P-ISSN :2580-4316
E-ISSN :2654-8054
10.37817/ikraith-informatika.v9i1

Implementasi VPN Antar Cabang Menggunakan Teknologi SDWAN Fortigate Dengan Metode Load Balance

Rizky Aury Murya[1], Muhamad Hadi Arfian[2], Nizirwan Anwar[3], Imam Sutanto[4]
Program Studi Teknik Informatika Fakultas Ilmu Komputer Universitas Esa Unggul

ABSTRAK

Penelitian ini mengkaji implementasi ***VPN* antar cabang** menggunakan teknologi ***SDWAN* Fortigate** dengan metode ***Loadbalance***. Dalam era digital, konektivitas yang andal dan aman antar cabang perusahaan menjadi sangat penting. *SDWAN* menawarkan solusi jaringan yang fleksibel, efisien, dan terpusat. Penelitian ini bertujuan mengevaluasi kinerja dan keamanan *VPN* menggunakan Fortigate serta menganalisis efektivitas metode *Loadbalance* dalam distribusi lalu lintas jaringan. Hasil implementasi menunjukkan bahwa ***SDWAN* Fortigate dengan *Loadbalance*** dapat meningkatkan keandalan dan efisiensi jaringan, mengurangi latensi, serta mengoptimalkan sumber daya jaringan. Pengujian melalui simulasi dan pengamatan langsung menguatkan kesimpulan ini. Penelitian ini memberikan solusi yang signifikan bagi perusahaan yang memerlukan konektivitas yang handal dan scalable antar cabang.

Kata kunci : ***SDWAN*, Load Balance, *VPN***

ABSTRACT

This research explores the implementation of ***VPN* between branches** using Fortigate's ***SDWAN* technology** with the ***Loadbalance* method**. In the digital era, reliable and secure connectivity between company branches is crucial. *SDWAN* technology provides an efficient solution with flexible and centralized network management.The study evaluates the **performance and security** of *VPN* implemented with Fortigate devices and examines the effectiveness of *Loadbalance* in optimizing network traffic distribution. Results indicate that **Fortigate *SDWAN* with *Loadbalance*** enhances network reliability, reduces latency, and optimizes resource utilization. Testing was conducted through simulation and direct observation, highlighting its contribution as a scalable and reliable connectivity solution for companies***Please write the***

Keyword : ***SDWAN*, Load Balance, *VPN***

1. PENDAHULUAN

Penggunaan jaringan privat virtual (VPN) telah menjadi semakin penting dalam beberapa tahun terakhir karena bisnis dan organisasi berupaya mengamankan komunikasi mereka dan melindungi data sensitif. Penggunaan Jaringan Privat Virtual (VPN) memang menjadi krusial bagi bisnis dan organisasi untuk mengamankan komunikasi mereka

dan melindungi data sensitif, terutama dalam konteks kerja jarak jauh dan perluasan infrastruktur digital. Teknologi ini telah merevolusi komunikasi bisnis dengan memungkinkan perusahaan untuk berkomunikasi dengan aman melalui infrastruktur jaringan publik, seperti Internet, yang menghasilkan penghematan biaya yang signifikan dibandingkan dengan menerapkan tautan privat ke kantor cabang dan mitra

Seiring dengan terus berkembangnya pekerjaan jarak jauh, pentingnya VPN dalam mengamankan jaringan perusahaan dan melindungi data sensitif kemungkinan akan semakin meningkat (Coro, 2024; Rah, 2024).

2. METODOLOGI

SDWAN Fortigate

SD-WAN Fortigate adalah solusi konektivitas modern yang menawarkan fleksibilitas, keamanan, dan efisiensi untuk perusahaan. Teknologi ini menggabungkan pendekatan **Software-Defined** dengan perangkat keras yang aman untuk mendukung aplikasi penting dan komunikasi antar cabang secara optimal.

Keunggulan SD-WAN Fortigate:

1. **Optimasi Aplikasi**
2. **Pemanfaatan Multi-WAN**
3. **Keamanan Terpadu**
4. **Visibilitas dan Kontrol Terpusat**
5. **Implementasi Mudah**

Dengan kemampuan ini, SD-WAN Fortigate memastikan jaringan perusahaan berjalan optimal, aman, dan mudah dikelola.

Kekurangan SD-WAN Fortigate

1. Kompleksitas Konfigurasi
2. Ketergantungan pada Internet
3. Keamanan
4. Biaya
5. Troubleshooting

Integrasi VPN dan SD-WAN Fortigate

Fortigate mengintegrasikan VPN dengan SD-WAN untuk solusi konektivitas yang aman dan efisien:

1. Keamanan Terpadu
2. Optimasi Performa
3. Fleksibilitas dan Skalabilitas

Komponen dan Konfigurasi VPN di SD-WAN Fortigate

1. Komponen Utama:
    - FortiGate Firewall (keamanan dan routing).
    - Jaringan SD-WAN (konektivitas cabang).
    - Load Balancing (distribusi lalu lintas).
    - Dashboard Monitoring (pantauan performa).
2. Langkah Konfigurasi:
    - Persiapan: Pastikan koneksi internet dan kredensial VPN tersedia.
    - Pengaturan VPN: Pilih tipe VPN (IPsec/SSL) dan atur keamanan.
    - Pengujian Koneksi: Verifikasi koneksi dan uji stabilitas.

Dengan fitur-fitur tersebut, SD-WAN Fortigate menjadi solusi unggulan untuk konektivitas jaringan modern yang aman, efisien, dan fleksibel.

2.2 Implementasi SDWAN

SD-WAN Fortigate bertindak sebagai pengelola cerdas berbagai jenis koneksi internet (fiber optic, coaxial, seluler), mengenali aplikasi, memprioritaskan aplikasi kritis seperti kasir, dan mengarahkan trafik ke jalur koneksi terbaik. Jika koneksi utama gagal, Fortigate otomatis mengalihkan trafik ke jalur cadangan untuk menjaga kelancaran operasional. Fitur VPN terintegrasi memastikan keamanan setiap koneksi antar cabang dengan enkripsi data, melindungi informasi dari ancaman siber.

Skenario Penggunaan Load Balancing

1. Koneksi Terputus:
2. Peningkatan Trafik
3. Pemeliharaan Terjadwal
4. Kegagalan Perangkat.

Dengan kemampuan ini, SD-WAN Fortigate mendukung kebutuhan operasional perusahaan retail secara efisien, aman, dan andal

3. HASIL DAN PEMBAHASAN

3.1.1 Pengertian Fortigate

Fortigate adalah sistem keamanan yang dikembangkan oleh Fortinet, perusahaan penyedia layanan keamanan jaringan global. Fortinet melayani perusahaan, instansi pemerintah, dan organisasi di seluruh dunia, termasuk mayoritas perusahaan dalam daftar Fortune Global 100 tahun 2009. Fortinet memimpin pasar dalam solusi Unified Threat Management (UTM), yang menyatukan berbagai fungsi keamanan dalam satu perangkat terpadu. Produk UTM Fortinet ini melahirkan Fortigate, solusi yang menggabungkan fitur seperti firewall, intrusion prevention system, web filtering, antivirus, serta fungsi jaringan tambahan seperti routing, menjadikannya solusi serbaguna untuk keamanan dan manajemen jaringan [18]

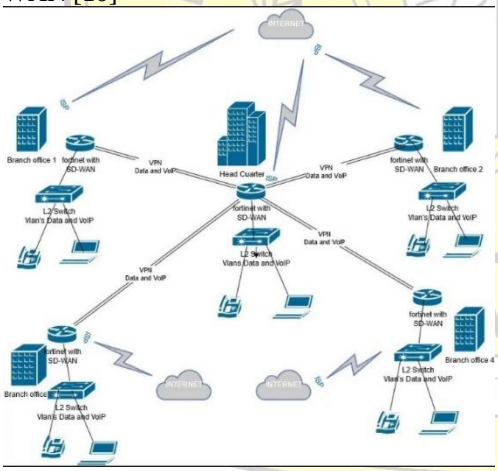
P-ISSN :2580-4316
E-ISSN :2654-8054
10.37817/ikraith-informatika.v9i1

Gambar 1 Firewall Fortigate

3.1.2 Konsep Dasar VPN

VPN (Virtual Private Network) adalah teknologi yang memungkinkan pembuatan koneksi jaringan pribadi (private) melalui jaringan publik, seperti internet. VPN menciptakan ‘‘terowongan‘‘ aman yang mengenkripsi data yang ditransmisikan, sehingga menjaga kerahasiaan dan integritas data meskipun melewati jaringan publik yang tidak aman. Dalam konteks implementasi VPN antar cabang (gambar 3) menggunakan teknologi SD-WAN Fortigate dengan metode load balance, VPN berperan penting dalam menjamin keamanan komunikasi antar cabang. Cara Kerja VPN [17]

Manfaat VPN dalam Implementasi SD-WAN [10]



Gambar 2 Arsitektur VPN SD-WAN

3.1.3 Teknologi SDWAN Fortigate

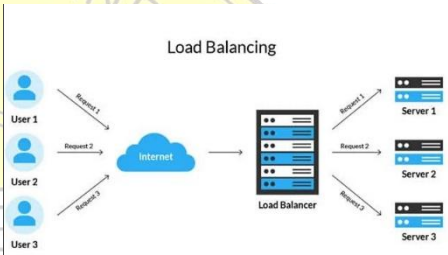
Pada masa sebelumnya, koneksi jaringan sering kali bergantung pada teknologi *WAN* tradisional seperti Multiprotocol Label *Switch*ing (*MPLS*) yang memiliki biaya tinggi dan fleksibilitas terbatas. Dengan kemajuan teknologi, implementasi *Software*-Defined Wide Area Network (*SD-WAN*) Fortigate menawarkan solusi jaringan yang lebih modern, efisien, dan fleksibel.[18]

Teknologi *SD-WAN* Fortigate berfungsi sebagai pengelola lalu lintas data yang cerdas, memungkinkan pemanfaatan berbagai jenis koneksi internet di setiap cabang, seperti fiber optic, kabel coaxial, atau koneksi seluler. Berikut adalah Manfaat Implementasi *SD-WAN* Fortigate dan perbandingan dengan *WAN* tradisional :

WAN Tradisional	*SD-WAN*
Arsitektur: *WAN* tradisional menggunakan infrastruktur yang lebih rumit, terutama perangkat keras seperti router dan *switch*, yang membutuhkan waktu dan biaya yang lebih banyak untuk diinstalasi dan dikonfigurasi.	Arsitektur: *SD-WAN* menggunakan arsitektur *WAN* virtual yang didorong oleh perangkat lunak, yang memungkinkan kontrol dan pengelolaan jaringan secara mudah dan efisien
Kontrol Jaringan: Jaringan ini memiliki kontrol yang terdistribusi, yang membuat pelaporan dan pemecahan masalah menjadi lebih sulit	Kontrol Jaringan: Kontrol jaringan terpusat, yang membuat pelaporan dan pemecahan masalah menjadi lebih mudah
Konfigurasi: Konfigurasi manual membutuhkan waktu yang lebih banyak dan memerlukan tenaga untuk onsite	Konfigurasi: Konfigurasi jaringan dapat dilakukan dengan mudah dan cepat melalui antarmuka pengguna yang intuitif
Biaya: Biaya yang diperlukan untuk membangun dan memelihara jaringan ini lebih tinggi	Biaya: Biaya relatif lebih terjangkau dan lebih efisien dalam hal biaya pemeliharaan

Tabel 1 Perbandingan WAN dan SDWAN

Load Balance



Gambar 3 Load Balancing

Load Balancing adalah teknik mendistribusikan trafik jaringan ke beberapa jalur koneksi untuk mengoptimalkan penggunaan *bandwidth*, meningkatkan kinerja, dan menjamin ketersediaan layanan. Dalam konteks *SD-WAN* Fortigate, *Load Balancing* memungkinkan perusahaan untuk memanfaatkan beberapa koneksi *WAN* secara efisien, baik itu koneksi internet, *MPLS*, atau lainnya. [18]

1.1.1 Metode Load Balancing SD-WAN Rules

Fitur "SD-WAN Rules" pada Fortigate adalah kunci untuk mengimplementasikan Load Balancing dan optimasi WAN. Dengan fitur ini, dapat membuat aturan yang cerdas untuk mengarahkan trafik melalui jalur WAN terbaik berdasarkan kriteria yang telah ditentukan.

Berikut penjelasan lebih lanjut tentang implementasi Load Balancing di Fortigate menggunakan "SD-WAN Rules":

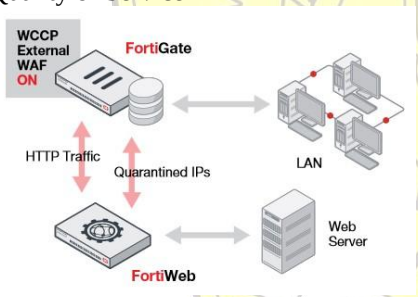
Berikut adalah tata cara implementasi Load Balancing di Fortigate menggunakan fitur "SD-WAN Rules":

1. **Akses Menu SD-WAN Rules**:
   - Masuk ke antarmuka Fortigate.
   - Navigasi ke *Network* > *SD-WAN*.
   - Pilih tab *SD-WAN Rules*.
2. **Membuat Aturan Baru**:

- Klik *Create New*.
- Berikan nama aturan yang mudah diidentifikasi.

3. **Menentukan Kriteria Pemilihan Jalur**:
   - Tentukan *Source/Destination* (alamat IP, subnet, atau grup).
   - Tentukan jenis *Service* (HTTP, HTTPS, DNS, FTP).
   - Tentukan *Performance SLA* (latency, jitter, packet loss) untuk memilih jalur terbaik.
   - Tentukan *Health Check* (ping, TCP, HTTP request) untuk memantau status koneksi WAN.
4. **Mengatur Metode Load Balancing**:
   - *Manual Weight*: Berikan bobot pada jalur berdasarkan prioritas.
   - *Volume-Based*: Trafik didistribusikan berdasarkan beban jalur.
   - *Quality-Based*: Pilih jalur dengan kualitas terbaik berdasarkan SLA.
   - *Session-Based*: Setiap sesi dialokasikan ke jalur WAN secara bergantian.
5. **Menerapkan Aturan**:
   - Klik *OK* untuk menyimpan aturan.

Quality of Service



Gambar 4 Implementasi QoS

Quality of Service (QoS) berperan sebagai pengatur lalu lintas jaringan, memastikan aplikasi penting seperti video conference dan VoIP mendapat prioritas untuk menjaga kelancaran dan stabilitas layanan.[18] Dalam implementasi Load Balancing, Fortigate menggunakan beberapa langkah untuk mengoptimalkan QoS:

1. **Identifikasi dan Klasifikasi**: Fortigate mengenali aplikasi berdasarkan port, protokol, atau isi data.
2. **Penentuan Prioritas**: Aplikasi kritis seperti VoIP atau transaksi keuangan mendapat prioritas tinggi.
3. **Pengaturan Bandwidth**: Bandwidth dialokasikan khusus untuk aplikasi penting, mencegah gangguan dari aplikasi lain.
4. **Antrian Trafik**: Fortigate mengelola lonjakan trafik dengan mengutamakan aplikasi prioritas di antrian.

3.1.5.1 Latency

Latency atau delay merupakan waktu yang dibutuhkan oleh data untuk berpindah dari sumber ke tujuan. Latency dipengaruhi oleh beberapa faktor, di antaranya media fisik yang digunakan, perangkat yang terlibat, jarak antara sumber dan tujuan, serta waktu proses data tersebut [19].

Delay (ms)	Deskripsi *Latency*
< 150 ms	Sangat Bagus
150 - 300 ms	Bagus
300 - 450 ms	Normal
> 450 ms	Buruk

Tabel 1 Tabel Latency

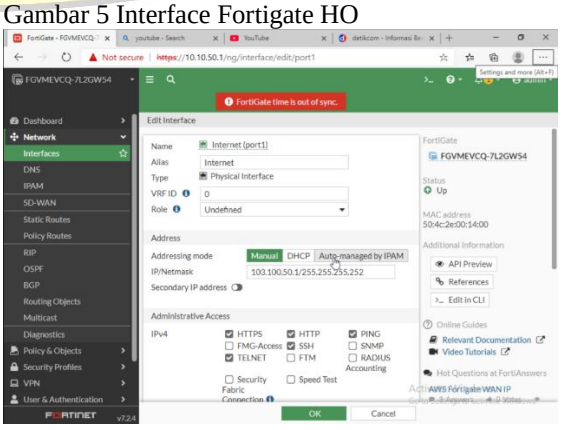
Konfigurasi Jaringan

Pada penilitian ini, Fortigate KVM digunakan sebagai sumber internet (*Internet Gateway*), Konfigurasi *IP interface, static route, NAT (Network Address Translation), firewall policy dan pengoperasian teknologi SDWAN (Load balance).*

3.2.3 Konfigurasi Interface Fortigate HO

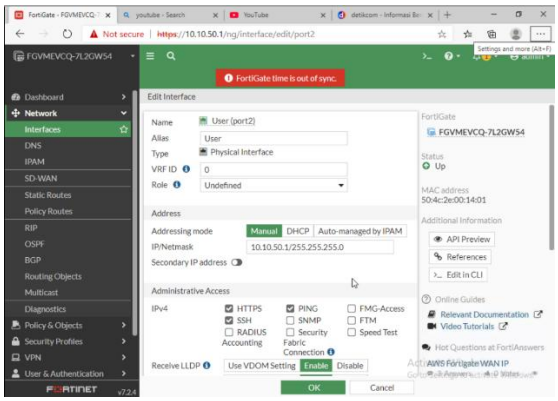
Gambar dibawah ini mendefinisikan *port-port* yang akan digunakan di *fortigate* HO serta konfigurasi *IP address* yang dipakai pada saat implementasi.

Gambar 5 Interface Fortigate HO

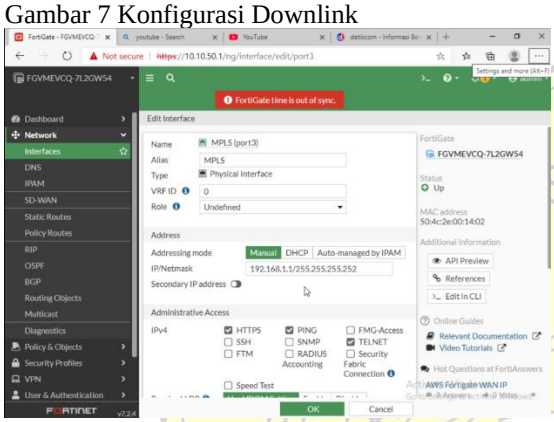


Gambar 6 Konfigurasi Port Internet

P-ISSN :2580-4316
E-ISSN :2654-8054
10.37817/ikraith-informatika.v9i1



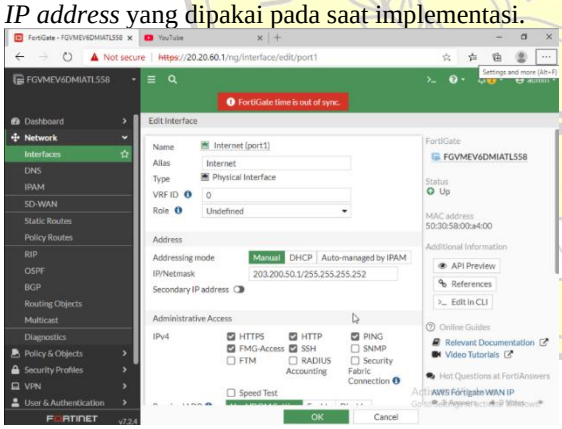
Gambar 7 Konfigurasi Downlink



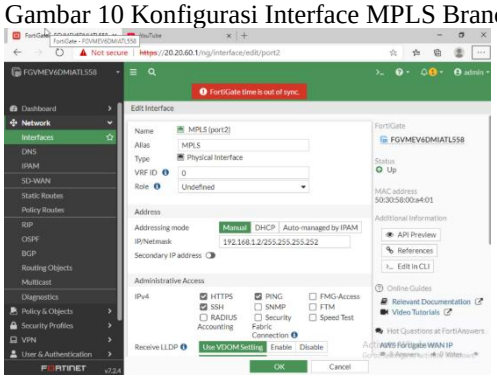
Gambar 8 Konfigurasi Interface MPLS

3.1.4 Konfigurasi Interface Fortigate Branch

Gambar dibawah ini mendefinisikan *port-port* yang akan digunakan di *fortigate* Branch serta konfigurasi *IP address* yang dipakai pada saat implementasi.



Gambar 10 Konfigurasi Interface MPLS Branch



Gambar 9 Konfigurasi Interface MPLS Branch

4. KESIMPULAN

Implementasi SD-WAN Fortigate dengan metode Load Balance meningkatkan efisiensi dan keandalan jaringan antar cabang. Teknologi ini mengoptimalkan distribusi lalu lintas melalui jalur WAN yang tersedia, menjaga stabilitas koneksi, dan melindungi data dengan enkripsi IPsec. Dengan fitur Performance SLA, pengalihan trafik secara dinamis memastikan kinerja aplikasi bisnis tetap optimal. Selain itu, SD-WAN Fortigate mendukung skalabilitas, memudahkan penambahan cabang baru, dan integrasi koneksi tanpa mengorbankan performa maupun keamanan

DAFTAR PUSTAKA

[1] H. Suryantoro, A. Sopian, and D. Dartono, “PENERAPAN TEKNOLOGI FORTIGATE DALAM PEMBANGUNAN JARINGAN VPN-IP BERBASIS IPSEC,” JEIS: JURNAL ELEKTRO DAN INFORMATIKA SWADHARMA, vol. 1, no. 1, pp. 1–7, Jan. 2021, doi:10.56486/jeis.vol1no1.64.

[2] S. Hidayat and Y. Akbar, “IMPLEMENTASI FAILOVER VPN KANTOR PUSAT DAN CABANG MENGGUNAKAN TEKNOLOGI SDWAN DENGAN STRATEGI BEST QUALITY,” Jurnal Indonesia : Manajemen Informatika dan Komunikasi, vol. 4, no. 3, pp. 1598–1608, Sep. 2023, doi: 10.35870/jimik.v4i3.386.

[3] K. G. Yalda, N. Tapus, and D. J. Hamad, “A survey on Software-defined Wide Area Network (SD- WAN) architectures,” Jun. 2022. doi: 10.1109/hora55278.2022.9799862.

[4] L. M. Silalahi, V. Amaada, A. D. Rochendi, S. Budiyanto, and I. U. V. Simanjuntak, “Implementation of auto failover on SD-WAN technology with BGP routing method on Fortigate routers at XYZ company,” International Journal of Electronics and Telecommunications, pp. 5– 11, Mar. 2024, doi: 10.24425/ijet.2024.149540.

[5] A. Awasthi, “SDWAN (Software Defined-WAN) Network Engineering and Project Management,” Semiconductor Science and Information Devices, vol. 2, no. 1, pp. 17–28, May 2020, doi: 10.30564/ssid.v2i1.1870..

[6] S. Narayan, S. De Vere, S. S. Kolahi, and K. Brooking, “Performance Evaluation of Virtual Private Network Protocols in Windows 2003 Environment,” Dec. 2008. doi: 10.1109/icacte.2008.187.

[7] J. R. Bustamante and D. Avila-Pesantez, “Comparative analysis of Cybersecurity mechanisms in SD-WAN architectures: A preliminary results,” Oct. 2021, vol. 3, pp. 1–4. doi: 10.1109/eircon52903.2021.9613418.

[8] M. B. Coro, “Information security in remote work: Strategies and challenges in a post-pandemic

P-ISSN :2580-4316
E-ISSN :2654-8054

world," Revista Sistemática, vol. 14, no. 4, pp. 995–999, Sep. 2024, doi: 10.56238/rcsv14n4-020.
[9] A. Rah, "The use of Virtual Private Network in the Context of 'Bring Your Own Device' in the Post Covid-19 Remote Workplace," International Journal of Computational Science, Information Technology and Control Engineering, vol. 11, no. 1/2, pp. 01–08, Apr. 2024, doi: 10.5121/ijcsitce.2024.11201.
[10] S. Murthy Pedapudi and N. Vadlamani, "A Comprehensive Network Security Management in Virtual Private Network Environment," May 2022. doi: 10.1109/icaaic53929.2022.9793196.
[11] M. Elezi and B. Raufi, "Conception of Virtual Private Networks Using IPsec Suite of Protocols, Comparative Analysis of Distributed Database Queries Using Different IPsec Modes of Encryption," Procedia - Social and Behavioral Sciences, vol. 195, pp. 1938–1948, Jul. 2015, doi: 10.1016/j.sbspro.2015.06.206.
[12] R. S. Kagan, "Virtual private networks-new strategies for secure enterprise networking," Sep. 1998. doi: 10.1109/wescon.1998.716461.
[13] J. S. Tiller, "Security of Virtual Private Networks," Information Systems Security, vol. 10, no. 1, pp. 1–19, Mar. 2001, doi: 10.1201/1086/43313.10.1.20010304/31393.5.
[14] J. M. Schneider, T. Preuß, and P. S. Nielsen, "Management of virtual private networks for integrated broadband communication," ACM SIGCOMM Computer Communication Review, vol. 23, no. 4, pp. 224–237, Oct. 1993, doi: 10.1145/167954.166259.
[15] Al-Sharafi, M. A., Al-Habsi, S. H., & Al-Harrasi, S. S. (2020). Performance analysis of SD- WAN technology for enhancing enterprise network connectivity. International Journal of Information Technology and Computer Science (IJITCS), 12(1), 70-78. DOI: 10.5815/ijitcs.2020.01.07
[16] Fadhil, A., & Ma'arif, A. (2021). Implementation of SD-WAN technology in improving network performance and security. Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK), 8(2), 397-404. DOI: 10.25126/jtiik.202182.1034
[17] Nugroho, A. S., & Prasetyo, E. (2022). Analysis of SD-WAN Fortigate implementation for optimizing branch office network connectivity. Jurnal Sistem Informasi (JSI), 14(1), 1-8. DOI: 10.21609/jsi.v14i1.847
[18] Andrew, M. F. W., & W. F. (2019). Penerapan Firewall Menggunakan Fortigate di PT. PLN Rayon Taman Sidoarjo. Jurnal Sistem Informasi (JSI) 7(2), 1-7. DOI: 10.559/ijitcs.2019
[19] R. Wulandari, "ANALISIS QoS (QUALITY OF SERVICE) PADA JARINGAN INTERNET (STUDI KASUS : UPT LOKA UJI TEKNIK PENAMBANGAN JAMPANG KULON – LIPI)," J. Tek. Inform. dan Sist. Inf., vol. 2, no. 2, pp. 162–172, 2016, doi: 10.28932/jutisi.v2i2.454
[20] E. R. Huddiniah, E. M. Safitri, S. A. Priyambada, M. Nasrullah, and N. D. Angresti, "Optimasi Rute Untuk Software Defined Networking-Wide Area Network (SDN-WAN) Dengan Openflow Protocol," Inform. Mulawarma, J. Ilm. Ilmu Komput., vol. 13, no. 1, p. 7, 2018, doi:10.30872/jim.v13i1.1006.