Analisa Layanan Keamanan, Performansi Pensinyalan dan Kualitas Panggilan Interkoneksi SIP *International Direct Dialing* Menggunakan *Softswitch Class 4* dan *Session Border Controller*

Purwo Panggalih Gentayu P.M dan Mudrik Alaydrus

Teknik Elektro, Universitas Mercu Buana

Abstrak

Dalam aplikasi SIP-*Based* VoIP, dua *end point* / *User Agent* (UA) dapat berkomunikasi secara *peer to peer* / *peering* menggunakan SIP, begitu juga interkoneksi antar SIP *server* sehingga implementasi SIP-*Based* VoIP tidak hanya dapat diterapkan untuk jaringan akses, namun juga interkoneksi antar operator melalui jaringan IP. Penelitian ini mencoba memberikan analisa interkoneksi antar operator untuk *International Direct Dialing* (IDD) yang diterapkan di internasional *switching center* PT. Indosat, Tbk. menggunakan protokol SIP yang mencakup mekanisme layanan keamanan *(security service)*, performansi pensinyalan SIP dan kualitas panggilan. Layanan keamanan mencegah terjadinya kemungkinan serangan DOS dari jaringan luar. Performansi pensinyalan setelah adanya layanan keamanan menunjukan performa yang sangat baik SEER 99.6% untuk *incoming* dan 98.94% untuk *outgoing*, SER sebesar 22.68 % untuk *incoming* dan 47.11% untuk *outgoing*. Kinerja kualitas panggilan dengan perspektif penilaian pengguna (*end user*), menggunakan parameter MOS didapatkan nilai 4.4 dan R-*Factor* diantara 93-93.2 setiap jam.

***Kata Kunci**:* SIP, Layanan keamanan, Performansi Pensinyalan, Kualitas Panggilan

1. PENDAHULUAN

VoIP secara umum merujuk kepada suatu teknik komunikasi protokol / teknologi / metodologi / teknik transmissi dalam mengantarkan komunikasi suara dan multimedia *session* melalui jaringan IP. VoIP diimplementasikan dengan menggunakan berbagai protokol dan standarisasi, contoh protokol yang digunakan didalam mengimplementasikan VoIP seperti: H.323, MGCP, SIP.

Saat ini, *Session Initiation Protocol* (SIP) merupakan sebuah protokol *signaling* yang secara luas digunakan untuk mengimplementasikan VoIP, disebut SIP-*Based* VoIP. Dalam aplikasinya, dua *end point* / *User Agent* (UA) dapat berkomunikasi secara *peer to peer* / *peering* menggunakan SIP, begitu juga interkoneksi antar SIP *server* sehingga implementasi SIP-*Based* VoIP tidak hanya dapat diterapkan untuk jaringan akses, namun juga interkoneksi antar operator melalui jaringan IP.

Perkembangan yang sangat cepat dan adopsi menggunakan sistem SIP-*Based* VoIP, masalah keamanan menjadi masalah yang serius. IP adalah sistem yang terbuka, sehingga sistem yang beroperasi diatasnya rentan terhadap ancaman keamanan, tidak terkecuali SIP-*Based* VoIP. Didalam penelitian-penelitian tentang SIP-*Based* VoIP, SIP-*Based* VoIP dapat terkena aspek-aspek ancaman layanan keamanan didalam jaringan IP, seperti: *registration hijacking, impersonating a proxy, message tampering, session tear down attacks, denial of service attacks and SIP Spam attacks* [3], dan lain lain. Untuk itu diperlukan adanya suatu mekanisme keamanan jaringan untuk melindungi elemen-elemen jaringan pembentuk sistem SIP-*Based* VoIP, dalam hal ini softswitch, SIP *server*, *media gateway* dan elemen jaringan lain, yang dimiliki oleh operator dari ancaman keamanan dari celah mekanisme SIP itu sendiri maupun dari serangan eksternal yang berasal dari jaringan IP. Tidak hanya masalah tentang layanan keamanan, kinerja SIP-Based VoIP menjadi sorotan agar dapat mencapai tingkat kualitas layanan seperti sistem telepon konvensional.

Dalam penelitian ini masalah yang dirumuskan adalah analisa interkoneksi antar operator untuk *International Direct Dialing* (IDD) yang diterapkan di internasional *switching center* PT. Indosat, Tbk. menggunakan protokol SIP yang mencakup mekanisme layanan keamanan *(security service)*, performansi pensinyalan SIP dan kualitas panggilan. Tujuan dari penelitian ini adalah melakukan implementasi layanan keamanan pada interkoneksi SIP IDD menggunakan *Session Border Controller* dan menganalisa performansi pensinyalan dan juga analisa kualitas panggilan dari perspektif pengguna.

2. KAJIAN PUSTAKA

2.1 Penelitian Terkait

Didapatkan beberapa penelitian sebelumnya yang terkait dengan penelitian ini. Pada penelitian yang dilakukan oleh M. Zubair Rafique, M. Ali Akbar dan Muddassar Farooq [2009] tentang "*Evaluating DOS Attack Against SIP-Based VoIP System*" [2] dan juga penelitian oleh Liancheng Shan, Ning Jing [2009] tentang "*Research on Security Mechanism of SIP-Based VoIP System*" [3].

M. Zubair Rafique, M. Ali Akbar dan Muddassar Farooq mencoba memberikan evaluasi pengaruh serangan DOS terhadap performansi *metrics* dari sistem *SIP-Based VoIP*. Serangan DOS yang dilakukan dengan cara mengirimkan banyak ilgal *invite message* dalam satu detik dengan sebutan "*invite of death"* ditujukan ke SIP server yang menggunakan *open source*. Performansi *metrics* yang diukur dalam penelitian tersebut adalah CCR, CEL, NRR, CPU usage dan CPU *interrupt rate*. Hasil yang didapat pada penelitian tersebut memperlihatkan bahwa serangan DOS dapat secara signifikan menurunkan performansi *metrics* yang diukur dimana hal tersebut dapat menyebabkan menurunya kemampuan layanan VoIP dari operator penyedia layanan. Didalam penelitian tersebut dijelaskan bahwa penurunan performansi *metrics* merupakan sebuah tolak ukur dari tingkat ancaman yang dapat terjadi didalam infrastruktur VoIP suatu operator.

Penelitian yang lain yang berhubungan adalah penelitian yang dilakukan oleh Liancheng Shan dan Ning Jing [2009] yang berjudul *"Research on Security Mechanism of SIP-Based VoIP System"*. Pada penelitian tersebut, Liancheng Shan

dan Ning Jing memperkenalkan sistem SIP-*Based* VoIP dapat dikenakan kepada 6 aspek serangan (*attack*) diantaranya *registration hijacking, impersonating a proxy, message tampering, session tear down attacks, denial of service* (DOS) dan *SIP spam attacks*. Didalam penelitian tersebut dijelaskan bahwa pada sistem VoIP dapat dibangun sistem keamanan (*Security*) sebagai suatu sistem pelengkap yang berarti didalam meningkatkan keamanan VoIP agar dapat mencapai keamanan sistem telepon konvensional.

2.2 Pemahaman *Session Initiation Protocol* (SIP) [4]

SIP adalah sebuah protokol *signaling* yang digunakan untuk pengaturan sesi komunikasi untuk *voice* dan *video* melalui *Internet Protocol* (IP). SIP dapat digunakan untuk membuat, memodifikasi dan mengakhiri *session two-party* (unicast) atau *session multi-party* (multicast).

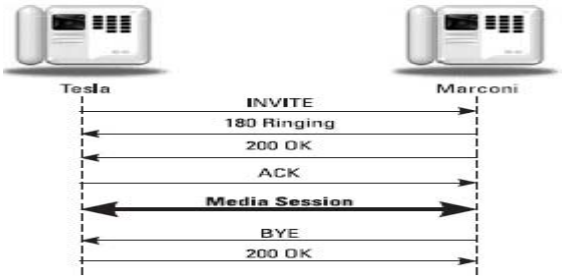
Protokol SIP merupakan protokol pada layer aplikasi yang didesain agar independen terhadap *transport layer*. SIP protocol dapat berjalan pada *Transmission Control Protocol* (TCP), *User Datagram Protocol* (UDP) ataupun *Stream Control Transmission Protocol* (STCP). SIP bersifat sederhana, berbasis teks dan sangat fleksibel terhadap pengembangan-pengembangan baru serta dapat mendukung implementasi berbagai layanan multimedia masa depan.

Fungsi utama SIP adalah untuk pembentukan dan pengakhiran panggilan *voice* atau *video*. SIP hanya terlibat pada bagian *signaling* dari suatu sesi komunikasi. Sedangkan, s*tream* komunikasi *voice* dan *video* dibawa menggunakan protokol lain yaitu, *Real-Time Protocol* (RTP). Parameter-parameter dari *stream voice* atau *video* (nomor port, jenis protokol, codec) didefinisikan dan dinegosiasikan menggunakan *Session Description Protocol* (SDP).SDP tersebut terdapat pada SIP *packet body*.

Untuk koneksi ke SIP *server*, SIP *client* biasanya menggunakan TCP atau UDP dengan nomor port 5060 atau 5061. Port 5060 biasanya digunakan untuk *signaling* pada trafik yang tidak terenkripsi *(non-encrypted traffic*) sedangkan port 5061 biasanya digunakan untuk *signaling* pada trafik yang terenkripsi (*encrypted traffic*).

2.2.1 Pembentukan SIP *Session*

Gambar 1 menunjukan pertukaran SIP *message* antara dua *end-point* melakukan koneksi SIP-*Based* VoIP. Mengasumsikan bahwa kedua *end-point* tersebut terkoneksi melalui jaringan IP dan keduanya mengetahui alamat IP masing-masing perangkat. Pemanggil (*Calling Party*), Tesla, memulai pertukaran informasi SIP *message* dengan mengirimkan *invite* ke Marconi selaku Penerima (*Called Party*).

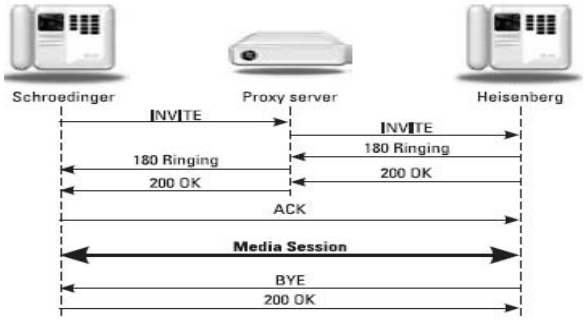


Gambar 1 Contoh Sederhana *Call Setup* SIP

Invite message berisikan tentang tipe panggilan / *session*. Tipe panggilan bisa berupa *voice session* atau *multimedia session* (*video, video converence*, dll).

Pada contoh pembentukan session sederhana, Tesla mengetahui alamat IP Marconi dan dapat secara langsung mengirimkan *invite* ke alamat yang dituju. Namun pada umumnya tidak seperti itu, alamat IP tidak bisa digunakan seperti nomer telepon terkait keterbatasan kesediaan alamat IP dan juga seluruh *user agent* tidak bisa terkoneksi satu sama lain secara langsung (direct) jika diimplementasikan untuk komunikasi suara jarak jauh.

Oleh karena itu dalam implementasinya dibutuhkan suatu server sebagai pusat yang menghandle registrasi *user agent / user gateway*, menyediakan lokalisasi dan *routing* antar *user*, menerima SIP *request* dan juga melakukan respon terhadap SIP request tersebut. Gambar 2.4 mengambarkan contoh pemanggil dan penerima melakukan panggilan melalui SIP *Server / Proxy Server*.



Gambar 2 Contoh *Call Setup* SIP menggunakan *Proxy Server*

Proxy server memfasilitasi dua *end-point* tersebut untuk melakukan lokalisasi dan pembentukan hubungan

2.3 VoIP dan Keamanan Jaringan

Keamanan jaringan merupakan dimensi yang dibutuhkan dalam upaya untuk mengamankan jaringan VoIP. Mengatasi serangan dan ancaman keramanan membutuhkan suatu proses / mekanisme. Proses ini harus dirancang untuk menggabungkan kontrol yang dapat mengatasi hal sebagai berikut:

- Mengidentifikasi ancaman dapat terjadi (*applicable threat*)
- Mengidentifikasi alur ancaman / serangan dan meminimalkan kemungkinan
- Meminimalkan dampak jika serangan / ancaman terjadi
- Mengelola dan mengurangi serangan yang terjadi

Keamanan jaringan didalam VoIP mencakup penggunaan suatu aturan keamanan (*security policy*) dan elemen jaringan (*network element*) yang digunakan untuk mengontrol, mencegah, melindungi *resource* atau pun infrastruktur jaringan VoIP. Elemen jaringan yang dapat digunakan untuk memberikan kontrol dan perlindungan terhadap VoIP salah satunya adalah *Session Border Control* (SBC).

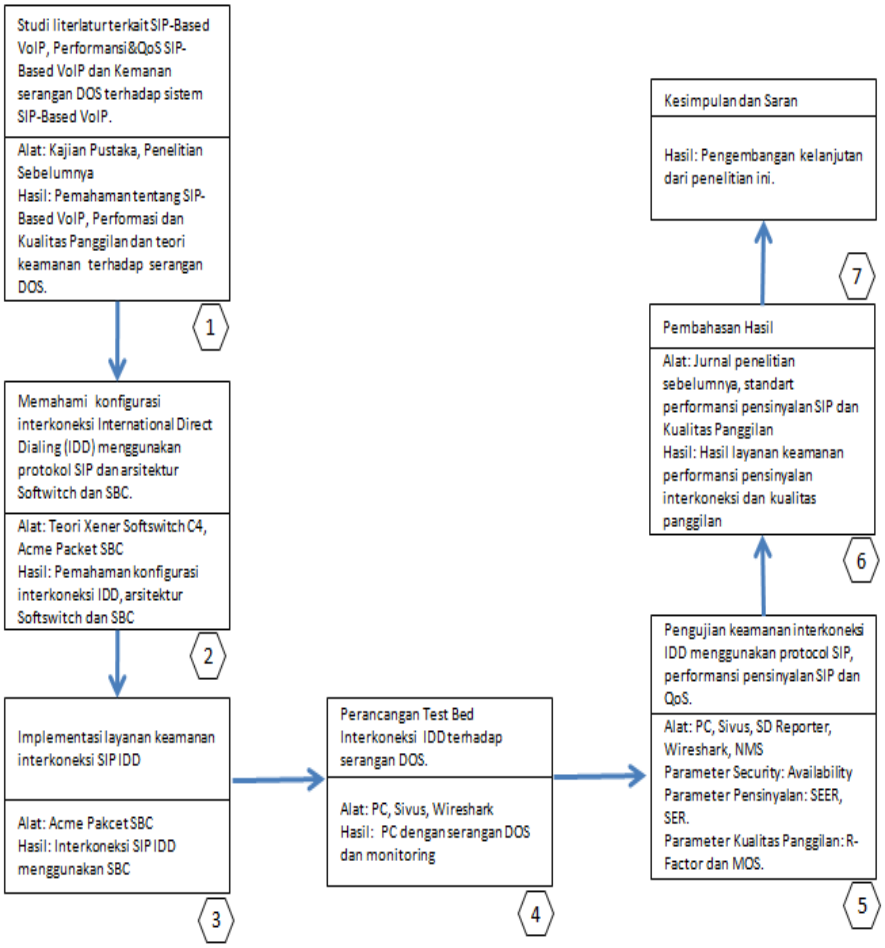
2.4 Layanan Keamanan (*Security Service*)

Security services adalah sebuah layanan yang memberikan jaminan untuk keamanan sistem atau data transfer, atau dengan kata lain *security service*

meningkatkan keamanan dari sistem dan pengiririman mereka. Pada RFC 2828, *security services* diartikan sebagai sebuah layanan pemrosesan atau komunikasi yang disediakan oleh sistem untuk memberikan sebuah proteksi tertentu untuk sumber daya sistem. Tujuan dari *security service* sendiri adalah untu melawan serangan keamanan (*security attack*). *Security service* dibagi menjadi 6 kategori, yaitu *Autentication, Access Control, Confidentiality, Integrity, Non-Repudiation dan Availability* [8].

3. METODOLOGI PENELITIAN

Metodologi yang digunakan dalam penelitian ini digambarkan sebagai berikut:

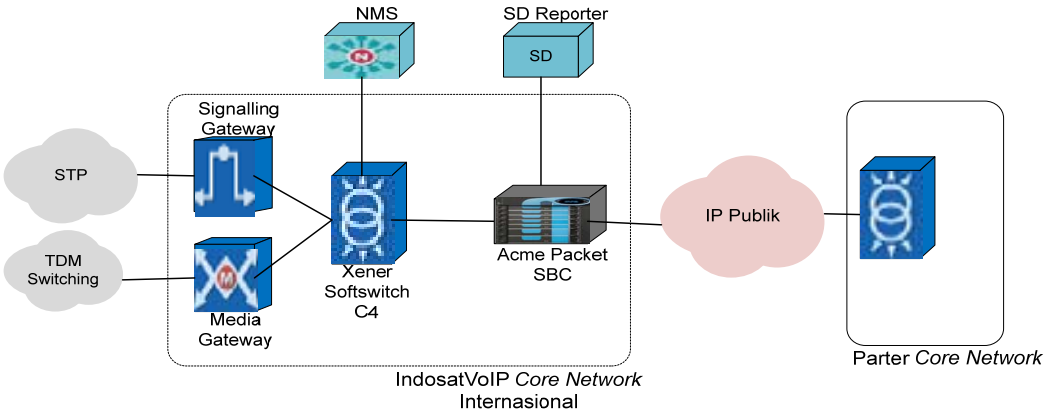


Gambar 3 Metodologi Penelitian

Penelitian ini menggunakan pendekatan secara kuantitatif dengan melakukan studi lapangan di *international switching center* PT. Indosat, Tbk. Penelitian ini melakukan beberapa tahapan untuk mencapai tujuan dalam penelitian ini, sebagaimana terlihat pada gambar di atas.

3.1 Konfigurasi Interkoneksi SIP *International Direct Dialing*

Berikut dibawah ini gambar konfigurasi interkoneksi SIP IDD sebagai berikut:



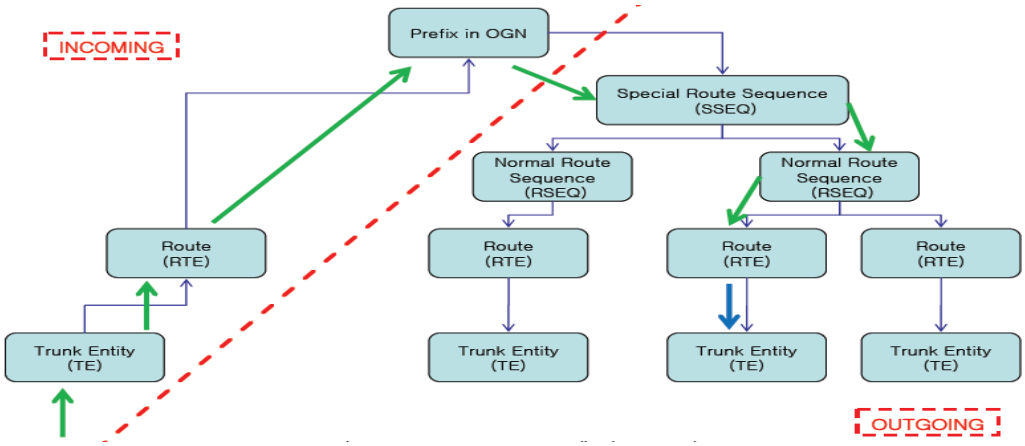
Gambar 4 Konfigurasi Interkoneksi SIP IDD

Elemen jaringan utama pembentuk interkoneksi SIP pada interkonesi IDD diantaranya adalah Softswitch dan SBC. Softswitch pada penelitian ini adalah Xener *Softswitch Class* 4 (C4) sebagai *core network* PT. Indosat, Tbk sedangkan elemen keamanan jaringan yang digunakan adalah Acme Packet *Session Border Controller* (SBC).

3.1.1 Xener Softswitch Class 4

Xener *Softswitch* C4 digunakan di internasional *switching center* pada PT. Indosat Tbk berfungsi sebagai *switching* sebagaimana fungsi *switching* pada umumnya, sebagai interkoneksi *switching* internasional untuk melakukan panggilan *incoming* dan *outgoing* maupun *terminating* dari / ke lokal TDM *switching* Indosat (domestik) dan *Mobile Switching Center* (MSC) Indosat, saat ini interkoneksi sambungan langsung internasional (SLI) melalui Xener *softswitch* C4, sebagai salah satu SLI yang dimiliki Indosat, memiliki *access code* +01016 dari nomer domestik atau *mobile* Indosat.

Interkoneksi SIP pada Xener *softswitch* C4 dilakukan dengan beberapa tahap membuat *database* interkoneksi SIP melalui OAM server. Berikut dibawah ini asosiasi data *routing* SIP yang pada Softswitch Xener C4.



Gambar 5 Asosiasi Data *Routing* Xener Softswitch C4 [6]

Gambar 5 adalah diagram perutingan panggilan. Didalam proses merutekan panggilan sebagai fungsi *switching* pada *softswitch*, *softswitch* memiliki beberapa

parameter yang saling memiliki asosiasi satu sama lain yang digunakan sebagai proses perutingan panggilan. Parameter parameter yang saling berasosiasi tersebut diantaranya adalah *Trunk Entity (TE), Route (RTE), Originating Number (OGN), Prefix, Special Route Sequence (SSEQ) dan Normal Route Sequence (RSEQ).*

Pada penelitian ini interkoneksi SIP yang digunakan adalah interkoneksi SIP menuju partner Taiwan NCI dengan nama *entity* di *sofswitch* adalah 1E-TWA-NCIC-SIP-ISBC dengan tipe SIG (*signaling*) SIP dan IP port 5060. Seperti pada Gambar 3.2 konfigurasi interkoneksi SIP IDD, protokol SIP digunakan untuk interkoneksi *softswitch* ke SBC. Berikut dibawah ini tabel *setting* SIP *Trunk Entity* pada *softswitch* C4:

Tabel 1 SIP *Trunk Entity*

ENT_NAME	DOMAIN	TYPE	COMP	IP_AUTH	IP_ADDR	IP_PORT	RTE
TWA-NCI-JKT-ISBC1-10.253.126.33		SIP	CS1	STATIC_IP_PORT	10.253.126.33	5060	1884

SIP *trunk* merupakan *physical* koneksi *softswith* ke sisi lawan. *Physical* koneksi ini direpresentasikan dengan alamat IP 10.253.126.33 *point to point* softwitch dengan SIP trunking disisi lawan dimana alamat IP tersebut merupakan IP *trunking* SBC, bukan merupakan *direct* IP Taiwan NCI. SIP *trunk* Taiwan NCI memiliki nomer perutingan / RTE 1884 pada *softswitch*. Nomer RTE kemudian akan didaftarkan pada distribusi perutingan *trunk* pada *Normal Route Sequence* (RSEQ).

Nomer perutingan / RTE adalah logical koneksi untuk setiap *trunk*. Pada *softswitch* masing-masing RTE dimiliki oleh masing-masing *trunk* / partner / *carrier*. pada RTE dapat dibuat manipulasi nomer seperti *insert* / *delete* digit untuk A ataupun B *number* dan juga setting *direction* / arah panggilan yang diperbolehkan melalui RTE tersebut. *Direction* dapat di set sebagai *incoming* maupun *outgoing only* ataupun di set sebagai *Both* (*incoming* dan *outgoing*). Berikut dibawah ini taber data setting pada RTE 1884:

Tabel 2 Data RTE

RTE	NAME	SIG	CARRIER	DIR	HUNT	SEL	INS	DEL
1884	1E-TWA-NCIC-SIP-ISBC	SIP	TWA-NCIC	BOTH	CIR	ASC	00	0

Kemudian *prefix / number* akan ditujukan ke SIP *trunk entity* menggunakan perutingan RSEQ. *Prefix* adalah digit nomer yang akan diarahkan ke suatu *trunk.* Seluruh *prefix / number* dikelompokan menggunakan *Originating Number* (OGN).

Tabel 3 *Prefix*

OGN	PFX	NUM_TYPE	CALL_TYPE	SEQ_TYPE	SEQ	MIN	MAX	SZ
85	00639	NORM	INTL	RSEQ	631	7	32	7
101	00639	NORM	INTL	RSEQ	631	7	32	7
102	00639	NORM	INTL	RSEQ	631	7	32	7
197	00639	NORM	INTL	RSEQ	631	7	32	7

Prefix yang menuju ke partner / *carrier* Taiwan – NCI memiliki 5 digit pertama ‘00639’ dengan tipe panggilan internasional. Sedangkan untuk panggilan nasional

dari partner akan dirutingkan ke masing-masing *trunk* nasional yang dituju melaui RSEQ yang berbeda.

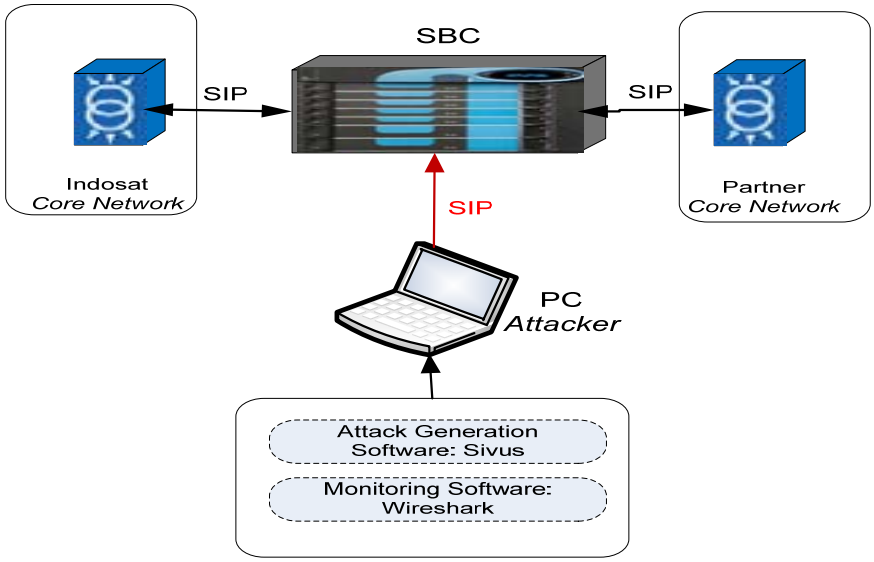
3.1.2 Acme Packet *Session Border Controller*

Acme Packet *Session Border Controller* (SBC) ditempatkan di perbatasan (border) jaringan *packet based* menggunakan protokol SIP untuk layanan keamanan interkoneksi *International Direct Dialing* (IDD) PT. Indosat Tbk. SBC melakukan fungsi kontrol yang diperlukan didalam interkoneksi sesi *signaling* dan kontrol media.

SBC difungsikan sebagai SIP *Back-to-Back User Agent* (B2BUA) yang berarti bahwa SBC dioperasikan sebagai *source* dan *destination* dari seluruh *signaling* dan *media* yang masuk ke *core network* dari IDD maupun yang keluar dari *core network* menuju ke IDD seperti pada Gambar 4, dimana antara *core network* Indosat dengan masing-masing partener IDD memiliki perbedaan *domain network*, *core network* Indosat dalam hal ini adalah Xener *softswtich* C4. SBC sebagai B2BUA yang dioperasikan tersebut merupakan model layanan sebagai *peering*.

3.2 Perancangan *Test Bed* Interkoneksi IDD

Penulis membuat *tes bed* sebagai media untuk pengujian terhadap serangan DOS yang mungkin terjadi didalam interkoneksi SIP. Gambar dari *test bed* interkoneksi IDD yang digunakan pada penelitian ini adalah sebagai berikut:



Gambar 6 *Test Bed* Interkoneksi IDD yang Digunakan

SBC menyediakan keamanan jaringan untuk softswitch sebagai *core network* dari serangan DOS. Seperti penjelasan yang ditemukan pada penelitian sebelumnya bahwa serangan DOS dapat membuat node, dalam hal ini *softswitch* / SIP *server*, didalam jaringan menjadi *unavailable* / *out of services*. Hasil *tes bed* akan dapat memberikan evaluasi terhadap hasil provisioning pada SBC. Apakah hasil layanan keamanan yang diberikan SBC yang diterapkan dapat melindungi dari serangan DOS. Alat / perangkat yang digunakan dan terlibat didalam pengetesan ini adalah *attack generation software* dan *monitoring software* yang sudah di *install* didalam PC. *Attack generation software* yang digunakan adalah

Sivus yang digunakan untuk menghasilkan SIP *invite message* sedangkan *monitoring software* yang digunakan adalah Wireshark sebagai perangkat lunak untuk melakukan analisa berkas monitoring protokol-protokol SIP.

3.3 Pengujian Layanan Keamanan, Pengukuran Performansi Pensinyalan SIP dan Kualitas Panggilan

Pada penelitian ini dibuat skenario pengujian berdasarkan Gambar 6 Untuk mendapatkan data-data layanan keamanan yang diperlukan dalam penelitian ini, dilakukan juga pengukuran terhadap performansi pensinyalan SIP dan juga kualitas panggilan SIP-*Based* VoIP yang dihasilkan pada interkoneksi IDD.

3.3.1 Pengujian Layanan Keamanan

Pada pengujian layanan keamanan akan berfokus pada aspek *Availability* didalam interkoneksi SIP. Pada layanan keamanan yang pertama akan membahas tentang *topology hiding infrasturktur core network* yang dihasilkan setelah diterapkanya SIP *Manipulation* pada SBC. Kemudian, layanan keamanan yang kedua membahas tentang pengujian serangan DOS yang akan dilakukan dengan cara mengirimkan *ilegal invite message* ke SBC menggunakan *test bed*.

Pada pengujian layanan keamanan yang pertama menggunakan panggilan (call) secara *real time* untuk melakukan analisa terhadap *topology hiding* infrastruktur *core network*. Sedangkan, untuk melakukan pengujian seranan DOS, PC yang dapat mengirim serangan diasumsikan sebagai *external node* seperti halnya *peering* partner pada interkoneksi IDD. PC diasumsikan mengetahui alamat IP SBC yang digunakan Indosat untuk interkoneksi SIP.

3.3.2 Pengukuran Performansi Pensinyalan SIP

Pengukuran performansi pensinyalan SIP pada interkoneksi SIP IDD ditujukan untuk mengetahui seberapa bagus performansi softswitch dan SBC didalam menyambungkan panggilan. Berdasarkan standar IETF RFC 6076 tahun 2011 tentang "*Basic Telephony SIP End-to-End Performance Metrics*", parameter yang akan digunakan untuk pengukuran performansi interkoneksi SIP IDD didalam penelitian ini adalah sebagai berikut.

1. *Session Establishment Effectiveness Ratio* (SEER)
2. *Session Establishment Ratio* (SER)

Untuk mendapatkan data-data pengukuran performansi pensinyalan SIP menggunakan *Network Management System* (NMS) yang sudah terintegrasi dengan *Call Detail Record* (CDR) dari *softswitch* seperti pada Gambar 4. Batas minimum yang digunakan PT. Indosat untuk parameter SEER adalah 98% sedangkan batas minimum untuk parameter SER adalah 20%. Adapun hasil prosentase SEER dan SER diperoleh dengan model perhitungan sebagai berikut:

$$SEER = \frac{(ANS+FLASH+BUSY+RNA+DIAL\ ERR)}{(ANS+FLASH+BUSY+RNA+DIALERROR+TECHFAIL+ADMIN+CONGESTION+OTHERS)}$$

$$SER = \frac{(ANS+FLASH)}{(ANS+FLASH+BUSY+RNA+DIALERROR+TECHFAIL+ADMIN+CONGESTION+OTHERS)}$$

3.3.3 Pengukuran Kualitas Panggilan

Setelah pengujian performansi pensinyalan SIP selanjutnya adalah mengukur kualitas panggilan yang dihasilkan setelah terbentuknya pensinyalan panggilan melalui interkoneksi SIP IDD. Hasil dari pengukuran tersebut akan memberikan informasi kualitas panggilan (*session* / *call*) yang terjadi.

Parameter pengukur kualitas panggilan yang digunakan pada penelitian ini berdasarkan standar ITU-T G.107 dan G.10 yaitu, R-*Factor* dan *Mean Opinion Score* (MOS). Menurut standarisasi ITU-T G.10, *Mean Opinion Score* (MOS) adalah nilai-nilai yang telah ditetapkan, dan pengguna menetapkan pendapat mereka mengenai kualitas penggilan yang digunakan baik untuk percakapan atau untuk mendengarkan materi pembicaraan. Namun, saat ini partisipasi pengguna untuk memberikan pendapat tidak lagi dibutuhkan untuk menentukan kualitas dari panggilan suara (*voice* / *audio*).

MOS adalah tolak ukur yang bersifat subjektif. Pengukuran kualitas panggilan VoIP tidak cukup hanya menggunakan parameter MOS, selain MOS, *R-Factor* adalah alternatif parameter lain untuk mengukur kualitas panggilan VoIP. *R-factor* dihitung dengan mengevaluasi persepsi pengguna dan juga faktor-faktor objektif yang berdampak kepada sistem VoIP. *R-Factor* memiliki skala 0 – 120 disisi lain MOS memiliki skala 1 – 5. Tabel dibawah ini adalah nilai / skala MOS dan *R-Factor* yang merepresentasikan tingkat penilaian pengguna didalam pengukuran kualitas panggilan sebagai berikut:

Tabel 4 MOS dan *R-Factor*

User Satisfaction Level	MOS	R-Factor
Maximum using G.711	4.4	93
Very satisfied	4.3-5.0	90-100
Satisfied	4.0-4.3	80-90
Some users satisfied	3.6-4.0	70-80
Many users dissatisfied	3.1-3.6	60-70
Nearly all users dissatisfied	2.6-3.1	50-60
Not recommended	1.0-2.6	Less than 50

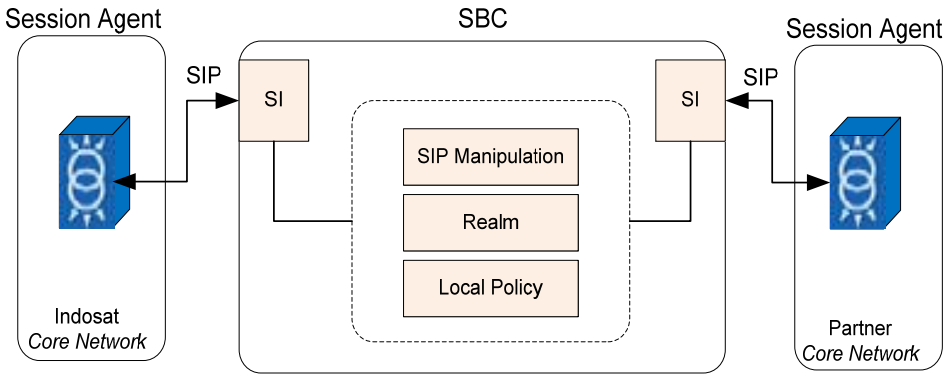
Pada penelitian ini digunakan *network analyzer* yaitu *SD Reporter* yang dapat memberikan pengukuran kualitas panggilan berdasarkan parameter MOS dan R-*Factor* untuk mengetahui seberapa tingkat kepuasan pelanggan dalam menilai kualitas panggilan yang dihasilkan, dengan cara mengolah data *Call Detail Record* (CDR) panggilan yang berlangsung. Seperti pada Gambar 4 SD Reporter yang digunakan telah terintegrasi dengan *Call Detail Record* (CDR) dari SBC.

4. HASIL

Pembahasan hasil berisi tentang implementasi layanan keamanan pada Acme Packet SBC sebagai elemen keamanan jaringan didalam interkoneksi SIP IDD seperti pada Gambar 4 yaitu hasil analisa dari layanan keamanan, performansi pensinyalan SIP dan kualitas panggilan yang dicapai.

4.1 Implementasi Layanan Keamanan Interkoneksi SIP Pada Acme Packet *Session Border Controller*

Proses implementasi keamanan interkoneksi SIP pada acme packet SBC sebagai B2BUA dilakukan dengan beberapa tahap seperti pada gambar sebagai berikut:



Gambar 7 SIP *Signaling Peering Environment*

Pada Gambar 7 menggambarkan komponen komponen yang akan dibuat *configuration* sebagai keamanan interkoneksi interkoneksi SIP. Komponen-komponen tersebut diantaranya adalah *Session Agent* (SA), SIP *Interface* (SI), *Realm*, SIP *Manipulation* dan *Local Policy*.

4.1.1 Session Agent

Session Agent mendefinisikan suatu *endpoint signaling* sebagai asal atau tujuan dari suatu *hop signaling*. *Session Agent* yang dikonfigur pada SBC didalam interkoneksi peering dengan TWA-NCI dibagi menjadi dua, yaitu alamat IP dari *softswitch* sebagai *Session Agent core* dan alamat IP dari SIP *server* / SIP *security* / *softswitch* TWA-NCI sebagai *Session Agent peer* (*partner)*. Berikut dibawah ini config dari masing-masing *Session Agent*:

i. Core:

```
hostname                        SAG:SIP-ISAT-CORE
        ip-address                      202.152.160.137
        port                            5060
        state                           enabled
        app-protocol                    SIP
        app-type
        transport-method                UDP+TCP
```

ii. Peer:

```
hostname                        NCI-TWA-SIP-SSW1E-SSW4B
        ip-address                      218.32.168.149
        port                            5060
        state                           enabled
        app-protocol                    SIP
        app-type
        transport-method                UDP+TCP
```

Session Agent untuk *core* memiliki *hostname* SAG:SIP-ISAT-CORE dengan alamat IP SIP *server* / *softswitch* 202.152.160.137 dengan protokol SIP dan mendukung *transport layer* UDP maupun TCP dengan port 5060. Sedangkan *Session Agent Peer* (partener) memiliki *hostname* NCI-TWA-SIP-SSW1E-SSW4B dengan alamat IP SIP *server* / SIP *security* / softswitch 218.32.168.149.

4.1.2 SIP Interface

SIP *interface* mendefinisikan sebagai alamat *transport* (alamat IP dan Port) yang digunakan SBC untuk menerima dan mengirim SIP *message*. Kemudian SIP *interface* akan didefinisikan pada suatu *Realm*. Seperti pada gambar 4. SIP *interface* masing-masing dibuat untuk arah *core* dan *peer* / partner.

i. Core:

```
state                           enabled
        realm-id                         ISAT-NCI-JKT-SSW-1E
        description
        sip-ports
        address                 10.253.126.33
        port                    5060
        transport-protocol      UDP
```

ii. Peer:

```
state                           enabled
        realm-id                peer-parent-SIP-SSW1E
        description
        sip-ports
        address                 114.5.6.4
        port                    5060
        transport-protocol      UDP
        allow-anonymous         realm-prefix
```

SIP *interface core* memiliki alamat *transport* 10.253.126.33 dengan *port* 5060 yang akan digunakan untuk *realm-id* ISAT-NCI-JKT-SSW-1E. Alamat *transport* ke arah *core* digunakan sebagai alamat IP *Trunk Entity* pada s*oftswitch*. Sedangkan alamat transport ke arah *peer* / partner adalah 114.5.6.4 dengan *port* 5060 yang digunakan untuk *realm-id* peer-parent-SIP-SSW1E. Alamat IP 114.5.6.4 merupakan alamat *transport* keseluruh *peer* / partner tidak hanya TWA-NCI. Seluruh *peer* / partner hanya akan mengenali IP 114.5.6.4 sebagai asal dan tujuan IP Signaling Indosat.

4.1.3 Realm

Realm merupakan suatu logical pembeda yang merepresentasikan perutingan. *Realm* juga merepresentasikan *network interface*. Didalam realm digunakan manipulasi SIP untuk *topology hiding*. Berikut dibawah ini *config realm* untuk pada SBC ke arah core dan partner:

i. Core:

```
identifier                      ISAT-NCI-JKT-SSW-1E
        description
        addr-prefix
        network-interfaces      M00:163
        in-manipulationid
        out-manipulationid      NAT_SIP
```

ii. Peer:

```
identifier                      SIP-NCI-SSW1E
        description
        addr-prefix             218.32.168.149
        network-interfaces      M10:158
        in-manipulationid
        out-manipulationid      NAT_SIP
```

Realm ISAT-NCI-JKT-SSW-1E menggunakan *network interface* M00:163 dengan menggunakan *outbond manipulasi* NAT_SIP. *Realm* ke arah *peer* / partner memiliki alamat *prefix* 218.32.168.149 menggunakan *network interface* M10:158. *Network interface* merupakan *port* fisik pada SBC. M00:163 adalah *network interface* yang digunakan untuk seluruh traffik yang memiliki asal dan

tujuan dari *softswitch* sedangkan M10:158 merupakan *network interface* yang memiliki asal dan tujuan dari partner.

4.1.4 Local Policy

Local policy mengindikasikan / menentukan kemana *session request* dirutekan dan diteruskan. Setelah seluruh *Session Agent*, SIP *Interface*, *Realm* masing-masing *core* dan *peer* / partner sudah dibuat selanjutnya adalah membuat *local policy* sebagai perutingan SIP session pada SBC. Berikut dibawah ini *local policy* yang digunakan:

i. Local policy *core* menuju ke partner:

```
from-address                    *
        to-address              *
        source-realm            ISAT-NCI-JKT-SSW-1E
        activate-time           N/A
        deactivate-time         N/A
        state                   enabled
        policy-priority         none
        description
        policy-attributes
                next-hop                NCI-TWA-SIP-SSW1E-SSW4B
                realm                   SIP-NCI-SSW1E
                start-time              0000
                end-time                2400
                days-of-week            U-S
                cost                    0
                app-protocol            SIP
                state                   enabled
```

ii. Local policy partner menuju ke *core*:

```
from-address                    *
        to-address              *
        source-realm            SIP-NCI-SSW1E
        activate-time           N/A
        deactivate-time         N/A
        state                   enabled
        policy-priority         none
        description
        policy-attributes
                next-hop                SAG:SIP-ISAT-CORE
                realm                   ISAT-NCI-JKT-SSW-1E
                action                  none
                start-time              0000
                end-time                2400
                days-of-week            U-S
                cost                    0
                app-protocol            SIP
                state                   enabled
```

Local policy core menuju ke partner, seluruh *session* yang berasal dari *realm* ISAT-NCI-JKT-SSW-1E akan dikirimkan ke *session agent* NCI-TWA-SIP-SSW1E-SSW4B melalui *realm* SIP-NCI-SSW1E. Sedangkan pada *local policy* partner menuju ke *core*, seluruh *session* yang berasal dari *realm* SIP-NCI-SSW1E akan dikirim menuju SIP *session agent* SAG:SIP-ISAT-CORE melalui *realm* ISAT-NCI-JKT-SSW-1E.

4.1.5 SIP Manipulation

Pada *realm* ISAT-NCI-JKT-SSW-1E dan SIP-NCI-SSW1E dibuat manipulasi SIP dengan tujuan sebagai *topology hiding* agar seluruh informasi alamat IP disisi *core* Indosat tidak terdeteksi oleh partner. Berikut dibawah ini manipulasi SIP disisi *realm*:

```
sip-manipulation
        name                            NAT_SIP
```

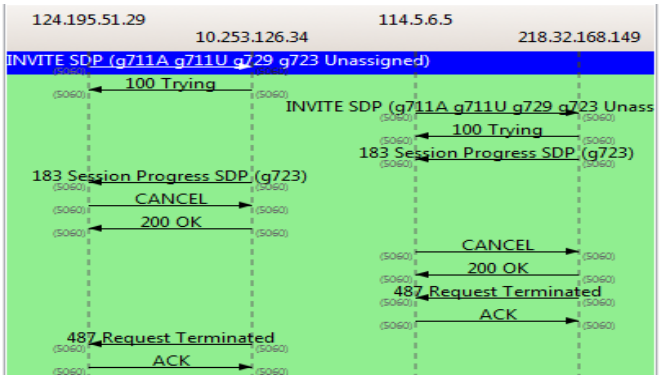
```
        description
        header-rules
                name                            From
                header-name                     From
                action                          manipulate
                match-value
                msg-type                        request
                comparison-type                 case-insensitive
                new-value
                methods
                element-rules
                        name                            chgFROM
                        parameter-name
                        type                            uri-host
                        action                          replace
                        match-val-type                  any
                        comparison-type
case-insensitive
                        match-value
                        new-value                       $LOCAL_IP
        header-rules
                name                            To
                header-name                     To
                action                          manipulate
                match-value
                msg-type                        request
                comparison-type                 case-insensitive
                new-value
                methods
                element-rules
                        name                            chgTO
                        parameter-name
                        type                            uri-host
                        action                          replace
                        match-val-type                  any
                        comparison-type
case-insensitive
                        match-value
                        new-value                       $REMOTE_IP
```

4.2 Hasil Layanan Keamanan

Pengujian menggunakan layanan keamanan untuk interkoneksi SIP Softswitch C4 dengan parter IDD yang diintegrasikan melalui SBC sebagai *security services* akan diuji dengan menggunakan parameter *availability*.

4.2.1 Layanan Keamanan *Topology Hiding*

Topology hiding bertujuan untuk melindungi alamat-alamat IP dan informasi-informasi perangkat-perangkat *core network* agar tidak diketahui dari sisi diluar *core network* pada saat proses *call setup* menggunakan protokol SIP. *Topology hiding* didapatkan dari hasil implementasi manipulasi SIP dan perutingan di SBC. Berikut dibawah ini contoh hasil *call setup* menggunakan interkoneksi SIP IDD:



Gambar 8 Hasil *Trace* Pensinyalan SIP

Topology hiding dapat dilihat menggunakan hasil trace pensinyalan SIP pada saat *call setup*. Pada Gambar 8 merupakan contoh salah satu proses call setup yang diambil menggunakan Wireshark. Panggilan berasal dari alamat IP *softswitch* 124.195.51.29 yang ditujukan ke partner dengan alamat IP 218.32.168.149 melalui SBC dengan alamat IP SIP *interface* 10.253.126.34 ke arah softswitch dan alamat IP SIP *interface* 114.5.6.5 ke arah parter. Informasi *softswitch* dalam bentuk alamat IP sebagai pengirim tidak dapat diketahui oleh partner maupun siapapun yang berada di jaringan luar *core network*. Hal ini dapat dilihat pada perbandingan SIP *message* yang dikirimkan oleh *softswitch* ke SBC dengan SIP *message* yang dikirimkan SBC ke partner pada proses *call setup* sebagai berikut:

- SIP message *softswitch* ke SBC

INVITE sip:829678618211748863@10.253.126.34:5060 SIP/2.0
Call-ID: AASMTAAAB-MAABeyfMMzGA--c34916751@xener.com
Content-Length: 254
CSeq: 34384980 INVITE
Contact: <sip:6281536007868@124.195.51.29:5060>
Content-Type: application/sdp
From: sip:6281536007868@124.195.51.29:5060;tag=7cc3331dt20i0a007491x003289k0021060020130115165651022
Max-Forwards: 69
To: sip:829678618211748863@10.253.126.34:5060
Allow: INVITE,CANCEL,ACK,BYE,OPTIONS,PRACK,INFO,UPDATE
Record-Route: <sip:124.195.51.29:5060;lr>
Via: SIP/2.0/UDP 124.195.51.29:5060;branch=z9hG4bKhsig0000006840AASNTAwhB-MAABeyfMMzGA7cc3331da007491c57029818

v=0
o=- 1682336879 0 IN IP4 124.195.49.135
s=-
c=IN IP4 124.195.49.135
t=0 0
m=audio 5210 RTP/AVP 8 0 18 4 80
a=fmtp:18 annexb=yes
a=rtpmap:4 G723/8000/1
a=fmtp:4 bitrate=6.3;annexa=yes
a=rtpmap:80 G723/8000/1
a=fmtp:80 bitrate=5.3;annexa=yes

SIP *message* yang dikirim softswitch ke SBC berisikan alamat dan nomer pengirim “From: sip:6281536007868@124.195.51.29:5060” kemudian ditujukan

ke alamat dan nomer penerima "To: sip:829678618211748863@10.253.126.34:5060" yang dikirim melalui "Via: SIP/2.0/UDP 124.195.51.29:5060" Sedangkan pada negosisasi media menggunakan protokol SDP terdapat informasi alamat IP *media gateway* yang digunakan (*origin*) "o=- 1682336879 0 IN IP4 124.195.49.135" dengan informasi koneksi IP ver4 (*connection*) "c=IN IP4 124.195.49.135".

Seluruh informasi alamat IP *core network*, IP signaling sofswitch 124.195.51.29 dan IP media 124.195.49.135 tidak di publish oleh SBC keluar *network* maupun ke parter. Setelah dilakukan manipulasi SIP pada SBC SIP message yang dikirimkan SBC ke arah partner menjadi sebagai berikut:

- SIP message SBC ke Parter

```
INVITE sip:829678618211748863@218.32.168.149:5060 SIP/2.0
Via: SIP/2.0/UDP 114.5.6.5:5060;branch=z9hG4bKng2vn7bg5nhfh199m73dj3c3t3
Call-ID: AASMTAAAB-MAABeyfMMzGA--c34916751@xener.com
Content-Length: 247
CSeq: 34384980 INVITE
Contact: <sip:6281536007868@114.5.6.5:5060;transport=udp>
Content-Type: application/sdp
From:
sip:6281536007868@114.5.6.5:5060;tag=7cc3331dt20i0a007491x003289k00210600201301151
65651022
Max-Forwards: 68
To: sip:829678618211748863@218.32.168.149:5060
Allow: INVITE,CANCEL,ACK,BYE,OPTIONS,PRACK,INFO,UPDATE

v=0
o=- 1682336879 0 IN IP4 114.5.6.21
s=-
c=IN IP4 114.5.6.21
t=0 0
m=audio 62728 RTP/AVP 8 0 18 4 80
a=fmtp:18 annexb=yes
a=rtpmap:4 G723/8000/1
a=fmtp:4 bitrate=6.3;annexa=yes
a=rtpmap:80 G723/8000/1
a=fmtp:80 bitrate=5.3;annexa=yes
r;priv
```

Pada SIP message yang dikirimkan SBC ke parter berisikan alamat dan nomer pengirim sebagai "From:sip:6281536007868@114.5.6.5:5060" yang ditujukan ke "To:sip:829678618211748863@218.32.168.149:5060" melalui "Via: SIP/2.0/UDP 114.5.6.5:5060" dengan alamat IP media "o=- 1682336879 0 IN IP4 114.5.6.21" dan informasi IP ver4 "c=IN IP4 114.5.6.21".

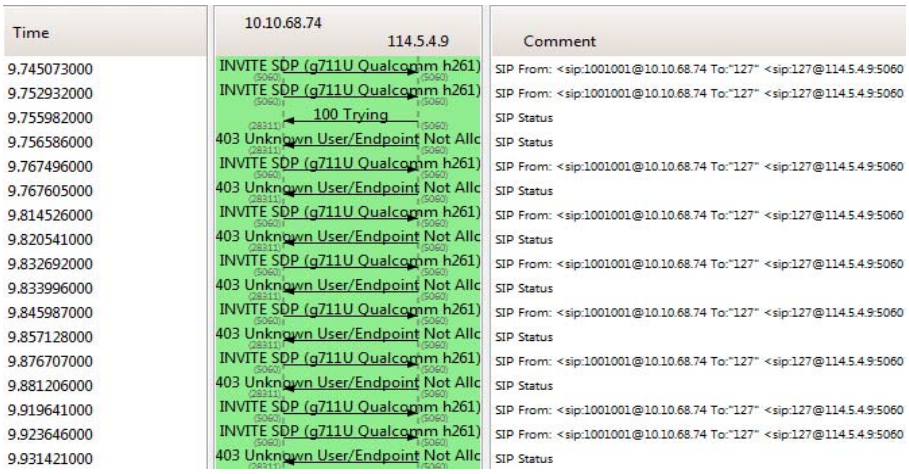
Dari hasil perbandingan SIP *message* yang dikirimkan *softswitch* dengan SIP *message* SBC ke partner informasi alamat IP *softswitch* sebagai *core network*, IP *signaling* dan media *softswitch*, tidak dapat diketahui dari jaringan diluar SBC dan partner yang melalui IP *public*. Dengan kata lain, partner dan jaringan luar hanya mengetahui IP 114.5.6.5 sebagai IP *signaling* untuk SIP dan 114.5.6.21 sebagai IP koneksi media.

4.2.2 Hasil Pengujian *Tes Bed*

Pengujian *test bed* bertujuan untuk memastikan *resource* (sumber daya) *sofswitch* hanya dapat diakses oleh partner IDD yang terotentikasi melalui SBC dikarenakan interkoneksi ke parter IDD menggunakan alamat IP publik. Skenario

yang dilakukan untuk melakukan pengujian ini adalah dengan menggunakan *test bed* interkoneksi seperti pada Gambar 6.

Serangan DOS yang dikirim menggunakan *invite message* ditujukan ke alamat publik IP *Signaling* Interkonksi SIP. Alamat IP yang digunakan untuk *test bed* interkoneksi menggunakan alamat publik IP *signaling* yang digunakan khusus untuk pengetesan terhadap serangan DOS dari jaringan luar dengan alamat IP 114.5.4.9. Berikut dibawah ini hasil serangan DOS menggunakan *invite message*.



Gambar 9 Serangan DOS Menggunakan SIP *Invite Message*

Pada Gambar 9 memperlihatkan proses terjadinya serangan menggunakan SIP *invite message* yang berasal dari alamat publik IP 10.10.68.74 sebagai PC yang menghasilkan *invite message*. Kemudian serangan tersebut ditujukan ke alamat IP *signaling* SBC 114.5.4.9 dengan asumsi bahwa jaringan diluar mengetahui IP *signaling* tersebut. Secara rinci *invite message* yang dihasilkan oleh PC adalah sebagai berikut:

- SIP *message* PC ke SBC

```
INVITE sip:127@114.5.4.9 SIP/2.0
Via: SIP/2.0/UDP 10.10.68.74:5060;branch=VSOse5g9HD07D9
From: <sip:1001001@10.10.68.74>;tag=ZlBVIPXoyE
To: "127" <sip:127@114.5.4.9:5060>
Call-ID: 9B9trWuVTLHX@10.10.68.74
CSeq: 123456 INVITE
Contact: <sip:1001001@10.10.68.74:5060>
Max_forwards: 70
User-Agent: test
Content-Type: application/sdp
Subject: test
Expires: 7200
Content-Length: 141

v=0
o=user 29739 7272939 IN IP4 10.10.68.74
s=
c=IN IP4 10.10.68.74
m=audio 49210 RTP/AVP 0 12
m=video 3227 RTP/AVP 31
a=rtpmap:31 LPC/8000
```

Invite message yang dihasilkan oleh PC berisikan alamat dan nomer pengirim "From: sip:1001001@10.10.68.74" yang ditujukan ke alamat dan nomer penerima "To: "127" sip:127@114.5.4.9:5060" melalui informasi koneksi alamat IP "Via: SIP/2.0/UDP 10.10.68.74:5060". Sedangkan alamat IP media pada SDP berisikan alamat asal pengirim media "o=user 29739 7272939 IN IP4 10.10.68.74" dan informasi koneksi media IP ver4 "c=IN IP4 10.10.68.74". *Invite message* yang dikirimkan oleh PC kemudian direspons oleh SBC dengan hasil sebagai berikut:

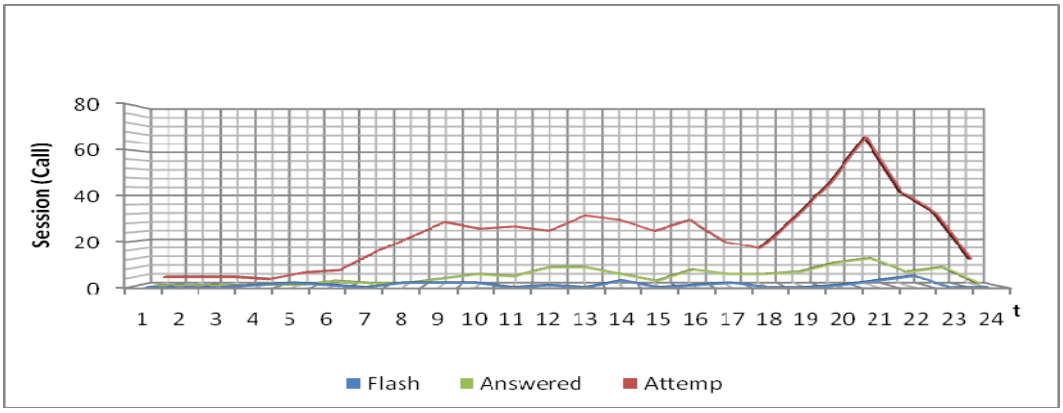
- Respons message dari SBC

SIP/2.0 403 Unknown User/Endpoint Not Allowed
Via:SIP/2.0/UDP
10.10.68.74:5060;received=124.195.15.162;branch=VSOse5g9HD07D9;rport=28311
From: <sip:1001001@10.10.68.74>;tag=ZlBVIPXoyE
To: "127" <sip:127@114.5.4.9:5060>;tag=aprqrjmtc-779ckr001go14
Call-ID: 9B9trWuVTLHX@10.10.68.74
CSeq: 123456 INVITE
Content-Length: 0

Hasil respons terhadap illegal invite message yang dikirimkan oleh PC adalah SIP Respons *code* 403 dengan deskripsi "*Unknown User/Endpoint Not Allowed*" atau "*Forbidden"*. Dari *respons* SBC, serangan DOS dengan cara mengirimkan *illegal* SIP *message* akan di-*reject* oleh SBC. Sehingga *illegal* SIP *invite message* tersebut tidak akan diteruskan ke *core network*.

4.3 Hasil Performansi Pensinyalan

Tujuan pengukuran performansi pensinyalan adalah untuk melihat kinerja softswitch dan SBC menyambungkan panggilan. Prosentase SEER dan SER didapat dari data seluruh panggilan per jam yang terjadi melalui interkoneksi SIP. Pengukuran performansi SEER dan SER diambil berdasarkan panggilan *incoming* dan *outgoing* melalui suatu RTE pada softswitch dimana RTE tersebut adalah RTE untuk SIP *Trunk Entity* yang diarahkan ke SBC.

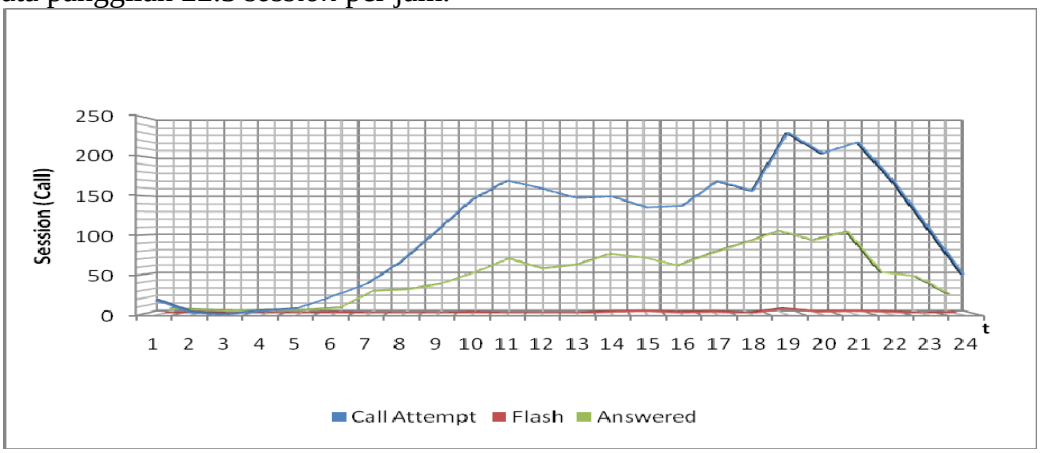


Gambar 10 Total Panggilan dan Panggilan Terjawab *Incoming* RTE 1884

Gambar diatas adalah grafik total panggilan masuk (*incoming call*) pada RTE 1884. Dari grafik diatas dapat dilihat fluktuasi peningkatan dan penurunan antara panggilan yang masuk (*attempt*) dan panggilan masuk yang terjawab (*answered* dan *flash*). Panggilan terjawab dengan durasi lebih besar atau sama dengan 6 detik

masuk ke dalam kategori *answered call*, sedangkan panggilan yang memiliki durasi kurang dari 6 detik dikategorikan kedalam *flash call*.

Dari data tersebut didapatkan perbandingan grafik total seluruh panggilan masuk yang terjadi setiap jam dengan grafik panggilan masuk yang terjawab. Data perhitungan dari panggilan masuk ini selanjutnya akan menjadi acuan prosentase *SEER* dan *SER* untuk *incoming call*. Dari data panggilan masuk selama 24 jam pada RTE 1884 didapatkan total panggilan masuk sebanyak 536 *call* (*session)* dan dengan panggilan masuk yang terjawab 99 *session* dengan rata-rata panggilan 22.3 *session* per jam.



Gambar 11 Total Panggilan dan Panggilan Terjawab *Outgoing* RTE 1884

Pada grafik total panggilan keluar (*outgoing call*) pada RTE 1884 juga dapat dilihat fluktuasi peningkatan dan penurunan antara total panggilan yang keluar (attempt) dan panggilan keluar yang terjawab (*answered* dan *flash*). Dari data CDR seperti pada grafik outgoing RTE 1884 terdapat total panggilan keluar selama 24 jam mencapai 2616 *session* dengan total panggilan terjawab sebanyak 1138 *session* dengan rata-rata 102 *session* per jam. Dari data total panggilan yang terjadi dengan total panggilan yang terjawab baik *incoming* dan *outoing* dapat dilihat dalam betuk tabel. Tabel 4 Dibawah ini merupakan rekap data *incoming* dan *outgoing* selama 24 jam pada RTE 1884 yang dimiliki oleh Taiwan-NCIC sebagai International Carrier (Partner).

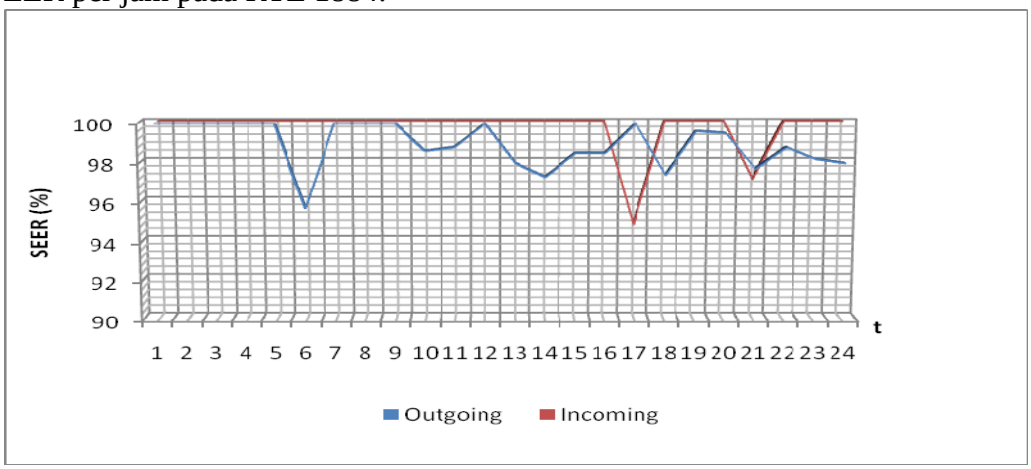
Tabel 5 *Statistic Summary Incoming* dan *Outgoing*

SUM	INT CARIER	INT TRUNK	CALL	FLASH	ANS	BUSY	RNA	DIAL ERR	TECH FAIL	ADMIN	CONG	OTHER
Out	TWA NCIC	1884	2616	25	1138	11	1407	3	9	0	9	14
In	TWA NCIC	1884	536	26	99	9	393	6	1	0	0	2

Dari data statistik *incoming* dan *outgoing* pada RTE 1884 per jam yang diperlihatkan pada Gambar 10 dan 11. Kemudian dapat diketahui seberapa tinggi tingkat keefektifan softswitch dan SBC melalui RTE 1884 didalam menyambungkan panggilan.

SEER digunakan untuk menggambarkan prosentase kemampuan Softswitch dan SBC sebagai B2BUA didalam menyambungkan panggilan terlepas dari perilaku adanya penolakan panggilan (*Busy*), panggilan tidak terjawab (*Ringing*

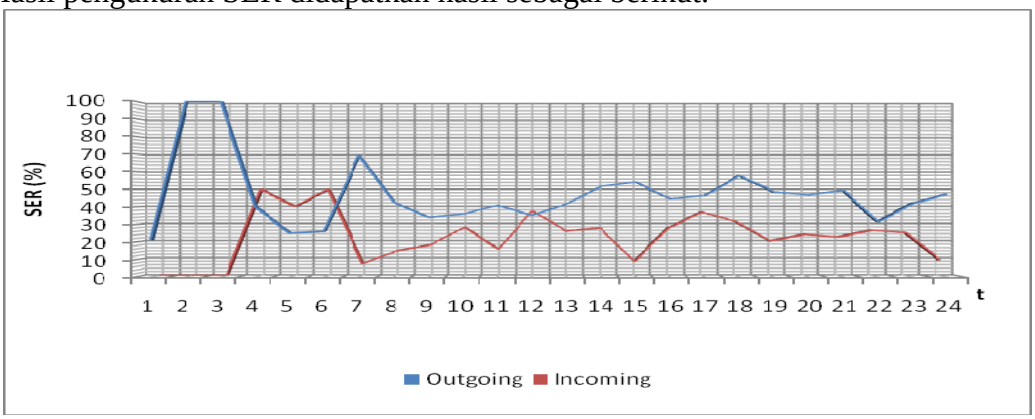
but No Answer / RNA) oleh nomer yang dipanggil maupun kesalahan pengiriman digit (*Dial Error*) oleh nomer pemanggil. Didalam perhitungan SEER *busy, RNA* dan *dial error* terkait perilaku *end user* dihitung sebagai pensinyalan panggilan yang berhasil. Berikut hasil performansi pensinyalan berdasarkan parameter SEER per jam pada RTE 1884:



Gambar 12 HasilPengukuran SEER *Incoming & Outgoing* RTE 1884

Gambar diatas adalah hasil pengukuran SEER berdasarkan *incoming* dan *outgoing* dari IP interkoneksi ke arah operator lawan (partner). Dari grafik pada gambar diatas menggambarkan performansi kemampuan interkoneksi SIP dari softswith dan SBC didalam menyambungkan panggilan. Dari data statistik *incoming* selama 24 jam didapatkan prosentase nilai SEER diantara 94.7% sampai dengan 100% dan nilai prosentase SEER *outgoing* diantara 95.7% sampai dengan 100%. Rata-rata performansi SEER *incoming* dan *outgoing* masing-masing didapatkan prosentase 99.6% dan 98.94%.

Pengukuran SEER hanya mewakili kemampuan sofswitch dan SBC didalam menyambungkan panggilan. Kemudian digunakan parameter SER untuk menghitung performansi pensinyalan dan hubunganya dengan performansi softswitch atau VoIP *core* disisi lawan (partner). Hasil pengukuran SER berbentuk prosentase panggilan yang sukses dari *session* yang telah terbentuk. Hasil pengukuran SER didapatkan hasil sebagai berikut:

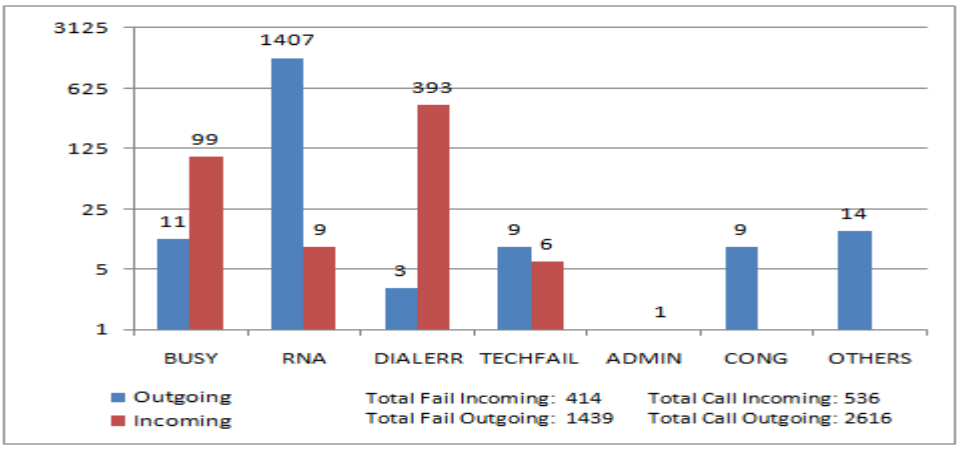


Gambar 13 Hasil Pengukuran SER *Incoming & Outgoing* RTE 1884

Tidak seperti parameter SEER, didalam pengukuran parameter SER hanya menggunakan *answered call* dan *flash call* sebagai pernsinyalan yang berhasil.

Dengan kata lain *session* yang memiliki *call duration* adalah session yang dianggap berhasil. Grafik diatas diperoleh dari data statistik incoming dan *outgoing* RTE 1884 dengan international *carrier* (partner) Taiwan – NCIC. Dari data statistik selama 24 jam didapatkan prosentase SER *incoming* diantara 0 % sampai dengan 50 % dengan rata-rata SER *incoming* selama 24 jam sebesar 22.68 %. Sedangkan prosentase SER *outgoing* diantara 21.1% sampai dengan 100% dengan rata-rata selama 24 jam 47.11%. Hasil pengukuran SER dapat disimpulkan sebagai rasio *call completed* dengan perspektif *end-to-end* antar operator melalui interkoneksi SIP pada RTE 1884.

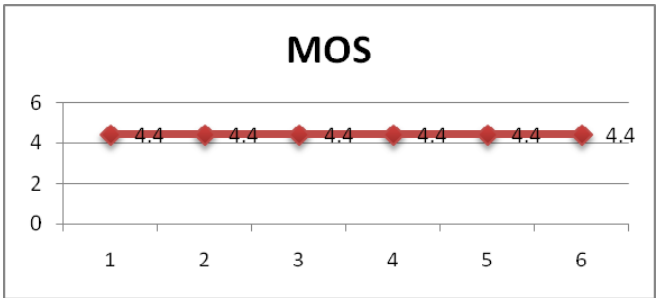
Sebesar 393 panggilan (77.36%) dari total keseluruhan kegagalan (*fail*) pada *incoming call* disebabkan oleh *Dial Error* oleh nomer pemanggil. Sedangkan sebesar 1407 panggilan (96.8%) dari keseluruhan kegagalan *outgoing call* disebabkan oleh RNA (*Ringing but No Answer*) oleh nomer yang dipanggil. Berikut dibawah ini kontribusi kegagalan panggilan yang terjadi selama 24 jam didalam interkoneksi RTE 1884.



Gambar 14 Grafik Kontribusi Kegagalan Panggilan Pada RTE 1884

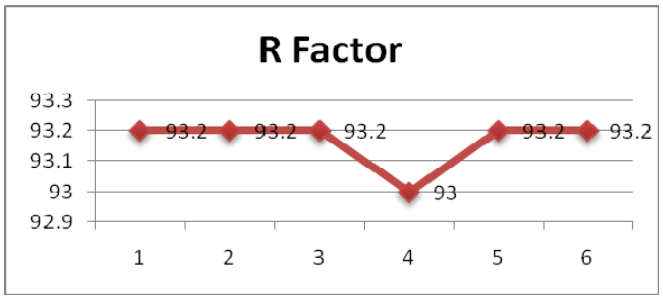
4.4 Hasil Kualitas Panggilan

Tujuan hasil pengukuran kualitas panggilan adalah untuk mengetahui seberapa tinggi kualitas panggilan yang dihasilkan melalui interkoneksi SBC sebagai B2BUA. Dimana proses pertukaran media juga terjadi melewati IP media SBC. Berdasarkan parameter MOS dari *network analyzer* SD Reporter yang menjalankan proses *artificial intelligent* yang juga berdasarkan kepada parameter *delay*, *packet loss* dan *jitter* yang terjadi pada saat proses pertukaran media RTP didapatkan hasil sebagai berikut:



Gambar 15 Hasil Pengukuran MOS

Hasil yang ditunjukan pada grafik di atas menunjukan performa MOS sangat baik yaitu dengan rata-rata keseluruhan dengan nilai 4.4. Sedangkan hasil pengukuran kualitas panggilan berdasarkan parameter R-*Factor* didapatkan hasil sebagai berikut:



Gambar 16 Hasil Pengukuran R-Factor

Hasil yang ditunjukan grafik di atas menujukan bahwa media yang melalui SIP TWA NCI memiliki R-*Factor* yang tinggi dengan nilai diantara 93-93.2 setiap jam. Dari hasil R-*factor* dan MOS yang didapat dapat menggambarkan penilaian pengguna (*user*) tentang kualitas suara yang dihasilkan masuk dalam kategori sangat baik secara *end-to-end* pengguna (*user*).

5. PEMBAHASAN HASIL

Untuk pengujian layanan keamanan *topology hiding* menunjukan hasil dari manipulasi SIP dan perutingan SBC melalui local policy. *Header field: from, to, via* dan *contact* pada SIP *message* yang dikirimkan softswitch akan mengalami manipulasi pada saat SBC mengirimkan SIP *message* ke alamat IP parter yang dituju sehingga alamat IP *signaling softswitch* dan media tidak dapat diketahui oleh parter dan jaringan luar. IP signaling dan media yang digunakan untuk proses *call setup* SBC dengan parter IDD akan menggunakan alamat publik IP *signaling* dan media SBC. Sehingga parter IDD hanya akan mengetahui alamat publik IP *signaling* dan media SBC sebagai alamat IP interkoneksi SIP.

Pengujian layanan kemanan terhadap aspek *availability*, dilakukan serangan DOS dengan cara mengirimkan illegal SIP *invite message* menggunakan skenario *test bed*. PC mengirimkan *illegal invite message* dari alamat publik IP yang ditujukan ke alamat IP *signaling* SBC. Dari hasil yang didapat, *illegal invite message* yang dihasilkan oleh PC mendapatkan SIP *respons* dengan cause code 403 / *Forbidden*. Hal ini disebabkan karena hanya alamat IP partner yang telah terotentikasi oleh SBC yang didaftarkan sebagai *Session Agent* yang hanya dapat melakukan *call setup* dan proses panggilan ke core network. Sehingga *core network* dapat terlindung dari ancaman serangan DOS yang berdasakan kepada protokol SIP dari jaringan luar.

Pengukuran performansi pensinyalan SIP pada interkoneksi SIP IDD, menggunakan parameter SEER dan SER selama 24 jam. Dari hasil pengukuran SEER dan SER yang dilakukan didapat rata-rata prosentase SEER *incoming* sebesar 99.6% dan rata-rata prosentase SEER *outgoing* sebesar 98.94%. Dari nilai prosentase rata-rata SEER yang didapat, tingkat keberhasilan Softswitch dan SBC sebagai B2BUA didalam menyambungkan panggilan setiap *session* sangat tinggi. Seluruh *session* (*call*) *incoming* dan *outgoing* dapat disambungkan ke sisi lawan

dengan baik. Sedangkan hasil pengukuran SER dimana merupakan prosentase *session* (*call*) yang benar-benar memiliki duration, didapatkan rata-rata SER *incoming* sebesar 22.68 % dan rata-rata SER *outgoing* sebesar 47.11%. Panggilan / *session* (*call*) yang gagal terkait performansi SER didapatkan penyebab kegagalan panggilan untuk *incoming* sebesar 393 *session* (*call*) dikarenakan oleh *dial error* oleh pemanggil dan sebesar 99 *session* (*call*) gagal dikarenakan oleh *user busy*. Dengan demikian prosentase SER sebesar 22.68% dinilai sangat baik karena kegagalan panggilan yang tertinggi bukan disebabkan oleh kategori *technical failure* maupun *switching congests*. Sedangkan kegagalan pada panggilan *outgoing* sebesar 1407 session (call) disebabkan oleh panggilan tidak terjawab (*Ringing but No Answer*). Dengan demikian prosentase SER 47.11% juga dinilai sangat baik.

Sedangkan untuk pengukuran kualitas panggilan yang dihasilkan pada penelitian ini menggunakan parameter R-*Factor* dan MOS. Tidak seperti SEER dan SER yang mengukur kualitas panggilan dari sisi pensinyalan, R-*Factor* dan MOS mengukur kualitas pertukaran media dari *core network* dengan parter IDD yang melalui alamat IP media SBC. Dari hasil yang didapat pengukuran kualitas panggilan berdasarkan parameter R-*Factor* didapatkan hasil 93-93.2 sedangkan parameter MOS didapatkan hasil 4.4. Dari hasil R-*Factor* dan MOS, secara *end-to-end* pengguna (*user*) masuk kedalam kategori sangat baik.

Secara keseluruhan interkoneksi SIP antar operator untuk *International Direct Dialing* (IDD) didapatkan hasil yang baik yang telah diuji menggunakan tiga aspek yaitu, layanan keamanan, performansi pensinyalan dan kualitas panggilan. Mekanisme layanan keamanan menggunakan SBC sebagai B2BUA dapat melindungi kemungkinan terjadinya serangan DOS yang terjadi pada jaringan luar core network. Dan performansi pensinyalan dari SEER dan SER softswitch dan SBC memiliki nilai yang bagus. Serta kualitas panggilan juga memiliki hasil kategori perspektif *end-to-end* pengguna (user) sangat baik.

5.1 Pembahasan dengan Penelitian Terkait

Penelitian yang terkait dengan penelitian yang dilakukan ini adalah *Evaluating DOS Attack Against SIP-Based VoIP System* yang dilakukan oleh M. Zubair Rafique, M. Ali Akbar dan Muddassar Farooq. Dari hasil penelitian yang dilakukan didapat evaluasi serangan DOS terhadap performansi sistem SIP-*Based* VoIP. Aspek utama dalam penelitian yang dilakukan oleh M. Zubair Rafique, M. Ali Akbar dan Muddassar Farooq adalah SIP *server* dapat berada dalam kondisi *out of service* hanya disebabkan dengan serangan *invite flooding* atau disebut juga dengan *invite of death*, dimana serangan invite flooding dikirim sebanyak 200, 500, 400 dan sampai 8000 invite paket/detik dengan beberapa SIP server berbeda. Sedangkan pada penelitian ini tidak melakukan *invite flooding* yang ditujukan ke Xener *softswitch* sebagai SIP Server namun memberikan evaluasi layanan keamanan yang dihasilkan setelah menenggunakan elemen *network security* Acme Packet SBC. Dari hasil penelitian ini *network security* SBC dapat memberikan layanan keamanan terhadap ancaman serangan DOS yang diutarakan oleh penelitian terkait yang diuji menggunakan *invite message*. *Invite message* yang dihasilkan oleh PC pada penelitian ini mendapatkan SIP *respons* dengan *cause code* 403 / *Forbidden* sehingga softswitch dapat terlindung dari ancaman keamanan dari serangan DOS dari jaringan luar. Aspek berikutnya pada

penelitian yang dilakukan oleh M. Zubair Rafique dan kawan-kawan adalah analisa pensinyalan *Call Completion Ratio* (CCR) dan *Call Rejection Ratio* (CRR) serta terdapat parameter lain seperti *Call Esthablishment Latency* (CEL), dan *Number of Retransmitted Request* (NRR). Performansi parameter-parameter pada penelitian tersebut dilakukan pada saat terjadinya serangan *invite flooding*. Hasil yang didapat performansi CCR semakin menurun sejalan dengan penambahan *invite* paket/detik. Begitu juga dengan CRR, CEL dan NRR yang semakin tinggi. Berbeda dengan penelitian tersebut, penelitian ini tidak mengukur performansi SIP server dalam lingkungan yang sedang diuji dengan serangan DOS. Penelitian ini mengukur performansi SEER dan SER sesuai dengan RFC 6076 tahun 2011, dimana pengukuran performansi dilakukan didalam lingkungan yang terproteksi oleh SBC. Pada penelitian ini didapatkan SEER *incoming* dan *outgoing* masing-masing didapatkan prosentase pengukuran 99.6% dan 98.94%. SER sama seperti CCR, incoming sebesar 22.68 % dan rata-rata SER outgoing sebesar 47.11%.

Penelitian terkait berikutnya adalah penelitian yang dilakukan oleh Liancheng Shan dan Ning Jing, yang berjudul *Research on Security Mechanism of SIP-Based VoIP System.* Pada penelitian tersebut, Liancheng Shan dan Ning Jing memperkenalkan sistem SIP-Based VoIP dapat dikenakan kepada 6 aspek serangan. Salah satu aspek serangan yang mungkin terjadi dan berhubungan dengan penelitian terkait sebelumnya adalah *denial of service* (DOS). Pada penelitiannya, Liancheng Shan dan Ning Jing, mengenai aspek serangan DOS, mekanisme SIP *security* harus memberikan proteksi terhadap serangan DOS, penggunaan TLS maupun IPsec tidak dapat memberikan proteksi sistem dari serangan DOS. Karena SIP server harus dapat dibuka ke jaringan publik, sehingga dapat dengan mudah menjadi target serangan DOS. Dari hasil yang didapat pada penelitian ini softswitch tidak dibuka ke jaringan publik. Sebagai gantinya SBC menyediakan alamat publik IP *signaling* dan media untuk dikenali parter IDD sebagai alamat IP interkoneksi dengan menggunakan metode SIP manipulasi dan *local policy* yang diimplementasikan.

6. KESIMPULAN

Kesimpulan yang dapat diperoleh pada penelitian yang telah dilakukan ini adalah sebagai berikut:

a) Layanan keamanan yang dihasilkan menggunakan elemen jaringan *Session Border Controller* (SBC) dapat diimplementasikan dengan baik didalam interkoneksi SIP untuk *International Direct Dialing* (IDD). Layanan keamanan *topology hiding* melalui SIP *Manipulation* SBC dapat menyembunyikan alamat IP signaling *softswitch* dan alamat IP media *softswitch* sehingga informasi tersebut tidak dapat diketahui dari jaringan luar. Hasil layanan keamanan terhadap serangan DOS yang ditujukan kepada alamat IP signaling SBC yang diuji menggunakan *test bed* menghasilkan bahwa PC yang mengirimkan *illegal invite message* mengunakan alamat IP publik akan di-*reject* dengan *code* 403 dengan deskripsi "*Unknown User/Endpoint Not Allowed*" oleh SBC.
b) Pengukuran performansi pensinyalan yang dihasilkan setelah adanya layanan keamanan didapatkan performansi pensinyalan, SEER, dengan rata-rata prosentase selama 24 jam sebesar 99.6% untuk *incoming* dan

98.94% untuk *outgoing* dengan standar batasan minimum yang digunakan PT. Indosat, Tbk adalah 98% untuk SEER. Sedangkan SER diperoleh rata-rata selama 24 jam sebesar 22.68 % untuk *incoming* dan 47.11% untuk *outgoing*, dengan standar batasan minimum untuk SER yang digunakan PT. Indosat, Tbk adalah 20%.

c) Pengukuran kinerja kualitas panggilan dengan perspektif penilaian pengguna (*end user*), parameter MOS sebesar 4.4 dan R-*Factor* diantara 93-93.2 dari hasil yang didapatkan berdasarkan standar ITU-T tingkat didapatkan tingkat kepuasan pengguna sangat memuaskan (*very satisfied*).

7. SARAN

Selain sistem SIP-*Based* VoIP, saat ini masih digunakannya protokol H.323 didalam membentuk suatu jaringan VoIP. Oleh karena masih digunakanya protokol VoIP seperti H.323, untuk itu saran bagi penelitian selanjutnya adalah dengan melakukan penelitian interkoneksi antar operator maupun antar sistem VoIP yang menggunakan protokol yang berbeda agar dapat bekerja, misalnya interkoneksi sistem SIP-*Based* VoIP dengan sistem VoIP H.323. Pada penelitian tersebut dapat dilakukan analisa mengenai *interworking* SIP dengan H.323 yang mengarah kepada suatu tolak ukur kinerja pensinyalan dan juga kualitas panggilan yang dihasilkan tidak hanya melalui layanan keamanan namun juga menggunakan layanan *interworking* antar protokol VoIP.

DAFTAR PUSTAKA

[1] Acme Packet, *Net-Net 9000 Configuration Guide Release Version S-D7.1.10*. Acme Packet, 2010.

[2] Rafique M. Z, Ali Akbar M., Farooq M., *Evaluating DoS Attacks Against SIP-Based VoIP Systems*. IEEE GLOBECOM, 2009, pp:1-6.

[3] Liancheng Shan, Ning Jiang, *Reasearch on Security Mechanisms of SIP-Based VoIP System*, IEEE Computer Society, Ninth International Conference on Hybrid Intelligent Systems, 2009, pp:408-410.

[4] Johnston, Alan B., *SIP: Understanding the Session Initiation Protocol*. Third Edition. Artech House, 2009.

[5] Hu Guang, Liu Yan, Yu Xin, *Reasearch and Implementation of NAT Traversal for SIP in Softswitch*, IEEE Computer Society, Second International Conference on Future Generation Communication and Networking, 2008, pp:449-453.

[6] Xener System. *Understanding Routing Data Association X-3000*. Xener System, 2008.

[7] Peter Thermos, Ari Takanen. *Securing VoIP Networks: Threat, Vulnerabilities and Countermeasures***.** Pearson Education, 2007.

[8] Behrouz A. Forouzan. *Data Communications & Networking***.** Fourth Edition. McGraw-Hill International Edition, 2007.

[9] Angela Orebaugh, Gilbert Ramirez, Josh Burke, Greg Morris, Larry Pesce, Joshua Wright. *Wireshark & Ethereal Network Protocol Analyzer Toolkit*. Syngress Publishing, 2007.

[10] Franklin D. Ohrtman, JR. *Softswitch Architecture for VoIP*. McGraw Hill, 2004.

[11] Sivus. *Sivus VoIP Vulnerability Scanner – User Guide v1.07*. www.voipsecure.org, 2004.