Jurnal Indonesia : Manajemen Informatika dan Komunikasi
www.journal.amikindonesia.ac.id/jimik/ Vol 4 No 3, September (2023)
E-ISSN: 2723-7079, P-ISSN: 2776-8074

IMPLEMENTASI *FAILOVER* VPN KANTOR PUSAT DAN CABANG MENGGUNAKAN TEKNOLOGI SDWAN DENGAN STRATEGI *BEST QUALITY*

Sahrul Hidayat [1*], Yuma Akbar [2]

[1*,2] Program Studi Teknik Informatika, Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika, Kota Jakarta Timur, Daerah Khusus Ibukota Jakarta, Indonesia.

Corresponding Email: sahrulhd21@gmail.com [1*]

Histori Artikel:
Dikirim 20 Juli 2023; *Diterima dalam bentuk revisi* 2 Agustus 2023; *Diterima* 15 Agustus 2023; *Diterbitkan* 10 September 2023. Semua hak dilindungi oleh Lembaga Penelitian dan Pengabdian Masyarakat (LPPM) STMIK Indonesia Banda Aceh.

Abstrak

Jaringan VPN kantor pusat dan cabang digunakan untuk menghubungkan kantor pusat dengan cabang-cabang yang tersebar di berbagai wilayah yang terpisah secara geografis. Namun, keamanan dan ketersediaan jaringan dapat terpengaruh oleh berbagai faktor, seperti kegagalan koneksi internet, penggunaan bandwidth yang berlebihan, dan gangguan lainnya. Untuk Mengatasi hal tersebut peneliti memberikan solusi untuk melakukan Implementasi Failover VPN kantor pusat dan cabang menggunakan teknologi SDWAN. Dengan SDWAN, perusahaan dapat memilih jalur koneksi yang lebih andal dan memiliki kecepatan yang lebih tinggi, sehingga dapat mengoptimalkan penggunaan bandwidth dan memperbaiki ketersediaan jaringan. Dalam penelitian ini, peneliti mencoba mensimulasikan Failover VPN Kantor pusat dan cabang Menggunakan Teknologi SDWAN Dengan Strategi Best Quality pada PNETLab. Pada penelitian ini menggunakan 2 koneksi, yaitu koneksi internet dan MPLS. MPLS sebagai Primary dan internet berperan sebagai Backup. Pengujian dilakukan dengan menggunakan tiga skema, skema 1 saat dalam kondisi normal, skema 2 saat packet loss pada link MPLS meningkat kemudian traffic diambil alih oleh koneksi internet, dan skema 3 pada saat packetloss pada link MPLS kembali normal.

Kata Kunci: SDWAN; Failover; VPN; MPLS.

Abstract

Head office and branch VPN networks are used to connect the head office with branches spread across geographically separated areas. However, network security and availability can be affected by various factors, such as internet connection failures, excessive bandwidth usage, and other disturbances. To overcome this, researchers provide a solution for implementing Failover VPN at the head office and branches using SDWAN technology. With SDWAN, companies can choose a connection path that is more reliable and has a higher speed, thereby optimizing bandwidth usage and improving network availability. In this study, researchers tried to simulate Headquarters and Branch Office VPN Failover Using SDWAN Technology with the Best Quality Strategy at PNETLab. This study uses 2 connections, namely internet connection and MPLS. MPLS is Primary and the internet as Backup. The test is carried out using three schemes, scheme 1 when in normal conditions, scheme 2 when the packet loss on the MPLS link increases then traffic is taken over by the internet connection, and scheme 3 when the packet loss on the MPLS link returns to normal.

Keyword: SDWAN; Failover; VPN; MPLS.

1. Pendahuluan

Pada era digital seperti saat ini, kebutuhan akan konektivitas jaringan yang cepat dan terpercaya sangatlah penting untuk menjamin kelancaran operasional suatu perusahaan. Salah satu bentuk konektivitas jaringan yang digunakan oleh perusahaan adalah VPN (*Virtual Private Network*) Hub *and* Spoke, yang digunakan untuk menghubungkan antara kantor pusat (hub) dan cabang (spoke) dalam suatu jaringan. Namun, seringkali masalah terjadi pada koneksi jaringan yang menyebabkan jaringan menjadi tidak stabil dan terputus. Berbagai upaya dilakukan untuk mengurangi *downtime* [1][2]. namun proses *failover* yang diteliti sebelumnya masih menggunakan Teknik traditional *network* [3][4].

Pengunaan SDN sebelumnya belum banyak membahas tentang *Failover* VPN seperti pada penelitian [5][6], dan pada penelitian Saputra & Dalimunthe (2021) [4] membahas terkait masalah keamanan seperti pencegahan DDoS pada data plane SDN [7]. Pada penelitian ini menggunakan perangkat *Firewall* sebagai sdwan edge sehingga keamanan pertukaran data terjamin. *Firewall* dalam jaringan komputer adalah sebuah sistem keamanan yang berfungsi untuk melindungi jaringan dan komputer dari ancaman yang datang dari luar [8]. Pada penelitian Fathsyah, Hadi & Salamah (2021) dan *Failover* menggunakan Netwatch, kondisi *downtime* menyebabkan *client* terganggu untuk mengakses internet ataupun server [9][10], sehingga implementasi *failover* sangat penting, *Failover* adalah salah satu metode pada jaringan untuk menghindari *down time* koneksi [11] .

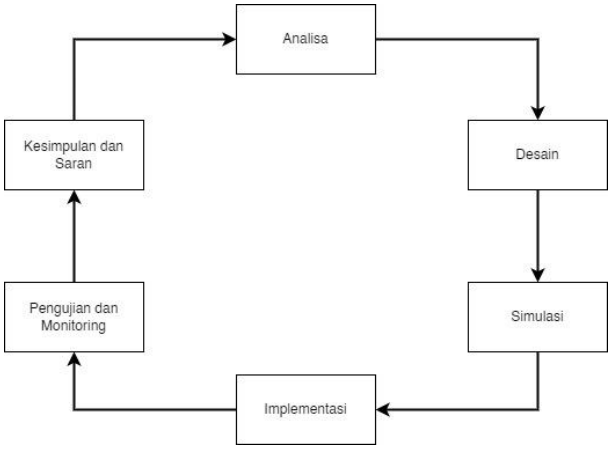
Pada penelitian Mustofa & Ramayanti (2020) membahas tentang SDN Viptela yang mengoptimalkan jaringan WAN dan konfigurasi jadi lebih mudah [12], Citraweb.com membahas tentang *failover* vpn menggunakan mikrotik dengan L2TP VPN untuk enkripsi datanya [10]. Pada penelitian Wahyudi (2022) dan Rifandy & Topiq (2023) proses *failover* dan load balance menggunakan metode NTH agar distribusi *traffic* terbagi secara merata [13][14]. Dengan Menggunakan VPN dan IP Private proses pertukaran data pada jaringan akan aman [15]. SD-WAN adalah bentuk aplikasi spesifik dari teknologi software-defined *networking* SDN yang diaplikasikan pada koneksi WAN wide area network [16]. Teknologi SDWAN (*Software Defined Wide Area Network*) adalah solusi yang dapat digunakan untuk memecahkan masalah tersebut, dengan mengatur trafik jaringan menggunakan beberapa koneksi internet yang tersedia sehingga jika salah satu koneksi gagal, trafik akan dialihkan secara otomatis ke koneksi lainnya.

Dengan SDWAN proses pertukaran data antara kantor pusat dan cabang sudah terjamin enkripsi datanya karena menggunakan teknologi IPSec. IPSec menambahkan enkripsi dan autentikasi untuk membuat protokol lebih aman. Misalnya, IPSec mengacak data di sumbernya dan menguraikannya di tujuannya [17]. Strategi Best Quality memilih link yang memiliki kualitas paling baik dengan membandingkan parameter packetloss, jitter dan latency pada link tersebut, proses Analisa parameter dapat melihat kualitas packetloss, jitter dan latency tidak seperti pada penelitian Kuswanto & Rahman (2019) [18] dan Arfan, Zainuddin, & Rahmania (2019) [19], dan penelitian Wartono & Pramono (2019) [20]. Penelitian ini bertujuan menganalisa *failover* VPN kantor pusat dan cabang dengan menggunakan teknologi sdwan dan strategi best *quality*, untuk memberikan kontribusi pada ilmu pengetahuan, yaitu memberikan informasi mengenai kinerja atau performa teknologi tersebut.

2. Metode Penelitian

Metode yang peneliti gunakan dalam pengerjaan skripsi ini adalah dengan metode NDLC (*Network Development Life Cycle*). Secara umum dalam teori NDLC terdapat beberapa tahapan berikut adalah penjelasan dari masing-masing tahapannya:

Jurnal Indonesia : Manajemen Informatika dan Komunikasi, Volume 4 No 3, September (2023), pp. 1598-1608
DOI : https://doi.org/10.35870/jimik.v4i3.386



Gambar 1. Metode Penelitian

Berikut penjelasan dari gambar diatas:

1) Analisis: Tahap ini melibatkan analisis permasalahan yang muncul, yaitu implementasi *failover* VPN Kantor Pusat dan Cabang menggunakan teknologi SDWAN dengan strategi Best *Quality*, serta cara meningkatkan performa dan ketersediaan jaringan. Solusi dan tujuan penelitian diidentifikasi dalam tahap ini.
2) Desain: Pada tahap ini, peneliti akan merancang desain topologi jaringan berdasarkan informasi yang telah dikumpulkan sebelumnya. Desain ini mencerminkan kebutuhan yang ada dan memberikan gambaran lengkap tentang jaringan yang akan dibangun.
3) Simulasi: Tahap ini melibatkan pembuatan simulasi sistem dalam lingkungan virtual menggunakan Pnetlabs sesuai dengan rancangan jaringan yang telah dibuat sebelumnya. Simulasi ini memungkinkan peneliti untuk menguji sistem sebelum dilakukan implementasi fisik.
4) Implementasi: Pada tahap ini, peneliti akan melaksanakan implementasi berdasarkan analisis kebutuhan dan desain yang telah dibuat. Implementasi ini mencakup konfigurasi *failover* VPN Kantor Pusat dan Cabang menggunakan teknologi SDWAN, serta pengujian unit sistem yang telah dibangun.
5) Pengujian dan Monitoring: Setelah implementasi selesai, tahap ini melibatkan pengujian sistem untuk membuktikan hasil implementasi. Selain itu, dilakukan monitoring untuk mendeteksi masalah yang mungkin terjadi pada sistem dan digunakan sebagai acuan dalam pemecahan masalah di masa depan.
6) Kesimpulan dan Saran: Pada tahap akhir, setelah pengujian dan monitoring selesai dilakukan, dilakukan penarikan kesimpulan dari penelitian yang telah dilakukan. Selain itu, diberikan saran untuk penelitian selanjutnya berdasarkan temuan dan pengalaman yang diperoleh dari penelitian ini.

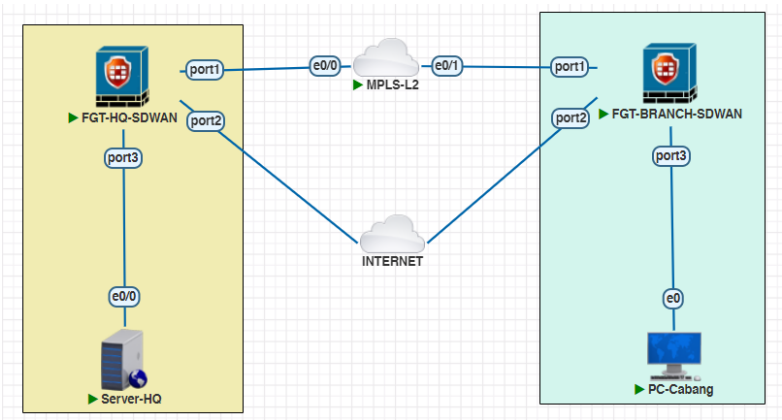
3. Hasil dan Pembahasan

3.1. Topologi Jaringan

Topologi jaringan yang akan digunakan dalam penelitian ini menggunakan lingkungan virtual Pnetlabs dan terdiri dari 2 *Firewall* Fortigate dan 2 host. Setiap *Firewall* Fortigate terhubung ke 2 koneksi WAN, dengan link pertama terhubung ke MPLS L2 dan link kedua terhubung ke internet. Dalam simulasi, router yang akan digunakan adalah *FortiGate*, sedangkan untuk clientnya menggunakan Cisco IOL L3 untuk server kantor pusat (hq) dan linux slax untuk komputer cabang.

Jurnal Indonesia : Manajemen Informatika dan Komunikasi, Volume 4 No 3, September (2023), pp. 1598-1608
DOI : https://doi.org/10.35870/jimik.v4i3.386

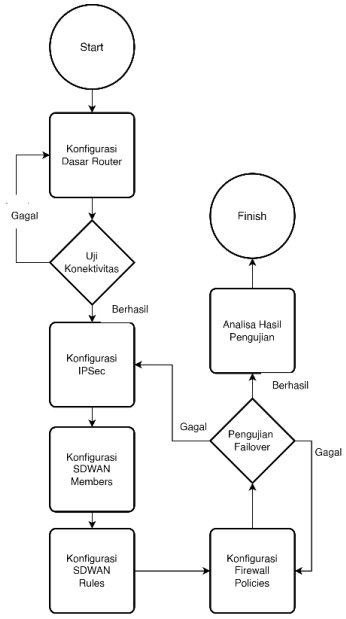
Jurnal Indonesia : Manajemen Informatika dan Komunikasi
www.journal.amikindonesia.ac.id/jimik/ Vol 4 No 3, September (2023)
E-ISSN: 2723-7079, P-ISSN: 2776-8074



Gambar 2. Topologi Jaringan Penelitian

3.2. Alur Implementasi

Untuk memvisualisasikan implementasi rancangan penelitian ini, berikut adalah diagram alur implementasi yang menggambarkan tahapan-tahapan yang dilakukan.



Gambar 3. Diagram Alur Implementasi

Berikut ini adalah penjelasan detail dari masing-masing tahapan implementasi yang terdapat dalam diagram tersebut:

1) Tahap pertama melibatkan konfigurasi dasar jaringan pada kedua router yang terlibat dalam topologi, terdiri dari konfigurasi nama host, Alamat IP, dan *routing*.
2) Uji Konektivitas. Setelah konfigurasi jaringan selesai, dilakukan uji konektivitas dari router ke koneksi WAN untuk memastikan bahwa semua antarmuka sudah terhubung dengan benar. Uji ping dilakukan antara router dengan koneksi WAN yang terlibat dalam topologi.
3) Konfigurasi IPSec. Pada tahap ini, dilakukan konfigurasi IPSec antara router kantor pusat dan router kantor cabang. Konfigurasi ini akan memungkinkan router dapat berkomunikasi secara aman dan terenkripsi.
4) Konfigurasi Anggota SDWAN. Setelah konfigurasi IPsec selesai, berikutnya adalah memasukkan IPsec ke dalam anggota SDWAN.

Jurnal Indonesia : Manajemen Informatika dan Komunikasi, Volume 4 No 3, September (2023), pp. 1598-1608
DOI : https://doi.org/10.35870/jimik.v4i3.386

5) Konfigurasi Aturan SDWAN. Tahap ini melibatkan konfigurasi aturan *failover*, seperti yang sudah dijelaskan dalam judul, aturan akan menggunakan strategi best quality, di mana nantinya packet loss akan menjadi parameter apakah suatu koneksi atau link kualitasnya baik atau tidak.
6) Konfigurasi Kebijakan *Firewall*. Setelah konfigurasi Aturan dan Anggota SDWAN selesai, berikutnya adalah membuat kebijakan agar lalu lintas data dari cabang ke pusat atau sebaliknya dapat saling terhubung.
7) Pengujian *Failover*. Pada tahap ini, dilakukan uji *failover* apakah berjalan dengan baik dan sesuai dengan skenario pada aturan SDWAN.
8) Analisis Hasil Pengujian. Hasil pengujian dianalisis untuk memastikan bahwa sistem SDWAN berfungsi sesuai dengan yang diharapkan. Hal ini meliputi pengecekan konektivitas, pemantauan kinerja jaringan, dan evaluasi terhadap fitur-fitur SDWAN yang diimplementasikan.

3.3. Skema Pengujian

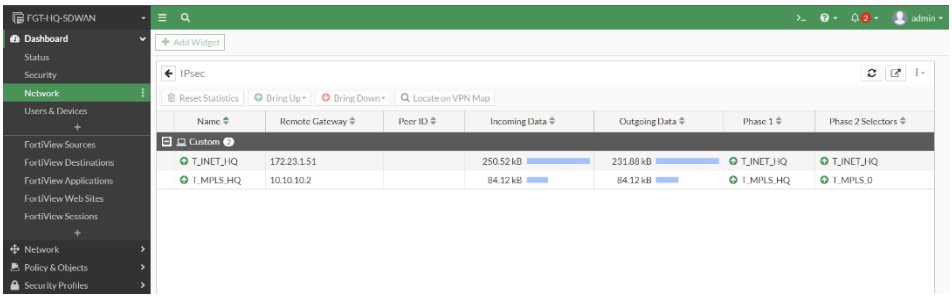
Pada pengujian hasil implementasi *Failover* VPN dengan Teknologi SDWAN akan dilakukan dengan beberapa skema yang bertujuan untuk memastikan kinerja dan fitur-fitur dari *Failover* VPN yang telah diimplementasikan. Berikut ini adalah tiga skema pengujian yang akan dilakukan:

1) Skema 1, pengujian dan pengukuran kualitas packetloss pada saat kondisi jaringan normal atau kedua koneksi dalam keadaan baik semua
2) Skema 2, pengujian dan pengukuran kualitas packetloss dan ketersediaan jaringan pada saat packetloss pada koneksi MPLS L2 mengalami peningkatan dan *traffic* akan ditangani oleh koneksi internet sebagai jalur backup
3) Skema 3, pengujian dan pengukuran kualitas packetloss dan ketersediaan jaringan Ketika packetloss pada jalur utama atau koneksi MPLS L2 dalam keadaan normal atau tidak mengalami kenaikan yang signifikan.

Dengan melakukan pengujian-pengujian ini, diharapkan dapat memvalidasi hasil implementasi *Failover* VPN dengan teknologi SDWAN dan memastikan bahwa ketersediaan jaringan tetap terjaga sesuai dengan tujuan dan fitur yang telah dirancang.

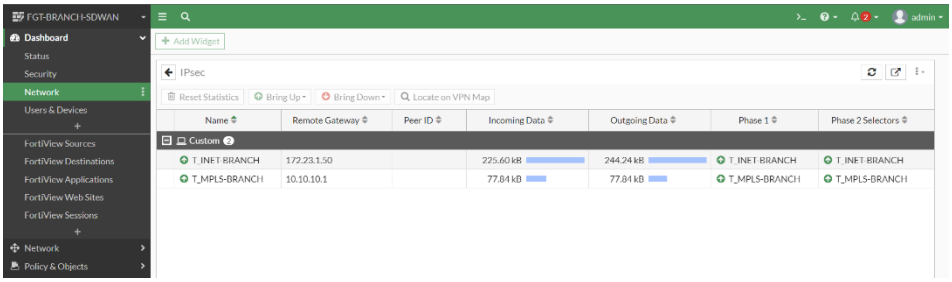
3.4. Verifikasi Konfigurasi Awal

Verifikasi IPSec VPN untuk memastikan apakah sudah dalam keadaan up atau masih down, apabila masih *down* nantinya kita perlu melakukan pengecekan Kembali terkait parameter konfigurasi seperti *pre-shared-key*, enkripsi, hashing, dan lain sebagainya.



Gambar 4. Monitoring IPSec VPN di HQ

Jurnal Indonesia : Manajemen Informatika dan Komunikasi, Volume 4 No 3, September (2023), pp. 1598-1608
DOI : https://doi.org/10.35870/jimik.v4i3.386

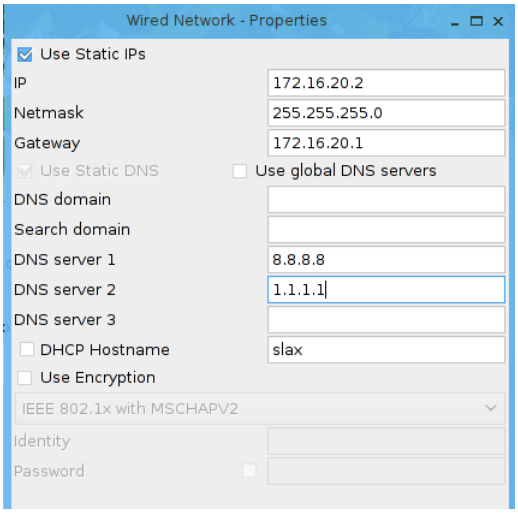


Gambar 5. Monitoring IPSec VPN di Branch

Berdasarkan gambar diatas kondisi tunnel IPSec sudah dalam keadaan up baik pada kantor pusat maupun pada kantor cabang. Sebelum kita lanjut ke tahap pengujian kita perlu melakukan konfigurasi IP Address pada server-HQ dan PC Cabang

```
Server-HQ(config)#interface e0/0
Server-HQ(config-if)#ip add 172.16.10.2 255.255.255.0
Server-HQ(config-if)#no shut
Server-HQ(config-if)#exit
Server-HQ(config)#ip route 0.0.0.0 0.0.0.0 172.16.10.1
```

Konfigurasi IP *Address* pada PC Cabang

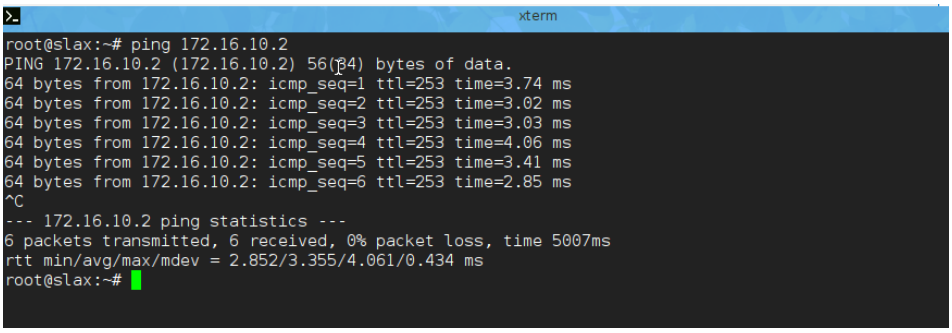


Gambar 6. Konfigurasi IP Address PC Cabang

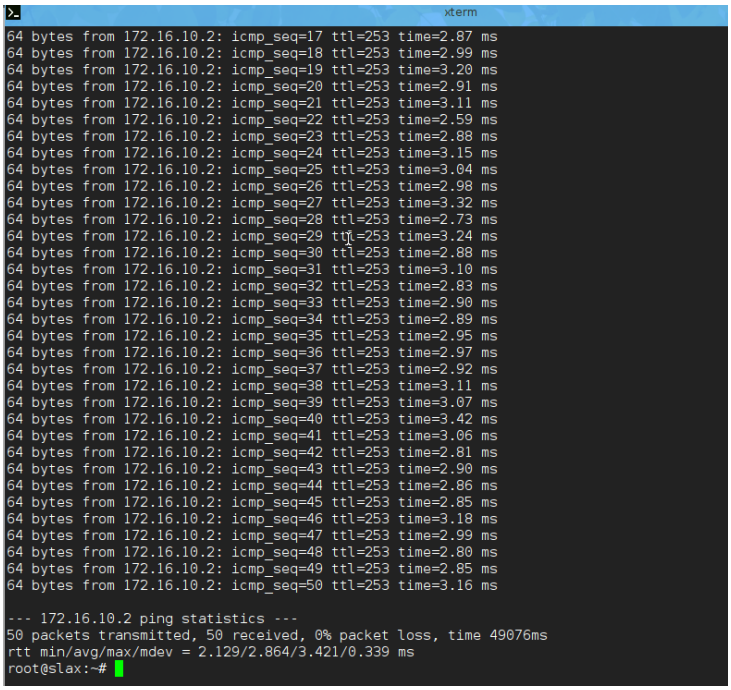
3.5. Pengujian Skema 1

Skema 1, pengujian dan pengukuran kualitas packetloss pada saat kondisi jaringan normal atau kedua koneksi dalam keadaan baik semua, dimana Tunnel MPLS akan bertindak sebagai primary. Berikut hasil pengujian test koneksi dari PC Cabang menuju Server HQ dengan ping dan *tracert* menggunakan terminal. Dapat dilihat pada gambar di bawah, traffic menuju server HQ dari PC Cabang akan melewati T_MPLS-BRANCH sebagai primary nya. Karena tunnel mpls bertindak sebagai *primary*.

Jurnal Indonesia : Manajemen Informatika dan Komunikasi, Volume 4 No 3, September (2023), pp. 1598-1608
DOI : https://doi.org/10.35870/jimik.v4i3.386



Gambar 7. Pengujian Ping Skema 1



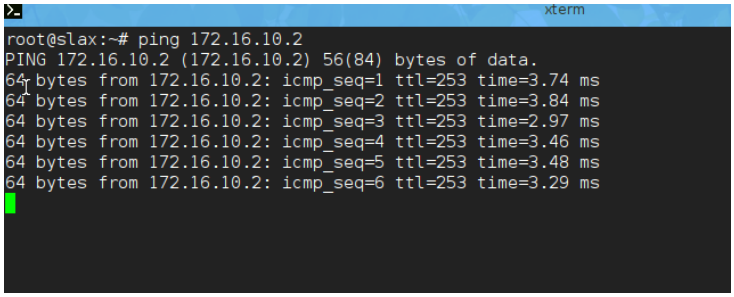
Gambar 8. Pengujian Ping 50 ICMP Packets

Berdasarkan gambar diatas, untuk latency masih aman di angka 4,06ms dan dari 50 paket ping yang dikirimkan tidak ada packetloss sama sekali. Dan dapat di lihat juga implementasi *Failover* VPN menggunakan teknologi SDWAN tidak ada pengaruh terhadap kualitas latency dan packetloss.

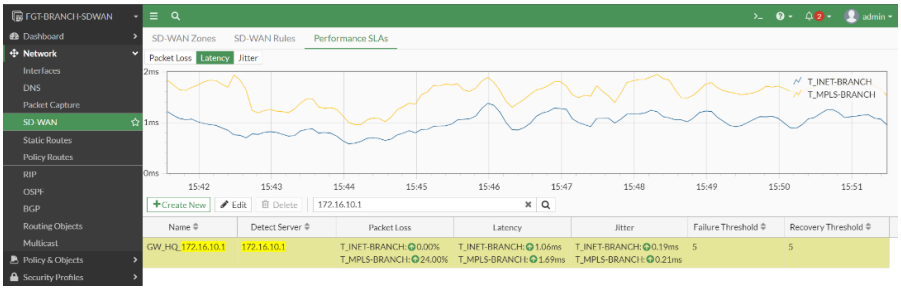
3.6. Pengujian Skema 2

Setelah pengujian skema 1 selesai dilakukan, selanjutnya akan dilakukan pengujian terhadap ketersediaan jaringan pada saat packetloss pada koneksi MPLS L2 mengalami peningkatan dan traffic akan ditangani oleh koneksi internet sebagai jalur backup. Di skema ini akan dilakukan pengujian dengan cara menaikan packetloss pada link MPLS sebagai simulasi link high packetloss, menaikan packetloss pada link MPLS, PC Cabang akan melakukan ping terus menerus kearah server HQ.

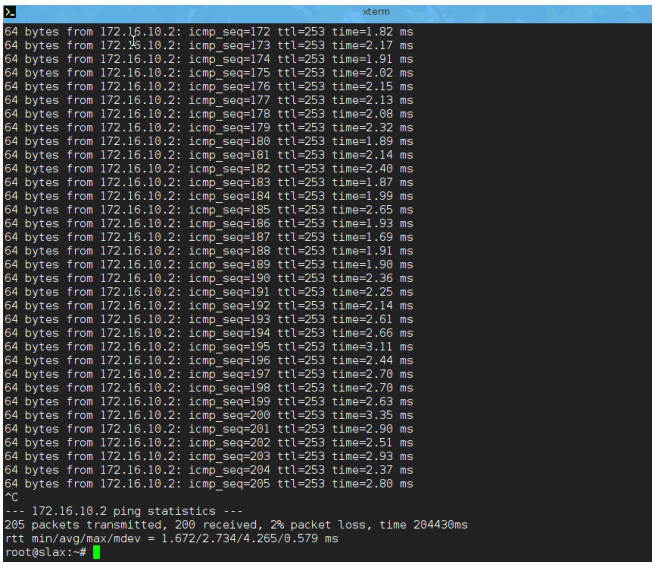
Jurnal Indonesia : Manajemen Informatika dan Komunikasi, Volume 4 No 3, September (2023), pp. 1598-1608
DOI : https://doi.org/10.35870/jimik.v4i3.386



Gambar 9. Pengujian Ping Skema 2



Gambar 10. Monitoring Kenaikan Packetloss di Branch



Gambar 11. Hasil Ping Saat Berpindah Link Skema 2

Dari hasil pengujian diatas, terlihat bahwa dari 205 paket yang dikirimkan terdapat dua packetloss yang terjadi ketika link MPLS mengalami kenaikan packetloss. dua packetloss ini terjadi karena proses perpindahan dari tunnel mpls ke tunnel internet. Dari hasil pengujian skema 2 di atas dapat dilihat ketika tunnel mpls mengalami kenaikan packetloss yang signifikan, maka jalur akan otomatis pindah ke tunnel internet. Dari hasil sistem VPN *failover* menggunakan teknologi SDWAN, mampu mengurangi downtime sebesar 97, 6%.

Jurnal Indonesia : Manajemen Informatika dan Komunikasi, Volume 4 No 3, September (2023), pp. 1598-1608
DOI : https://doi.org/10.35870/jimik.v4i3.386

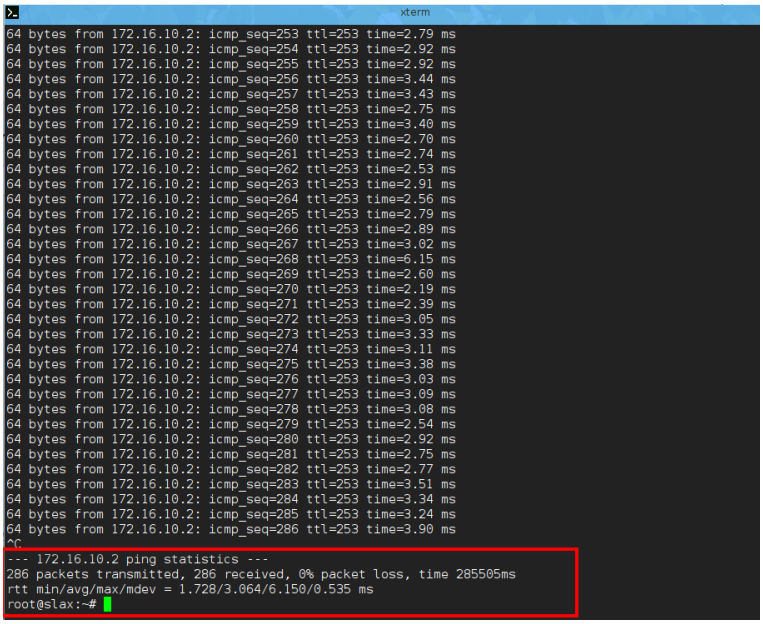
$$\text{Rumus Presentase Downtime} = \frac{\text{Jumlah ICMP yang diterima}}{\text{Jumlah ICMP yang dikirim}} \text{ x } 100\%$$

$$\text{Hasil Presentase Downtime} = \frac{200}{205} \; x \; 100\% = 97{,}6\%$$

Gambar 12. Rumus Presentase Skema 2

3.7. Pengujian Skema 3

Pada pengujian skema 3 ini akan dilakukan recovery di link tunnel mpls, ini bertujuan untuk menguji bagaimana kualitas jaringan yang dirasakan client ketika tunnel mpls atau link utama jumlah packetloss nya kembali normal. Proses pengujian masih sama dengan skema 2 dimana PC Cabang akan terus melakukan ping dengan menggunakan terminal linux slax, setelah itu dilakukan monitoring pada *fortiview session* untuk melihat traffic dilewatkan ke jalur mana.



Gambar 13. Pengujian Skema 3

Dari tiga skema yang diuji cobakan dengan cara mengirim paket ping dengan jumlah paket mencapai 491 paket tidak terlihat adanya paket loss yang signifikan ketika tunnel mpls mengalami kenaikan packetloss atau ketika packetloss pada tunnel mpls kembali normal. Berdasarkan uji coba pada ketiga skema di atas, hasil sistem VPN *failover* menggunakan teknologi SDWAN, mampu mengurangi downtime sebesar 99%. Artinya pc cabang hampir tidak merasakan gangguan sama sekali Ketika proses *failover* terjadi.

$$\text{Rumus Presentase Downtime} = \frac{\text{Jumlah ICMP yang diterima}}{\text{Jumlah ICMP yang dikirim}} \text{ x } 100\%$$

$$\text{Hasil Presentase Downtime} = \frac{486}{491} \; x \; 100\% = 99\%$$

Gambar 14 Rumus Presentase Skema 3

Berdasarkan hasil pengujian diatas, maka didapat hasil perbandingan antara sebelum implementasi *Failover* VPN menggunakan Teknologi SDWAN dan setelah implementasi *Failover* VPN menggunakan teknologi SDWAN

Jurnal Indonesia : Manajemen Informatika dan Komunikasi, Volume 4 No 3, September (2023), pp. 1598-1608
DOI : https://doi.org/10.35870/jimik.v4i3.386

Tabel 1. Tabel Perbandingan Sebelum dan Sesudah Implementasi

Parameter	Sebelum	Sesudah
Memiliki link redudansi	✗	✓
Pertukaran data terenkripsi	✗	✓
Strategi *Failover* Berdasarkan Kualitas Link (Packetloss, latency dan jitter)	✗	✓
Traffic Steering	✗	✓

4. Kesimpulan

Implementasi *Failover* VPN Menggunakan teknologi SD-WAN Dengan Strategi *Best Quality* akan menjamin ketersediaan jaringan untuk client atau users yang berada pada kantor cabang ataupun kantor pusat. Tingkat ketersediaan jaringan dengan menggunakan SDWAN bisa mencapai 99%. Pada Saat Tunnel MPLS mengalami kenaikan packetloss yang signifikan proses *failover* dari Tunnel MPLS ke Tunnel Internet akan berjalan secara otomatis yang artinya tidak perlu memindahkan *gateway* secara manual ke Tunnel Internet.

5. Daftar Pustaka

[1] Setiawan, O., Muhammad, M., & Syahroni, M. (2021). Implementasi *Failover* Dengan Metode Recursive Gateway Pada Jaringan Local Area Network (LAN) Berbasis Router Mikrotik RB951UI. *Jurnal TEKTRO*, *5*(2). DOI: https://DOI.org/10.36982/jiig.v10i1.732.

[2] Adhiwibowo, W., & Irawan, A. R. (2019). Implementasi Redundant Link Untuk Mengatasi Downtime Dengan Metode *Failover*. *Jurnal Pengembangan Rekayasa Dan Teknologi*, *15*(1), 48-53. DOI: http://dx.doi.org/10.26623/jprt *failover*.v15i1.1490

[3] Oktavian, B. D., & Sobari, I. A. (2022). IMPLEMENTASI JARINGAN TERPUSAT MENGGUNAKAN OSPF DAN VPN DENGAN *FAILOVER* LINK DI PT. ADVANTAGE SCM. *Jurnal Teknik Mesin, Industri, Elektro dan Informatika*, *1*(3), 69-88. DOI: https://doi.org/10.55606/jtmei.v1i3.569.

[4] Saputra, H., & Dalimunthe, R. A. (2021). IMPLEMENTASI *FIREWALL* PADA DATA LINK LAYER MENGGUNAKAN ARSITEKTUR SOFTWARE DEFINED NETWORK. *JURTEKSI (Jurnal Teknologi dan Sistem Informasi)*, *7*(3), 245-250. DOI: 10.33330/jurteksi.v7i3.1199.

[5] Hadiyansyah, D., Yahya, W., & Kurniawan, W. (2018). Implementasi Penentuan Bobot Link Menggunakan Logika Fuzzy Untuk Pencarian Jalur Terpendek Pada Software Defined Networking. *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, *2*(9), 2677-2685.

[6] Radito, R., Trisnawan, P. H., & Amron, K. (2020). Implementasi Pencarian Jalur berdasarkan Bandwidth dengan menggunakan Algoritme Dijkstra pada Arsitektur Jaringan Software-Defined Networking (SDN). *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, *4*(5), 1372-1379.

[7] Muntaha, M. F., Trisnawan, P. H., & Primananda, R. (2019). Implementasi Intrusion Prevention System (IPS) berbasis Athena untuk Mencegah Serangan DDoS pada Arsitektur Software-Defined Network (SDN). *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, *3*(7), 6847-6855. [Online]. Available: http://j-ptiik.ub.ac.id.

[8] Novianto, D., & Helmud, E. (2019). Implementasi *Failover* dengan Metode Recursive Gateway Berbasis Router Mikrotik Pada STMIK Atma Luhur Pangkalpinang. *Jurnal Ilmiah Informatika Global*, *10*(1). DOI: https://doi.org/10.36982/jiig.v10i1.732.

[9] Fathsyah, M. M., Hadi, I., & Salamah, I. (2021). Implementasi Virtual Private Network *Failover* Menggunakan Mikrotik Pada Jaringan Lokal Politeknik Negeri Sriwijaya. *Jurnal Khatulistiwa Informatika*, *7*(2), 222-228. DOI: 10.31294/jtk.v4i2.

[10] "Citraweb.com : *Failover* menggunakan Netwatch." https://citraweb.com/artikel/429/ (accessed Jul. 11, 2023).

[11] Bagono, B. J. (2022). OPTIMALISASI JARINGAN WIDE AREA NETWORK MENGGUNAKAN SOFTWARE DEFINED NETWORK VIPTELA. *Jurnal Sibernetika*, *7*(2), 49-61.

[12] 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), 139-144. DOI: 10.25126/jtiik.202071638.

[13] Wahyudi, H. (2022). Implementasi Load Balancing dan *Failover* pada Jaringan Internet Menggunakan Metode Nth. *Jurnal Informatika Teknologi dan Sains (Jinteks)*, *4*(3), 131-136. DOI: https://DOI.org/10.51401/jinteks.v4i3.1904.

[14] Rifandy, A. S., & Topiq, S. (2023). Analisa dan Implementasi VPN Dinamis Menggunakan Hamachi Pada PT. Jaindo Metal Industries. *Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)*, *6*(2). DOI: https://doi.org/10.32672/jnkti.v6i2.5904.

[15] "Apa Itu SD-WAN dan bagaimana perkembangannya?" https://blog.lintasarta.net/article/solution/managed-services/sdwan/apa-itu-sd-wan (accessed Jul. 11, 2023).

[16] "Apa itu IPSec - IPSec di Amazon Web Services." https://aws.amazon.com/id/what-is/ipsec/ (accessed Jul. 11, 2023).

[17] Badrul, M., & Akmaludin, A. (2019). IMPLEMENTASI AUTOMATIC *FAILOVER* MENGGUNAKAN ROUTER MIKROTIK UNTUK OPTIMALISASI JARINGAN. *PROSISKO: Jurnal Pengembangan Riset dan Observasi Sistem Komputer*, *6*(2).

[18] Kuswanto, H., & Rahman, T. (2019). *Failover* Gateway Menggunakan Protokol Virtual Router Redundancy Protocol (VRRP) pada Mikrotik Router. *JUSTIN (Jurnal Sistem dan Teknologi Informasi)*, *7*(1), 60-66.

[19] Arfan, M. A., Zainuddin, Z., & Rahmania, R. (2019). Implementasi Router Mikrotik dan Modem Mifi Smartfren sebagai Backup Akses Data dengan Menggunakan Sistem *Failover*. *Ainet: Jurnal Informatika*, *1*(1), 13-20. DOI: https://doi.org/10.26618/ainet.v1i1.2253

[20] Wartono, W., WA, B. S., & Pramono, E. (2019). Analisa Optimasi Penggunaan Bandwidth Dengan *Failover* Dan Load Balance Pada Mikrotik. *Jurnal Informa: Jurnal Penelitian dan Pengabdian Masyarakat*, *5*(3), 33-39. DOI: https://doi.org/10.46808/informa.v5i3.142