnel* dibuat untuk menjaga kemanan data antar *IPSec gateway*. *IPSec gateway* bertanggung jawab menjaga kerahasiaan, keutuhan dan keaslian data karena hanya di *endpoint IPSec tunnel* saja yang dapat membuka enkripsi dari data yang sudah dienkripsi di *IPSec gateway* sebelumnya.

IP Security merupakan protokol yang mengintegrasikan fitur kemanan yang didalamnya meliputi proses autentikasi, integrasi, dan kepastian ke dalam *Internet Protocol (IP)*. Dalam *OSI Layer* proses tersebut dilakukan di *layer network* dengan melakukan *tunneling* atau biasa disebut *IPSec Tunnel*. Dalam proses komunikasi akan dilakukan enkripsi dan atau dibuatkan media komunikasi *(tunnel)* yang protokol kemanannya ditentukan oleh dua *peer* tersebut. Adapun protokol yang digunakan dalam proses enkripsi yaitu :

1. *Authentication Header* (AH)
   Protokol AH berfungsi melakukan proteksi pencurian data yang dibuat dengan cara melakukan enkapsulasi paket IP asli ke dalam paket baru yang mengandung IP *Header* yang baru yaitu AH *Header* disertai dengan *header* yang asli.
2. *Encapsulated Security Payload* (ESP)
   Protokol ini berfungsi untuk menjaga kepastian data, autentifikasi sumber data, dan proteksi gangguan terhadap data. Protokol ESP dibuat dengan mengenkripsi pada paket IP dan membuat paket IP lain yang mengandung *header* IP asli dan *header* ESP. Data yang terenkripsi (yang mengandung *header* IP asli) dan *trailer* ESP, hanya sebagian yang terenkripsi dan lainnya tidak.



(a) **(b)**

Gambar 1 Paket *header* AH (a) dan paket *header* ESP (b) [6]

B. *Multi Protocol Label Switching-Virtual Private Network (MPLS-VPN)* [1] [4] [5]

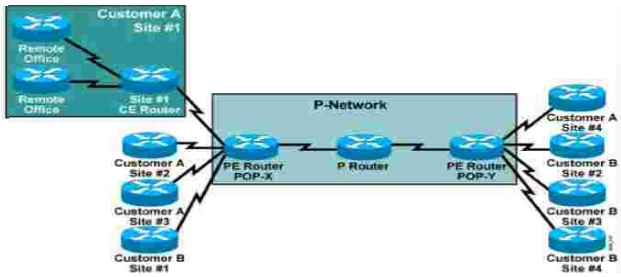
Multi Protocol Label Switching merupakan teknologi yang memberikan alternatif baru dalam proses pengiriman paket pada jaringan. Arsitektur MPLS memberikan solusi tentang mekanisme pemberian label *switching*, hal ini merupakan gabungan dari kelebihan kecepatan pengiriman paket pada *switching layer 2* dengan kelebihan-kelebihan dari proses *routing* dengan skalabilitas *layer 3*. Seperti pada jaringan-jaringan layer

2 (*frame relay* atau ATM), MPLS memberikan label pada tiap paket agar dapat melewati sebuah jaringan.

Proses pengiriman melalui suatu jaringan disebut dengan *packet swapping*. Perbedaan mendasar antara MPLS dengan teknologi IP biasa adalah pemberian label-label pada paket dan pada *label stack* yang disisipkan pada paket. Dalam prosesnya paket diteruskan berdasarkan *label switching* dan bukan menggunakan *IP Switching*. Label tersebut dimuat bersama dengan paket IP, yang selanjutnya router akan meneruskan trafik dengan melihat label, bukan berdasarkan alamat IP.

Gambar 2 Format *MPLS header* [4]

MPLS VPN membagi keseluruhan jaringan ke dalam *customer-controlled part* (jaringan-C) dan *provider-controlled part* (jaringan-P). Bagian yang berdekatan dari jaringan-C dinamakan *site* dan terhubung dengan jaringan-P via router CE. Router CE terhubung ke router PE, yang bertindak sebagai perangkat bagian tepi dari jaringan-P. Perangkat *core* di jaringan-P yaitu router P menyediakan transit *transport* melewati jaringan utama *(backbone)* dari *Service Provider* tanpa membawa rute pelanggan [3].



Gambar 3 Arsitektur MPLS VPN [3]

C. Celah Keamanan Jaringan

1. Port Scanning

Melalui *port scanning* seorang *attacker* bisa melihat fungsi dan cara bertahan sebuah sistem dari berbagai macam *port*. Seorang *attacker* bisa mendapatkan akses kedalam sistem melalui *port* yang tidak dilindungi. Contohnya *scanning* bisa digunakan untuk menentukan dimana *default FTP string* di buka untuk publik, yang artinya informasi bisa digali lebih lanjut dan selanjutnya melakukan proses *remote.*

2. Denial of Service (DoS)

Seorang *attacker* bisa mengurangi kecepatan *network* dan *host-host* yang berada di dalamnya secara signifikan dengan cara terus melakukan *request* terhadap suatu informasi dari *sever* yang bisa menangani serangan klasik *Denial Of Service (Dos)*, mengirim *request* ke satu *port* secara berlebihan dinamakan *flooding*, kadang hal ini juga disebut *spraying*. Ketika permintaan *flood* ini dikirim ke semua *station* yang berada dalam *network* serangan ini dinamakan *broadcasting*.

3. Exploit

Berbicara masalah sistem kemanan maka *password* merupakan sesuatu yang umum jika kita bicara tentang kemanan. *Password* adalah salah satu prosedur kemanan yang sangat sulit untuk diserang, seorang *attacker* mungkin saja mempunyai banyak *tools* (secara teknik maupun dalam kehidupan sosial) hanya untuk membuka sesuatu yang dilindungi oleh *password*. Ketika seorang *attacker* berhasil mendapatkan password yang dimiliki oleh seorang user, maka ia akan mempunyai kekuasaan yang sama dengan user tersebut. Kebanyakan serangan yang dilakukan terhadap *password* adalah menebak (*guessing), brute force, cracking dan sniffing.*

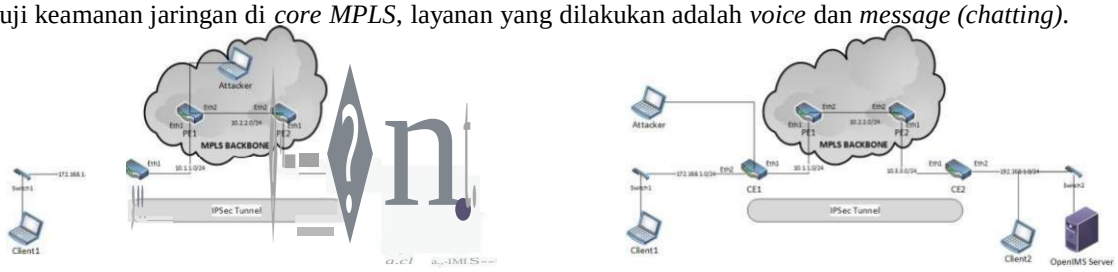
4. Eavesdropping (Traffic Capturing)

Pada kasus ini seorang pengguna layanan mengirimkan isi message dengan kunci enkripsi yang diketahui oleh suatu proxy. Meskipun proxy tersebut dapat dipercaya, namun jika administrator jaringan tersebut nakal maka mungkin saja untuk mendekripsi encrypted-text tersebut, bahkan memodifikasi kunci enkripsi. Hal ini dikategorikan sebagai serangan man-in-the middle yang mengubah karakteristik keamanan yang diinginkan oleh pengguna.

3. Perancangan Dan Implementasi

A. Implementasi Sistem

Perencanaan topologi jaringan dilakukan dengan mengkonfigurasi dua komponen terlebih dahulu yaitu *server IMS* dan *MPLS-VPN*. Dalam tugas akhir ini *MPLS-VPN* menggunakan 4 buah *router* mikrotik rb750 dimana 2 *router* difungsikan sebagai *Customer Edge* dan 2 router lagi difungsikan sebagai *Provider Edge*, dimana *Provider Edge* diasumsikan terhubung dengan *router Provider* di *cloud* jaringan. Setelah dilakukan konfigurasi keempat *router* mikrotik kemudian dilakukan konfigurasi *IP Security tunnel* (*IPSec tunnel*) di sisi *gateway*, dalam hal ini CE1 dan CE2 merupakan *gateway* dari dua *customer* dengan jaringan yang berbeda. Setelah itu dilakukan konfigurasi pada *OpenIMSCore* sebagai IMS *Server*. Apabila masing-masing komponen telah berjalan semestinya dan terkoneksi dengan baik maka dilanjutkan dengan konfigurasi untuk *server* dan *client*. Ketika sistem sudah berhasil dijalankan selanjutnya dilakukan pengujian sesuai skenario yang telah didesain untuk menguji keamanan jaringan di *core MPLS*, layanan yang dilakukan adalah *voice* dan *message (chatting)*.



(a) (b)

Gambar 4 Topologi serangan (a) dari dalam *core* dan (b) serangan dari luar *core*

B. Perangkat Implementasi

Pada tabel dibawah terdapat beberapa perangkat lunak yang dibutuhkan dalam rencana implementasi tugas akhir ini.

Tabel 1 Perangkat lunak pada implementasi Tugas Akhir

No	Perangkat	Jumlah	Keterangan
1	OpenIMSCore	1	Digunakan sebagai sistem *IP Multimedia Subsystem*.
2	Boghe / UctIMSClient	2	Digunakan sebagai perangkat *client IMS* dalam menggunakan layanan yang *diinstal* di *PC client*
3	Operating System Linux Backtrack 5 R3	1	Digunakan sebagai *Operating System* bagi *attacker* dalam usaha meretas sistem kemanan.
4	Winbox	1	Tools yang digunakan untuk melakukan konfigurasi router mikrotik.
5	Wireshark	1	Tools yang digunakan untuk *analysis traffic* dan *sniffing.*
6	Loki	1	Tools yang digunakan untuk *label injection* di *core MPLS*

Adapun beberapa perangkat keras untuk merealisasikan dan menganalisis sistem di atas, diantaranya.

Tabel 2 Perangkat keras pada implementasi Tugas Akhir

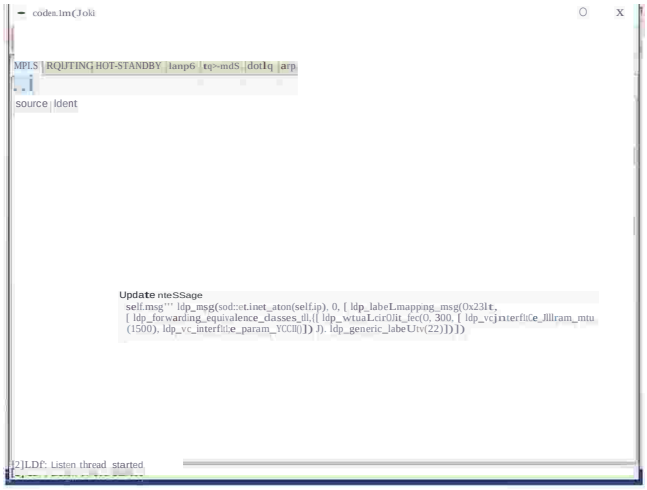
No	Perangkat	Spesifikasi / Tipe	Jumlah	Keterangan
1	Personal Computer	Intel Core i3 3Ghz, 4GB DDR3, 500GB	1	Digunakan sebagai dan *server IMS*

2	Router	Mikrotik RB750	4	Digunkan sebagai perangkat *MPLS* dan *IPSec*
3	Laptop	Intel Core i3 2.4 Ghz. 4GB DDR2, Hardisk 320GB	2	Digunakan sebagai *attacker* dan *client* IMS.
4	Kabel UTP	Kategori 5	Menyesuaikan	Link penghubung pada layer *physics.*

4. Pengujian Dan Analisis

A. Pengujian Skenario 1

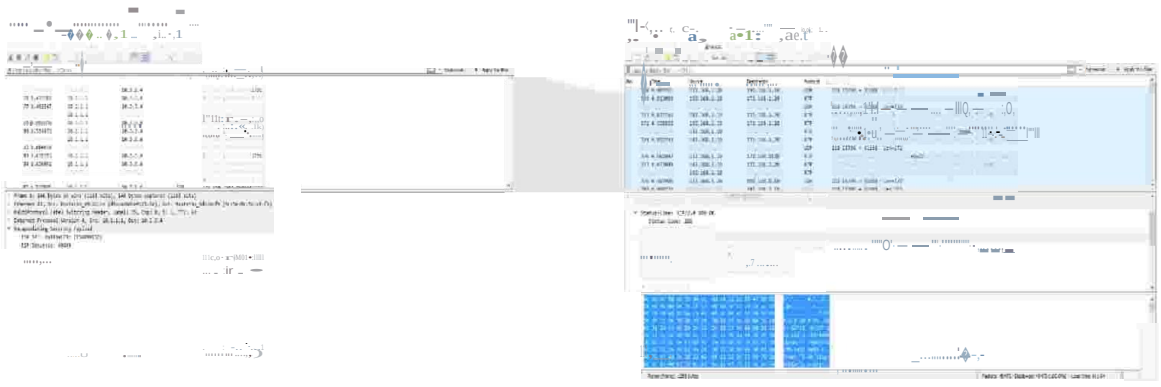
Dari pengujian tidak didapatkan gambaran dari topologi *core MPLS-VPN* yang digunakan oleh *client IMS* untuk melakukan komunikasi. Hal ini disebabkan pada router PE dilakukan penambahan alamat ip menggunakan *route distinguisher (rd)* sebesar 64 bit yang ditambahkan pada alamat ip sebesar 32 bit sehingga membentuk alamat unik sebesar 96 bit untuk membuat *Label Switch Path* (LSP) berdasarkan label. Karena menggunakan jalur yang dibentuk LSP berdasarkan label maka penyerang tidak dapat melakukan tracing melalui pengiriman paket ICMP (ping). Penambahan Enkripsi IPSec membuat keamanan meningkat jika penyerang berupaya membuka isi komunikasi di luar core MPLS-VPN, hal ini dikarenakan sudah terbentuk *tunnel* antara 2 *router gateway*. Jadi dalam hal ini fungsi enkripsi *IPSec* menjaga keamanan data saat penyerang berusaha membongkar isi komunikasi sebelum data masuk ke dalam core MPLS-VPN.



Gambar 5 Proses *network scanning* tidak berhasil

B. Pengujian Skenario 2

Pada pengujian terhadap celah keamanan di dalam *core MPLS-VPN* tanpa *IPSec Tunnel* dalam melewati layanan *voice* yang dilakukan oleh *2 client*. Dari paket-paket yang ditangkap dan dianalisa dapat diketahui bahwa pengamanan *MPLS-VPN* dengan pemisahan jalur belum cukup kuat dan meninggalkan banyak celah keamanan jika dilakukan proses *sniffing* yang dilakukan dari dalam *core MPLS-VPN*, terutama paket data *rtp* yang tidak dilindungi. Dari paket data tersebut kita dapat melihat secara jelas alamat ip dari *user* (baik *client 1* maupun *client 2*), dan juga alamat ip dari *server*. Dengan penambahan tunnel IPSec didapat hasil *sniffing* berupa protokol ESP. Hal ini dikarenakan sebelum paket-paket dilewatkan, *router* CE1 dan CE2 akan melakukan 2 *phase* dalam SA yaitu yang pertama adalah *IKE* dan selanjutnya membentuk *IPSec tunnel*. Dalam prosesnya, paket yang dilewatkan pada tunnel akan dienkripsi dengan protokol ESP, jalur *inbound* dan *outbound* akan dikonfirmasi oleh 2 *gateway tunnel* melalui *Security Parameter Index* (*SPI*). Dengan menggunakan algoritma enkripsi *3DES 168 bit* kemanan dan kerahasiaan percakapan dapat terjamin dan keaslian data pun terjamin karena melalui proses *authentication* antara *router CE1* dan *router CE2* yang menggunakan algoritma SHA1 dalam prosesnya. Aspek kemanan terutama *confidentiality* (kerahasiaan) dan *authentication* (keaslian) terpenuhi dari uji coba keamanan IPSec Tunnel di dalam core MPLS-VPN.

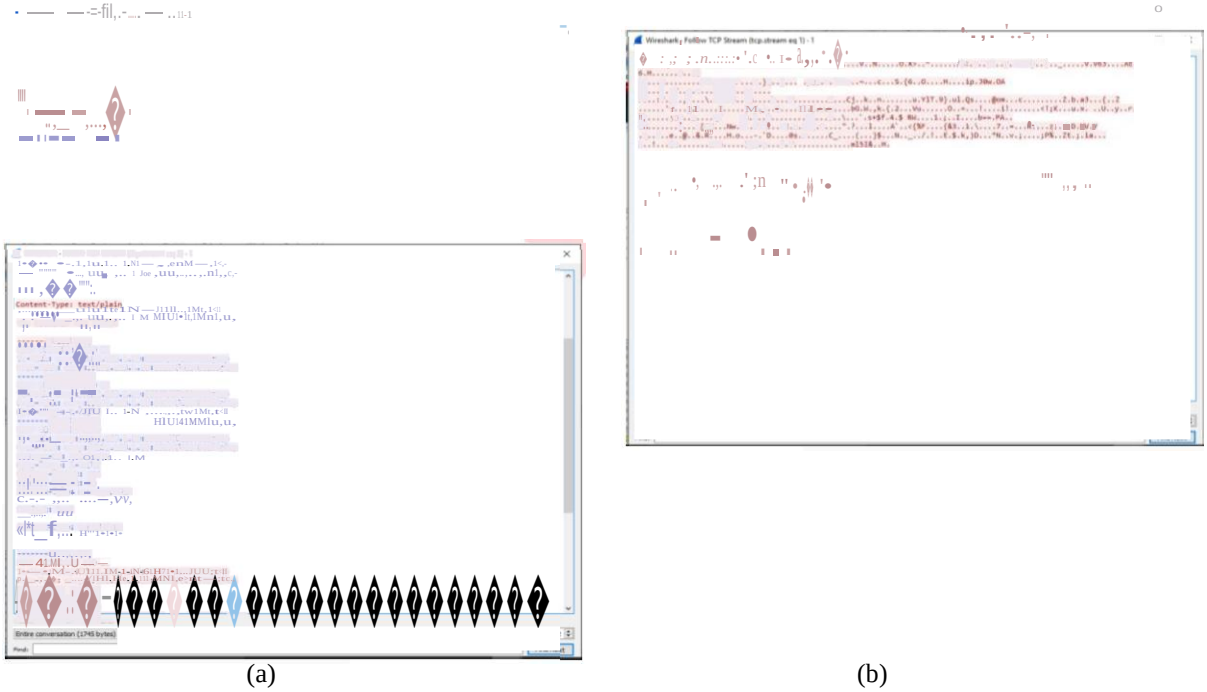


(a) (b)

Gambar 6 Hasil *sniffing* (a) di *core* MPLS-VPN dan (b) MPLS-VPN *IPSec tunnel* untuk layanan *voice*

C. Pengujian Skenario Ketiga

Dari hasil pengujian terbukti bahwa tanpa proses enkripsi, jika penyerang melakukan serangan di dalam core MPLS kemungkinan komunikasi yang dilakukan dapat dilihat isinya oleh si pelaku *sniffing*. Protokol *msrp* yang pada dasarnya berbasis *text* seperti halnya *http*, *sip* atau *rtsp* sangat mudah untuk men- *decode* paket sehingga isi komunikasi dapat terlihat. Hal ini dikarenakan sudah banyak format yang mendukung seperti ASCII. Selain paket yang dapat di *decode* dan dilihat isi komunikasi *client* terdapat juga beberapa informasi lain berupa alamat ip *client*. Hal ini sangat riskan karena penyerang dapat merencanakan penyerangan lainnya dari informasi yang didapat. Dengan menambahkan *IPSec tunnel* isi dari komunikasi *client* tidak dapat dibuka karena sudah dienkripsi oleh protokol ESP antara *router* CE1 dengan *router* CE2. Dari hasil *capture* hanya didapat protokol-protokol yang digunakan dalam proses *routing* antar *router* PE1 dan PE2 sehingga informasi hanya sebatas mengenai protokol yang hanya ada di dalam *core MPLS*, namun untuk data layanan IMS tidak dapat dilihat karena sudah dienkripsi terlebih dahulu, dengan kata lain paket yang diterima oleh *client* adalah paket asli dari jaringan *client 1* dan *client 2* tanpa campur tangan penyerang. Hal ini karena diterapkannya proses *authentication* menggunakan algoritma *sha1* pada *router* CE1 dan *router* CE2.

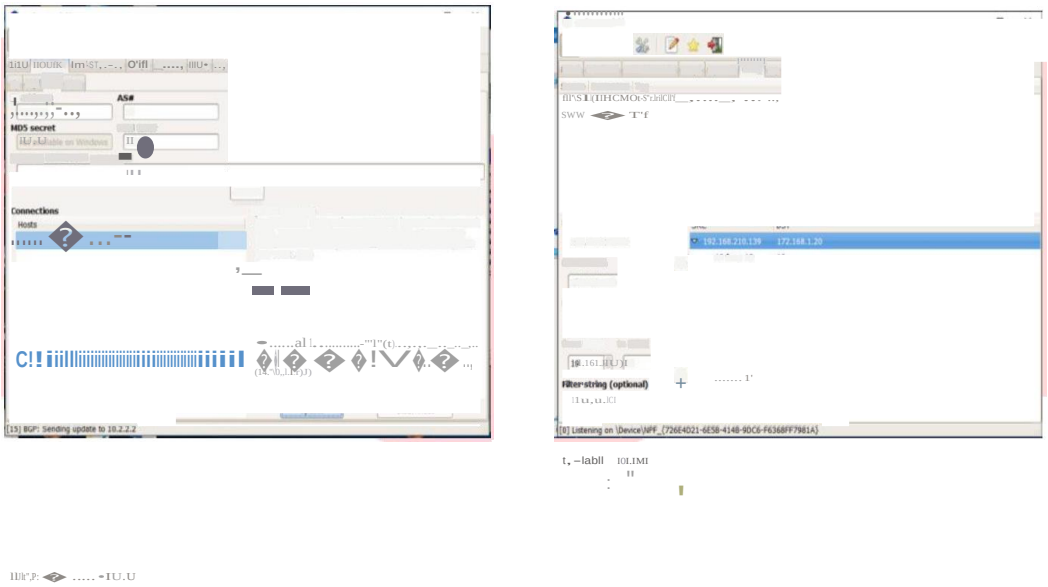


(a) (b)

Gambar 7 Isi komunikasi layanan *chat* pada (a) *core* MPLS-VPN dan (b) *core* MPLS-VPN *IPSec tunnel*

D. Pengujian Skenario Keempat

Dari pengujian modifikasi jalur dan penyisipan trafik dapat dilakukan dari dalam *core* menuju *client*. Hal ini dilakukan setelah protokol *ldp* dan *bgp* dapat dimodifikasi. Proses pembagian informasi perutingan berdasarkan label oleh protokol *ldp* dapat di-*capture* oleh penyerang. Pengiriman paket *tcp* dilakukan setelah *'hello' message* diberikan kepada *host* yang diserang. Setelah koneksi terbentuk maka secara periodik akan dilakukan *'update'* message untuk mempertukarkan informasi ruting antar penyerang dan *host* yang diserang. Dalam tahap ini *virtual circuit* yang mempertukarkan label telah terbentuk sehingga modifikasi protokol *bgp* dapat dilakukan agar pembentukan dengan *autonomous system* yang berbeda dapat terbentuk. Injeksi perutingan dari penyerang berhasil setelah *keep alive message* dan *update message* secara berkala dapat dilakukan untuk menentukan parameter-parameter perutingan yang dilakukan oleh protokol bgp. Penyisipan paket dari dalam *core mpls* menuju *client* dapat dilakukan karena protokol *ldp* dan *bgp* beserta parameter-parameternya berhasil dimodifikasi. Pada pegujian dengan IPSec Tunnel data sudah dienkripsi sehingga penyerangan terhadap *server* atau *client* dari dalam *core mpls* tidak dapat dilakukan. Hal ini dikarenakan router CEs sebagai *ipsec peer* melakukan proses *inter key exchange (ike)* dimana diantaranya dilakukan pemilihan algoritma keamanan yang digunakan , sehingga trafik yang bisa memasuki jaringan lokal *router CEs* harus melewati negosiasi antar *gateway ipsec (SA)*. Karena penyisipan paket dilakukan di dalam *core mpls* yang notabene berasal dari tengah *tunnel* sehingga trafik akan ditolak oleh *gateway ipsec* karena tidak melalui proses *SA* antar *gateway*.



(a) (b)

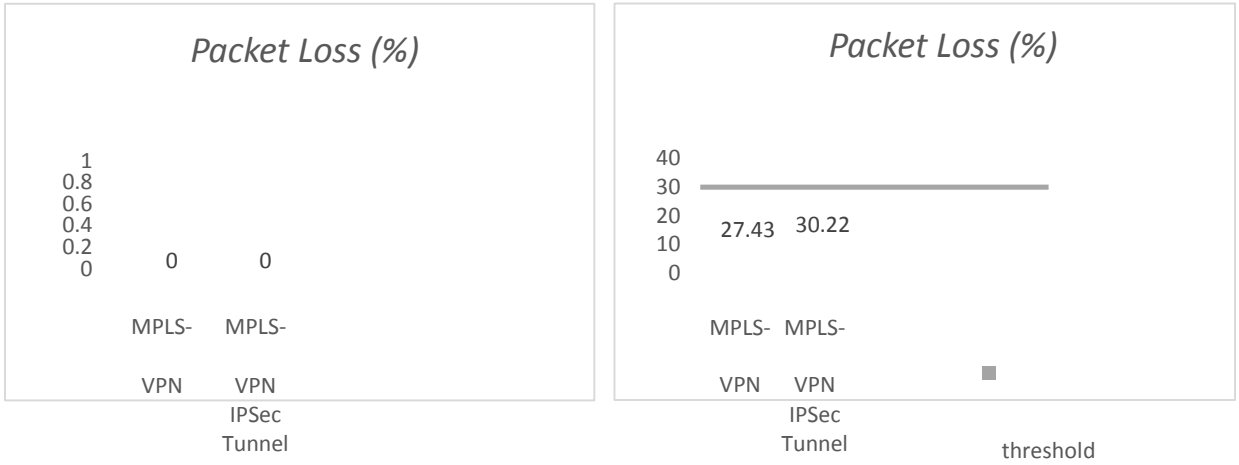
Gambar 8 Serangan (a) menuju protokol BGP dan (b) Penentuan jalur untuk penyisipan trafik

E. Pengujian Skenario Kelima

Dari pengujian serangan di core MPLS-VPN dan coe MPLS-VPN IPSec Tunnel dapat dibuktikan bahwa serangan *Denial of Service* menuju *router* PE1 menyebabkan layanan terganggu. Hal tersebut dapat dilihat dari percobaan panggilan yang gagal 6 kali dari 10 percobaan. Penyebab terganggunya layanan adalah karena *router* PE1 dibanjiri paket *TCP* yang dikirim oleh *tools slowloris* dan juga *hping3* sehingga *router* terpaksa harus membalas paket-paket TCP yang dikirim penyerang dalam jumlah sangat banyak sehingga pengiriman data antar *client IMS* yang seharusnya dilayani malah terganggu.

(a) (b)

Gambar 9 Serangan (a) menggunakan *slowloris (b) Call Terminated* dialami client akibat serangan *DDoS*



(a) (b)

Gambar 10 Hasil pengukuran *packet loss* (a) *sebelum* serangan dan (b) saat serangan

Dari hasil pengukuran parameter *QoS* dapat dilihat *delay* dan *jitter* tidak terlalu terpengaruh serangan *DoS*, namun *packet loss* melewati batas toleransi dari standar ITU-T G.104 bahwa maksimal *packet loss* adalah 20 % sehingga kualitas layanan akan sangat buruk. Hal ini dapat terjadi karena *router PE1* yang tidak dapat melayani banyaknya trafik yang masuk ke router sehingga ada sejumlah paket yang di drop. *Packet loss* disebabkan karena *router* PE1 yang terbebani, dimana *router* harus memberikan *acknowledge* dari paket-paket *tcp* yang dikirmkan oleh penyerang. Paket *tcp* harus dikonfirmasi oleh router bahwa paket sudah diterima, sedangkan komunikasi *voice* yang menggunakan protokol udp dimana paket yang dikirimkan ke *router* tidak harus mengirimkan *acknowledge* sehingga prioritasnya dibawah paket *tcp*, hal inilah yang menyebabkan *packet loss*.

5. Kesimpulan

Kesimpulan yang dapat diambil dari hasil penelitian dan analisis yang telah dilakukan adalah *MPLS-VPN* pada implementasi tugas akhir menyediakan jalur yang terpisah yang dibentuk dari alamat *IPv4* sebesar 32 bit dan alamat yang ditambahkan oleh *route distinguisher (rd)* sebesar 64 bit. Dengan metode *tunneling IPSec* yang ditambahkan pada *MPLS-VPN backbone* akan menghubungkan dua *site* yang terpisah secara *point to point* yaitu antara r*outer CE1* dengan *interface* 10.1.1.1 dan router CE2 dengan *interface* 10.3.3.4. *MPLS-VPN* memberikan keamanan dari serangan *intrusion* oleh penyerang yang berasal dari luar *core* menuju *router* PE1. Hal ini dikarenakan propagasi *TTL* baik *forwarded traffic* dan *local traffic* dikonfigurasi secara selektif. Upaya menyisipkan paket dari dalam *core MPLS VPN* menuju *client* berhasil dilakukan namun jika ditambahkan *IPSec tunnel* gagal dilakukan. Serangan *Denial of Service (DoS)* yang menuju *router* PE1 membuat kualitas layanan sangat buruk bahkan hingga tidak dapat digunakan. Dari pengujian keamanan dapat disimpulkan bahwa *IPSec tunnel yang ditambahkan pada MPLS-VPN* memberikan pengamanan terhadap 3 aspek yaitu *confidentiality* (kerahasiaan), *integrity* (keutuhan) dan *authentication* (keaslian) namun tidak memenuhi *availability* (ketersediaan).

Daftar Pustaka

[1] Cisco Corporation (2002). "*MPLS-VPN Technology*". Cisco System.

[2] Elezi, Muhamed. Raufi, Bujar (2015). "*Conception of Virtual Private Network Using IPSec Suite of Protocols, Comparative Analysis Of Distributed Database Queries Using Different IPSec Modes of Encryption*". South East European University.

[3] Mende, Daniel. Rey, Enno dan Schmidt, Hendrik (2011). "*Practical Attacks Against MPLS Or Carrier Ethernet Networks*". ERNW Providing Security.

[4] Rashed, Shawl Q. Rukhsana, Thaker. Singh, Er. Jasvinder (2014). "*A Review : Multi Protocol Label Switching*". Department of Computer Science Engineering. BUEST.

[5] Safitri, Ellen (2013). "Implementasi Dan Analisis Perfomansi Multi Protocol Label Switching Virtual Private Network Pada Layanan Berbasis IP Multimedia Subsystem". Fakultas Elektro dan Komunikasi. Institut Teknologi Telkom.

[6] Victor A. Villagra (2002). "*Security Architecture For The Internet Protocol:IPSEC*". Telematics Department (DIT). Technical University Of Madrid.