

PENERAPAN VPN IP SECURITY SITE TO SITE DI KEMENTERIAN PERHUBUNGAN

Luthfi Firdhaus¹; Fatmawati²; Bambang Wijonarko³

Teknik Informatika
STMIK Nusa Mandiri
www.nusamandiri.ac.id
luthfi.firdhaus@gmail.com

Sistem Informasi
STMIK Nusa Mandiri
www.nusamandiri.ac.id
fatmawati.fmw@gmail.com

Teknologi Komputer
Universitas Bina Sarana Informatika
www.bsi.ac.id
bambang.bwo@bsi.ac.id



Abstract—The current network technology is not covering one building, or one office or one area, but it is progressing some convarege area different from province, island difference even can also different continent. The Ministry of Transportation is a government office where security in data delivery is of paramount importance. Problems that occurred in the Ministry of Perhubunhan is not secure the process of sending data that is done from the head office to the branch office. The presence of VPN provides a mediation of communication path through the public network with the encryption process on the data, so that the data to be transmitted can only be accessed by the client and kept confidential. Using IPSecurity VPN infrastructure is one of the solutions to improve data security on computer networks that support many authentication and encryption methods. IPsec works by encrypting the data packets automatically before being sent. Thus, although the data successfully intercepted by a third party then the data will not be useful because the data has been encrypted. This kind of problem is basically a common problem that is common in many companies around the world.

Keyword: Virtual Private Network, Wide Scale Network, IP Security.

Abstrak—Teknologi jaringan saat ini sudah bukan mencakup satu gedung, atau satu kantor atau satu area saja, tetapi saat ini perkembangannya beberapa convarege area beda propinsi, beda pulau bahkan bisa juga beda benua. Kementerian perhubungan merupakan kantor pemerintahan yang di mana keamanan dalam pengiriman data adalah suatu hal yang sangat penting. Permasalahan yang terjadi di Kementerian Perhubungan adalah belum amannya proses pengiriman data yang di lakukan dari kantor pusat ke kantor cabang. Hadirnya VPN memberikan suatu mediasi jalur komunikasi melalui jaringan publik dengan proses enkripsi pada data, sehingga data yang akan di transmisikan hanya dapat di akses oleh client dan terjaga kerahasiaannya. Dengan menggunakan infrastruktur VPN IPSecurity merupakan salah satu solusi untuk meningkatkan keamanan data pada jaringan komputer yang mendukung banyak metode otentikasi dan enkripsi. IPsec bekerja dengan melakukan enkripsi pada paket data secara otomatis sebelum dikirimkan. Dengan demikian walaupun data berhasil disadap oleh pihak ketiga maka data tidak akan berguna karena data telah terenkripsi. Permasalahan seperti ini pada dasarnya merupakan masalah umum yang biasa terjadi di banyak perusahaan diseluruh dunia.

Kata Kunci: Virtual Private Network, Jaringan Skala Luas, IP Security

PENDAHULUAN

Kementerian Perhubungan atau yang lebih lama disebut Departemen Perhubungan merupakan salah satu instansi besar negara. Kementerian ini memiliki *scope* atau jangkauan yang sangat luas, sehingga diperlukan penerapan informasi teknologi yang mendukung kinerja dari Kementerian ini dimana setiap aktifitasnya menggunakan komputer dan jaringan internet, yaitu mulai dari sharing data dari kantor cabang menuju kantor pusat atau sebaliknya. Jaringan komputer memang menjadi pilihan yang tepat baik itu perusahaan maupun personal untuk menyediakan informasi dan menghubungkan jaringan LAN ke internet (Varianto & Badrul, 2015). Kementerian Perhubungan Dalam melaksanakan tugas dan Pekerjaannya masih menggunakan E-mail Sebagai Sarana Pengiriman data, E-mail umumnya dilakukan melalui internet yang merupakan jalur publik sehingga memungkinkan terjadinya serangan oleh digital attacker seperti penyadapan dan modifikasi informasi (Pt & Frasti, 2017). keamanan di dalam pengiriman serta penerimaan data sangat penting, untuk menjamin bahwa data yang dikirim tidak jatuh ke pihak ketiga, terutama jika data tersebut bersifat rahasia, Untuk itu perlu adanya pengamanan data pada jaringan (Hidayatulloh, 2014) hal yang perlu dilakukan adalah dengan melakukan analisis resiko pada jaringan, menentukan level keamanan yang diperlukan pada suatu organisasi, serta melakukan identifikasi terhadap informasi-informasi yang perlu untuk dilindungi dari serangan pada jaringan.

Teknologi jaringan yang dapat mendukung hal ini adalah teknologi *Virtual Private Network* (VPN), yang dapat mengemulasikan dua jaringan yang lokasinya berjauhan saling berkomunikasi seakan-akan kedua jaringan tersebut di dalam suatu jaringan internet yang besar (Suryanto & Dewi, 2013).

Virtual Private Network (VPN) banyak digunakan untuk meningkatkan keamanan data-data komunikasi yang bersifat rahasia. Pada prinsipnya, VPN merupakan sebuah sambungan komunikasi yang bersifat pribadi dan dilakukan secara virtual (Supriyono, Widjaya, & Supardi, 2013) dan VPN bukanlah hal baru, yang membuat VPN ini menjadi menarik dikarenakan kemampuannya untuk mengamankan intranet dengan kedinamisannya untuk mengakomodasi lingkungan bisnis yang selalu berubah-ubah pesat (Munandar & Badrul, 2015). Sedangkan ketika akan mengimplementasikan IPSec, hal yang penting untuk diketahui adalah adanya suatu keseimbangan antara mengamankan data dari user yang tidak berhak dan membuat user yang

memiliki akses untuk dapat masuk ke dalam jaringan (Hidayatulloh, 2014).

Site to site VPN merupakan jenis implementasi VPN yang menghubungkan antara dua tempat atau lebih yang letaknya berjauhan, seperti halnya menghubungkan kantor pusat dengan kantor cabang (Hendriana, 2012). Dari permasalahan di atas maka penulis mengimplementasikan *Virtual Private Network, IP Security Site to Site* pada Kementerian Perhubungan sebagai solusi tingkat keamanan yang bisa di terapkan. Sedangkan tujuan dari penelitian ini adalah mengimplementasikan VPN *IP Security site to site* untuk meningkatkan keamanan data pada jaringan komputer yang mendukung banyak metode otentikasi dan enkripsi sehingga dapat terjaga kerahasiaannya.

BAHAN DAN METODE

Adapun metode yang penulis gunakan dalam penelitian ini adalah:

A. Teknik Pengumpulan data

Dalam penelitian ini penulis menggunakan beberapa teknik pengumpulan data yaitu:

1. Pengamatan (Observasi)

Pada tahap ini penulis melakukan pengamatan serta pengumpulan data secara langsung ke Kementerian Perhubungan.

2. Wawancara (*Interview*)

Pada tahap wawancara penulis melakukan tanya jawab langsung dengan Bapak Sigit Sukmoro selaku operator IT di kementerian perhubungan.

3. Studi Pustaka

Sedangkan pada studi pustaka adapun cara yang penulis lakukan adalah mencari dan membaca buku-buku dari sumber-sumber yang berhubungan dengan penelitian yang penulis lakukan.

B. Analisa Penelitian

1. Analisa Kebutuhan

Pada analisa kebutuhan ini penulis membuat bagaimana sebuah jalur *public* atau internet seperti jalur local dengan meningkatkan sistem akses pada jalur koneksi karena data secara *public* belum tentu tingkat keamanannya terjamin, oleh karena itu proses data yang berjalan harus melewati beberapa network. Kejahatan dunia *cyber* seperti penyadapan, pencurian data dan lain-lain yang menjadi alasan ketidak amanan jalur data tersebut pada jalur *public* atau internet.

2. Desain

Pada tahap ini penulis mendesain jaringan dengan menggunakan Software Cisco Packet Tracer.

3. Testing
Penulis melakukan testing koneksi untuk implementasi jaringan di kementerian perhubungan dengan menggunakan software Cisco Packet Tracer yang mana aplikasi ini bertujuan untuk merancang jaringan sebelum di implementasikan ke dunia.
4. Implementasi
Sedangkan pada tahap implementasi penulis melakukan percobaan VPN IP Scurity antara kantor cabang dengan kantor pusat kementerian perhubungan.

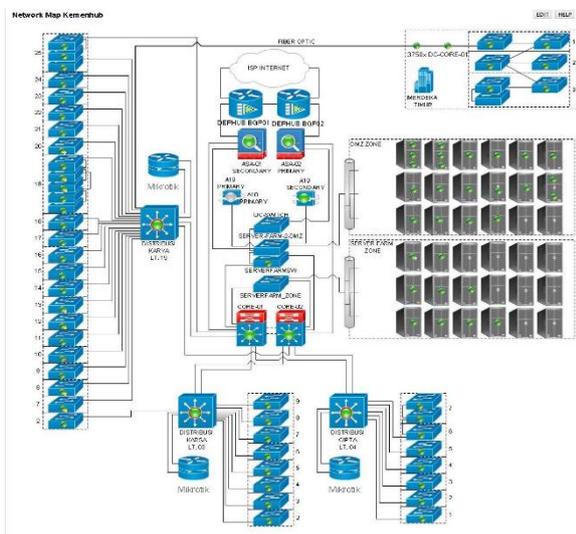
HASIL DAN PEMBAHASAN

Pada pembahasan ini penulis menjelaskan jaringan yang sedang diterapkan dan jaringan usulan, yaitu:

A. Jaringan yang sedang di terapkan

1. Topologi Jaringan

Topologi jaringan yang digunakan oleh Kementerian Perhubungan menggunakan topologi *star* karena topologi *star* masing-Masing *workstation* dihubungkan secara langsung ke server atau *switch*. Keunggulan dari topologi *star* ini yaitu bahwa dengan adanya kabel tersendiri untuk setiap *workstation* ke server maka *bandwith* atau lebar jalur komunikasi dalam kabel akan semakin lebar sehingga akan meningkatkan unjuk kerja jaringan komputer secara keseluruhan.



Sumber : (Firdhaus, Fatmawati, & Wijonarko, 2018) Gambar 1. Topologi Jaringan

Tabel 1. Komponen Topologi Gedung Karsa

NO	KOMPONEN	JUMLAH	KET
1	Switch HP 2610	3	Lantai 5
2	Wireless HP E-MSM410	1	Ruang SSP Dan ruang Dirjen

Acces Point	Topologi Star
Sumber : (Firdhaus et al., 2018)	

Tabel 2. Komponen Topologi Gedung Karya

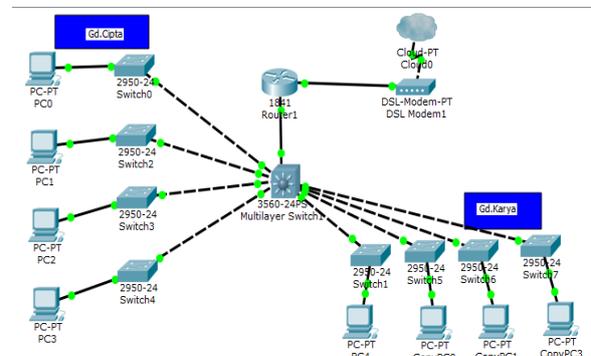
NO	KOMPONEN	JUMLAH	KET	
1	Switch HP 2610	1	Lantai 24	
	Wireless HP E-MSM410	3	Topologi Star	
2	Switch HP 2610	1	Lantai 23	
	Wireless HP E-MSM410	6	Topologi Bus	
	Firewall	2		
	Core Switch	1		
	Server Switch	1		
	Switch HP 2610	1		
3	Wireless HP E-MSM410	6	Lantai 22	
	MSM410	1	Topologi	
	Server nms	1	Half Mash	
	Server Aplication	1	/Hierarki	
	Server Database	1		
	Server Idap dan Dhep	1		
	Server Report	1		
	Server Mobile	1		
	Voluntari	1		
	4	Switch HP 2610	1	Lantai 21
		Wireless HP E-MSM410	3	Topologi Star
5	Switch HP 2610	1	Lantai 20	
	Wireless HP E-MSM410	2	Topologi Star	

Sumber : (Firdhaus et al., 2018)

2. Arsitektur Jaringan

Arsitektur jaringan yang digunakan pada kementerian Perhubungan adalah sistem operasi jaringan model *public service*, dimana jaringan yang ada sekarang diperuntukan untuk kebutuhan akses publik atau masyarakat yang memerlukan informasi dari Kementerian Perhubungan, sehingga publik bisa mengetahui informasi-informasi yang terdapat di dalam portal Kementerian Perhubungan.

3. Skema Jaringan



Sumber : (Firdhaus et al., 2018)

Gambar 2. Skema Jaringan

Skema jaringan pada Kementerian Perhubungan pusat disini yaitu, semua komputer di hubungkan ke sebuah switch pusat, sehingga switch pusatlah yang bertugas untuk mengontrol lalu lintas data, jika satu user ingin mengirim data ke user lain maka data akan dikirim ke switch utama dan langsung di kirimkan menuju user atau komputer tujuan tanpa melewati komputer lain, sehingga proses pengiriman data akan terasa cepat.

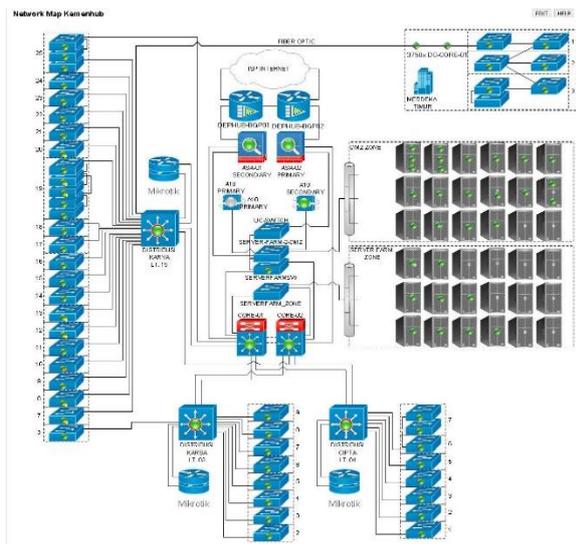
4. Keamanan jaringan

Keamanan yang diterapkan dalam implemenetasi yang sedang berjalan adalah menggunakan *firewall* ASA untuk memfilter trafik. Dan untuk login hak akses dan tracking penggunaan menggunakan perangkat Radio *Mikrotik*.

B. Jaringan usulan

1. Topologi jaringan usulan

Topologi yang di gunakan dan diusulkan penulis pada kementerian perhubungan, yaitu topologi star, pada topologi usulan ini penulis tidak merubah topologi yang sudah ada pada kantor pusat maupun kantor cabang karena pada instansi telah mnggunakan topologi star yang menurut penulis sudah topologi tersebut sudah cukup baik, berdasarkan rancangan jaringan usulan ini maka untuk *IP Address* pada jaringan internal kantor masih tetap.

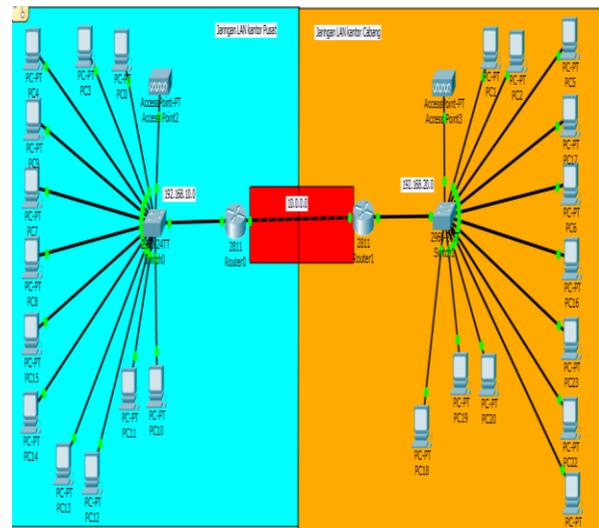


Sumber : (Firdhaus et al., 2018)
Gambar 3. Topologi Jaringan Usulan

2. Skema Jaringan Usulan

Di dalam skema jaringan usulan penulis mencoba mengusulkan pemecahan masalah yang terjadi pada Kementerian Perhubungan adalah

dengan mengkonfigurasi router *cisco* dengan *VPN IP Security*. Pengkonfigurasi router *cisco* ini difungsikan sebagai penghubung antara kantor pusat dengan Kantor dengan kantor cabang dan sebagai jalur *VPN (Virtual Private Network)* dari *client-client* kantor cabang yang akan mengamankan *Internet Protocol (IP)* komunikasi dengan otentikasi dan mengenkripsi setiap paket *IP* dari suatu sesi komunikasi. *Ipssec* melindungi lalu lintas aplikasi di jaringan *IP. Virtual Private Network (VPN)* sendiri merupakan sebuah teknologi komunikasi yang memungkinkan adanya koneksi dari dan ke jaringan publik serta menggunakannya bagaikan menggunakan jaringan lokal dan juga bahkan bergabung dengan jaringan lokal itu sendiri. Dengan menggunakan jaringan publik ini, maka user dapat mengakses fitur-fitur yang ada di dalam jaringan lokalnya, mendapatkan hak dan pengaturan yang sama bagaikan secara fisik kita berada di tempat dimana jaringan lokal itu berada. Hal yang perlu diingat adalah sebuah *private network* haruslah berada dalam kondisi diutamakan dan terjaga kerahasiaannya. Keamanan data tertutupan transfer data dari akses ilegal serta skalabilitas jaringan menjadi standar utama dalam *Virtual Private Network* ini.



Sumber : (Firdhaus et al., 2018)
Gambar 4. Skema Jaringan Usulan

3. Keamanan Jaringan

VPN merupakan teknik pengaman jaringan yang bekerja dengan cara membuat suatu tunnel sehingga jaringan yang terpercaya dapat terhubung dengan jaringan yang ada di luar melalui internet. Infrastruktur publik yang paling digunakan adalah *internet*, di perlukan protokol khusus untuk mengatur pengamanan datanya. Penggunaan *VPN IP security* sangat tepat. Dimana *Internet Protocol (IP)* komunikasi dengan otentikasi dan mengenkripsi setiap paket *IP* dari

suatu sesi komunikasi. IPsec juga mencakup protokol untuk mendirikan otentikasi bersama antara agen pada awal sesi dan negosiasi kunci kriptografi yang akan digunakan selama sesi.

4. Rancangan Aplikasi

Dalam perancangan aplikasi ini penulis menggunakan Packet traser dikarenakan sesuai dengan perangkat keras yang dipakai, serta untuk membuktikan dan perancangan *internet working*. Berdasarkan skema jaringan tersebut penulis mencoba menuangkan rancangan aplikasi yang di terapkan yaitu dengan konfigurasi VPN pada Router Cisco pada konfigurasi ini penulis menuangkan bagaimana mengkonfigurasi VPN yang terdapat di dalam perangkat *router Cisco*.

a. Konfigurasi Router Kantor Pusat

Tabel 3. Konfigurasi Router Cisco pada Kantor Pusat

No	Perintah Pada Router
1.	Router >
2.	Router > enable
3.	Router # configure terminal
4.	Router (config)# interface fastethernet0/0
5.	Router (config-if)# ip address 192.168.10.1 255.255.255.0
6.	Router (config-if)# no shutdown
7.	Router (config-if)# exit
8.	Router (config)# interface fastethernet0/1
9.	Router (config-if)# ip address 10.0.0.1 255.0.0.0
10.	Router (config-if)# no shutdown
11.	Router (config-if)# exit
12.	Router (config-if)# router rip
13.	Router (config-router)# network 192.168.10.0
14.	Router (config-router)# network 10.0.0.0
15.	Router (config-router)# version 2
16.	Router (config-router)# exit
17.	Router (config)# crypto isakmp policy 10
18.	Router (config-isakmp)# authentication pre-share
19.	Router (config-isakmp)# hash sha
20.	Router (config-isakmp)# encryption aes 256
21.	Router (config-isakmp)# group 2
22.	Router (config-isakmp)# lifetime 86400
23.	Router (config-isakmp)# exit
24.	Router (config)# crypto isakmp key toor address 10.0.0.2
25.	Router (config-if)# crypto ipsec transform-set TSET es-aes esp-sha-hmac
26.	Router (config-if)# access-list 101 permit ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
27.	Router (config-if)# crypto map CMAP 10 ipsec-isakmp
28.	Router (config-crypto-map)# set peer 10.0.0.2
29.	Router (config-crypto-map)# match address 101
30.	Router (config-crypto-map)# set transform-set TSET
31.	Router (config-crypto-map)# Exit
32.	Router (config)# Interface fastethernet0/1
33.	Router (config)# crypto map CMAP
34.	Router # Write

Sumber : (Firdhaus et al., 2018) Konfigurasi Router pada Kantor Cabang

Tabel 4. Konfigurasi Router Cisco pada Kantor Cabang

No	Perintah Pada Router
1.	Router >
2.	Router > enable
3.	Router # configure terminal
4.	Router (config)# interface fastethernet0/0
5.	Router (config-if)# ip address 192.168.20.1 255.255.255.0
6.	Router (config-if)#no shutdown
7.	Router (config-if)# exit
8.	Router (config)# interface fastethernet0/1
9.	Router (config-if)# ip address 10.0.0.2 255.0.0.0
10.	Router (config-if)# no shutdown
11.	Router (config-if)# exit
12.	Router (config-if)# router rip
13.	Router (config-router)# network 192.168.20.0
14.	Router > network 10.0.0.0
15.	Router (config-router)# version 2
16.	Router (config-router)# exit
17.	Router (config)# crypto isakmp policy 10
18.	Router (config-isakmp)# authentication pre-share
19.	Router (config-isakmp)# hash sha
20.	Router (config-isakmp)# encryption aes 256
21.	Router (config-isakmp)# group 2
22.	Router (config-isakmp)# lifetime 86400
23.	Router (config-isakmp)# exit
24.	Router (config)# crypto isakmp key toor address 10.0.0.1
25.	Router (config-if)# crypto ipsec transform-set TSET es-aes esp-sha-hmac
26.	Router (config-if)# access-list 101 permit ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255
27.	Router (config-if)# crypto map CMAP 10 ipsec-isakmp
28.	Router (config-crypto-map)# set peer 10.0.0.1
29.	Router (config-crypto-map)# match address 101
30.	Router (config-crypto-map)# set transform-set TSET
31.	Router (config-crypto-map)# Exit
32.	Router (config)# Interface fastethernet0/1
33.	Router (config)# crypto map CMAP
34.	Router# Write

Sumber : (Firdhaus et al., 2018)

5. Manajemen Jaringan

Dengan menggunakan infrastruktur VPN yaitu *VPN IP Security Site to site*. Dari kantor pusat Kementerian Perhubungan maupun dari kantor cabang digunakan *Router* yang menghubungkan

Pada Gambar 7. Menunjukkan keberhasilan pengkoneksian antar kantor cabang dengan kantor pusat, pengetesan dilakukan dengan cara menembak IP *access router* yang bertujuan untuk mengetahui sudah atau belumnya jaringan terkoneksi. Dan jaringan tersebut sudah di konfigurasi menggunakan teknologi VPN IP *Security*, dari segi keamanannya jaringan yang sekarang sudah di enkripsi dengan teknologi VPN IP *Security*. Untuk pengujiannya tertera pada gambar VI.6.

1) Pengujian *command* untuk memverifikasi koneksi VPN

```

Router0
Physical Config CLI
IOS Command Line Interface
Router#show crypto ipsec sa
interface: FastEthernet0/1
Crypto map tag: CMAP, local addr 10.0.0.1

protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.20.0/255.255.255.0/0/0)
current_peer 10.0.0.2 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 6, #pkts encrypt: 6, #pkts digest: 0
#pkts decaps: 7, #pkts decrypt: 7, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 10.0.0.1, remote crypto endpt.: 10.0.0.2
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/1
current outbound spi: 0x2FE56A04(803564036)

inbound esp sas:
spi: 0x622B293E(1646995774)
transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel,}
conn id: 2004, flow_id: FPGA-1, crypto map: CMAP
sa timing: remaining key lifetime (k/sec): (4525504/3130)
IV size: 16 bytes
--More--
    
```

```

Router0
Physical Config CLI
IOS Command Line Interface
inbound esp sas:
spi: 0x622B293E(1646995774)
transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel,}
conn id: 2004, flow_id: FPGA-1, crypto map: CMAP
sa timing: remaining key lifetime (k/sec): (4525504/3130)
IV size: 16 bytes
replay detection support: N
Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x2FE56A04(803564036)
transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel,}
conn id: 2005, flow_id: FPGA-1, crypto map: CMAP
sa timing: remaining key lifetime (k/sec): (4525504/3130)
IV size: 16 bytes
replay detection support: N
Status: ACTIVE

outbound ah sas:

outbound pcp sas:

Router#
    
```

Sumber : (Firdhaus et al., 2018)

Gambar 8. Pengujian *command* untuk memverifikasi koneksi VPN

Pada Gambar 8. menunjukkan keberhasilan dalam penerapan VPN IP *security*, pada tes konfigurasi dengan aplikasi *Command Line Interface* tertera terdapat paket yang terenkripsi dan terenkapsulasi pada saat client di kantor cabang mengirim paket

ke kantor pusat. Dan tertera tipe transform yang di gunakan *esp-aes esp-sha-hmac* maksudnya adalah digunakan untuk menyediakan layanan *confidentiality*, *authentication* dan *integrity* terhadap komunikasi data, Di dalam *ESP header* terdapat informasi yang diperlukan untuk dekripsi dan autentikasi data.

KESIMPULAN

Kementerian Perhubungan pada setiap aktifitasnya masih menggunakan komputer dan jaringan internet yaitu mulai dari mengirimkan data dari kantor cabang menuju kantor pusat atau sebaliknya. Untuk proses pengiriman data kementerian perhubungan masih menggunakan elektronik mail (*e-mail*), di mana proses tersebut masih sangat rawan dari pencurian lewat jaringan internet. Dan dengan adanya penerapan VPN (*Virtual Private Network*) IP *Security* staf IT atau pegawai dapat mengirim data secara mudah, cepat dan aman. Sedangkan dalam penggunaan jaringan VPN IP *Security* memerlukan adanya router sebagai alamat server VPN. Ini dikarenakan router hanya sebagai media pengenkripsian jalur yang akan digunakan. Sedangkan topologi jaringan yang ada di dalam Kementerian Perhubungan adalah topologi *star* dengan perangkat *switch* sebagai pusat dari perangkat-perangkat jaringan computer yang ada dan perkembangan teknologi informasi terus berkembang dengan penerapan router *cisco* yang mempunyai nilai investasi panjang.

REFERENSI

Firdhaus, L., Fatmawati, & Wijonarko, B. (2018). *Laporan Hasil Penelitian*.

Hendriana, Y. (2012). Evaluasi Implementasi Keamanan Jaringan Virtual Private Network (VPN) (Studi Kasus Pada CV. Pangestu Jaya). *Jurnal Teknologi*, 5, 132-142.

Hidayatulloh, S. (2014). Analisis Dan Optimalisasi Keamanan Jaringan Menggunakan Protokol IPsec. *Jurnal Informatika*, 1(2), 93-104.

Munandar, A., & Badrul, M. (2015). Penerapan Open Vpn Ipcop Sebagai Solusi Permasalahan Jaringan Pada PT. Kimia Farma Trading & Distribution. *Teknik Komputer AMIK BSI*, 1(1), 30-41.

Pt, K., & Frasti, T. (2017). Implementasi Protokol S / Mime Pada Layanan E-Mail Peningkatan Jaminan Keamanan Secara Online Pada, 2(2).

Supriyono, H., Widjaya, J. A., & Supardi, A. (2013).

- Penerapan Jaringan Virtual Private Network Untuk Keamanan Komunikasi Data Bagi PT. Mega Tirta Alami. *Warta*, 16, 88–101.
- Suryanto, & Dewi, S. (2013). Implementasi Jaringan VPN Berbasis IP-MPLS Pada PT. Mhe Demag Indonesia. *Paradigma*, XV(1), 98–105.
- Varianto, E., & Badrul, M. (2015). Implementasi Virtual Private Network dan Proxy Server Menggunakan Clear OS Pada PT . Valdo International. *Teknik Komputer AMIK BSI*, 1(1), 54–65.