

IMPLEMENTASI SD-WAN UNTUK MENINGKATKAN KEANDALAN JARINGAN DI SUBBIDANG ROUTER DAN KEAMANAN PT PLN ICONPLUS

Taufik Rahman, M.Iksan Susanta Ramada

Teknologi Informasi, Universitas Bina Sarana Informatika
taufik@bsi.ac.id

ABSTRAK

Meningkatnya permintaan akan konektivitas jaringan yang andal dan aman di perusahaan skala besar, seperti PT PLN Icon Plus, telah mendorong kebutuhan akan inovasi dalam arsitektur jaringan. Arsitektur WAN tradisional sering kali mengalami latensi tinggi, fleksibilitas terbatas, dan manajemen yang kompleks, terutama saat mengintegrasikan beberapa koneksi cabang dan layanan berbasis cloud. Untuk mengatasi keterbatasan tersebut, penelitian ini menerapkan teknologi *Software-Defined Wide Area Network* (SD-WAN) untuk meningkatkan keandalan, efisiensi, dan keamanan jaringan di lingkungan Subdivisi Router dan Keamanan di PT PLN Icon Plus. Tujuan dari penelitian ini adalah untuk mengevaluasi peningkatan kinerja yang dicapai melalui implementasi SD-WAN dibandingkan dengan sistem WAN konvensional. Penelitian ini menerapkan metodologi eksperimental dan komparatif. Hasilnya menunjukkan peningkatan yang signifikan dalam kinerja jaringan: latensi rata-rata menurun dari 65 ms menjadi 28 ms, kehilangan paket dihilangkan (dari 5% menjadi 0%), dan waktu pemulihan failover meningkat dari 60 detik menjadi kurang dari 2 detik. Selain itu, SD-WAN mengaktifkan perutean dinamis, pemantauan waktu nyata, dan keamanan terintegrasi melalui enkripsi IPsec otomatis dan mekanisme pencegahan intrusi. Kesimpulannya, implementasi SD-WAN berhasil mencapai tujuan penelitian dengan meningkatkan keandalan, keamanan, dan pengelolaan jaringan secara substansial. Studi di masa mendatang direkomendasikan untuk mengeksplorasi integrasi SD-WAN dengan analitik berbasis AI untuk manajemen dan pengoptimalan jaringan prediktif.

Kata kunci : SDWAN, Keandalan Jaringan, Fortigate, Failover, SLA

1. PENDAHULUAN

Keandalan konektivitas Wide Area Network (WAN) merupakan salah satu aspek penting dalam mendukung aktivitas operasional pada Subbidang Router dan Keamanan PT PLN Iconplus, terutama karena pengelolaan router, konektivitas antarjaringan, serta kebijakan keamanan membutuhkan jalur komunikasi yang tetap tersedia ketika terjadi gangguan pada salah satu koneksi. Permasalahan yang menjadi perhatian dalam penelitian ini bukan sekadar keterbatasan jaringan komputer secara umum, tetapi bagaimana ketergantungan terhadap jalur WAN tertentu, proses perpindahan jalur ketika terjadi gangguan, dan pengelolaan routing yang belum adaptif dapat memengaruhi kontinuitas komunikasi antarsite. Pada arsitektur WAN konvensional, gangguan pada jalur utama dapat menyebabkan terputusnya komunikasi sampai mekanisme routing atau failover mengalihkan trafik ke jalur alternatif. Kondisi tersebut menjadi semakin penting ketika jaringan menggunakan lebih dari satu jenis koneksi WAN yang memiliki karakteristik performa berbeda. Dalam konteks SD-WAN, pemilihan jalur dapat dilakukan berdasarkan kondisi aktual seperti *latency*, *jitter*, dan *packet loss*, sehingga jalur yang tidak memenuhi parameter SLA dapat dikeluarkan dari kelompok forwarding dan trafik dialihkan ke jalur lain.

Perkembangan penelitian menunjukkan bahwa SD-WAN dan mekanisme failover bukan lagi teknologi yang baru, sehingga implementasi SD-

WAN semata tidak cukup untuk menjadi pembeda penelitian. Heriaji *et al.* melakukan perbandingan performa routing MPLS dan SD-WAN menggunakan parameter *convergence time*, throughput, delay, dan packet loss, dan memperoleh hasil bahwa SD-WAN memiliki keunggulan pada *convergence* serta beberapa parameter QoS[1]. Penelitian lain pada PT XYZ menerapkan SD-WAN berbasis FortiGate dengan dua ISP dan BGP serta menguji kondisi normal dan dua skenario *failover*[2]. Sementara itu, penelitian pada perusahaan FIF telah mengimplementasikan FortiGate SD-WAN dengan Astinet dan VPN IPsec untuk menguji *auto link failover*, keamanan, dan penggunaan trafik[3]. Bahkan, kajian survei SD-WAN menunjukkan bahwa *failover and recovery* telah menjadi salah satu bidang penelitian SD-WAN yang cukup banyak dikaji melalui simulasi maupun *testbed*[4].

Perkembangan teknologi informasi meningkatkan kebutuhan perusahaan akan jaringan yang andal, aman, dan efisien. Jaringan komputer berperan penting dalam komunikasi dan pertukaran data antarperangkat di berbagai lokasi[5]. dengan menghubungkan perangkat seperti router, sakelar, dan server melalui media kabel maupun nirkabel [6]. PT PLN Icon Plus membutuhkan jaringan yang andal untuk mendukung operasional, tetapi gangguan konektivitas antar cabang dan pengelolaan jaringan secara manual dapat menurunkan kinerja aplikasi serta memperlambat proses *failover*[7]. *Software Defined Networking*

(SDN) menawarkan pengelolaan jaringan secara terpusat dengan memisahkan fungsi kontrol dari perangkat keras[8]. Salah satu penerapannya adalah *Software Defined Wide Area Network* (SD-WAN), yang mampu memilih jalur komunikasi secara dinamis dan mengintegrasikan koneksi MPLS, broadband, serta LTE melalui manajemen terpusat sehingga meningkatkan efisiensi jaringan [9], [10].

FortiGate menyediakan fitur SD-WAN dengan *load balancing*, keamanan terintegrasi, dan *failover* otomatis yang dapat mengalihkan lalu lintas ke jalur cadangan saat terjadi gangguan[11]. Penerapan *failover* otomatis pada FortiGate SD-WAN terbukti meningkatkan keandalan koneksi dan mengurangi waktu henti[2]. Implementasi SD-WAN di Subbidang Router dan Keamanan PT PLN Icon Plus diharapkan mampu meningkatkan keandalan jaringan melalui pemilihan jalur dinamis tanpa intervensi manual. Hal ini didukung penelitian yang menunjukkan bahwa kombinasi SD-WAN dan *failover* FortiGate mampu menjaga stabilitas koneksi dan mendukung aplikasi perusahaan[12]. SD-WAN juga terbukti mampu meningkatkan stabilitas koneksi dan mengurangi biaya operasional hingga 63%[13]. sementara pendekatan hibrida MPLS dan SD-WAN menawarkan kombinasi keandalan, fleksibilitas, dan efisiensi[14].

Implementasi SD-WAN FortiGate dengan *load balancing* dapat meningkatkan keandalan VPN, distribusi lalu lintas, dan mengurangi latensi[10]. Penggunaan FortiGate 40F juga terbukti mengurangi *downtime* melalui *failover* cepat dan distribusi lalu lintas yang efisien[15]. SD-WAN menawarkan manajemen WAN yang lebih fleksibel dan aman dibandingkan jaringan tradisional[16]. termasuk melalui arsitektur hibrida VyOS dan SD-WAN yang skalabel[17]. Teknologi ini juga efektif dalam memenuhi kebutuhan bandwidth melalui *failover* dan *load balancing* otomatis[7]. Penggunaan LTE sebagai jalur cadangan pada Cisco SD-WAN terbukti efektif untuk *failover*[18]. sedangkan kombinasi internet dan MPLS dapat meningkatkan keandalan jaringan[19]. Sistem SD-WAN dengan MPLS sebagai jalur utama dan internet sebagai cadangan mampu menjaga kontinuitas melalui pengalihan otomatis[8]. Kombinasi SD-WAN dan HA FortiGate bahkan dilaporkan mengurangi *downtime* lebih dari 91%[20]. Selain itu, Viptela SDN menyederhanakan pengelolaan WAN melalui visualisasi kinerja jaringan[21]. sedangkan Fortinet dengan IPSec Tunnel efektif menjaga ketersediaan layanan melalui koneksi cadangan[22]. Studi lain menunjukkan pfSense unggul dalam QoS *load balancing*, sementara flexiWAN menjadi alternatif SD-WAN yang fleksibel[23].

Pengujian *load balancing* dan *auto failover* pada FortiGate dilakukan untuk mengevaluasi kemampuan SD-WAN dalam menjaga konektivitas antar situs dan keamanan jaringan [24], [4], [7].

Berdasarkan penelitian terdahulu tersebut, research gap penelitian ini terletak pada belum tersedianya evaluasi yang secara spesifik menggabungkan kebutuhan operasional Subbidang Router dan Keamanan PT PLN Iconplus dengan pengujian keandalan SD-WAN dalam lingkungan simulasi yang terkontrol. Penelitian sebelumnya telah membuktikan kemampuan SD-WAN dalam melakukan *failover*, membandingkan SD-WAN dengan MPLS, atau menguji FortiGate dengan beberapa ISP, tetapi belum secara khusus menjawab bagaimana rancangan SD-WAN yang disesuaikan dengan kebutuhan subbidang router dan keamanan dapat mempertahankan konektivitas ketika terjadi kegagalan link, seberapa cepat perpindahan jalur dilakukan, serta bagaimana perubahan tersebut terlihat pada parameter performa jaringan. Dengan demikian, penelitian ini tidak menempatkan *failover FortiGate* sebagai kebaruan utama, melainkan menggunakan mekanisme tersebut sebagai bagian dari rancangan untuk mengevaluasi keandalan jaringan secara terukur. Penggunaan *Performance SLA* juga memungkinkan kondisi link dinilai berdasarkan latency, jitter, dan packet loss sebelum keputusan pemilihan atau perpindahan jalur dilakukan.

Novelty penelitian ini terletak pada penyusunan dan evaluasi rancangan SD-WAN yang berorientasi pada kebutuhan Subbidang Router dan Keamanan PT PLN Iconplus, dengan menghubungkan aspek *multi-WAN*, *dynamic path selection*, keamanan, dan *automatic failover* dalam satu skenario pengujian. Penelitian dilakukan dalam lingkungan simulasi, bukan pada jaringan produksi PT PLN Iconplus, sehingga perubahan konfigurasi dan skenario kegagalan dapat diuji tanpa mengganggu layanan operasional perusahaan. Evaluasi diarahkan pada kondisi sebelum dan sesudah penerapan rancangan SD-WAN dengan parameter yang dapat diukur, yaitu latency rata-rata, jitter, packet loss, throughput, waktu konvergensi/failover, serta ketersediaan koneksi setelah kegagalan link. Parameter tersebut digunakan untuk menentukan apakah rancangan yang diusulkan benar-benar memberikan peningkatan keandalan, bukan sekadar menunjukkan bahwa fitur SD-WAN atau failover dapat berjalan.

Berdasarkan permasalahan dan *research gap* tersebut, penelitian ini bertujuan merancang dan mengimplementasikan simulasi SD-WAN pada lingkungan jaringan yang merepresentasikan kebutuhan Subbidang Router dan Keamanan PT PLN Iconplus, kemudian mengukur dampaknya terhadap keandalan jaringan. Secara khusus, penelitian ini bertujuan untuk: (1) mengidentifikasi performa jaringan sebelum penerapan SD-WAN berdasarkan latency, jitter, packet loss, throughput, dan ketersediaan jalur; (2) merancang SD-WAN dengan *multi-WAN*, *Performance SLA*, dan

failover; (3) mengukur waktu perpindahan ke jalur alternatif saat terjadi gangguan; dan (4) membandingkan performa jaringan sebelum dan sesudah penerapan. Pertanyaan penelitian meliputi: (1) bagaimana merancang SD-WAN yang sesuai dengan kebutuhan Subbidang Router dan Keamanan PT PLN Iconplus dalam simulasi; (2) bagaimana pengaruhnya terhadap parameter kinerja jaringan; (3) berapa waktu *failover* saat jalur utama terganggu; dan (4) sejauh mana SD-WAN meningkatkan keandalan jaringan dibandingkan konfigurasi sebelumnya.

Hasil penelitian diharapkan memberikan kontribusi praktis berupa rancangan dan parameter evaluasi yang dapat dijadikan acuan awal dalam pengembangan jaringan perusahaan, khususnya dalam menentukan strategi penggunaan beberapa jalur WAN, pemantauan kualitas link, serta mekanisme perpindahan jalur ketika terjadi gangguan. Kontribusi akademiknya adalah memberikan studi berbasis simulasi yang tidak hanya membahas implementasi SD-WAN, tetapi menguji keandalan jaringan secara kuantitatif berdasarkan skenario gangguan dan parameter performa yang terukur. Penelitian ini juga tidak menarik kesimpulan mengenai penghematan biaya karena analisis biaya bukan bagian dari variabel penelitian. Dengan batasan bahwa seluruh pengujian dilakukan pada lingkungan simulasi, hasil penelitian digunakan sebagai dasar evaluasi dan rekomendasi teknis, bukan sebagai klaim bahwa rancangan telah diterapkan pada jaringan produksi PT PLN Iconplus.

2. TINJAUAN PUSTAKA

2.1. Software-Defined Wide Area Network (SD-WAN)

merupakan teknologi pengelolaan WAN yang memungkinkan beberapa jalur jaringan dikelola secara terpusat dan dipilih secara dinamis berdasarkan kondisi jaringan. Pada FortiGate, SD-WAN mendukung *traffic steering*, *SLA monitoring*, *load balancing*, dan *failover* untuk meningkatkan keandalan koneksi[25].

2.2. Traffic steering

adalah mekanisme untuk mengarahkan trafik melalui jalur WAN tertentu berdasarkan aturan dan kondisi jaringan, seperti *latency*, *jitter*, *packet loss*, dan *bandwidth*. Mekanisme ini memungkinkan trafik menggunakan jalur yang paling sesuai dengan kebutuhan layanan.

2.3. Best Quality

merupakan strategi SD-WAN yang memilih jalur berdasarkan kualitas terbaik. FortiGate dapat menggunakan parameter *latency*, *jitter*, dan *packet loss* untuk menentukan jalur yang optimal[6].

2.4. Automatic failover

memungkinkan trafik berpindah secara otomatis ke jalur cadangan ketika jalur utama gagal memenuhi kriteria yang ditetapkan. Mekanisme ini bertujuan mempertahankan konektivitas dan mengurangi waktu gangguan layanan.

2.5. SLA/health check

digunakan untuk memantau kualitas link berdasarkan parameter seperti *latency*, *jitter*, dan *packet loss*. Hasil pengukuran menjadi dasar SD-WAN dalam menentukan kelayakan suatu link dan melakukan pengalihan trafik.

2.6. Network reliability

menunjukkan kemampuan jaringan dalam mempertahankan konektivitas dan layanan secara konsisten. Dalam penelitian ini, keandalan diukur melalui *latency*, *jitter*, *packet loss*, *throughput*, *failover time*, dan *availability*.

2.7. Link degradation

merupakan kondisi ketika koneksi masih aktif tetapi kualitasnya menurun, misalnya akibat meningkatnya *latency*, *jitter*, atau *packet loss*. SD-WAN dapat mendeteksi kondisi tersebut melalui SLA dan mengarahkan trafik ke jalur yang lebih baik.

Secara keseluruhan, SD-WAN menggunakan SLA/health check untuk mendeteksi kondisi link, kemudian melakukan *traffic steering* dengan strategi *Best Quality* dan *automatic failover* ketika terjadi *link degradation*. Mekanisme tersebut menjadi dasar dalam meningkatkan *network reliability*[25].

3. METODE PENELITIAN

3.1. Jenis dan Pendekatan Penelitian

Penelitian ini menggunakan pendekatan studi kasus dengan jenis penelitian deskriptif eksperimental. Pendekatan ini dipilih karena penelitian difokuskan pada analisis kondisi jaringan internal di PT PLN Icon Plus Kantor Gandul dan simulasi implementasi Software-Defined Wide Area Network (SD-WAN) sebagai solusi untuk meningkatkan keandalan jaringan. Penelitian dilakukan dengan pendekatan eksperimental melalui simulasi virtual menggunakan perangkat FortiGate di lingkungan PNETLab, untuk mengamati hasil implementasi secara terukur.

3.2. Objek dan Ruang Lingkup Penelitian

Objek penelitian ini adalah jaringan internal di Subbagian Router & Keamanan PT PLN Icon Plus Kantor Gandul. Ruang lingkup penelitian terbatas pada proses desain dan simulasi SD-WAN, tanpa aplikasi langsung di lingkungan produksi. Fokus utama penelitian ini adalah untuk menilai efektivitas SD-WAN dalam mengelola redundansi tautan dan mekanisme failover otomatis untuk meningkatkan keandalan jaringan.

3.3. Teknik Pengumpulan

Data Data dalam penelitian ini diperoleh melalui dua metode: a. Observasi, Dilakukan langsung di Subbagian Router & Keamanan PT PLN Icon Plus Gandul untuk mengamati perangkat jaringan yang digunakan, serta memahami bagaimana infrastruktur jaringan berjalan dan dikelola. b. Wawancara, dilakukan dengan berdiskusi langsung dengan staf senior yang memiliki pengalaman dalam manajemen jaringan di kantor. c. Studi Sastra, Dilakukan dengan mencari dan mempelajari referensi dari buku, jurnal ilmiah, dan artikel online yang membahas topik terkait seperti SD-WAN, jaringan komputer, dan mekanisme failover.

3.4. Alat dan Bahan yang Digunakan

Penelitian ini menggunakan perangkat dan perangkat lunak berikut: FortiGate Virtual Appliance, sebagai alat utama untuk implementasi SD-WAN. PNETLab, sebagai media virtualisasi untuk membuat dan menguji topologi jaringan. Laptop/PC dengan spesifikasi yang memadai, untuk menjalankan simulasi jaringan. Selain itu, konfigurasi jaringan dasar dan parameter pengujian dibuat menggunakan antarmuka grafis FortiGate tanpa melibatkan perangkat atau sistem eksternal lainnya.

3.5. Prosedur Penelitian atau Magang

Prosedur penelitian ini terdiri dari empat tahapan utama yang digunakan sebagai pedoman dalam merancang dan menganalisis implementasi SD-WAN di lingkungan jaringan internal PT PLN Icon Plus Gandul. Setiap tahap memiliki peran penting dalam menghasilkan desain jaringan yang terukur dan andal.



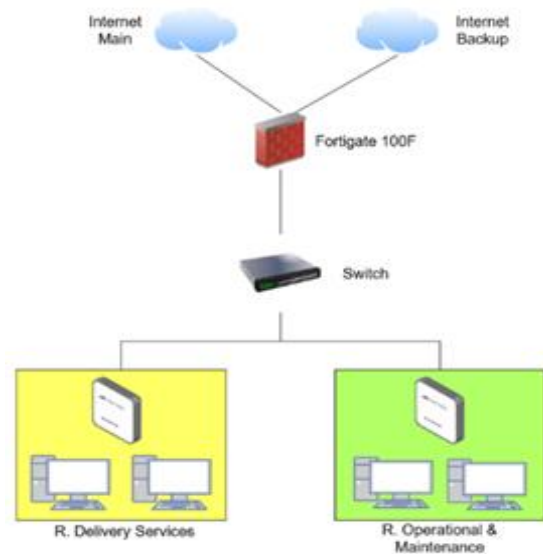
Gambar 1. Analisis Penelitian

a. Analisis Kebutuhan

Tahap ini bertujuan untuk mengidentifikasi kondisi jaringan yang ada, termasuk struktur topologi, perangkat yang digunakan, dan masalah yang mempengaruhi keandalan jaringan. Hasil analisis digunakan sebagai dasar untuk merancang solusi berbasis SD-WAN yang lebih adaptif dan efisien.

b. Desain

Pada tahap ini, desain arsitektur jaringan SD-WAN dilakukan secara virtual menggunakan perangkat FortiGate yang diimplementasikan melalui platform PNETLab. Desainnya mencakup pembentukan topologi jaringan, konfigurasi jalur primer dan cadangan, dan penerapan kebijakan pemilihan jalur otomatis dengan metode Kualitas Terbaik.



Gambar 2. Topologi

1. Konfigurasi sdwan pada Fortigate

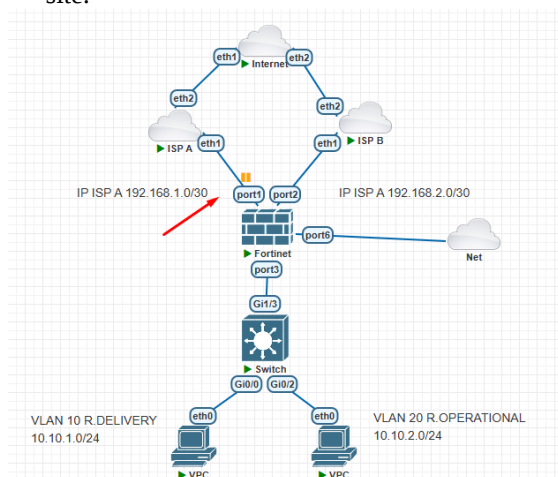

```

config system sdwan
set status enable
config zone
edit "virtual-wan-link"
next
end
config members
edit 1
set interface "port1"
set gateway 192.168.1.1
next
edit 2
set interface "port2"
set gateway 192.168.2.1
next
end
config health-check
edit "SLA_INET"
set server "8.8.8.8"
set members 0
config sla
edit 1
set latency-threshold 50
set jitter-threshold 50
set packetloss-threshold 10
next
end
next
end
config service
edit 2
set name "vlan-10-to-isp-a"
set dst "all"
set src "vlan-r.delivery address"
set priority-members 1
next
edit 3
set name "vlan-20-to-isp-b"
set dst "all"
      
```

- ```

set src "vlan-r.ops address"
set priority-members 2
next
edit 1
set name "rules-to-inet"
set mode priority
set dst "all"
set src "all"
set health-check "SLA_INET"
set priority-zone "virtual-wan-link"
next
end
end

```
- Konfigurasi routing pada Fortigate  
 config router static  
 edit 1  
 set distance 1  
 set sdwan-zone "virtual-wan-link"  
 next  
 end
  - Konfigurasi policy pada Fortigate  
 config firewall policy  
 edit 1  
 set name "lan-to-inet"  
 set srcintf "LAN"  
 set dstintf "virtual-wan-link"  
 set action accept  
 set srcaddr "all"  
 set dstaddr "all"  
 set schedule "always"  
 set service "ALL"  
 set logtraffic all  
 set nat enable  
 next  
 end
  - Pengujian  
 Tahap pengujian dilakukan untuk mengevaluasi performa dan keandalan jaringan berdasarkan parameter yang telah ditentukan. Pengujian meliputi simulasi kondisi normal dan gangguan (link utama terputus) guna menilai kecepatan proses failover serta kestabilan koneksi antar-site.



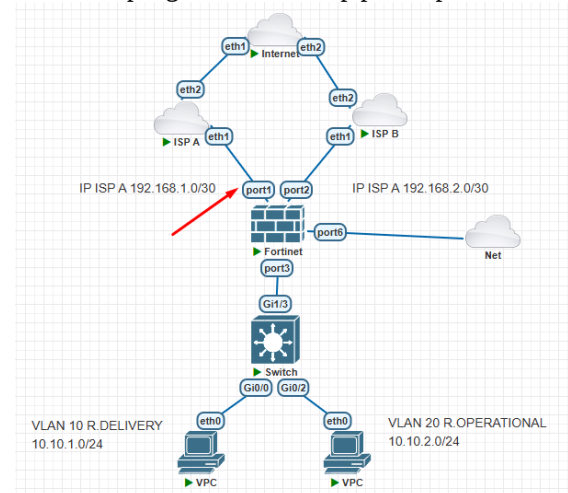
Gambar 3. Simulasi tautan mati

Berdasarkan hasil pemantauan, FortiGate secara otomatis mengalihkan trafik ke jalur WAN cadangan tanpa memerlukan tindakan manual dari administrator.

| ID | Name             | Source                | Destination | Criteria | Members        | Hit Count |
|----|------------------|-----------------------|-------------|----------|----------------|-----------|
| 2  | vlan-SD-to-isp-a | vlan-delivery address | all         |          | port1          | 0         |
| 3  | vlan-SD-to-isp-b | vlan-ops address      | all         |          | port2          | 0         |
| 1  | rules-to-inet    | all                   | all         | Latency  | port1<br>port2 | 0         |

Gambar 4. Menangkap Aturan SDWAN

Setelah jalur utama diaktifkan kembali, dilakukan pengamatan terhadap proses pemulihan.



Gambar 5. Resume link pada jaringan usulan

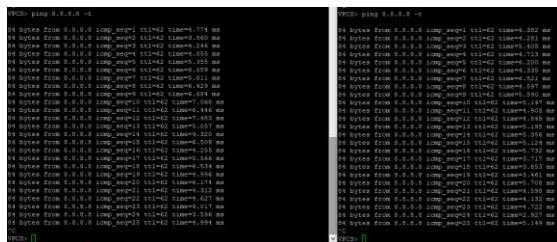
FortiGate secara otomatis mengembalikan penggunaan jalur utama, sesuai dengan konfigurasi prioritas dan parameter performa yang telah ditentukan sebelumnya.

| ID | Name             | Source                | Destination | Criteria | Members        | Hit Count |
|----|------------------|-----------------------|-------------|----------|----------------|-----------|
| 2  | vlan-SD-to-isp-a | vlan-delivery address | all         |          | port1          | 0         |
| 3  | vlan-SD-to-isp-b | vlan-ops address      | all         |          | port2          | 0         |
| 1  | rules-to-inet    | all                   | all         | Latency  | port1<br>port2 | 0         |

Gambar 6. Trafik setelah resume link pada jaringan usulan

Pengamatan dari Perspektif Pengguna Akhir

- Selama proses perpindahan jalur berlangsung, dilakukan uji koneksi dari sisi pengguna lokal melalui perintah ping ke alamat internet publik.
- Hasilnya menunjukkan koneksi tetap terjaga, dengan gangguan yang sangat minimal dan tidak memerlukan perubahan konfigurasi di sisi pengguna.



Gambar 7. Hasil pengujian jaringan usulan

Dari hasil pengujian ini dapat disimpulkan bahwa fitur SD-WAN yang diterapkan pada perangkat FortiGate mampu menjalankan fungsi failover otomatis dengan baik. Sistem dapat menjaga ketersediaan layanan internet secara terus-menerus, sekaligus meminimalkan dampak gangguan terhadap aktivitas pengguna di jaringan lokal.

Tahap ini merupakan penerapan keseluruhan hasil konfigurasi dan pengujian ke dalam skenario simulasi akhir. Data hasil pengujian dianalisis untuk menilai efektivitas penerapan SD-WAN dalam meningkatkan keandalan jaringan internal.

#### 4. HASIL DAN PEMBAHASAN

Penelitian ini menghasilkan rancangan dan simulasi implementasi fitur automatic failover berbasis SD-WAN pada perangkat FortiGate yang digunakan untuk meningkatkan keandalan koneksi internet di lingkungan internal PT PLN Icon Plus Gandul. Topologi yang diuji terdiri dari dua jalur koneksi internet yang terhubung ke satu perangkat FortiGate. Jalur pertama berfungsi sebagai link utama (primary), sedangkan jalur kedua sebagai link cadangan (backup). Pengujian dilakukan melalui simulasi pada PNETLab, dengan memantau parameter latency, packet loss, dan waktu perpindahan (failover time) saat koneksi utama mengalami gangguan.

Hasil pengujian menunjukkan bahwa ketika koneksi utama mengalami timeout atau packet loss melebihi ambang batas yang ditentukan, sistem secara otomatis mengalihkan trafik ke koneksi cadangan. Proses ini berlangsung dalam waktu singkat tanpa memutuskan sesi komunikasi yang sedang berjalan, sehingga memastikan ketersediaan layanan tetap stabil.

Berikut ini adalah dokumentasi konfigurasi yang diterapkan pada perangkat FortiGate untuk mendukung implementasi SD-WAN. Konfigurasi Alamat dan Antarmuka, Implementasi Failover menggunakan Software-Defined Wide Area Network (SD-WAN) pada perangkat FortiGate menunjukkan efektivitas tinggi dalam menjaga kontinuitas layanan jaringan. Berdasarkan pengujian, sistem mampu melakukan failover otomatis pada dua kondisi: ketika jalur utama terputus dan ketika kualitas koneksi menurun signifikan. Pada kedua skenario, perpindahan trafik ke jalur cadangan terjadi dalam waktu kurang dari

lima detik tanpa gangguan yang terasa oleh pengguna.

Keberhasilan ini didukung oleh penerapan strategi Best Quality, yang secara dinamis memilih jalur terbaik berdasarkan parameter latency dan packet loss. Ketika performa link utama menurun di bawah ambang batas, sistem secara otomatis mengalihkan trafik untuk mempertahankan kualitas koneksi. Mekanisme ini memungkinkan peningkatan keandalan dan ketersediaan jaringan tanpa memerlukan intervensi manual dari administrator.

Dibandingkan metode konvensional seperti manual failover atau static routing, pendekatan berbasis SD-WAN lebih adaptif terhadap perubahan kondisi jaringan. Kemampuan pemantauan dan pengambilan keputusan secara real-time menjadikan sistem lebih responsif terhadap gangguan, sekaligus meningkatkan stabilitas jaringan internal di PT PLN Icon Plus Gandul.

Hasil penelitian ini memiliki implikasi praktis dalam pengelolaan jaringan perusahaan, khususnya bagi organisasi yang mengandalkan koneksi internet untuk aktivitas operasional. Penerapan fitur automatic failover berbasis SD-WAN dapat menjadi solusi efektif dan efisien untuk mengurangi dampak gangguan jaringan tanpa perlu intervensi manual.

Selain itu, hasil penelitian ini juga memberikan kontribusi akademik berupa pembuktian empiris bahwa SD-WAN mampu meningkatkan keandalan jaringan, sehingga dapat menjadi referensi untuk pengembangan sistem serupa di lingkungan yang lebih kompleks.

Penelitian ini hanya berfokus pada penerapan fitur automatic failover SD-WAN di perangkat FortiGate, tanpa melibatkan konfigurasi IPsec VPN, manajemen keamanan, atau pengujian pada jaringan nyata. Selain itu, pengujian dilakukan pada lingkungan virtual PNETLab, sehingga hasil yang diperoleh mungkin sedikit berbeda dari kondisi jaringan produksi sesungguhnya. Keterbatasan ini diharapkan dapat menjadi dasar untuk penelitian selanjutnya yang dapat menguji kinerja SD-WAN secara langsung di lingkungan operasional dengan parameter yang lebih luas.

#### 5. KESIMPULAN DAN SARAN

Berdasarkan hasil implementasi dan pengujian teknologi Failover menggunakan SD-WAN pada Subbidang Router dan Security di PT PLN Icon Plus Gandul, dapat disimpulkan hal-hal sebagai berikut:

Sebelum penerapan SD-WAN, jaringan internal hanya menggunakan satu jalur koneksi (single link) tanpa mekanisme manajemen trafik yang adaptif. Kondisi ini menyebabkan keterbatasan dalam hal keandalan dan fleksibilitas koneksi, terutama ketika terjadi gangguan pada link utama. Strategi Best Quality digunakan sebagai metode utama dalam pengaturan routing. Strategi ini secara otomatis memilih jalur dengan kualitas terbaik

berdasarkan parameter seperti latency dan packet loss, sehingga meningkatkan keandalan konektivitas. Selain strategi Best Quality, SD-WAN juga menyediakan opsi strategi lain seperti Lowest Cost, Maximize Bandwidth, dan Manual. Ketiga strategi tersebut tidak diterapkan pada penelitian ini, namun dapat digunakan sesuai kebutuhan tertentu seperti efisiensi biaya, pemanfaatan seluruh link, atau pengaturan jalur tetap. Hasil pengujian menunjukkan bahwa penerapan strategi Best Quality mampu menjaga kestabilan koneksi dan menjalankan mekanisme automatic failover secara efektif saat terjadi gangguan pada jalur utama, sehingga meminimalkan potensi downtime jaringan. Implementasi SD-WAN juga memberikan kemudahan dalam pemantauan trafik secara real-time, manajemen kebijakan routing yang lebih fleksibel, serta efisiensi dalam operasional jaringan. Hal ini memberikan nilai tambah bagi pengelolaan infrastruktur jaringan internal secara keseluruhan

#### DAFTAR PUSTAKA

- [1] G. W. Heriaji, S. A. Karimah, and S. A. Mugitama, "Perbandingan Performansi Routing pada Multiprotocol Label Switching (MPLS) dan Software-Defined Wide Area Network (SDWAN)," *eProceedings Eng.*, vol. 10, no. 3, 2023, [Online]. Available: <https://openlibrarypublications.telkomuniversi ty.ac.id/index.php/engineering/id/article/view/20633>
- [2] L. M. Silalahi, V. Amaada, and S. Budiyo, "Implementation of auto failover on SD-WAN technology with BGP routing method on Fortigate routers at XYZ company," *Int. J. Electron. Telecommun.*, vol. 70, no. 1, pp. 5–11, 2024, doi: 10.24425/ijet.2024.149540.
- [3] A. V. S. Putra, L. V. Yovita, and L. Hafiza, "Implementasi Fortigate Sd-Wan Menggunakan Link Astinet dan VPN IPsec pada Perusahaan FIF," *eProceedings Eng.*, vol. 11, no. 6, 2024, [Online]. Available: <https://openlibrarypublications.telkomuniversi ty.ac.id/index.php/engineering/article/view/24676/23644>
- [4] C. Fu, B. Wang, and W. Wang, "Software-Defined Wide Area Networks (SD-WANs): A Survey," *Electron.*, vol. 13, no. 15, 2024, doi: 10.3390/electronics13153011.
- [5] D. Bahtiar, D., Febrianto, W. J., Maulana, A., Saputra, S. and R. W., Tafonao, R. P., Julianto, R., Zai, R., & Djutalov, *Pengenalan Dasar Instalasi Jaringan Komputer Menggunakan Mikrotik*. 2021.
- [6] Desmira, D. Apriana, and M. A. H.B.H, "Analisa Jaringan Local Area Network Pada Laboratorium Komputer SMK Informatika Kota Serang," *Insa. – J. Inov. dan Sains Tek. Elektro*, vol. 3, no. 1, pp. 23–31, 2022, doi: <https://doi.org/10.31294/instk.v3i1.532>.
- [7] T. Mardianto, A. Fitrianyah, A. Nugroho, and P. A. Nugroho, "Optimalisasi Layanan Bandwidth Internet Menggunakan Teknologi Sd (Software Defined)-Wan," *J. ELEKTRO Inform. SWADHARMA*, vol. 4, no. 2, pp. 66–79, 2024, doi: <https://doi.org/10.56486/jeis.vol4no2.474>.
- [8] S. Hidayat and Y. Akbar, "IMPLEMENTASI FAILOVER VPN KANTOR PUSAT DAN CABANG MENGGUNAKAN TEKNOLOGI SDWAN DENGAN STRATEGI BEST QUALITY," *J. Indones. Manaj. Inform. dan Komun.*, vol. 4, no. 3, pp. 1598–1608, 2023, doi: <https://doi.org/10.35870/jimik.v4i3.386>.
- [9] M. Fikri and M. Rifqi, "Implementasi VPN Antar Cabang Menggunakan Teknologi SDWAN dengan Metode Load Balance (Studi Kasus: PT. Mitra Solusi Infokom)," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 10, no. 1, pp. 105–114, 2023, doi: 10.25126/jtiik.2023105236.
- [10] R. Aury Murya, M. Hadi Arfian, N. Anwar, and I. Sutanto, "Implementasi VPN Antar Cabang Menggunakan Teknologi SDWAN Fortigate Dengan Metode Load Balance," *IKRAITH-INFORMATIKA*, vol. 9, no. 1, pp. 164–169, 2025, doi: 10.37817/ikraith-informatika.v9i1.
- [11] A. D. N. Fauziah, H. Nirwana, A. Litha, and I. Mahjud, "Analisis Penerapan Teknologi Traffic Steering SD-WAN Menggunakan Perangkat Forti Gate," *J. Teknol. Elekterika*, vol. 19, no. 2, pp. 97–105, 2022, doi: <http://dx.doi.org/10.31963/elekterika.v6i2.3478>.
- [12] C. Rizal, Supiyandi, M. Zen, and M. Eka, "Perancangan Server Kantor Desa Tomuan Holbung Berbasis Client Server," *Bull. Inf. Technol.*, vol. 3, no. 1, pp. 27–33, 2022, doi: 10.47065/bit.v3i1.255.
- [13] M. B. Yel, D. I. Mulyana, J. R. F. D. Nurfaishal, and M. H. T. B, "Optimalisasi Keamanan Firewall Pada Infrastruktur Jaringan Smk Idn Bogor," *J. Cahaya Mandalika*, vol. 4, no. 1, pp. 594–610, 2023, doi: <https://doi.org/10.36312/jcm.v4i1.1393>.
- [14] M. Alfaujianto, F. Muttaqi, and N. Badriah, "Analisis Perbandingan Multi-Protocol Label Switching (MPLS) dan Software-Defined WAN (SD-WAN) sebagai Solusi Jaringan dalam Meningkatkan Optimasi Kinerja Jaringan untuk Digitalisasi Bisnis," *Intech*, vol. 6, no. 1, pp. 83–93, 2025, doi: 10.54895/intech.v6i1.3028.
- [15] D. B. Radityo and A. Rustianto, "Peningkatan Efisiensi Jaringan Internet Menggunakan Firewall Fortigate Studi Kasus: PT. Jarvis Integrasi Solusi," *DBESTI J. Digit. Bus. Technol. Innov.*, vol. 2, no. 1, pp. 96–102, 2025, doi: 10.54914/dbesti.v2i1.1695.
- [16] H. Ramdani, T. Budiman, A. Z. Sianipar, I.

- Riris, R. Hartawan, and I. Junaedi, "Analisis Penerapan Sistem Keamanan Software Defined Wide Area Networking (Sd-Wan) Pada Kantor Direktorat Jenderal Pajak," *Zo. J. Sist. Inf.*, vol. 7, no. 2, pp. 611–623, 2025, doi: <https://doi.org/10.31849/2vw4wx41>.
- [17] B. H. Khofifah, "PERANCANGAN ARSITEKTUR JARINGAN HYBRID BERBASIS VIRTUAL ROUTER DAN TEKNOLOGI SD- WAN UNTUK OPTIMALISASI KONEKSI MULTI-," *Semin. Nas. CORISINDO*, no. September 2025, pp. 457–463, 2025, doi: <https://doi.org/10.30812/corisindo.v1.5539>.
- [18] Jeperson, Irvan, and A. Syamsumar, "IMPLEMENTASI LTE BACKUP FAILOVER DENGAN METODE LAST RESORT CIRCUIT PADA TEKNOLOGI CISCO SD-WAN," *J. Inf. dan Komput.*, vol. 13, no. 2, pp. 100–104, 2025, doi: <https://doi.org/10.35959/jik.v13i02.752>.
- [19] M. Muchlisin and B. Yuliadi, "Improving Network Performance of Headquarters and Branches Using Software-Defined Network WAN (SD-WAN)," *PIKSEL Penelit. Ilmu Komput. Sist. Embed. Log.*, vol. 12, no. 1, pp. 23–34, 2024, doi: [10.33558/piksel.v12i1.8115](https://doi.org/10.33558/piksel.v12i1.8115).
- [20] N. R. Fattahilah, F. Nurfadila, and Y. Setiawan, "High Availability's Implementation on the Fortigate Firewall Using SD-WAN Zone and HA Cluster Active-Passive," *Indones. J. Multidiscip. Sci.*, vol. 2, no. 11, pp. 3937–3952, 2023, doi: [10.55324/ijoms.v2i11.622](https://doi.org/10.55324/ijoms.v2i11.622).
- [21] Santoso and B. J. Bagono, "Optimalisasi Jaringan Wide Area Network Menggunakan Software Defined Network Viptela," *J. Sibernetika*, vol. 7, no. 2, pp. 49–61, 2022, [Online]. Available: <https://jurnas.saintekmu.ac.id/index.php/siber-netika/id/article/view/6>
- [22] Andre, C. A. N. Saputra, S. Hanief3, and I. M. A. Santosa, "Implementasi Failover Link Backup VPN Menggunakan Fortinet Untuk ATM Pada PT. Aplikanusa Lintasarta Denpasar," *Pros. Semin. Has. Penelit. Inform. dan Komput.* 2025, vol. 2, no. 1, pp. 709–714, 2025, [Online]. Available: <https://spinter.stikom-bali.ac.id/index.php/spinter/article/view/763>
- [23] Haeruddin, S. E. Prasetyo, and Sugianto, "ANALISIS PERBANDINGAN QOS PFSENSE, OPNSENSE, DAN FLEXIWAN MENGGUNAKAN METODE LOAD BALANCING," *J. Inf. Syst. Manag.*, vol. 6, no. 2, pp. 179–186, 2025, doi: <https://doi.org/10.24076/joism.2025v6i2.1984>.
- [24] R. Almakhi, A. Anton, and F. S. Nugraha, "Implementasi Load Balancing Dan Failover Menggunakan IP SLA Pada PT Pan Pacific Insurance," *J. Infortech*, vol. 4, no. 2, 2022, doi: <https://doi.org/10.31294/infortech.v4i2.13614>. g5719.
- [25] "PNETLab." [Online]. Available: <https://pnetlab.com/pages/documentation?slug=what-is-PNETlab>
- [26] "FortiOS." [Online]. Available: <https://www.fortinet.com/corporate/about-us/about-us>