DESAIN DAN IMPLEMENTASI TUNNELING IPSEC BERBASIS UNIX DENGAN ESP (ENCAPSULATING SECURITY PAYLOAD) (STUDI KASUS : PT. SUMEKS TIVI PALEMBANG & PT. SUMATERA EKSPRES)

Zaid Amin

STMIK PalComTech Palembang

Abstract

Implementation of authentication methods and encryption of data packets in the communication process on the current internet is not too bothered the security aspects in depth, because security is still done by third parties and service providers usually only runs on application layer. As one of TCP/ IP Protocol Suite, IP Security as part of the transmission of security-based internetwork datagram. Encapsulating Security Payload (ESP) is one of key protocol in the IPsec (Internet Security) architecture, which is designed to provide confidentiality, connectionless integrity, authentication, and anti-replay by encrypting data to be protected.

Keywords : *IP Security, Tunneling, Encapsulation Security Payload*

PENDAHULUAN

Pentingnya keamanan sistem informasi dalam suatu organisasi atau perusahaan sangatlah bergantung pada kompleksitas penggunaan dan pengembangan sistem tersebut nantinya, didukung juga oleh kemampuan membangun infrastruktur (kondisi finansial perusahaan), dan kebijakan yang akan diberlakukan pada sistem organisasi tersebut.

Dalam konteks keamanan jaringan dan permasalahan teknologi informasi ini, maka penulis mencoba untuk melakukan penelitian pada salah satu media terbesar di Indonesia yaitu Jawa Pos Group yang anak perusahaan nya bernama Sumatera Ekpsres Group, dimana sebagai perusahaan media elektronik dan cetak yang memiliki jaringan yang tersebar dan terbesar di Provinsi Sumatera Selatan, sangatlah bergantung kepada pemanfaatan teknologi jaringan internet sebagai media lalu lintas pengiriman data dan informasinya.

Sumatera Ekpres Group mempunyai tanggung jawab yang besar dalam menjaga independensi setiap informasi yang didapatkan, agar informasi tersebut, harus berdasarkan fakta, tidak cacat dan bersifat rahasia, juga dapat terdistribusikan secara baik dan terpercaya (*reliable*) pada tiap-tiap anak perusahaan yang tergabung didalam group tersebut. dengan melihat kebutuhan dan masalah yang terjadi di Sumatera Ekspres Group saat ini, sudah

seharusnya dibutuhkan suatu jalur lalu lintas pengiriman data yang khusus (aman dan terpercaya) yang salah satunya dengan metode *Tunneling*. Untuk itulah pada kesempatan penelitian penulis memilih metode *Tunneling* dengan menggunakan protokol *IP Sec, IPSec/IP Security* digunakan agar pada setiap kegiatan lalu lintas pengiriman data dapat melalui suatu proses enkripsi, autentikasi yang ditambah dengan metode kriptografi yang dapat dijamin keamanannya beserta integritas keaslian (*originality*) dari data tersebut.

LANDASAN TEORI

Pengertian Desain dalam Kegiatan Penelitian

Menurut Nazir (2003:84), desain penelitian merupakan proses yang diperlukan dalam perencanaan dan pelaksanaan penelitian, sehingga bisa dikatakan bahwa desain penelitian diperlukan untuk melakukan penelitian mulai dari tahap awal berupa merumuskan masalah hingga sampai pada tahap pelaporan hasil penelitian.

Pengertian Implementasi

Menurut Purwanto (2006:255) implementasi adalah tahapan penerapan atau tindakan yang diperlukan agar mencapai sukses dalam suatu penelitian. Oleh karenanya, tahapan ini bukan lagi sebagai wacana pemikiran atau ide lagi, tetapi sudah berada pada tahapan perilaku dan tindakan yang diperlukan dalam penelitian.

Pengertian *Tunneling*

Tunneling adalah suatu proses komunikasi di dalam jaringan komputer yang melindungi isi daripada paket-paket suatu protokol dengan melakukan metode enkapsulasi baru paket-paket tersebut dengan protokol yang lain. Enkapsulasi paket tersebut berjalan pada suatu tunnel (terowongan) pada jaringan publik yang belum terjamin keamanannya. Jalur jaringan virtual tersebut berjalan diantara kedua titik lokasi terakhir yang saling berkomunikasi (*end communication*) yang dimana pada setiap titik komunikasi tersebut melakukan proses enkapsulasi dan de enkapsulasi paket (Stewart, et.al, 2005:123).

Konsep Dasar Protokol IPSec (IP *Security*)

Internet Protokol Security (IPSec), seperti yang telah ditetapkan di dalam dokumen *Request For Comment* (RFC 2401), berisikan mengenai penyediaan jaminan untuk suatu proses autentikasi (*authenticity*), integritas keutuhan data (*integrity*), dan kerahasiaan (*confidentiality*) dari suatu data di lapisan network (*network layer*) dalam lapisan OSI (*Open System Interconnection*).

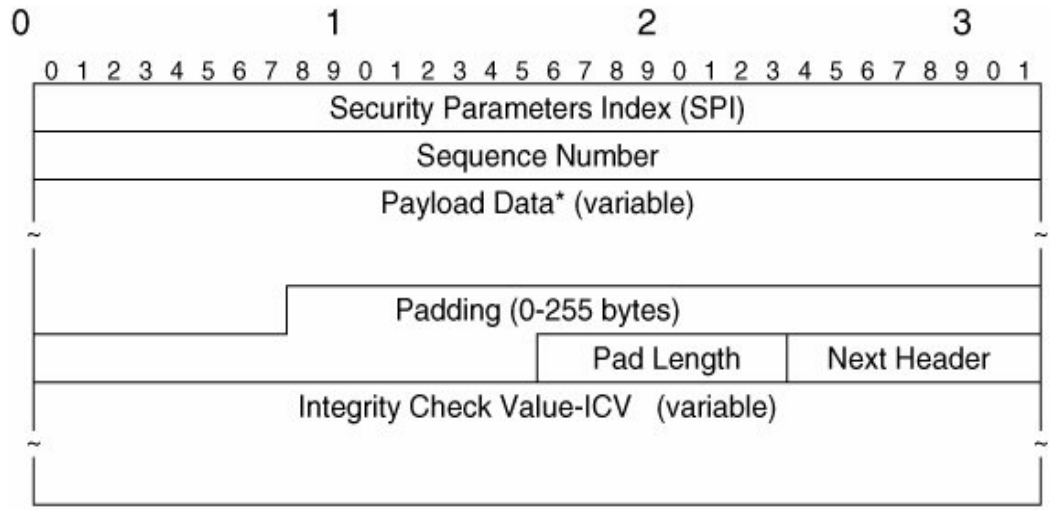
Arsitektur Protokol *IPSec*

Arsitektur *IPSec* menggunakan dua protokol untuk menyediakan keamanan lalu lintas pada suatu proses pengiriman data, yaitu AH (*Autentication Header*) dan ESP (*Encapsulating Security Payload*). Adapun layanan protokol IPSec tersebut adalah (Kent et al.2005):

1. ***Authentication Header* (AH)** memungkinkan verifikasi daripada identitas pengirim. AH juga memungkinkan pemeriksaan integritas dari pesan/informasi atau menyediakan servis *data integrity* dan *origin authentication* (keaslian data).

2. ***Encapsulating Security Payload*** **(ESP)** memungkinkan enkripsi informasi sehingga tetap rahasia, istilah lainnya adalah menyediakan servis data *confidentiality*. Sebuah paket IP asli dibungkus (dienkapsulasi).

Protokol *Encapsulating Security Payload* (ESP) *Format*



Gambar 1. *Encapsulating Security Payload* (ESP) *Header Format*

Field Format* Protokol ESP *Header

Banyak daripada *Field-field* yang berada pada Format ESP *header* memiliki kesamaan fungsi seperti pada AH. Adapun fungsi *field-field* tersebut adalah sebagai berikut :

a. ***Payload Data*** : *Field* ini berisi paket data pengguna. *Field* ini juga berisi *Initialization Vektor* (IV) *dan* Lapisan *Traffic Flow Confidentiality* (TFC). Algoritma enkripsi tertentu menggunakan *Initialization Vektor* (IV) untuk mengenkripsi blok pertama pada paket data pengguna (*user data packet*) dan Lapisan TFC digunakan untuk menyembunyikan suatu karakter yang terjadi pada lalu lintas data seperti ukuran (*size*) suatu paket.

b. ***Padding*** **:** *Field* ini digunakan untuk memastikan paket data pengguna adalah kelipatan dari sejumlah *byte* tertentu (hal ini diperlukan oleh algoritma enkripsi yang kita gunakan) dan memastikan daripada panjang *Pad* (*Pad Length*) dan *field* untuk *header* selanjutnya masuk dalam sususan secara tepat pada 4 *byte* yang telah dibatasi dari keselruhan paket yang ada.

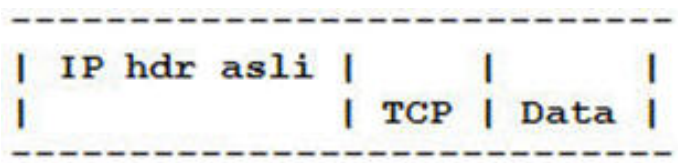
c. **ICV :** *Field* ini adalah *field* yang opsional, yang fungsinya sama dengan ICV yang berada pada AH. *Field* ICV akan digunakan pada ESP apabila autentikasi pada ESP dikonfigurasi.

ESP dapat berjalan dalam dua *mode*:

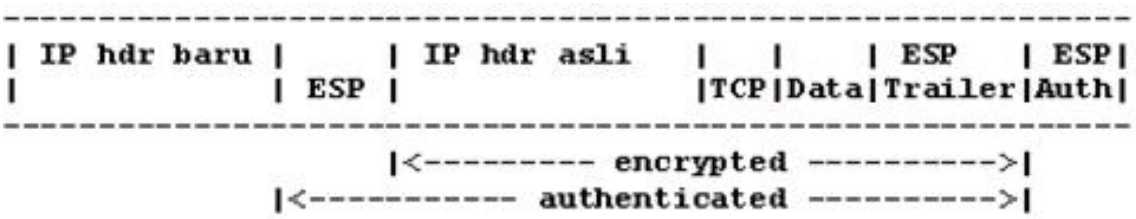
1. ***Transport Mode***
2. ***Tunnel Mode***

Penambahan Protokol ESP (*Encapsulating Security Payload)* pada mode Tunnel :

Sebelum dibungkus protokol ESP

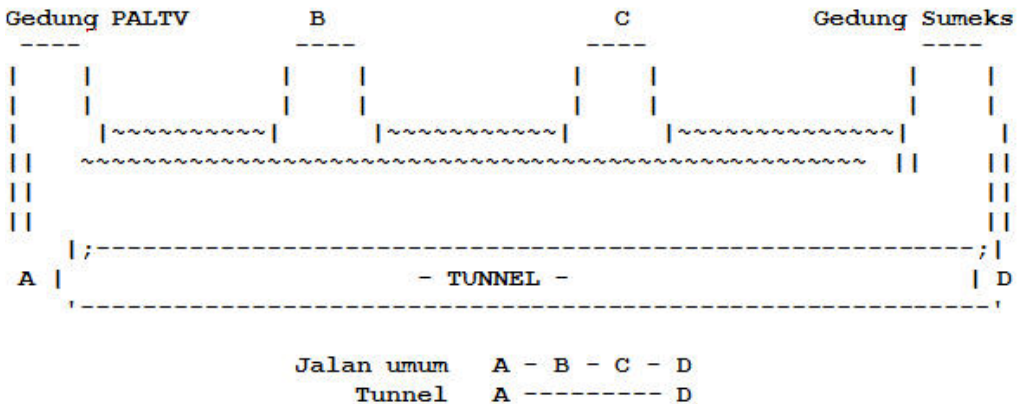


Setelah dibungkus protokol ESP



Analogi *Mode Tunnel*

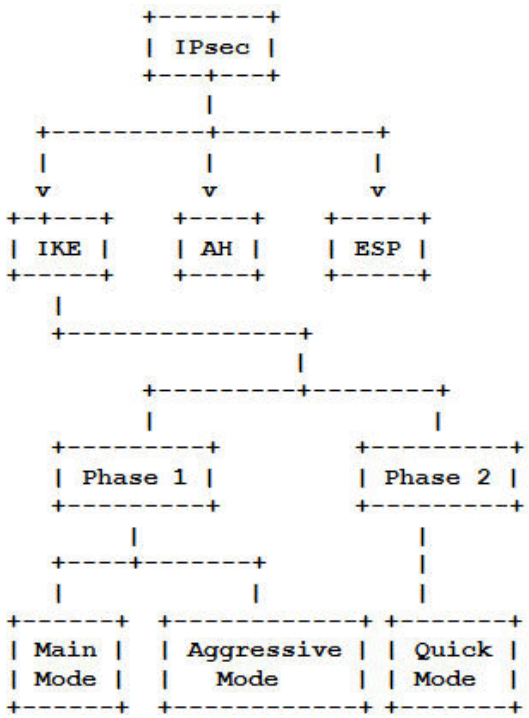
Tunneling dengan menggunakan protokol IPSec adalah sebenarnya suatu hubungan *logical* atau non fisik secara *point to point* dengan metode autentikasi dan ekripsi. *Tunneling* dapat mudah kita pahami dengan analogi seperti jalur kendaraan yang melewati dua tempat yang berbeda (gedung) melalui jalur khusus seperti suatu terowongan (jalur yang tidak umum) seperti diagram dibawah ini (Nemo, 2008) :



Gambar 2. Analogi *Mode Tunnel*

Key Management

Selain daripada protokol AH (*Authentication Header*) dan ESP (*Encapsulation Security Payloads*), teknologi keamanan *tunneling* pada protokol IPSec juga menyediakan fasilitas tambahan dalam pertukaran suatu kunci digital yang dinamakan *Internet Key Exchange* (IKE).



Gambar 3. Penambahan Protokol *Internet Key Exchange* (IKE).

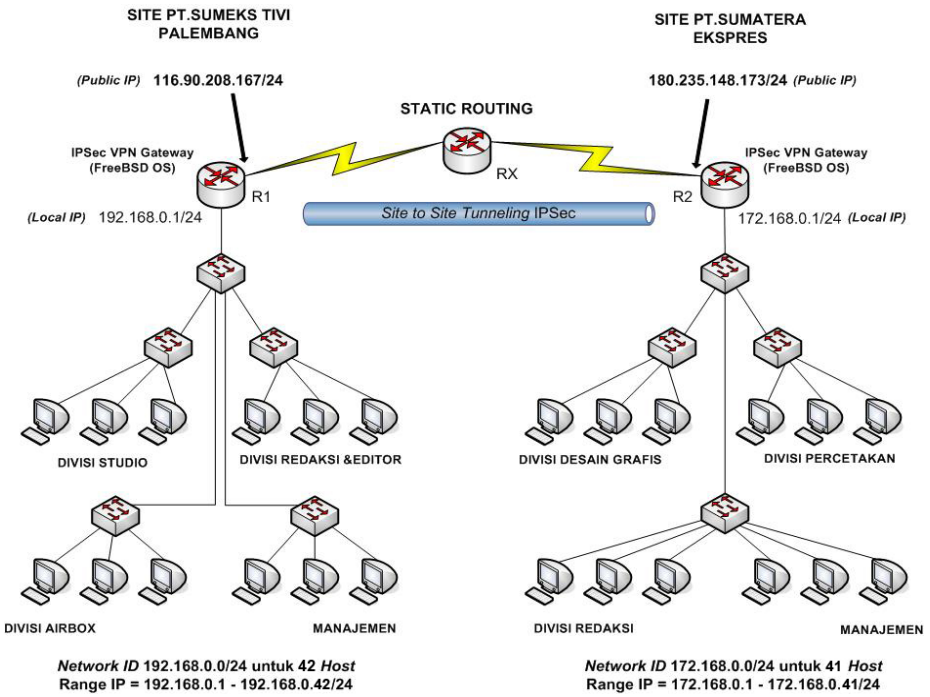
DESAIN *TUNNELING* YANG DIUSULKAN :

Tabel 1. Konfigurasi IP *Address* Jaringan LAN PT.Sumeks Tivi Palembang

KETERANGAN	R1_PALTV	*LOCAL NETWORK*
IP ADDRESS	**202.10.10.1 (PUBLIC)** **192.168.0.1 (PRIVATE)** **10.10.10.1 (GIF0)**	**192.168.0.0/24**

Tabel 2. Konfigurasi IP *Address* Jaringan LAN PT.Sumatera Eskpres Palembang

KETERANGAN	R2_SUMEKS	*LOCAL NETWORK*
IP ADDRESS	**202.10.10.2 (PUBLIC)** **172.168.0.1 (PRIVATE)** **10.10.10.2 (GIF0)**	**172.168.0.0/24**



Gambar 4. Topologi jaringan komputer yang akan diterapkan pada PT.Sumeks Tivi Palembang dan PT.Sumatera Ekspres

Pemilihan Parameter Kebijakan *Tunneling* IP *Security* :

Tabel 3. Pemilihan Parameter *IPSec*

Authentication method	***Pre-shared secret key "abcdefg"***
Encryption Algorithm	***3des***
Authetication Algorithm	***HMAC_SHA1***
Encryption Mode	***Tunnel***
DH Group	***2***
PFS	***Yes***
Phase 1 lifetime	***30 Sec***
Phase 2 lifetime	***15 Sec***
Compression Algorithm	***Deflate***

PEMBAHASAN

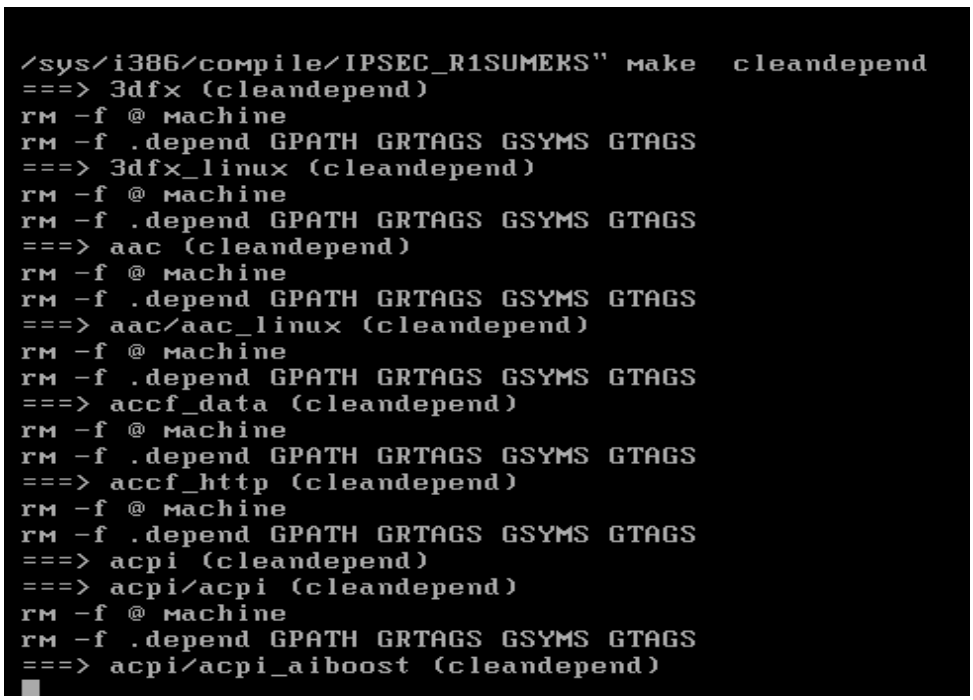
A. Penambahan opsi pada Kernel

1. Menambahkan opsi-opsi pendukung, seperti dukungan untuk protokol IP *Security* dan dukungan *firewall*, dimana penambahan opsi *firewall* tersebut dibutuhkan sebagai

aturan *default* untuk mengizinkan semua lalu lintas port dan protokol yang akan berjalan pada *tunneling* Protokol IPSec nantinya, dan konfigurasi penambahan nya adalah sebagai berikut :

```
Options    IPSEC

Options    IPSEC_DEBUG

Device     crypto

Options    IPFIREWALL
```

Gambar 5. *Opsi pada Kernel*



Gambar 6. Proses *recompile kernel*

Konfigurasi *Setkey IPSec.conf* pada R1_PALTV

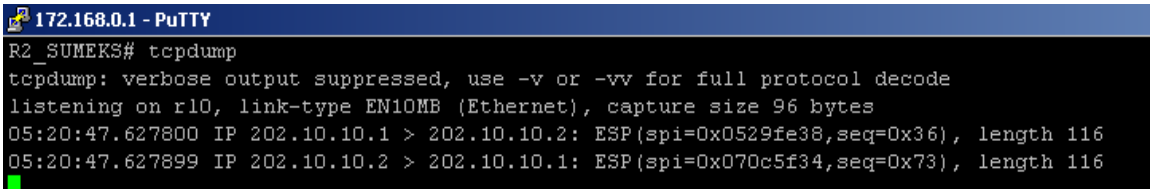
```
flush;

spdflush;

spdadd 10.10.10.1 10.10.10.2 any –P out ipsec
esp/tunnel/202.10.10.1-202.10.10.2/require;

spdadd 10.10.10.2 10.10.10.1 any –P in ipsec
esp/tunnel/202.10.10.2-202.10.10.1/require;

spdadd 10.10.10.1 172.168.0.0/24 any –P out ipsec
esp/tunnel/202.10.10.1-202.10.10.2/require;

spdadd 172.168.0.0/24 10.10.10.1 any –P in ipsec
esp/tunnel/202.10.10.2-202.10.10.1/require;
```

Konfigurasi *Setkey IPSec.conf* pada R2_SUMEKS

```
flush;

spdflush;

spdadd 10.10.10.1 10.10.10.2 any –P in ipsec
esp/tunnel/202.10.10.1-202.10.10.2/require;

spdadd 10.10.10.2 10.10.10.1 any –P out ipsec
esp/tunnel/202.10.10.2-202.10.10.1/require;

spdadd 10.10.10.1 172.168.0.0/24 any –P in ipsec
esp/tunnel/202.10.10.1-202.10.10.2/require;

spdadd 172.168.0.0/24 10.10.10.1 any –P out ipsec
esp/tunnel/202.10.10.2-202.10.10.1/require;
```

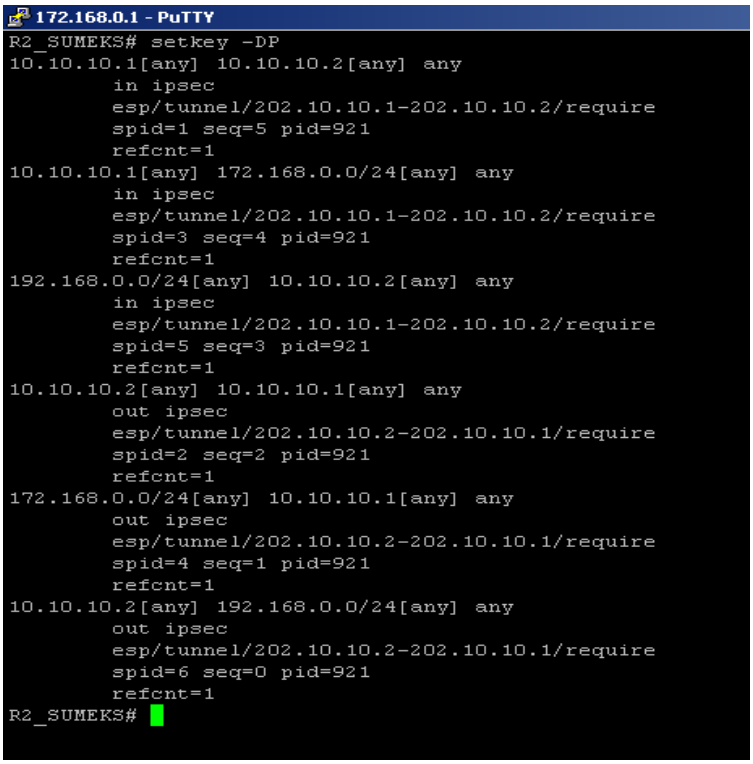
Pembuktian tunneling menggunakan *IPSec*

```
R1_PALTV#ping 172.168.0.1
```



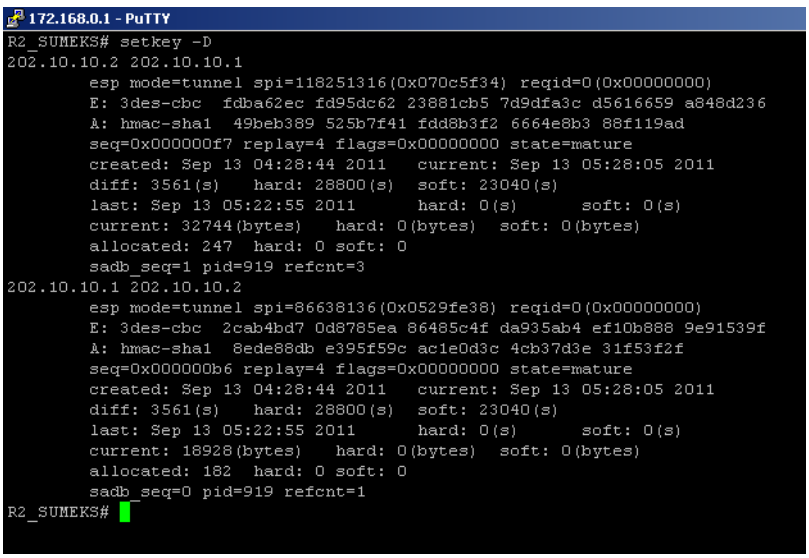
Gambar 7. Hasil *output* pembuktian *capture packet tunneling* dengan protokol *IPSec*

```
R2_SUMEKS#setkey -DP
```



Gambar 8. Hasil *output* pembuktian database *tunneling* dengan protokol *IPSec*

```
R2_SUMEKS#setkey -D
```



Gambar 9. Hasil *output* pembuktian database *tunneling* dengan protokol *IPSec*

PENUTUP

Berdasarkan dari hasil desain dan implementasi penelitian yang menggunakan teknologi *tunneling* protokol IPSec yang telah dilakukan serta analisa dan pembahasan yang telah diuraikan pada PT.Sumeks Tivi Palembang dan PT.Sumatera Ekspres, maka penulis dapat menarik simpulan, bahwa telah dihasilkan sebuah jalur lalu lintas komunikasi proses pertukaran data yang aman dan terpercaya (*secure and reliable*) diantara kedua perusahaan. Dengan model tipe *tunneling* IPSec yang mencakup keseluruhan daripada *site to site* di kedua perusahaan tersebut, maka hal ini dapat mencegah kemungkinan secara menyeluruh sampai ke *level Local Area Network* (LAN) diantara kedua perusahaan.

DAFTAR PUSTAKA

Baharun, Segaf Hasan. 2005, ***Bagaimanakah Anda Menunaikan Zakat Dengan Benar,*** Cetak Kedua, yayasan Pondok Pesantren Darullughan Wadda'wah, Bangil Pasuruan.

Alshamsi, dkk. 2004. ***A Technical Comparison of IPSec and SSL.*** Tokyo University Technology: (*http://eprint.iacr.org/2004/314.pdf, diakses 29 April 2011*).

Carmouche, Henry, James. 2006. ***IPsec Virtual Private Network Fundamentals.*** Cisco Press : Indianapolis, USA.

Danimartiawan, dkk. Tt, IPSec: ***Aplikasi Teknik Kriptografi untuk Keamanan Jaringan Komputer.*** Departemen Teknik Informatika ITB : Bandung.

Feilner, Markus. 2006. ***OpenVPN Building and Integrating Virtual Private Networks.*** Packt Publishing : Birmingham.

Farrokhi, Babak. 2008. ***Network Administration with FreeBSD 7.*** Packt Publishing : Birmingham.

Jogiyanto. 2005. ***Analisis dan Disain Sistem Informasi Pendekatan Terstruktur Teori dan Praktek Aplikasi Bisnis,*** Cetakan Ketiga, Andi :Yogyakarta.

Kusmayadi, dkk. 2008. ***Be Smart Bahasa Indonesia***. Grafindo Media Pratama : Bandung.

Kent, dkk. 1998. ***Security Architecture for the Internet Protocol.*** Internet Engineering Task Force. *(http://www.ietf.org/rfc/rfc2401.txt, diakses pada 29 April 2011, Pukul: 09:10:44 wib).*

Kent, dkk. 2005. ***Security Architecture for the Internet Protocol.*** Internet Engineering Task Force***.*** *(http://tools.ietf.org/html/rfc4301#section-3.1, diakses pada 29 April 2011, Pukul: 09:40:04 wib).*

Lammle, Todd. 2007. ***CCNA Cisco Certified Network Associate Study Guide***. Wiley Publishing,Inc: Indianapolis,Indiana.

Lewis, Mark. 2006. ***Comparing, Designing, and Deploying VPNs***. Cisco Press : Indianapolis, USA

Nazir, Moh. 2003. ***Metode Penelitian***. Ghalia Indonesia:Jakarta.

Nemo. 2008. ***Fun with the IP Security Protocol.*** Terbitan Online Kecoak Elektronik. *(http://www.kecoak.org/ezine/toket4/0x01-fun-ipsec.txt, diakses pada 29 April 2011, Pukul: 08:40:14 wib).*

Ramadhan, Arief. 2006. ***Student Guides Series Pengenalan Jaringan Komputer.*** PT Elex Media Komputindo: Jakarta.

Rafiudin, Rahmat. 2003. ***Panduan Membangun Jaringan Komputer untuk Pemula***. PT Elex Media Komputindo : Jakarta.

Rafiudin, 2002 , ***Security Unix***. PT Elex Media Komputindo : Jakarta.

Syafrizal, Melwin. 2005. ***Pengantar Jaringan Komputer*** . Andi : Yogyakarta.

Stewart, James, dkk. 2005***. CISSP Certified Information Systems Security Professional Study Guide.*** Sybex Inc : United States of America.

Tim Madcoms. 2010. ***Sistem jaringan Komputer untuk Pemula***. Andi, Madcoms : Yogyakarta.

Widjono. 2007. ***Bahasa Indonesia Mata Kuliah Pengembangan Kepribadian di Perguruan Tinggi***. PT Grasindo : Jakarta.

Tim Wahana, Komputer. 2006. ***Menginstalasi Perangkat Jaringan Komputer***. PT Elex Media Komputindo : Jakarta.

Yani, Ahmad. 2008. ***Panduan Membangun Jaringan Komputer***. PT Kawan Pustaka : Jakarta.