Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK) DOI: 10.25126/jtiik.2023105236
Vol. 10, No. 1, Februari 2023, hlm. 105-114 p-ISSN: 2355-7699
Akreditasi KEMENRISTEKDIKTI, No. 36/E/KPT/2019 e-ISSN: 2528-6579

IMPLEMENTASI VPN ANTAR CABANG MENGGUNAKAN TEKNOLOGI SDWAN DENGAN METODE LOAD BALANCE (STUDI KASUS: PT. MITRA SOLUSI INFOKOM)

Muhammad Fikri*[1], Muhammad Rifqi[2]

[1,2] Universitas Mercu Buana, Yogyakarta
Email: [1]41517110084@student.mercubuana.ac.id, [2]muhammad.rifqi@mercubuana.ac.id
*Penulis Korespondensi

(Naskah masuk: 30 Juni 2021, diterima untuk diterbitkan: 27 Februari 2023)

Abstrak

Perkembangan komunikasi jaringan yang cepat, proses mengelola dan monitoring jaringan akan lebih kompleks. Pada perusahaan yang memiliki kantor cabang yang letaknya terpisah secara geografis maka diperlukan *Wide Area Network* (WAN) sebagai media komunikasi, pada kasus ini mulai terdapat masalah mulai dari *speed, bandwidth, delay*, dan koneksi jalur komunikasi (redundansi). PT Mitra Solusi Infokom memiliki kantor cabang yang memiliki perbedaan area secara geografis. Permasalahan yang dihadapi adalah komunikasi antara kantor cabang dan kantor pusat hanya memiliki satu jalur yaitu MPLS (*Multiprotocol Label Switching*) dimana tidak adanya redundansi *link* komunikasi antar kantor pusat dan kantor cabang, yang mengakibatkan komunikasi tersebut akan putus apabila *link* MPLS sedang mengalami gangguan. Melihat permasalahan ini, peneliti akan mencoba mengembangkan topologi yang sedang berjalan dengan menggunakan metode penelitian pengembangan PPDIOO (*Prepare, Plan, Design, Implement, Operate, and Optimize*) agar membantu dan memberikan tahapan instalasi, pemantauan, dan pengembangan jaringan. Pengembangan ini menggunakan 2 *link* komunikasi antar *site*, salah satunya menggunakan jaringan internet yang dilapisi IPSec VPN dan pada jaringan utama MPLS juga dilapisi dengan IPSec VPN. Kemudian 2 *link* tersebut akan di *handle* dengan adanya teknologi SD-WAN. Peneliti mengembangkan sistem jaringan agar mempunyai *backup* jalur sebagai sistem redundansi dan load balance. Hasil yang diharapkan adalah 2 link tersebut dapat menghandle traffic secara bersamaan, dan mampu membackup apabila salah satu link down. Hasil dari penelitian ini, link internet mampu menghandle traffic yang telah di load balance dan membackup apabila koneksi MPLS down, sistem failover menggunakan teknologi SDWAN mampu mengurangi downtime sebesar 95%, Sehingga mengurangi tingkat kegagalan jaringan.

Kata kunci: SDWAN, *load balance*, *failover*, FortiGate, *Networking*

IMPLEMENTATION OF INTER-BRANCH VPN USING SDWAN TECHNOLOGY WITH LOAD BALANCE METHOD (CASE STUDY: PT. MITRA SOLUSI INFOKOM)

Abstract

The rapid development of network communication, the process of managing and monitoring the network will be more complex. In companies that have branch offices that are geographically separated, a Wide Area Network (WAN) is needed as a communication, in this case there are problems ranging from speed, bandwidth, delay, and communication line connections (redundancy). PT Mitra Solusi Infokom has branch offices that have different geographical areas. The problem faced is that communication between branch offices and head office only has one path, namely MPLS (Multiprotocol Label Switching) where there is no redundancy of links communication between the head office and branch offices, which causes the communication to break if the link MPLS issues. Seeing this problem, researchers will try to develop an ongoing topology using the PPDIOO development research method (Prepare, Plan, Design, Implement, Operate, and Optimize) to assist and provide stages of network installation, monitoring, and development. This development uses 2 links communication between sites, one of which uses the internet using IPSec VPN and the main MPLS network is also using IPSec VPN. Then the 2 links will be handled with the SD-WAN technology. Researchers develop a network system to have backup paths as a redundancy and load balance system. The expected result is that the 2 links can handle traffic simultaneously, and be able to backup if one link down. The results of this study, link the internet is able to handle traffic that has been load balanced and backed up if the MPLS connection is down, system failover using SD WAN technology is able to reduce downtime by 95%, thereby reducing network failure rates.

Keywords: SDWAN, *load balance*, *failover*, FortiGate, *Networking*

1. PENDAHULUAN

Perkembangan komunikasi jaringan yang cepat, proses mengelola dan monitoring jaringan akan lebih kompleks. Pada perusahaan yang memiliki kantor cabang yang lokasinya berada terpisah secara geografis untuk dapat terhubung harus menggunakan *Wide Area Network* (WAN). Pada komunikasi memiliki kasus mulai dari *speed*, *bandwidth*, *delay*, dan koneksi jalur komunikasi (redundansi).

PT Mitra Solusi Infokom adalah perusahaan yang bergerak dalam bidang *Computer Network* dan *System Integrator*. PT Mitra Solusi Infokom mengkhususkan diri dalam bidang Perencanaan, Desain, Instalasi, Manajemen Proyek dan Pemeliharaan bagi para pelanggannya melalui fitur – fitur maupun kualitas yang lebih baik, respon yang cepat dalam penyelesaian masalah dan meningkatkan pengalaman pengguna. PT Mitra Solusi Infokom mempunyai satu kantor cabang yang berfungsi sebagai gudang persediaan barang. Untuk mendapatkan data/ informasi antara kantor pusat dan kantor cabang, PT Mitra Solusi Infokom menggunakan jaringan MPLS yang dapat menghubungkan jaringan lokal kantor pusat dengan jaringan luar kantor/kantor cabang. Pada kasus ini, komunikasi antara kantor cabang dan Kantor Pusat hanya memiliki satu jalur yaitu MPLS (*Multiprotocol Label Switching*) dimana tidak adanya redundansi jalur komunikasi antar kantor cabang dan Kantor Pusat, yang mengakibatkan komunikasi antara kantor cabang dan Kantor Pusat akan putus apabila jalur MPLS sedang mengalami gangguan, dan tidak adanya toleransi kesalahan dalam jaringan komputer pada PT. Mitra Solusi Infokom.

Melihat permasalahan pada PT. Mitra Solusi Infokom terkait redundansi dan *management bandwidth*, dimana peneliti akan mencoba melakukan desain ulang terhadap topologi yang ada dan *traffic flow* yang sedang berlangsung, dalam desain ulang ini digunakan 1 jalur komunikasi IPSec VPN menggunakan jaringan *internet* yang sudah tersedia Kantor pusat menggunakan Biznet dan Kantor Cabang menggunakan Indihome, pada jaringan utama MPLS dilapisi dengan IPSec VPN agar pertukaran data antara kantor pusat dan kantor cabang akan lebih aman dengan IPSec VPN, kemudian 2 jalur (IPSec VPN) tersebut akan dihandle dengan adanya SD-WAN.

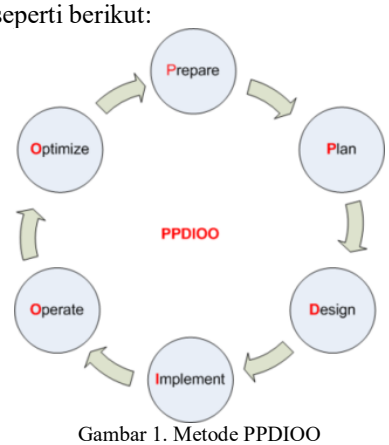
Dengan adanya 2 jalur komunikasi maka, ditambah dengan metode *load balance* menggunakan teknologi SDWAN, dimana *load balance* berguna untuk meningkatkan kualitas jaringan dan membagi beban *traffic* antara jalur 1 dengan jalur lainnya. Dengan adanya hal tersebut maka didapatkan kestabilan komunikasi antara kantor pusat dan kantor cabang, seperti halnya penelitian yang dilakukan oleh (Armanto, 2017) Dengan teknologi *load balancing* maka dapat diperoleh keuntungan seperti menjamin reabilitas servis, availabilitas dan skalabilitas suatu jaringan.

Kemudian diterapkan pula metode *failover* yang bertujuan untuk mengatasi masalah apabila salah satu jalur komunikasi antara kantor pusat dan kantor cabang *down* dan dapat di*backup* otomatis oleh jalur lainnya.

Dengan diterapkannya dua metode tersebut diharapkan dapat meningkatkan kualitas, tingkat redundansi dan *management bandwidth* pada jaringan perusahaan, dikarenakan hanya perangkat perusahaan yang memiliki kemampuan dalam mengatur lalu lintas pertukaran data baik dari metode *load balancing* dan *failover*.

2. METODE PENELITIAN

Metode penelitian merupakan cara untuk mendapatkan suatu tujuan tertentu. Dalam mencapai tujuan tersebut, penelitian ini dilakukan dengan cara mengikuti metode penelitian PPDIOO (Solikin, 2017), seperti berikut:



Gambar 1. Metode PPDIOO

Tahap pertama *prepare*, peneliti mengidentifikasi masalah yang bertujuan mengetahui permasalahan yang ada dalam pertukaran data dan komunikasi jaringan. Teknik pertama yang dilakukan yaitu pengumpulan data, dengan melakukan pengumpulan data dari wawancara kepada *Operation Manager* yang bertanggung jawab atas infrasturuktur jaringan di PT. Mitra Solusi Infokom. Setelah itu studi literatur dilakukan melalui pengumpulan data dan informasi dengan mencari dan memperoleh data-data yang diperlukan baik jurnal penelitian terkait, literatur, dan *website* sebagai referensi. Kemudian, melakukan peninjauan langsung, dengan cara observasi langsung ke lapangan untuk mendapatkatan informasi terkait permasalahan dan keadaan jaringan yang sedang berjalan.

Pada tahapan kedua *plan*, peneliti menganalisa masalah dan melakukan rencana terkait permasalahan yang dihadapi. Dilakukan analisa masalah pada PT. Mitra Solusi Infokom, dimana implementasi pada konektifitas jaringan saat ini hanya 1 yang berperan sebagai jalur utama dan tidak memiliki jalur cadangan yang berfungsi menggantikan jalur utama apabila terdapat kegagalan jaringan (terputus) pada jalur utama. Hal ini menjadi kelemahan atas sistem sebelumnya yang menjadi pertimbangan peneliti

dalam melakukan penelitian terkait sistem yang berjalan saat ini.

Pada tahapan ketiga *design*, peneliti merancang jaringan baru dari analisa masalah yang ditemukan. Peneliti mengembangkan metode komunikasi data antara jaringan kantor pusat dan jaringan kantor cabang yang menggunakan dual jalur sebagai media komunikasi data berskala bisnis enterprise dengan metode *load balance*. Yang bertujuan agar dual jalur yang diimplementasikan dapat aktif keduanya untuk proses pertukaran data antara jaringan kantor pusat dengan kantor cabang. Adapun peneliti melakukan perancangan menggunakan jaringan dari *Fiber Optic* (MPLS) dan jaringan *Internet* yang masing masing sudah dilapisi dengan *site-to-site* IP *Security* VPN menggunakan perangkat fortigate agar kedua *site* dapat terhubung menggunakan dual jalur dan *traffic* dilindungi dengan *site-to-site* IP *Security* VPN, adapun parameter yang di ukur meliputi *packetloss*, *delay*, *latency*, yang diharapkan dapat menekan *downtime* dan mengurangi penggunaan *bandwidth* berlebih pada 1 jalur.

Pada tahapan keempat *implement*, peneliti mengimplementasikan *site-to-site* IP *Security* VPN antara kantor pusat dan kantor cabang menggunakan jalur existing MPLS dan menggunakan *internet*. Pada implementasi ini, dibutuhkan 2 perangkat *Firewall* yakni pada kantor pusat terdapat FortiGate 140D sebagai *dial-up server* dan pada kantor cabang terdapat FortiGate 60F sebagai *dial-up client*.

Tahap kelima *operate*, pada tahapan peneliti melakukan percobaan pada sistem baru yang sudah dikerjakan dan percobaan pada skenario tes yang sudah disiapkan.

Tahap keenam *optimize*, pada tahapan ini peneliti mengoptimalisasi atau menyesuaikan sistem baru dengan lingkungan yang lama guna memperlancar sistem baru dalam beradaptasi dengan perangkat lain agar terintegrasi dengan optimal.

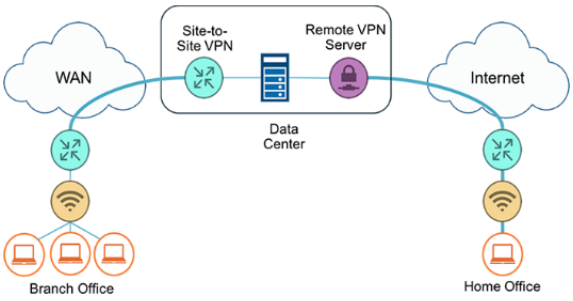
3. LANDASAN TEORI

Penelitian ini mengacu pada penelitian-penelitian sebelumnya yang berkaitan dengan jaringan komunikasi antar cabang, metode *load balancing* dan *fail over*. Adapun perangkat lunak dan perangkat keras yang digunakan dalam penelitian ini, antara lain:

3.1 Site-to-site IP Security VPN

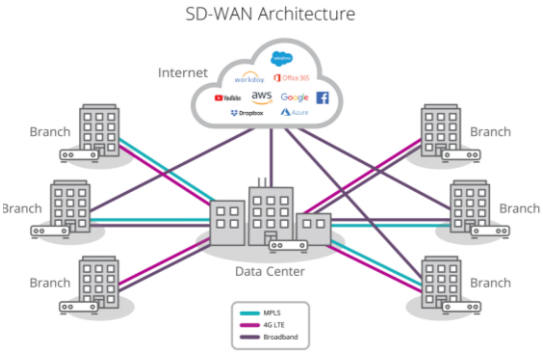
IP Security merupakan protokol yang mengintegrasikan fitur kemanan yang didalamnya meliputi proses autentikasi, integrasi, dan kepastian ke dalam Internet Protocol (IP) IPsec menggunakan enkripsi, mengenkapsulasi paket IP di dalam paket IPsec. De-enkapsulasi terjadi di ujung terowongan, dimana paket IP asli didekripsi dan diteruskan ke tujuan yang diinginkan. (M. Elezi and B. Raufi, 2015)

Pengimplementasian *Site-to-site* IP *Security* VPN dengan memanfaatkan perangkat *dedicated* yang dihubungkan via *Internet*. *Site-to-site* IP *Security* VPN digunakan untuk menghubungkan kantor yang terpisah secara geografis, misal kantor cabang dengan kantor pusat. Komunikasi yang terjadi antara kantor yang terpisah secara georafis berlangsung secara terus menerus.



Gambar 2. Ilustrasi *Site-to-site* IPSec VPN

3.2 Software Defined – WAN (SDWAN)



Gambar 3. Ilustrasi SDWAN

SD-WAN menggunakan perangkat lunak dan memiliki fungsi kontrol terpusat untuk mengarahkan *traffic* lintas WAN secara lebih *smart*. Salah satu kelebihan teknologi SD-WAN adalah kemampuan untuk membangun infrastruktur jaringan yang menggabungkan berbagai jenis sambungan untuk mendapatkan keandalan dan *bandwidth* yang lebih baik dengan biaya terjangkau .

3.3 Load Balance

load-balancing adalah teknik yang digunakan dalam dunia komputer untuk melakukan *traffic steering* atau pengarahan traffic ke destinasi dengan jalur yang sudah ditentutukan. *Load balance* bertujuan agar membagi *traffic* yang lewat dengan tujuan tertentu ke berbagai jalur yang sudah ditetapkan, agar mengurangi pemakaian *bandwidth* dalam satu jalur dan menyeimbangkan setiap koneksi agar konektifitas tetap stabil. (Armanto, 2017)

3.4 *Failover*

Failover adalah teknik yang digunakan dalam dunia *networking* dengan mengimplementasikan beberapa jalur atau jalur komunikasi untuk mencapai suatu *network* tujuan pada kondisi hanya ada satu

jalur yang digunakan dan jalur lainnya akan berfungsi sebagai jalur cadangan. Jalur cadanagan akan menggantikan jalur utama apabila jalur utama gagal atau terputus. (D. Darmawan and T. Imanto, 2017)

3.5 FortiGate

Pada implementasi ini, FortiGate berperan sebagai *Gateway* yang dapat membuat *tunnel* (IP *Security*) *site-to-site* yang menghubungkan jaringan kantor pusat dengan kantor cabang. Selain berperan dalam pengoperasian teknik *failover*, FortiGate berperan pula dalam melakukan *load balancing traffic* dengan penggunaan sistem SDWAN yang sudah ada pada sistem FortiGate.

4. HASIL DAN PEMBAHASAN

4. 1 Pembahasan

Melihat permasalahan tersebut pada PT. Mitra Solusi Infokom akan dilakukan desain ulang terhadap topologi yang ada dan *traffic flow* yang sedang berlangsung. Berupa penambahan 1 jalur sebagai redundansi jalur, serta menggunakan komunikasi IP *Security* VPN *site-to-site* pada 1 jalur baru dan pada jalur MPLS akan dilapisi dengan IP *Security* VPN *site-to-site* juga, agar komunikasi data antara kantor pusat dan kantor cabang akan lebih aman. Kemudian yang mengatur redundansi untuk *load balance* 2 jalur tersebut akan di*handle* dengan adanya SD-WAN (Ali, Manel and Habib, 2018). Dan pula diperbaharui dengan feature *Traffic Steering* yang membantu traffic untuk mengarahkan *apps* atau traffic lain berdasarkan *best path*.

4. 2 Desain Sistem

Pada desain sistem meliputi penggunaan perangkat keras dan perangkat lunak, baik berupa sistem hingga desain topologi jaringan.

4.2.1. Spesifikasi Perangkat Lunak dan Perangkat Keras

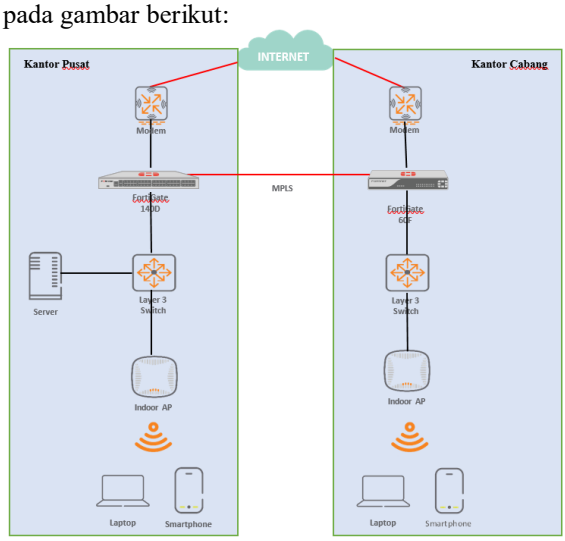
Untuk membangun infrastruktur dari penelitian ini melalui pengamatan dari beberapa bahan yang dikumpulkan, berikut ini adalah spesifikasi dari perangkat lunak dan perangkat keras yang digunakan:

Tabel 1. Spesifikasi Perangkat Keras

Hardware	Spesifikasi	
FortiGate 140D	CPU	Intel(R) Atom(TM) CPU D525 @ 1.80GHz
	RAM	3954 MB
	Main Storage	30533 MB
	LAN Port	38
	Power Source	100–240V AC, 50–60 Hz
	OS	FortiOS v6.2.7
FortiGate 60F	CPU	ARMv8
	RAM	1918 MB
	Main Storage	Not Available
	LAN Port	8
	Power Source	100–240V AC, 50–60 Hz
	OS	FortiOS v7.0.0
Client / User	CPU	Intel(R) Core(TM) i5 CPU M 380 2.53 GHz
	CPU	4096 MB
	OS	Windows 10 64bit
Server	CPU	4 CPUs x Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz
	RAM	95.96 GB
	Main Storage	7.62 TB
	OS	Linux esxi 6.5

4.2.2. Desain Topologi Jaringan *Existing*

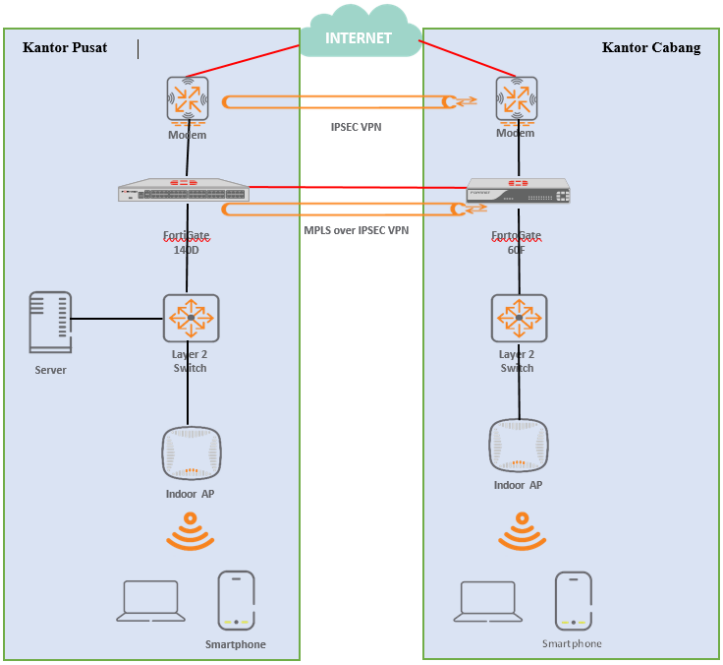
Antara kantor pusat dan kantor cabang memiliki router dan 1 jalur koneksi *internet*. Kantor pusat dan cabang dapat terhubung melalui jalur MPLS. Di kantor cabang *client/user* hanya terhubung ke jaringan melalui *wifi* saja tidak ada yang menggunakan kabel. Topologi tersebut ditunjukkan pada gambar berikut:



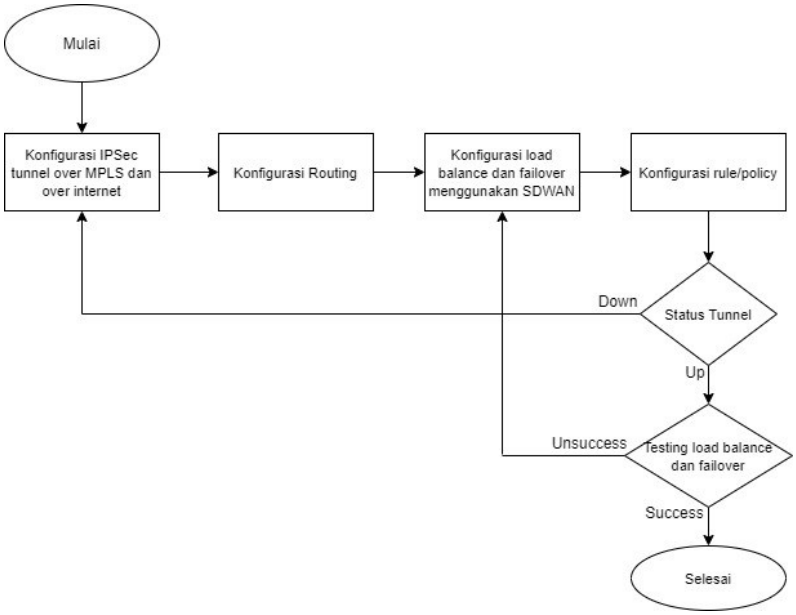
Gambar 4. Topologi *Existing*

4.2.3. Desain Topologi Jaringan Usulan

Berdasarkan pada analisis desain topologi seperti yang diajukan sebagai solusi. Pada desain topologi baru menambahkan 1 jalur untuk komunikasi antar *site* dengan menggunakan teknologi IP *Security site-to-site* menggunakan jalur *internet*, sebagai *back up* dari jalur MPLS yang sudah ada. Nanti nya 2 jalur (MPLS & *internet*) yang sudah dilapisi VPN, akan diatur menggunakan teknologi SDWAN dengan *load balancing* untuk mengatur *traffic* akses antara kantor pusat dan kantor cabang, maupun *traffic internet*, dan atau melakukan jalur *failover* apabila terdapat jalur yang putus.



Gambar 5. Topologi Usulan



Gambar 6. Diagram Alur Implementasi

4. 3 Perancangan Sistem

Pada perancangan sistem, peneliti menambahkan jalur antara kantor pusat dengan kantor cabang menggunakan jalur *internet* yang dilapisi *site-to-site* IP *Security* VPN kemudian jalur existing (MPLS) akan dilapisi juga dengan *site-to-site* IP *Security* VPN, agar mempermudah dalam melakukan *load balancing* ataupun *failover*.

Pada diagram alur implementasi diatas, perancangan sistem ini dimulai dengan mengkonfigurasi *site-to-site* IP *Security* VPN menggunakan jalur MPLS dan *Internet* pada FortiGate kantor pusat dan FortiGate kantor cabang. Kemudian dilanjutkan dengan mengkonfigurasi *routing* pada kedua perangkat, agar *traffic client* mengetahui destinasti yang dituju.

```
# show vpn ipsec phase1-interface
config vpn ipsec phase1-interface
    edit "IPSEC_MPLS"
        set interface "wan1"
        set mode aggressive
        set peertype any
        set net-device disable
        set proposal aes128-sha256 aes256-sha256
        set remote-gw [redacted]
    next
    edit "IPSEC_INET"
        set type ddns
        set interface "wan2"
        set mode aggressive
        set peertype any
        set net-device disable
        set proposal aes128-sha256 aes256-sha256
        set remotegw-ddns [redacted]
    next
end
```

Gambar 7. Konfigurasi *site-to-site* IP *Security* VPN

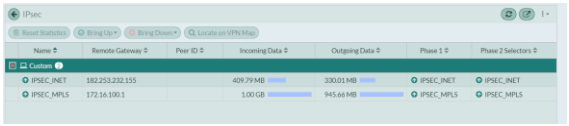
Kemudian dilanjutkan dengan mengkonfigurasi *load balancing* dan juga *failover* menggunakan teknologi SDWAN yang terdapat pada OS FortiGate.

```
# show system sdwan
config system sdwan
    set status enable
    set load-balance-mode measured-volume-based
    config zone
        edit "virtual-wan-link"
        next
    end
    config members
        edit 1
            set interface "IPSEC_MPLS"
            set source 10.
            set volume-ratio 255
        next
        edit 2
            set interface "IPSEC_INET"
            set source 10.
        next
        edit 3
            set interface "wan2"
        next
    end
    config health-check
        edit "Health Check Server"
            set server "192.
            set members 2 1
            config sla
                edit 1
                next
            end
        next
        edit "Health Check Google"
            set server "8.8.8.8"
            set members 1 3
            config sla
                edit 1
                next
            end
        next
    end
```

Gambar 8. Konfigurasi SDWAN

Setelah itu masuk ke tahap konfigurasi *rule* atau *policy* yang bertujuan agar hanya *traffic* dengan sumber IP atau destinasi IP tertentu yang diperbolehkan lewat.

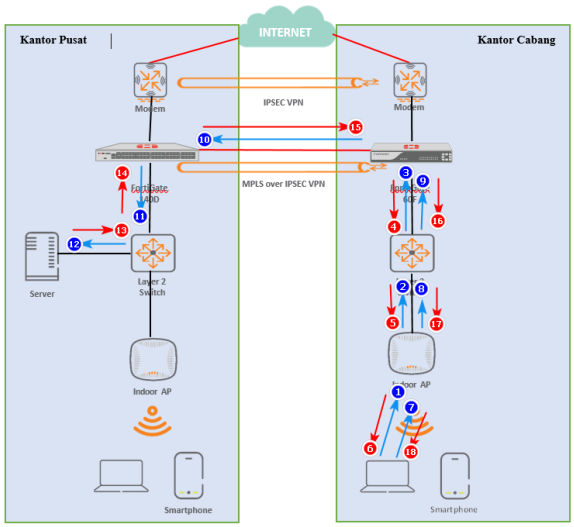
Kemudian melakukan pengecekan status *tunnel* IP *Security site-to-site*. Apabila status *tunnel down*, maka peneliti meninjau kembali konfigurasi pada kedua perangkat baik dari segi parameter *pre-sharedkey*, *algorithm,* serta parameter enkripsi yang dipakai pada ipsec ini.



Gambar 9. Status *Tunnel*

Apabila status *tunnel up*, maka berlanjut ketahap pengetesan metode *load balance* dan *failover* dengan cara *user client* kantor cabang melakukan akses ke *server* yang ada pada kantor pusat, kemudian melakukan skenario agar *traffic* ter *load balance* dan *traffic* berpindah jalur (*failover*) apabila salah satu jalur terputus. Jika testing kurang optimal atau gagal, maka peneliti melakukan *troubleshooting* dan penyesuaian pada konfigurasi SDWAN. Jika sudah sukses, maka implementasi sudah selesai dan masuk ke tahap *monitoring*.

4. 4 Alur Proses *Traffic*



Gambar 10. Alur Proses *Traffic*

Pada gambar diatas diuraikan rangkaian alur proses *traffic* pada sistem infrastruktur dengan *load balance* dan *failover* yang dibuat. Berikut ini alur kerja sistem tersebut tersebut:

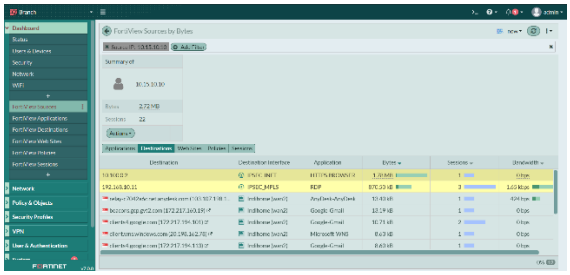
1. User cabang konek ke jaringan/wifi kantor cabang.
2. User mendapatkan IP DHCP, apabila tidak mendapatkan IP, maka user melakukan konek ulang pada media wifi atau kabel.
3. User melakukan akses ke server yang terdapat pada kantor pusat.
4. *Firewall* kantor cabang, melakukan pengecekan routing dan rule yang sudah dikonfigurasi, apabila di *block*, *user* diharuskan untuk memastikan IP yang digunakan dan IP destinasti yang dituju, serta memastikan *service/protocol* yang dipakai sesuai dengan ketentuan.
5. *Firewall* kantor cabang menentukan jalur *traffic* menggunakan teknologi SDWAN berdasarkan kriteria yang telah dikonfigurasi, dan pada tahap ini juga *failover* akan berjalan apabila terdapat jalur yang putus.
6. *Firewall* kantor cabang meneruskan paket/*traffic* ke *Firewall* kantor pusat via IP *Security*.
7. *Firewall* kantor pusat menerima paket dan melakukan pengecekan *rule/policy*. Apabila di *block* maka *user* cabang diharuskan untuk memastikan IP yang digunakan dan IP destinasti yang dituju , serta memastikan *service/protocol* yang dipakai sesuai dengan ketentuan.
8. Jika berhasil dalam pengecekan *rule/policy* maka paket atau *traffic* akan dilanjutkan ke server yang dituju.

4. 5 Pengujian

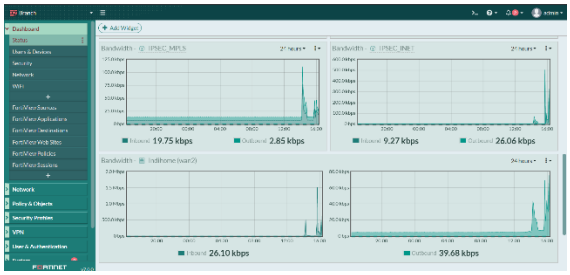
Pengujian pada sistem jaringan yang telah didesain dan dibangun, memiliki beberapa tahap pengujian diantaranya sebagai berikut:

4.5.1. Pengujian *Load Balancing*

Pada tahap pengujian *load balancing* peneliti melakukan pengujian yang dilakukan dari *user client* yang berada di kantor cabang untuk melakukan komunikasi ke *server* yang ada di kantor pusat.



Gambar 11. *Log traffic load balance*

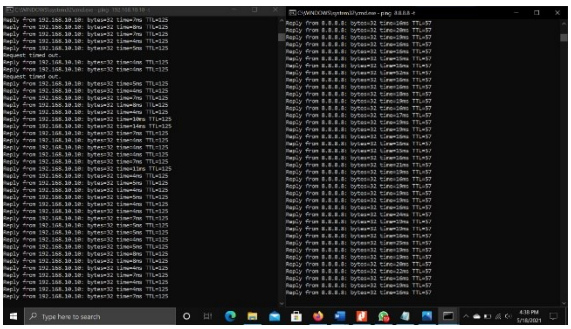


Gambar 12. *Bandwidth monitoring*

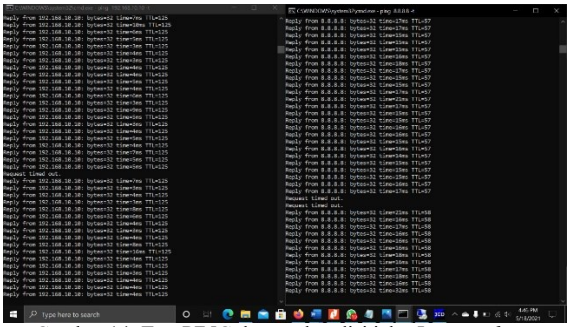
Berdasarkan hasil pengujian pada gambar 11 dan 12, terdapat bahwa kedua penerapan metode *load balance* dapat digunakan untuk komunikasi antara kantor pusat dan kantor cabang dengan melihat pada *bandwidth monitoring* yang menjelaskan bahwa *traffic* berjalan pada kedua jalur, tidak menjadikan salah satu jalur *active*/*passive*.

4.5.2. Pengujian *Failover*

Pengujian ini dilakukan dari *user client* yang berada di kantor cabang untuk melakukan komunikasi ke *server* yang ada di kantor pusat. Kemudian dihadapi dengan adanya koneksi terputus baik *tunnel* MPLS ataupun *tunnel internet.*



Gambar 13. Test PING dengan kondisi jalur MPLS *down*



Gambar 14. Test PING dengan kondisi jalur Internet *down*

Berdasarkan hasil pengujian pada Gambar 13 dan 14 didapati hasil, *traffic* dapat dihandle oleh *backup* jalur lain apabila terdapat salah satu jalur putus/*down*. Dan dari pengujian ini didapati, apabila *tunnel* internet yang *down*, maka *client* kantor cabang masih bisa menggunakan internet melalui internet kantor pusat.

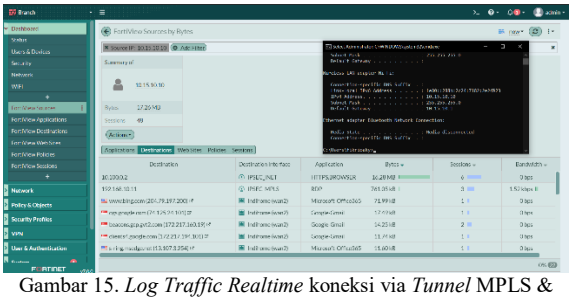
Dari hasil sistem *failover* menggunakan teknologi SDWAN, mampu mengurangi *downtime* sebesar 95%.

$$Presentase\ Downtime = \left(\frac{Packet\ ICMP\ yang\ berhasil\ diterima}{Jumlah\ packet\ ICMP}\right) \times 100\%$$

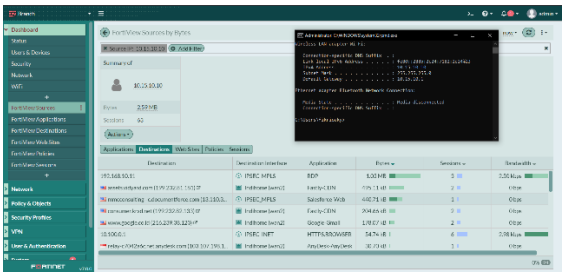
$$Presentase\ Downtime = \left(\frac{38}{40}\right) \times 100\% = 95\%$$

4.5.3. Pengujian *Traffic Steering*

Pengujian ini dilakukan dari *user client* yang berada di kantor cabang untuk melakukan komunikasi ke *server* yang ada di kantor pusat. Dengan kondisi *traffic* destinasi IP atau aplikasi yang dituju, untuk melakukan komunikasi menggunakan jalur yang sudah ditentukan.



Gambar 15. *Log Traffic Realtime* koneksi via *Tunnel* MPLS & *Tunnel Internet*



Gambar 16. *Log Traffic Realtime* koneksi ke *sales force* via Internet kantor pusat (*tunnel MPLS)*

Berdasarkan hasil pengujian pada gambar 15 dan 16, mendapatkan hasil bahwa dengan teknologi

SDWAN ini, dapat digunakan untuk melakukan *traffic steering*, dimana pada gambar tersebut menjelaskan, *traffic* dengan tujuan *server prod (192.168.x.x)* diharuskan melalui *tunnel* MPLS, dan *traffic* dengan tujuan *server lab (10.100.x.x)* diharuskan melalui *tunnel internet*. Dan juga pada gambar 16, menjelasakan apabila *client* melakukan akses ke *cloud website sales force* diharuskan menggunakan internet kantor pusat via *tunnel* MPLS.

4.5.4. Hasil Pengujian

Berdasarkan hasil pengujian dari sub bab sebelumnya, maka didapatkan perbandingan antara sebelum diimplementasikannya *site-to-site* IP *Security* VPN dengan teknologi SDWAN dan setelah dilakukan implementasi infrastruktur tersebut.

Tabel 2. Perbandingan Sebelum dan Sesudah

Parameter	Sebelum Implementasi VPN dengan SDWAN	Sesudah Implementasi VPN dengan SDWAN
Menghubungkan Antar *Site*	✓	✓
Load Balance	×	✓
Traffic Steering	×	✓
Redundansi Jalur	×	✓
Keamanan Pertukaran Data	×	✓
Memiliki *Bandwidth* Tambahan	×	✓

5. KESIMPULAN

Berdasarkan hasil penelitian ini dapat disimpulkan, jalur komunikasi MPLS dan Internet yang digunakan untuk komunikasi antara kantor pusat dan kantor cabang dapat dilapisi oleh VPN IP *Security* sehingga dapat dikategorikan koneksi MPLS dan Internet dibuat khusus sebagai jalur *traffic* antara kantor pusat dengan kantor cabang.

Kedua jalur VPN IP *Security* (MPLS dan interet) berhasil diimplementasikan dengan metode *load balance* dan *failover* menggunakan teknologi SDWAN, berdasarkan kriteria dan batas yang ditentukan.

Dengan diimplementasikannya metode *load balance,* didapati hasil beban *traffic* antara kantor pusat dan kantor cabang berhasil dibagi dengan menggunakan kedua jalur VPN IP *Security* berdasarkan *rule* dan *threshold* yang ditentukan didalam teknologi SDWAN, sehingga dapat meningkatkan kualitas jaringan dan mengurangi kemacetan lalu lintas data dari *bandwidth* setiap jalur. Dapat diketahui dari *bandwidth monitoring* dan *traceroute,* bahwa metode *load balance* berhasil berjalan pada system yang sudah diimplementasikan.

Begitu pula juga diimplementasikannya metode *failover* didapati hasil, bahwasanya *traffic* antara kantor pusat dan kantor cabang dapat berpindah otomatis apabila terdapat salah satu jalur *down*. Dengan hasil pengujian yang didapat dalam scenario *failover*, sistem dan metode *failover* berhasil berjalan dengan menunjukkan maksimal RTO (*Request Time Out*) 2x dan mampu mengurangi *downtime* sebesar 95% dari pengujian yang telah dilakukan. Kedua jalur mampu meng*handle* beban *traffic* apabila salah satu diantaranya *down*.

DAFTAR PUSTAKA

ALI, E. K., MANEL, M., & HABIB, Y. 2018. An efficient MPLS-based source routing scheme in software-defined wide area networks (SD-WAN). *Proceedings of IEEE/ACS International Conference on Computer Systems and Applications, AICCSA*, *2017-Octob*, 1205–1211. https://doi.org/10.1109/AICCSA.2017.165

EKO SUMARNO, HANUGRAH PROBO HASMORO. 2011. Implementasi metode load balancing dengan dua jalur (. *Implementasi Metode Load Balancing Dengan Dua* Jalur, 28–34.

HARYAMTO, M. D., & RIADI, I. 2014. Analisa Dan Optimalisasi Jaringan Menggunakan Teknik Load Balancing. *Jurnal Sarjana Teknik Informatika*, *2*, 1370–1378. http://www.mendeley.com/research/analisa-dan-optimalisasi-jaringan-menggunakan-teknik-load-balancing

HUDDINIAH, E. R., SAFITRI, E. M., PRIYAMBADA, S. A., NASRULLAH, M., & ANGRESTI, N. D. 2018. Optimasi Rute Untuk Software Defined Networking-Wide Area Network (SDN-WAN) Dengan Openflow Protocol. *Informatika Mulawarman : Jurnal Ilmiah Ilmu Komputer*, *13*(1), 7. https://doi.org/10.30872/jim.v13i1.1006

ISKANDAR, I., & HIDAYAT, A. 2015. Analisa Quality of Service (QoS) Jaringan Internet Kampus (Studi Kasus: UIN Suska Riau). *Jurnal CoreIT*, *1*(2), 67–76.

KHAZAAL, H. F., AL-ABASSI, H. K., AL-SADI, A. M., & AL-SHERBAZ, A. 2020. Evaluating healthcare system based sd-wan backbone. *International Journal of Advanced Science and Technology*, *29*(1), 671–680.

MUSTOFA, A., & RAMAYANTI, D. 2020. Implementasi Load Balancing dan Failover to Device Mikrotik Router Menggunakan Metode NTH (Studi Kasus: PT.GO-JEK Indonesia). *Jurnal Teknologi Informasi Dan Ilmu Komputer*, *7*(1), 139. https://doi.org/10.25126/jtiik.2020701638

PARASIAN SILITONGA1, I. S. M. 2014. Analisis QoS (Quality of Service) Jaringan Kampus

dengan Menggunakan Microtic Routerboard (Studi Kasus : Fakultas Ilmu Komputer Unika Santo Thomas S.U). *Jurnal TIMES*, *III*(2), 19–24.

RAHMAD DANI, F. S. 2017. *khazanah informatika BALANCING DAN FAILOVER MENGGUNAKAN*. *3*(1), 43–50.

SISTEM, R., AGUSTINA, W., & RIFQI, M. 2021. *JURNAL RESTI Implementasi Dual* Jalur *IPVPN dan GSM Berbasis IPSec pada Fortigate*. *1*(10), 228–236.

SYAIFUDDIN, A., YUNUS, M., & SUNDARI, R. 2005. Perbandingan Metode Simple Queues dan Queues Tree untuk optimasi manajemen Bandwidth jaringan komputer di STIMIK PPKIA Pradnya Paramita Malang. *JURNAL TEKNOLOGI INFORMASI: Teori, Konsep, Dan Implementasi*, *4*(2), 60–74. http://ejurnal.stimata.ac.id/index.php/TI/article/view/106/147

TEKNIOT. (n.d.). *Apa itu Software-Defined WAN (SD-WAN)?* https://www.teknoiot.com/teknologi-sd-wan/

WULANDARI, R. 2016. Analisis Qos (Quality Of Service) Pada Jaringan Internet (Studi Kasus : Upt Loka Uji Teknik Penambangan Jampang Kulon – Lipi). *J. Tek. Inform. Dan Sist. Inf*, *2*, *no*. https://doi.org/10.28932/jutisi.v2i2.454

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.

D. DARMAWAN and T. IMANTO, 2017. "Analisa Jalur 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.

SOLIKIN, I. 2017. Penerapan Metode PPDIOO Dalam Pengembangan LAN Dan WLAN', *Teknomatika*, 07(01), pp. 65–73. Available at: http://ojs.palcomtech.ac.id.

HUDDINIAH, E. R., dkk. 2018. Optimasi Rute Untuk Software Defined Networking-Wide Area Network (SDN-WAN) Dengan Openflow Protocol. Informatika Mulawarman: Jurnal Ilmiah Ilmu Komputer, 13(1), p. 7. doi: 10.30872/jim.v13i1.1006.