Terakreditasi SINTA Peringkat 2
Surat Keputusan Dirjen Penguatan Riset dan Pengembangan Ristek Dikti No. 10/E/KPT/2019
masa berlaku mulai Vol. 1 No. 1 tahun 2017 s.d Vol. 5 No. 3 tahun 2021

Terbit online pada laman web jurnal: **http://jurnal.iaii.or.id**

JURNAL RESTI
(Rekayasa Sistem dan Teknologi Informasi)
Vol. 4 No. 2 (2020) 228 - 236 ISSN Media Elektronik: 2580-0760

Implementasi Dual Link IPVPN dan GSM Berbasis IPSec pada Fortigate 50 E

Winarti Agustina[1], Muhammad Rifqi[2]
[1,2]Teknik Informatika, Ilmu Komputer, Universitas Mercu Buana
[1]41515120122@student.mercubuana.ac.id, [2]m.rifqi@mercubuana.ac.id

Abstract

At this technological era that everything is almost online-based, the effort to keep a good quality of network that is given to customer, we need the system or network that can help to resolve the problem in long term on customer. To resolve the problem, PT. Lintasarta utilizes Internet Protocol Virtual Private Network (IPVPN) service and Fiber Optic access that is connected each head office and branch. In general, fiber optic access has problem such as FO Cut, where it takes a long time to be solved. It is become a reason for writer to propose to customer to have back up link that can be installed fast and easy at implementation process with fail over system which can minimalize downtime up to 80%. Fortigate 50 can be alternative if sometime the main link gets problem. Backup link uses internet The Global System for Mobile Communications (GSM) that is made as Virtual Private Network (VPN). One of VPN fiture is IPSec Tunneling that gives security for internet protocol (IP) as data-changing. The expected result from this research with dual link fiber optic will be better than GSM modem, with average value of FO such as packet loss 1% , delay FO 0,105 s, and very well latency dual link. But in the other side, GSM network is able to be back up link when FO network is going down, so it can be minimalized the occurrence of downtime.

Keywords: : IPVPN (Internet Protocol Virtual Private Network), IPSec (IP Security), GSM, Fortigate, Failover.

Abstrak

Pada era teknologi yang serba *online* saat ini, salah satu upaya untuk menjaga kualitas jaringan yang diberikan kepada pelanggan dibutuhkan suatu sistem atau *network* yang membantu untuk mengatasi gangguan yang berkepanjangan di pelanggan. Untuk upaya mengatasi dalam permasalahan ini PT Lintasarta menggunakan jasa *Internet Protokol Virtual Private Network* (IPVPN) dan akses *Fiber Optic(FO)* yang terhubung antar kantor pusat dan kantor cabang. Pada umumnya akses *fiber optic* mengalami gangguan seperti FO *Cut*, dimana dibutuhkan waktu penanganan yang cukup lama. Dengan ini peneliti mengusulkan di suatu perusahaan mempunyai *backup link* yang cepat pemasangannya dan mudah dalam implementasi dengan sistem *failover*, dengan minimalisir *downtime* sebesar 80 %. *Fortigate* 50 E menjadi alternatif pengganti jika akses *mainlink* bermasalah. *Backup link* menggunakan *internet The Global System for Mobile Communications* (GSM) yang dibuat *Virtual Private Network* (VPN), salah satu fitur dari VPN yaitu IPSec *Tunneling* yang memberikan keamanan pada lapisan *internet protokol* (IP) sebagai pertukaran data. Hasil dari penelitian dengan dual link jaringan FO lebih bagus dibanding dengan *modem* GSM, dengan nilai rata – rata FO sebagai berikut *packet loss* 1% , *delay* FO 0,105 s, dan *latency dual link* sangat bagus. Namun disisi lain jaringan GSM mampu mem*backup* ketika jaringan FO *down*, sehingga meminimalisir terjadinya *downtime*.

Kata kunci: IPVPN (*Internet Protocol Virtual Private Network*), IPSec (*IP Security*), GSM, *Fortigate, Failover*.

Diterima Redaksi : 02-12-2019 | Selesai Revisi : 22-03-2020 | Diterbitkan Online : 20-04-2020

1. Pendahuluan

Di era teknologi yang serba *online* ini, kebutuhan akses *internet* sangat diperlukan bagi dunia bisnis. Setiap perusahaan memiliki infrastruktur jaringan untuk mendukung keperluan operasional. PT Lintasarta adalah perusahan di bidang telekomunikasi atau ISP (*Internet Service Provider*) dan penyedia layanan pusat data terbesar di Indonesia seperti jasa komunikasi data, *internet* & IT *Services*. layanan terbaik dari PT Lintasarta yaitu memberikan solusi untuk penyediakan layanan IP VPN (*Internet Protokol Virtual Private Network*) menggunakan teknologi berbasis MPLS (*Multiprotocol Label Switching*). Layanan IPVPN memberikan keamanan berbasis IP terutama memanfaatkan privasi data atau jaringan dimana tidak semua orang dapat mengaksesnya. Dengan adanya, VPN (*Virtual Private Network*) menyediakan suatu transmisi data yang aman dan pribadi melalui infrastruktur jaringan dari ISP[1], *customer* dapat mengakses komputer atau pun jaringan kantor, dari mana saja selama terhubung ke jaringan *intranet* atau *private*.

Salah satu upaya untuk memenuhi kualitas *SLA* atau *service* ke *customer* agar tetap *online* dengan memberikan kualitas jaringan yang stabil dan bagus. Untuk menjaga kualitas jaringan tetap stabil, yang akan diberikan kepada *customer*. Maka dibutuhkan suatu sistem atau *network* yang membantu untuk mengatasi gangguan yang berkepanjangan di cabang *customer*. Pada studi kasus kali ini penanganan akses *fiber optic*, jika mengalami gangguan seperti FO *Cut*, membutuhkan waktu penanganan yang cukup lama. Dengan ini peneliti mengusulkan di suatu perusahaan mempunyai *backup link* yang cepat pemasangan dan mudah dalam implementasi. Dengan ditambahkan sistem *failover, s*upaya jaringan cabang tidak terlalu lama dalam kondisi mati atau *downtime*. Implementasi ini menggunakan *fortigate* 50 E, dimana menjadi alternatif pengganti jika akses *mainlink* bermasalah. *Backup link* menggunakan *internet* GSM (*The Global System for Mobile Communications*) yang dibuat VPN (*Virtual Private Network*), salah satu fitur dari VPN yaitu IPSec *Tunneling*. *Internet Protocol Security* (IPSec) merupakan metode pada protokol yang mendefinisikan algoritma kriptografi yang digunakan untuk mengenkripsi, mengotentikasi, dan mendekripsi paket yang memberikan keamanan pada lapisan IP sebagai pertukaran data yang aman dan manajemen data[2].

Secara sederhana jaringan komunikasi data dapat diartikan sebagai penghubung antar kantor pusat dengan kantor cabang untuk saling berkomunikasi. Sistem komunikasi jaringan menggunakan layanan VPN (*Virtual Privat Network*) berbasis teknologi IP MPLS (*Internet Protokol Multi Protocol Label Switching*) dimana merupakan teknologi penyampaian paket pada jaringan *backbone* (jaringan utama) berkecepatan tinggi yang menggabungkan beberapa kelebihan dari sistem komunikasi *circuit-switched* dan *packet-switched*. Tujuan dari sistem komunikasi jaringan perusahaan ini adalah untuk menjalankan aplikasi-aplikasi yang digunakan oleh perusahaan, seperti aplikasi perusahan, dan mentransfer data dari kantor pusat ke cabang dan sebaiknya.

Virtual Private Network (VPN), Sebuah teknologi komunikasi yang dapat terkoneksi ke jaringan publik dan menggunakannya untuk dapat bergabung dengan jaringan lokal disebut *Virtual Private Network* [4]. Pada PT Lintasarta menggunakan layanan IPVPN, dimana memanfaatkan jaringan pribadi yang aman dan cepat bagi *end user* dengan koneksi MPLS (*Multiprotocol Label Switching). Multiprotocol Label Switching* (MPLS) adalah teknologi pembawa paket yang digunakan dalam penyedia layanan dan jaringan perusahaan[3].

IP *Security* merupakan standar yang didefinisikan oleh RFCs 2401 untuk memastikan kemanan dan privasi dalam komunikasi menggunakan protokol IP. Standar IPSec menyediakan kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan autentikasi perangkat (*authentication*). IPSec *Tunnel* dibuat untuk menjaga kemanan data antar IPSec *gateway*. IPSec *gateway* bertanggung jawab menjaga kerahasiaan, keutuhan dan keaslian data karena hanya di *endpoint* IPSec *tunnel* saja yang dapat membuka enkripsi dari data yang sudah di enkripsi di IPSec *gateway* sebelumnya. IP *Security* merupakan protokol yang mengintegrasikan fitur kemanan yang didalamnya meliputi proses autentikasi, integrasi, dan kepastian ke dalam *Internet Protocol* (IP) IPsec menggunakan enkripsi, mengenkapsulasi paket IP di dalam paket IPsec. De-enkapsulasi terjadi di ujung terowongan, dimana paket IP asli didekripsi dan diteruskan ke tujuan yang diinginkan[1].

Failover adalah teknik yang menerapkan beberapa jalur untuk mencapai suatu *network* tujuan. Namun dalam keadaan normal hanya ada satu *link* yang digunakan, *link* yang lain berfungsi sebagai cadangan dan hanya akan digunakan bila *link* utama terputus[4].

The Global System for Mobile Communications (GSM), Pada awal pencarian bentuk dari sistem komunikasi yang baru, terdapat berbagai macam sistem seluler yang ada di dunia. Pada tahun 1979 diperkenalkan sistem seluler pertama AMPS (*Advanced Mobile Phone Service*) di Amerika Serikat setelah jaringan pre-operasional pertamanya dibuka di Chicago, Illinois. Kemudian perkembangan ini diikuti negara-nagara di Eropa Utara yang mengeluarkan sistem NMT (*Nordic Mobile Telephone*) yang diperkenalkan pertama kali di Swedia pada bulan September 1981 dan diikuti Inggris pada tahun 1985[5].

Teknologi 4G LTE atau *Long Term Evolution* (LTE) merupakan teknologi *standard 3rd generation partnership project* (3GPP), evolusi dari teknologi

GSM dan UMTS. Data *rate* LTE lebih besar dibanding teknologi yang pernah dikembangkan sebelumnya. LTE disebut sebagai teknologi *4th generation* atau biasa disebut 4G setelah sebelumnya dikembangkan teknologi 3G, sebenarnya LTE belum sepenuhnya memenuhi kriteria sebagai teknologi 4G lebih tepatnya masih 3,9G. LTE memiliki kelebihan diantaranya : a. *Latency/delay* lebih rendah; b. Data *rate* lebih tinggi; c. Meningkatkan kapasitas dan *coverage*; d. *Cost-reduction*[6].

Internet Of Things atau IoT merupakan segala aktifitas yang pelakunya saling berinteraksi dan dilakukan dengan memanfaatkan *internet*. Dalam penggunaannya *Internet of Thing* banyak ditemui dalam berbagai aktifitas, contohnya : banyaknya transportasi *online, e-commerce*, pemesanan tiket secara *online, live streaming, e-learning* dan lain-lain bahkan sampai alat-alat untuk membantu dibidang tertentu seperti *remote temperature sensor*, GPS *tracking*, and sebagainya yang menggunakan *internet* atau jaringan sebagai media untuk melakukannya. Dengan banyaknya manfaat dari *Internet of Things* maka membuat segala sesuatu nya lebih mudah, dalam bidang pendidikan IoT sangat diperlukan untuk melakukan segala aktifitas dengan menggunakan sistem dan tertata serta sistem pengarsipan yang tepat bisa dilihat pada Gambar 1[7].

Gambar 1 Sistem dari *Internet OF Things*

Fortinet merupakan perusahaan, penyedia layanan, dan badan pemerintah di seluruh dunia, termasuk mayoritas dari perusahaan Fortune Global 100 tahun 2009. Fortinet merupakan pemimpin pasar untuk *unified threat management* (UTM). *Unified Threat Management* atau UTM adalah segmen produk jaringan yang dikhususkan untuk menangani fungsi keamanan jaringan secara terpadu. Pada produk UTM ini menghasilkan *fortigate* yang memiliki fitur-fitur seperti *firewall, Intrusion Prevention System, web filtering*, antivirus yang digabungkan menjadi satu kesatuan dengan tambahan fitur jaringan lain seperti *routing* dalam satu *box hardware*.

Gambar 2 Perangkat Fortigate

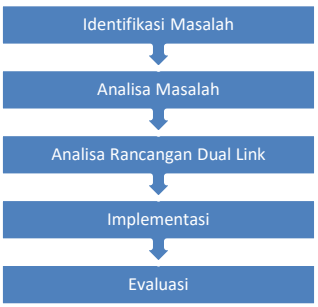
Untuk *device* yang digunakan menggunakan *fortigate*, bias dilihat pada Gambar 2. *Fortigate* sebagai perangkat yang menjamin keamanan jaringan secara keseluruhan sekaligus berfungsi sebagai gateway dan router bagi jaringan LAN (*Local Area Network*) sehingga tidak dibutuhkan lagi *router* ataupun perangkat *tambahan load balancing* bila ada lebih dari satu koneksi WAN (*Wide Area Network*). Satu perbedaan yang utama, konten FortiASIC yang di *custom* sendiri serta prosesor jaringan fortinet memungkinkan sistem *fortigate* mendeteksi dan mengeliminir secara *real time* ancaman yang terintegrasi, bahkan dalam skala kompleks, tanpa menurunkan kinerja jaringan, sementara serangkaian proses manajemen, analisa, *database* dan solusi perlindungan *endpoint* bekerja meningkatkan penyebaran fleksibilitas dan memberikan dampak yang nyata dalam mengurangi biaya operasional manajemen keamanan jaringan[8].

Pada penelitian sebelumnya, saat kualitas dari internet yang tidak stabil maupun gangguan koneksi fisik kabel dan bencana berskala besar yang menyebabkan kegagalan komunikasi dalam kasus IPsec VPN. Untuk menanggulangi masalah tersebut diperlukan solusi yaitu failover. Dengan menggunakan perangkat fortinet dapat berkomunikasi untuk membentuk sebuah tunnel[9].

Adapun peneliti melakukan analisa performasi *dual link* yang berbeda untuk dilakukan implementasi teknologi dari VPN menggunakan *Fiber Optic* dan GSM menggunakan perangkat *fortigate* terhadap performasi jaringan, adapun parameter yang di ukur meliputi *failover*, *delay*, dan *latency* yang di harapakan dapat menekan downtime.

2. Metode Penelitian

Kerangka penelitian adalah suatu cara untuk mendapatkan suatu tujuan tertentu. Dan untuk mencapai tujuan tersebut penelitian ini akan dilakukan dengan cara mengikuti kerangka kerja penelitian seperti pada Gambar 3.



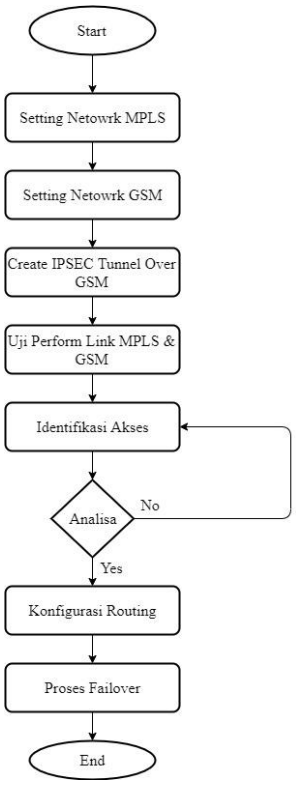
Gambar 3 Kerangka Kerja Penelitian

Masalah yang akan diidentifikasi adalah untuk mengetahui permasalahan yang terjadi dalam konektifitas jaringan komunikasi menggunakan *single link* yang akan diimplementasikan dengan menambahkan link backup GSM menggunakan perangkat fortigate 50 E.

Adapun tahapan dalam melakukan kajian penelitian ini dilakukan teknik pengumpulan data yang diperlukan untuk menyelasaikan masalah. Teknik pertama dilakukan adalah dengan melakukan meninjau dan mengamati secara langsung kegiatan implementasi di lapangan terhadap objek penelitian, dengan teknik ini disebut teknik observasi. kemudian melakukan mengumpulkan data secara tatap muka kepada salah satu staf IT di perusahan PT Lintasarta dilakukan dengan teknik wawancara untuk dapat mengetahui permasalahan yang terjadi secara akurat, sehingga *user* dapat menjaga dan mengontrol kestabilan jaringan. Setelah itu studi literatur dilakukan dengan pengumpulan data dan informasi dengan mencari dan memperoleh data-data yang diperlukan baik jurnal penelitian terkait, *literature* dan *website* sebagai referensi untuk membantu dan mempermudah saat implementasi yang dibuat.

Pada tahap analisa masalah dilakukan analisa pada *customer* PT Lintasarta yang hanya memiliki *single link* saja. Dimana jika *single link* tersebut mengalami kegagalan, maka dibutuhkan suatu sistem atau network, yang berfungsi sebagai *backup link*.

Pada tahap analisa rancangan dual link, dengan menambahkan *backup link* modem GSM dengan berbasis IPSec pada perangkat fortigate 50 E. Proses dual link ini dilakukan aktif pastif menggunakan metode *Failover*, dimana sistem *failover*, dapat meminimalisir adanya kegagalan dari salah satu sistem atau *downtime* yang terlalu lama. Prosedur ini melibatkan permindahan *link* utama secara otomatis ke *link* cadangan sehingga prosedur tersebut memudahkan bagi *user*. Adapun alur Penelitian ini bisa dilihat [ada Gambar 4 bertujuan untuk mengukur dan menganalisa performasi jaringan *dual link* IPVPN & GSM berbasis IPSec pada *Fotigate* 50E. Berikut adalah diagram alur penelitian yang akan dilaksanakan dalam tugas akhir ini.



Gambar 4 Diagram Alur Penelitian

Implementasi IPSec dan failover pada dual link ini dibutuhkan 2 perangkat fortigate 50 E, sebagai *gateway* dan *client*. Disisi gateway diletakkan pada server, yang menghubungkan ke fortigate client di PC *client* sebagai *user*[9].

Quality of Service pada dual link dengan diterapkan Ipsec dan Failover sudah selesai dari tahap implementasi. Maka dari hasil tersebut dapat dilihat *quality of service* atau layanan pada dual link dengan fortigate 50 E.

Terdapat beberapa parameter yang harus dipertimbangan untuk menentukan *quality of service*[10], yaitu Delay merupakan waktu yang dibutuhkan untuk menempuh jarak dari asal ke tujuan. Menurut versi TIPHON, delay dapat diklasifikasikan sebagai berikut, lihat Tabel 1.

Tabel 1 Kategori Delay

Kategori Delay	Besar Delay (ms)	Indeks
Sangat Bagus	<150 ms	4
Bagus	150 ms – 300 ms	3
Sedang	300 ms – 450 ms	2
Jelek	>450 ms	1

Untuk mengukur nilai delay dapat menggunakan rumus persamaan sebagai berikut :

$$Rata\ Rata\ Delay = \left(\frac{Total\ Delay}{Total\ Paket\ Yang\ DiTerima}\right) \quad (1)$$

Packet Loss merupakan suatu parameter yang mengGambarkan suatu kondisi yang menunjukkan total paket yang hilang, dapat terjadi karena collision dan congestion pada jaringan dan hal ini berpengaruh pada semua aplikasi karena retransmisi akan mengurangi efesiensi jaringan secara keseluruhan meskipun jumlah bandwidth cukup tersedia untuk aplikasi-aplikasi tersebut. Jika terjadi kongesti yang cukup lama, buffer akan penuh, dan data baru tidak akan diterima. Nilai packet loss sesuai dengan versi TIPHON sebagai berikut, lihat Tabel 2.

Tabel 2 Kategori Packet Loss

Kategori Packet Loss	Packet Loss	Indeks
Sangat Bagus	0%	4
Bagus	3%	3
Sedang	15%	2
Jelek	25%	1

Untuk mengukur nilai packet loss dapat menggunakan rumus persamaan sebagai berikut :

$$\%Paketloss = \left(\frac{data\ yang\ dikirim - paket\ data\ yang\ diterima}{paket\ data\ yang\ dikirim}\right) \text{x } 100\% \quad (2)$$

Latency merupakan berapa lama perjalanan data antara sumber dan tujuan, diukur dalam milidetik.

3. Hasil dan Pembahasan

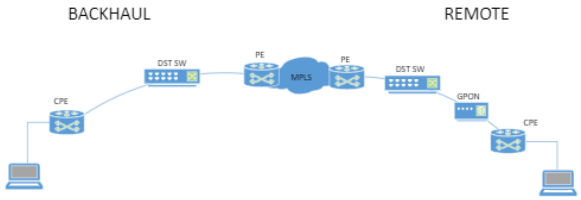
3.1 Pembahasan

Sistem Jaringan yang diusulkan adalah dengan menggunakan VPN yang akan menghubungkan kantor pusat dan kantor cabang customer PT. Lintasarta. VPN mempunyai fungsi yaitu membuat jaringan *private* atau lokal dengan melewati jaringan *public* seperti *internet*, *internet* yang digunakan menggunakan *internet* GSM 4G sehingga teknologi ini memungkinkan dapat menghemat biaya dan aman karena menggunakan metode enkripsi.

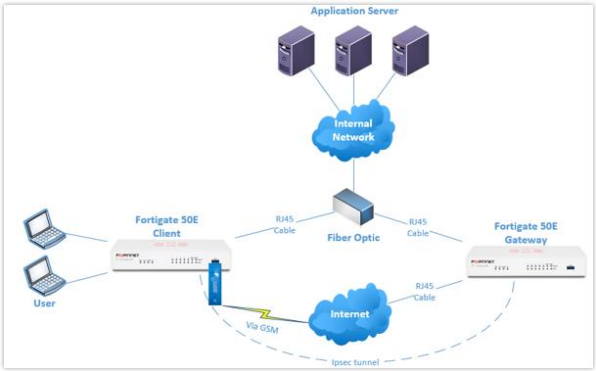
3.1.1 Topologi Jaringan

Skema jaringan *existing* hanya menggunakan 1 *link* saja, dimana jika *link* FO terputus maka *user* tidak bisa terkoneksi dengan aplikasi kantor. Untuk topologi jaringan *existing* dapat dilihat pada Gambar 5, maka dari itu peneliti ini mengusulkan untuk mengganti perangkat router *existing* dengan router *fortigate* 50E dan *modem* USB sebagai media akses *back up* untuk koneksi VPN ke *gateway* atau *backhaul* tujuan. Untuk topologi jaringan usulan dapat di lihat pada Gambar 5.

Dari Gambar topologi 6 kegiatan implementasi ini menggunakan topologi *mesh*. Dimana penelitian ini dibutuhkan 2 perangkat *fortiGate* sebagai implementasi sistem ini, dengan menggunakan *dual link* yang *auto failover* yaitu akses *mainlink* menggunakan *fiber optic* dan *backuplink* menggunakan *internet* GSM. *Internet* ini di buat VPN menggunakan *tunneling* IPSec dimana memberikan keamanan pada jaringan *internet* dari luar yang dilakukan *scaning* atau *filtering* IP *public* ke IP *private*. IPSec membuat jalur baru seperti terowongan untuk jalannya data atau *transport*. Sehingga terhindar dari *hacker*, sadap, dan lain lain.



Gambar 5 Topologi Jaringan Existing



Gambar 6 Topologi Jaringan Usulan

3.1.2 Perangkat Sistem

Adapun pada Tabel 3 perangkat yang digunakan untuk implementasi ini.

Tabel 3. Perangkat Sistem

Device	Qty	Keterangan
Client / User	1	Prosesor : Intel(R) Core(TM) i5 CPU M 380 2.53 GHz, RAM : 4096 MB
Router	2	Router I : Fortigate 50E Client, Router II : Fortigate 50E Gateway
Modem USB	1	Huawei, Model : E353S-2
Server	1	Procesor Intel ® Core ™ i3-2330 CPU @2.20 GHz (4 CPUs),RAM: 8192 MB ; Storage: HDD 1TB Ethernet Card: Realtek PCIe GBE Family Controller
Operating System	1	Komputer Client : Windows 10 64bit, Komputer Server : Sistem operasi Linux Ubuntu Server 12.04 amd64

3.1.3 Rancangan Sistem

Tahap rancangan konfigurasi perangkat router *fortigate* pada PT Lintasarta menggunakan GUI (*Graphical user interface*) dari *web browser*. Tahap pertama, *login* perangkat menggunakan *web browser*. Kedua, pengaturan IP *address* pada perangkat router *fortigate* di PT Lintasarta. Pada router *fortigate* 50E Client menggunakan 2 *port Ethernet* dan 1 *port* USB, *port* WAN 1 sebagai akses FO *mainlink*, *port* LAN 5 sebagai *user*, dan 1 *port* USB sebagai *internet modem*

4G sedangkan pada *fortigate* 50E *Gateway* menggunakan 2 *port Ethernet, port* WAN 1 sebagai akses *Internet* dan *port* Wan 2 sebagai koneksi *private* atau IPVPN. adapun langkah untuk memberikan IP *address* pada masing masing *interface* pada menu di perangkat router. Ketiga, pengaturan *default route* kearah *internet* dan *static route* ke arah WAN. Keempat Pengaturan NAT. *Network Address Translation* (NAT) adalah suatu metode yang menghubungkan lebih dari satu komputer ke jaringan *internet* dengan menggunakan satu alamat IP. Kelima, Pengaturan IPSec *Tunnel*. IPSec *Tunnel* adalah sebuah protokol yang digunakan untuk mengamankan transmisi datagram dalam jaringan. Selanjutnya keenam, Pengaturan *Create policy* untuk mengizinkan koneksi dari *Tunnel* IPsec ke WAN.

3.1.4 *Virtual Private Network* IPSec *Tunneling*

Pengujian IPSec *Tunneling* ini berfungsi melihat *tunneling* menggunakan akses *internet* GSM sudah UP atau terkoneksi dengan router *gateway*nya. Hal ini agar *auto failover* dapat berjalan dengan baik apabila akses *mainlink* sedang mengalami masalah atau *problem*.

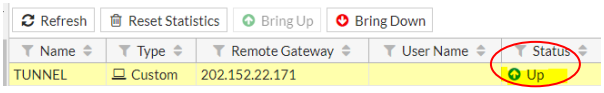
Proses pengujian IPSec sebagai berikut :

Pertama, atur konfigurasi kedua router , router *client* dan *gateway*

```
# show vpn ipsec phase1-interface
config vpn ipsec phase1-interface
    edit "TUNNEL"
        set interface "modem"
        set mode aggressive
        set peertype any
        set dpd on-idle
        set remote-gw 202.152.22.171
        set psksecret ENC teSBjUscbg6Je5
    next
end

# show vpn ipsec phase2-interface
config vpn ipsec phase2-interface
    edit "TUNNEL"
        set phase1name "TUNNEL"
        set src-subnet 192.168.1.0
255.255.255.0
    next
end
```

kedua, untuk melihat status *tunneling* IPSec , hasilnya dapat dilihat di Gambar 7.



Gambar 7 Status Tunnel IPSec

3.1.5 Pengujian waktu *response failover*

Pada pengujian waktu *response failover*, akan diuji berapa lama waktu *response failover*, atau waktu berpindahnya jalur data yang digunakan dari akses utama ke akses backup, dengan kondisi, hanya satu *link* yang berfungsi untuk menyalurkan data dan akses lainnya sebagai *backup* apabila akses utama terputus.

Adapun tahap proses pengujian waktu *response failover* adalah sebagai berikut :

Pertama, mengirimkan paket ICMP dengan menggunakan perintah "PING" pada *command prompt* komputer *user* ke IP *address* aplikasi *server* untuk melihat terkoneksinya suatu jalur ke komputer server seperti yang terlihat pada Gambar 8.

Kedua, untuk melihat jalur akses yang dipakai untuk mengirimkan paket ICMP ke aplikasi *server*, ketikan perintah.

#tracert (ip address server)

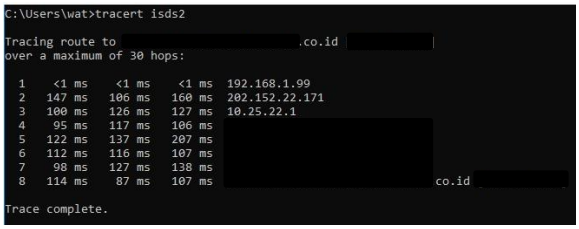
Ketiga, pada saat bersamaan *shutdown* kan jaringan akses *mainlink* seolah-olah jalur *mainlink* dalam keadaan *fault* atau gangguan yang dipakai untuk mengirimkan paket ICMP ke *server* dengan mengetikan perintah.

```
#config system interface
#edit wan
#set status down
```

Maka terlihat seperti yang ada pada Gambar 8.

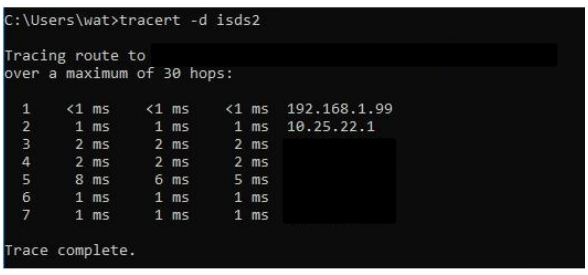
Gambar 8 Jalur Akses Mainlink dalam keadaan mati

Terlihat pada Gambar 9 dibawah ini , jalur pengiriman paket ICMP dari jalur akses *mainlink* yaitu 10.25.22.1 berubah menggunakan jalur 202.152.22.171 atau jalur akses *backup link.*



Gambar 9 Jalur Akses mainlink berubah ke backup link

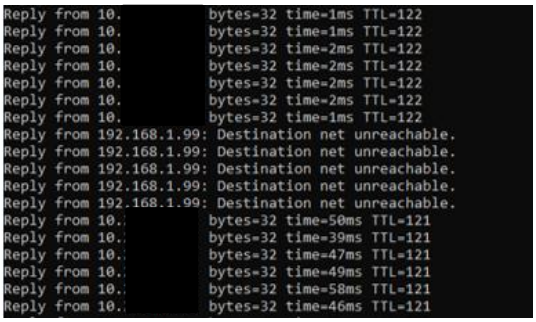
Sedangkan Gambar 10 merupakan jalur pengiriman dari *backup link* ke jalur *mainlink.*



Gambar 10 Jalur Akses backup link berubah ke mainlink

Pada saat bersamaan indikator perintah PING akan terlihat pada *command prompt* sepeti terlihat pada Gambar 11. Terlihat terjadi *paket loss* pada saat terjadi

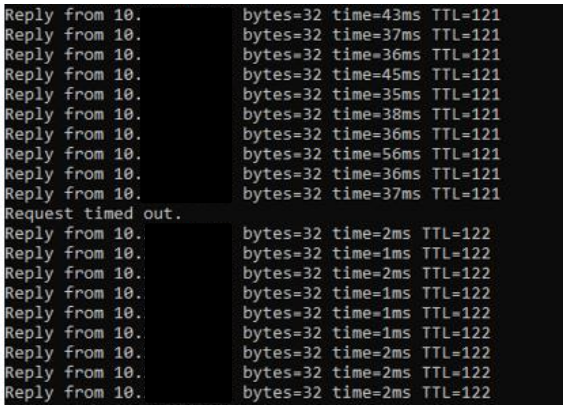
perpindahan jalur otomatis dari akses *mainlink* ke akses *backup link* akibat terjadinya *fault/problem*.



Gambar 11 Perpindahan dari akses mainlink ke akses backup link

Keempat, berapa lama waktu yang dibutuhkan sampai jalur paket ICMP dapat terkirim kembali saat setelah terjadi nya *fault* dicatat.

Kelima, langkah 1 sampai 4 diulangi kembali dengan mengganti jalur akses *backup link* ke *mainlink* karena *mainlink* sudah tidak masalah atau *problem.* Bisa dilihat Gambar 12 merupakan perpindahan ke akses *mainlink*.



Gambar 12 Perpindahan dari akses backup link ke akses mainlink

3.2 Hasil Implementasi

3.2.1 Data Waktu *Response failover*

Dari hasil pengujian waktu *response failover* pada *fortigate* 50E, dapat di peroleh hasil pada Tabel 4.

Tabel 4. Waktu Response Failover

No	Akses yang digunakan	Kondisi	Waktu Response Failover
1	Fiber Optic	DOWN	5 detik
	Modem GSM	UP	
2	Fiber Optic	UP	1 detik
	Modem GSM	DOWN	
	Rata - Rata		3 detik

Pada Tabel 4. diatas terlihat waktu *response failover* yang diambil implementasi secara langsung menggunakan router *fortigate* 50E. Ketika akses *fiber optic* tersebut dimatikan atau di *setting* dalam keadaan mati atau down, maka waktu perpindahan jalur data ke akses *modem* GSM membutuhkan waktu hanya 5 detik. Sedangkan ketika akses *modem* GSM berganti sebagai akses utama dan akses *fiber optic* sebagai *backup*, lalu akses *modem* GSM tersebut dimatikan atau di *setting* dalam keadaan *down*, maka perpindahan jalur data ke akses *fiber optic* membutuhkan waktu 1 detik, atau terjadinya 1 *packet loss*. Sehingga jika di rata-ratakan waktu *response failover* untuk implementasi secara langsung hanya membutuhkan waktu 3 detik.

Perpindahan rata-rata selama 3 detik tersebut sangat bagus. Karena waktu 3 detik jika mengirimkan PING atau mengirimkan paket ICMP, hanya terjadi 1 *packet loss* atau paket yang dibuang.

Kita anggap jumlah paket 100 buah yang akan dikirimkan sehingga :

$$\%Paketloss = \left(\frac{data\ yang\ dikirim - paket\ data\ yang\ diterima}{paket\ data\ yang\ dikirim}\right) \text{ x } 100\%$$

$$\%Paketloss \text{ FO} = \left(\frac{100-99}{100}\right) \text{ x } 100\% = 1\%$$

$$\%Paketloss \text{ GSM} = \left(\frac{100-95}{100}\right) \text{ x } 100\% = 5\%$$

Dari hasil yang didapat sistem *failover* menggunakan router *fortigate* 50E sangat direkomendasikan karena masuk dalam kategori sangat bagus. Serta untuk sistem *failover* ini, mengurangi *downtime* sebesar 80 %.

$$Persentase\ Downtime = \left(\frac{Downtime\ GSM}{Downtime\ FO}\right) x\ 100\%$$

Downtime = 100% - Persentase Downtime

$$Persentase\ Downtime = \frac{1}{5} x\ 100\% = 20\ \%$$

Downtime = 100 % - 20 % = 80 %

3.2.2 Kinerja *Dual Link* pada FTP *server* Variasi Ukuran *File*

3.2.2.1 *Delay*

Dari hasil pengujian *Delay* didapatkan hasil pada Tabel 5.

Tabel 5. Perbandingan Delay pengujian kinerja dual link pada FTP Server variasi ukuran file

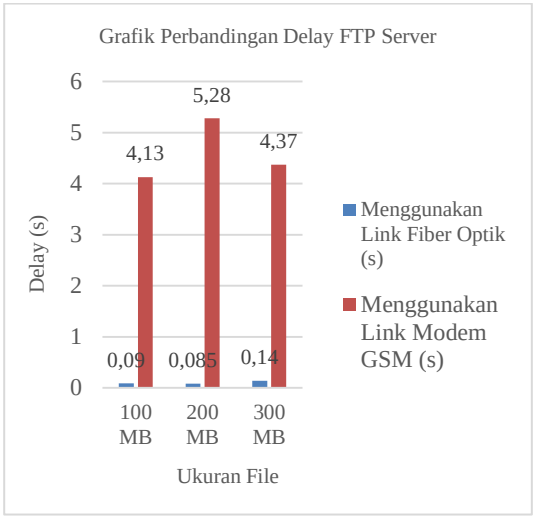
No	Ukuran File (MB)	Menggunakan Link Fiber Optic (s)	Menggunakan Link Modem GSM (s)
1	100 MB	0.09 seconds	4,13 seconds
2	200 MB	0,085 seconds	5,28 seconds
3	300 MB	0.14 seconds	4,37 seconds

$$Rata\ Rata\ Delay = \left(\frac{Total\ Delay}{Total\ Paket\ Yang\ DiTerima}\right)$$

$$Rata\ Rata\ Delay\ FO = \frac{0{,}09 + 0{,}085 + 0{,}14}{3} = 0{,}105$$

$$Rata\ Rata\ Delay\ GSM = \frac{4{,}13 + 5{,}28 + 4{,}37}{3} = 4{,}593$$

Pada Tabel 5 diatas dapat direpresentasikan dalam bentuk grafik pada Gambar 13..



Gambar 13 Grafik Delay pengujian kinerja dual link pada FTP Server

Pada Gambar 13 diatas juga terdapat perbedaan yang sangat signifikan antara penggunaan *link* akses *fiber optic* dan *link* akses *modem* GSM, besar *delay* pada saat pengiriman *file* pada akses *modem* GSM sangat besar dari pada menggunakan *link* akses *fiber optic*. Selisih perbedaannya mencapai rata-rata sebesar 4,5 s. Hal ini dikarenakan akses *modem* GSM mengandalkan sinyal *internet* yang ada pada lokasi tersebut jadi solusi ini memang hanya bersifat temporer.

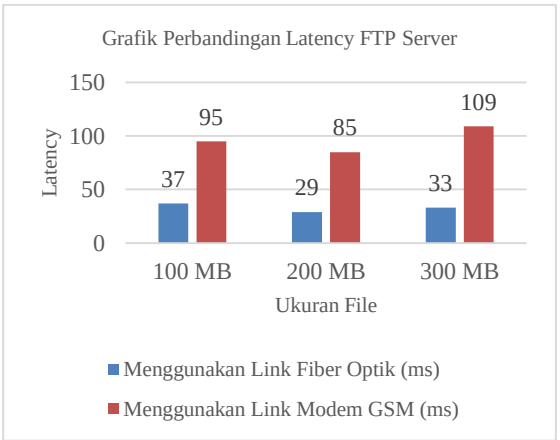
3.2.2.2 *Latency*

Dari Hasil pengujian *latency* didapatkan hasil pada Tabel 6.

Tabel 6. Perbandingan latency pengujian kinerja dual link pada FTP Server variasi ukuran file

No	Ukuran File (MB)	Menggunakan Link Fiber Optic (ms)	Menggunakan Link Modem GSM (ms)
1	100 MB	37 ms	95 ms
2	200 MB	29 ms	85 ms
3	300 MB	33 ms	109 ms

Pada Tabel 5 diatas dapat direpresentasikan dalam bentuk grafik pada Gambar 14.



Gambar 14 Grafik latency pengujian kinerja dual link pada FTP Server

Pada pengujian *Latency*, seperti yang terlihat pada Gambar 14 pengiriman *transfer file* pada akses *modem* GSM memiliki nilai *latency* yang tinggi. Besarnya *latency* dapat mempengaruhi kualitas dari suatu jaringan. *Latency* adalah waktu yang dibutukan data untuk menempuh jarak dari asal ke tujuan lalu kembali ke sumber. Namun ukuran *latency* yang didapat masih tergolong bagus, hal ini berdasarkan standarisasi ITU-T besarnya *latency* dapat diklarifikasikan sebagai berikut pada Tabel 7

Tabel 7. Standarisasi ITU-T Latency

Kategori Latency	Besar Delay	Indeks
Sangat Bagus	< 150 ms	4
Bagus	150 s/d 300 ms	3
Sedang	300 s/d 450 ms	2
Jelek	> 450 ms	1

Jika kita melihat pada standarisasi pada Tabel 6 diatas maka penggunaan akses *fiber optic* saat *traffic* padat atau *full* sangat dianjurkan yaitu rata rata sebesar 33 ms Pada saat *traffic* padat, dengan besar *delay* nilai *latency* FO masih dikategorikan sangat bagus yaitu <150 ms sama juga halnya ketika menggunakan akses *modem* GSM pada saat *traffic* padat. Ketika mengirimkan *file* FTP dengan besar *delay* masih masuk dalam kategori sangat bagus < 150 ms, namun rata-rata nilai *latency* yang dihasilkan lebih besar dari FO yaitu 96,3 ms.

4. Kesimpulan dan saran

Berdasarkan hasil penelitian dan analisa dapat disimpulkan bahwa : Akses FO lebih bagus akses nya karena meliputi delay 0,105 s dan packet loss 1%, namun latency dual link sangat bagus (sesuai pada standar ITU-T). Konfigurasi failover saat implementasi dual link dapat meminimalisir terjadinya downtime sebesar 80%.

Saran

Peneliti baru dapat meminimalisir downtime sebesar 80%, bagi peneliti selanjutnya bisa di tingkatkan hingga menjadi zero downtime.

Dengan adanya link backup ini dapat membantu user mengakses situs kantor, hanya saja link backup ini menggunakan sistem kouta. Sehingga jika kouta habis, perlu dilakukan pengisian secara rutin, untuk peneliti selanjutnya mungkin bisa memberikan kontribusi lagi dengan membuat pemakaian kuota yang lebih efesien maupun efektif.

Daftar Rujukan

[1] M. Elezi and B. Raufi, 2015. “Conception of Virtual Private Networks Using IPsec Suite of Protocols, Comparative Analysis of Distributed Database Queries Using Different IPsec Modes of Encryption,” *Procedia - Soc. Behav. Sci.*, vol. 195, pp. 1938–1948.

[2] S. Hidayatulloh, 2014. “ANALISIS DAN OPTIMALISASI KEAMANAN JARINGAN

MENGGUNAKAN PROTOKOL IPSEC," *J. Inform.*, vol. 1, no. 2.

[3] I. Nurhaida, D. Ramayanti, and I. Nur, 2019. "Performance Comparison based on Open Shortest Path First (OSPF) Routing Algorithm for IP Internet Networks," *Commun. Appl. Electron.*, vol. 7, no. 31, pp. 12–25.

[4] D. Darmawan and T. Imanto, 2017. "Analisa Link Balancing dan Failover 2 Provider Menggunakan Border Gateway Protocol (BGP) Pada Router Cisco 7606s," *J. Nas. Teknol. dan Sist. Inf.*, vol. 3, no. 3, pp. 326–333.

[5] I. Maududy and Z. Ahyadi, 2018. "PERKEMBANGAN TEKNOLOGI JARINGAN GSM DALAM KOMUNIKASI SELULER," vol. 10, no. 2, pp. 73–81.

[6] S. Ariyanti, 2014. "Studi Perencanaan Jaringan Long Term Evolution Area Jabodetabek Studi Kasus PT . Telkomsel Study of Long Term Evolution Network Planning in Jabodetabek , Case Study of PT . Telkomsel,".

[7] D. Prihatmoko, 2016. "PENERAPAN INTERNET OF THINGS (IoT) DALAM PEMBELAJARAN DI," vol. 7, no. 2, pp. 567–574.

[8] S. S. Kardono, 2016. "ARSITEKTUR E-KIOS DI SURABAYA," vol. 5, no. 1.

[9] A. Darojat and I. Nurhaida, 2019. "ANALISA QOS ADMINISTRATIVE DISTANCE," vol. 3, no. 1, pp. 11–21.

[10] I. P. Sari and S. Sukri, 2018. "Analisis Penerapan Metode Antrian Hirarchical Token Bucket untuk Management Bandwidth Jaringan Internet," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 2, no. 2, pp. 522–529.