Jurnal Sistem Komputer dan Informatika (JSON)
Volume 7, Nomor 1, September 2025
e-ISSN 2685-998X
DOI : 10.30865/json.v7i1.9012

SD-WAN SLA Optimization Using Fortigate NGFW Firewall Policy: A Case Study of XYZ Institution

Abdul Rahim, Denar Regata Akbi*
Department of Informatics Engineering, Faculty of Engineering, University of Muhammadiyah Malang, Indonesia
Email: [1]abdulrhm2043@gmail.com, [2,*] dnarregata@umm.ac.id
Correspondence Author Email: dnarregata@umm.ac.id*
Submitted: **10/08/2025**; Accepted: **02/09/2025**; Published: **08/09/2025**

Abstract−The development of network technology demands reliable, efficient, and secure connectivity, especially for institutions with high operational needs. Software-Defined Wide Area Network (SD-WAN) emerges as an innovative solution to overcome the limitations of traditional networks, such as reliance on a single internet service provider (ISP) and inadequate security. This research aims to implement Maximize Bandwidth (SLA) on SD-WAN technology with firewall policies in Fortigate Next-Generation Firewall (NGFW) to improve network performance and security at Institution XYZ. The research method involves network simulation using Graphical Network Simulator 3 (GNS3) with a tree topology, two ISP clouds, and Fortigate configuration as NGFW. Testing was conducted through bandwidth monitoring, ICMP testing, and network parameter measurement using Iperf3. The results show that the implementation of SD-WAN with the Maximize Bandwidth (SLA) method successfully optimized bandwidth distribution and reduced connection disruptions. The implemented firewall policies were also effective in network segmentation, restricting inter-divisional access, and enhancing security. Testing confirmed network stability with a consistent bitrate of 1.05 Mbits/sec, low jitter (0.371–0.841 ms), and no packet loss. In conclusion, this solution not only addresses bandwidth limitations but also improves network security, thus serving as a reference for other institutions facing similar challenges.

Keywords: bandwidth; firewall policy; Fortigate; network security; SD-WAN; service level agreement.

1. INTRODUCTION

The development of network technology has undergone significant transformation in recent years, driven by the growing demand for reliable, efficient, and secure connectivity. Software-Defined Wide Area Network (SD-WAN) has emerged as an innovative solution to overcome the limitations of traditional networks by offering greater flexibility and scalability in bandwidth management. Unlike conventional WAN infrastructures that rely heavily on static routing and expensive MPLS lines, SD-WAN leverages software-based control to dynamically route traffic based on real-time network conditions. Recent studies indicate that SD-WAN technology is capable of enhancing network performance through bandwidth optimization, latency reduction, and significantly improved connection reliability [1][2]. The central concept of SD-WAN lies in its ability to abstract network hardware from its control mechanism, allowing administrators to centrally manage traffic policies across multiple locations. In today's increasingly competitive digital era, both public and private institutions are required to have a network infrastructure that can support operational activities optimally while ensuring an adequate level of security [3][4]. The need for continuous data flow, high availability, and protection against cyber threats has become essential, especially for organizations that rely on digital operations. As revealed in a comprehensive study by Mufti Kholil Romadhoni (2025), the implementation of an appropriate interface selection method on Fortigate SD-WAN has proven effective in optimizing network performance even under bandwidth constraints [5]. This finding highlights the importance of adaptive network policies and intelligent path selection in ensuring uninterrupted connectivity even when limited resources are available.

The main issue faced by XYZ Institution is its reliance on a single Internet Service Provider (ISP), which must serve three floors with many users. This situation results in decreased overall internet performance, especially when one floor experiences high usage, thereby impacting the productivity of the entire institution [6][7]. With a centralized traffic flow through one bandwidth source, congestion becomes inevitable during peak hours. This leads to network delays, dropped connections, and degradation in service quality, especially for critical functions such as cloud-based collaboration tools, video conferencing, and real-time data processing. Another challenge is the lack of network security, where all floors are interconnected without proper access restrictions, creating vulnerabilities to unauthorized access and potential intervention from other divisions [8][9]. This flat network structure increases the attack surface and reduces visibility into traffic flows, making it difficult to detect anomalies and implement isolation measures in the event of a breach. Previous research on SD-WAN technology implementation indicates that limitations in connectivity and flexibility in traditional networks can lead to significant operational bottlenecks and security risks that must be addressed comprehensively [2][10]. The inability to segment network traffic by department or location results in a higher likelihood of internal security breaches, data leaks, and unauthorized resource access. Additionally, a recent study on SD-WAN security threats highlights the importance of simultaneously addressing bandwidth and security issues to achieve optimal network performance [4][11]. A layered security model that integrates firewall, intrusion prevention, and dynamic path selection is increasingly recognized as a best practice in SD-WAN deployments.

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 7, Nomor 1, September 2025
e-ISSN 2685-998X
DOI : 10.30865/json.v7i1.9012

This research makes a significant contribution through the implementation of Maximize Bandwidth (SLA) on SD-WAN technology, which allows for the integration of two different ISPs into a unified system [5][12]. This approach not only ensures failover capabilities in the event one ISP goes down but also enables load balancing, which intelligently distributes traffic across all available links. The result is a more resilient and responsive network infrastructure. This approach enables all users in XYZ Institution, from the first to the third floor, to access the internet with optimal and stable speed [13][7]. Fortinet documentation (2025) shows that the Maximize Bandwidth (SLA) method is capable of distributing data traffic across all links that meet the Service Level Agreement (SLA) criteria, thereby maximizing the use of available bandwidth [12][14]. This feature utilizes performance metrics such as latency, jitter, and packet loss to determine the most efficient path for data transmission in real time. It also allows administrators to define SLA thresholds based on application priorities, ensuring mission-critical traffic is always given preference. Meanwhile, the implementation of Firewall Policy on Fortigate NGFW creates effective network segmentation, ensuring that each floor with different divisions is not interconnected, except from the floor of the institution's head [8][9]. This configuration significantly enhances network security and reduces the risk of unauthorized access between divisions, as outlined in the Fortigate administration guide, which emphasizes the importance of proper firewall policies in SD-WAN environments [2][3]. Such segmentation also supports compliance with data protection standards and enables forensic investigation when needed by isolating traffic logs by zone or division.

This research on the implementation of Maximize Bandwidth (SLA) in SD-WAN technology with Firewall Policy on Fortigate NGFW provides a comprehensive solution to connectivity and network security issues at XYZ Institution [5][6]. It bridges the gap between performance optimization and risk mitigation, two pillars of modern network infrastructure. Performance evaluation studies from previous research show that a properly implemented SD-WAN infrastructure can increase operational efficiency by up to 30% and significantly reduce network disruptions [3][7]. Improvements are especially evident in environments that require high throughput and minimal downtime, such as educational institutions, healthcare systems, and financial organizations. The findings of this study are expected to serve as a reference for similar institutions facing challenges in network optimization and information security [1][11]. In addition, the dual ISP configuration promotes operational continuity during maintenance or outages, minimizing disruptions that can affect business operations. In the long term, the implementation of this technology has the potential to enhance institutional productivity and operational efficiency through more reliable connectivity and improved network security, in line with previous findings on the importance of maintaining network performance in SD-WAN deployments [4][10]. As institutions continue to embrace digital transformation, the demand for flexible, scalable, and secure networking solutions like SD-WAN is projected to increase. Therefore, adopting such innovations not only addresses current limitations but also prepares the organization for future technological demands and resilience against evolving cyber threats.

2. RESEARCH METHODOLOGY

2.1 Research Stages

The network experiment in this study was designed using a virtual environment on Graphical Network Simulator 3 (GNS3) [19] with a tree topology. The network architecture consists of two internet clouds simulating two different service providers, one Fortigate virtual machine serving as a Next-Generation Firewall (NGFW), three layer-2 switches, and three virtual PCs representing users on three different floors. Each floor is connected to a separate switch to facilitate the addition of devices without modifying the core network configuration. The switches are configured in access mode, allowing PCs to connect directly without VLAN tagging. On Fortigate, firewall policies and SD-WAN rules are implemented to optimize bandwidth allocation based on the Service Level Agreement (SLA) and to segment the network according to the role of each floor. General access is limited to IP 8.8.8.8 and Microsoft services, Asset Monitoring access is limited to IP 1.1.1.1 and Gmail, while the Head of Institution floor has full access to all services available on the other two floors. Network performance testing was conducted in three phases: file transfer simulation with bandwidth monitoring on Fortigate, ICMP ping tests to target IP addresses to verify accessibility through Fortigate's forward traffic logs, and measurement of latency, jitter, and packet loss using Iperf3 between cross-floor PCs. This testing sequence provides a comprehensive overview of the network's stability and efficiency following the implementation of SD-WAN and firewall policies.

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 7, Nomor 1, September 2025
e-ISSN 2685-998X
DOI : 10.30865/json.v7i1.9012

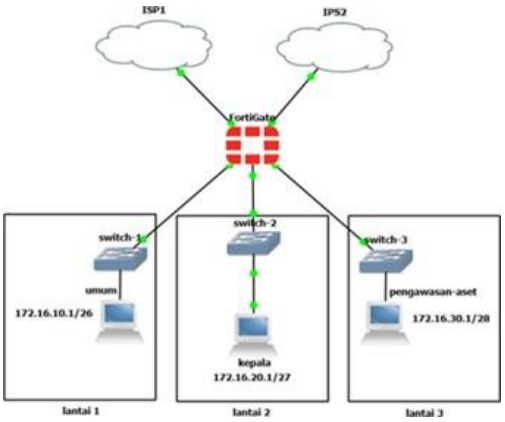

Figure 1. GNS3 Tree Topology

The SD-WAN Rules were implemented using the Maximize Bandwidth (SLA) method, which has been proven to deliver optimal performance [5]. Traffic distribution was handled using a round-robin load balancing algorithm to ensure optimal utilization of all available links, with automatic failover mechanisms triggered upon link degradation.

Firewall Policy is a core component in Fortigate's security implementation, used to control traffic flow between networks. In this study, Firewall Policies were configured in a sequential and structured approach, starting from the most specific to the more general rules. Each policy was configured with parameters including source and destination interfaces, source and destination addresses, service types, access schedules, and the corresponding action. Fortigate, when equipped with properly configured security profiles, is effective in detecting and blocking network attacks such as ICMP Flooding and Port Scanning, thus significantly enhancing the security of the network infrastructure [15].

The network infrastructure upgrade at XYZ Institution involved transitioning from a single ISP servicing all three floors to a dual-ISP architecture integrated via Fortigate SD-WAN using the Maximize Bandwidth (SLA) strategy. This approach maximizes the available bandwidth by intelligently distributing traffic between the two providers using a load balancing algorithm, ensuring uninterrupted connectivity across all floors—even during partial service outages [16]. The initial network configuration previously allowed unrestricted IP address access between floors, creating significant security vulnerabilities. This study implemented network segmentation through granular firewall policies that restrict IP access based on floor location, aligning with modern micro-segmentation security practices [17]. The hierarchical access control model allows the Head of Institution's floor to access all network segments while restricting other floors from accessing the asset monitoring or general operational floors—effectively creating isolated network zones. Recent studies show that such network micro-segmentation significantly improves security posture by limiting breach potential and preventing lateral movement within an organization's network [18]. This implementation aims to enhance network reliability through intelligent bandwidth aggregation and security through strategic segmentation—preventing unauthorized access and potential sabotage or intervention attempts on critical servers.

3. RESULT AND DISCUSSION

This section provides a comprehensive overview of the research findings and testing that have been conducted. The analysis includes the presentation of data obtained through three distinct methods: bandwidth monitoring and forward traffic log analysis using Fortigate devices, as well as network performance testing using Iperf3. In addition to presenting the data, this section offers an in-depth discussion on the implications of the findings, including the interpretation of significant results and their relevance to the research objectives.

3.1 Bandwidth on Fortigate

This subsection discusses the results of the bandwidth tests conducted on the Fortigate device. The objective of this testing was to observe bandwidth usage across several ports. Each tested port exhibited different bandwidth usage patterns, which are described in detail below.

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 7, Nomor 1, September 2025
e-ISSN 2685-998X
DOI : 10.30865/json.v7i1.9012

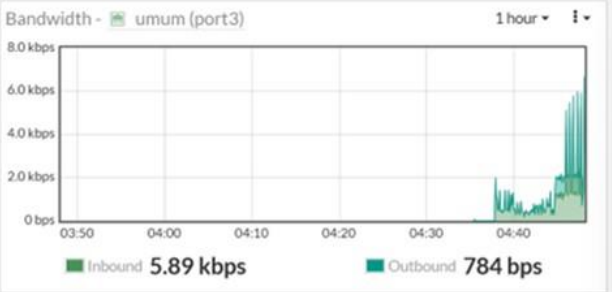

Figure 2. Use of Bandwidth General Section

In the bandwidth test on port3 (General Access), a significant fluctuation in outbound traffic was observed following a relatively stable period at the beginning of the monitoring session. The graph shows inbound traffic peaking at 5.89 kbps, while outbound traffic was recorded at 784 bps. The sharp increase in outbound traffic after 04:40 indicates an unexpected traffic spike, likely caused by bandwidth-intensive applications or network activities occurring at that time.

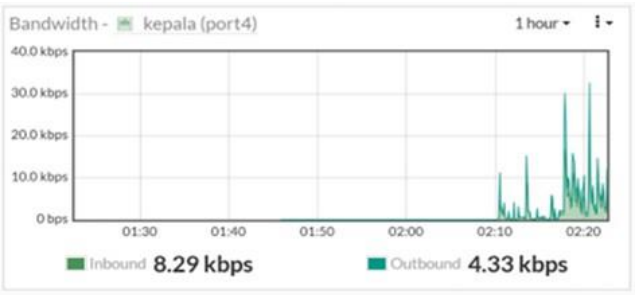

Figure 3. Use of Bandwidth Head Section

In the test on port4 (Head of Institution), the results showed a higher inbound bandwidth usage at 8.29 kbps, while outbound traffic was 4.33 kbps. There were larger fluctuations in outbound traffic, with a peak exceeding 30 kbps around 02:20. This sudden increase could indicate large data uploads or system activities such as updates or downloads. The instability in usage may suggest a reliance on certain applications or systems operating at specific times.

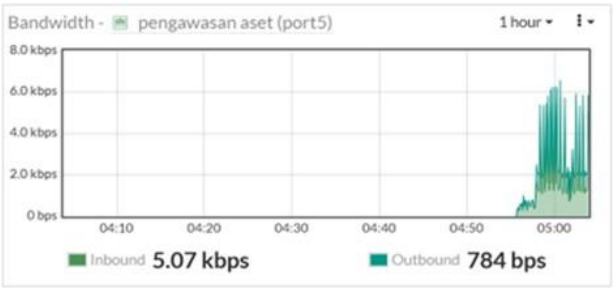

Figure 4. Use of Bandwidth Asset Control Section

In the test on port5 (Asset Supervisor), inbound traffic was recorded at 5.07 kbps, and outbound traffic was again measured at 784 bps. As in previous tests, there was a noticeable spike in outbound traffic beginning after 04:50, reaching levels significantly higher than in the initial observation period. This suggests intensive bandwidth usage at that time, possibly related to system updates or large-scale data transfers, potentially affecting the overall network quality.

3.2 ICMP testing

The purpose of this test was to evaluate the effectiveness of access restrictions applied to devices on each floor, in alignment with the implemented firewall policies. The test was conducted on three different devices: General Access PC, Head PC, and Asset Supervisor PC. Each device was subject to differentiated access policies based on its role within the network. Data collected included source and destination IP addresses, volume of data sent and received, and specific policies applied to each device.

The results, which include an analysis of data traffic for each device, provide insight into the implementation and effectiveness of the applied network security policies. The table below presents the test results related to data

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 7, Nomor 1, September 2025
e-ISSN 2685-998X
DOI : 10.30865/json.v7i1.9012

traffic on each device:

Table 1. Testing ICMP General Section

Source	Destination	Result	Policy ID
172.16.10.2	40.126.35.144 (microsoft)	21.42kB/21.42kB	akses umum (1)
172.16.10.2	8.8.8.8	1.6 kB/1.6 kB	akses umum (1)

Table 2. Testing ICMP Head Section

Source	Destination	Result	Policy ID
172.16.20.2	40.126.35.144 (microsoft)	20.42kB/20.42kB	akses kepala (2)
172.16.20.2	74.125.68.17 (gimail)	20.53kB/20.53kB	akses kepala (2)
172.16.20.2	8.8.8.8	1.6 kB/1.6 kB	akses kepala (2)
172.16.20.2	1.1.1.1	1.2 kB/1.2 kB	akses kepala (2)

Table 3. Testing ICMP Asset Control Section

Source	Destination	Result	Policy ID
172.16.30.2	74.125.68.17 (gimail)	22.43kB/22.43kB	akses pengawas aset (3)
172.16.30.2	1.1.1.1	1.5 kB/1.5 kB	akses pengawas aset (3)

The ICMP testing conducted on three different computers, General Access PC, Head PC, and Asset Supervisor PC, indicates the successful implementation of differentiated access policies within the Fortigate network. Based on the analysis of the generated forward traffic logs, it is evident that all devices were able to communicate with their designated targets symmetrically, with no signs of packet loss or significant transmission disturbances.

The General Access PC, operating under the general access policy (Policy ID 1), successfully communicated with the Microsoft server (40.126.35.144) and Google DNS (8.8.8.8). The volume of data transmitted and received was relatively balanced at 21.42 kB and 1.6 kB, respectively. These results confirm that the access for the General PC is restricted to public and commonly used destinations, in line with the limitations enforced through the configured firewall policy.

In contrast, the Head PC, governed by the head access policy (Policy ID 2), demonstrated a broader range of access. This device successfully communicated with Microsoft (40.126.35.144), Gmail (74.125.68.17), Google DNS (8.8.8.8), and Cloudflare DNS (1.1.1.1), with data volumes ranging from 1.2 kB to 20.53 kB. The ability to access both Gmail and Cloudflare underscores the higher level of authority and responsibility entrusted to the Head PC. This is reflected in its firewall policy, which provides greater access compared to both the General Access PC and Asset Supervisor PC. The broader access allows the Head PC to effectively manage and monitor network resources.

The Asset Supervisor PC, subject to the asset supervisor access policy (Policy ID 3), exhibited a distinct communication pattern. This device communicated with Gmail (74.125.68.17) and Cloudflare DNS (1.1.1.1), with data volumes of 22.43 kB and 1.5 kB, respectively. These results indicate that access for the Asset Supervisor PC is limited to services relevant to asset monitoring functions, consistent with the restrictions applied by its specific firewall policy.

3.3 Iperf3 Testing

Iperf3 testing was conducted to measure network performance on each device, namely the General Access PC, Head PC, and Asset Supervisor PC. The parameters measured included the testing interval, the volume of data transferred (Transfer), data transfer speed (Bitrate), delay variation or jitter, as well as the number of lost packets (Lost) relative to the total packets sent (Total).

Table 4. Testing Iperf3 General Section

Destination	Interval	Transfer	Bitrate
PC Kepala	0.00-10.00	1.25 MBytes	1.05 Mbits/sec
PC Pengawas aset	0.00-10.00	1.25 MBytes	1.05 Mbits/sec

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 7, Nomor 1, September 2025
e-ISSN 2685-998X
DOI : 10.30865/json.v7i1.9012

Table 5. Testing Iperf3 Head Section

Destination	Interval	Transfer	Bitrate
PC Umum	0.00-10.00	1.25 MBytes	1.05 Mbits/sec
PC Pengawas Aset	0.00-10.00	1.25 MBytes	1.05 Mbits/sec

Table 6. Testing Iperf3 Asset Control Section

Destination	Interval	Transfer	Bitrate
PC Umum	0.00-10.00	1.25 MBytes	1.05 Mbits/sec
PC Kepala	0.00-10.00	1.25 MBytes	1.05 Mbits/sec

Based on the network testing using Iperf3 from the General Access PC during the time interval from 0 to 10 seconds, the results showed that the device was able to transmit 1.25 MBytes of data with an average speed of 1.05 Mbits/sec in two different testing scenarios. The recorded jitter values of 0.841 ms and 0.725 ms indicate low and stable packet delivery time fluctuations. Additionally, no packet loss was detected (0/906 or 0%) in both test sessions, reflecting optimal network quality with no disruptions during data transmission.

Meanwhile, the results from the Head PC showed similar performance, with a data transfer volume of 1.25 MBytes and a constant bitrate of 1.05 Mbits/sec in both testing directions. The recorded jitter values of 0.451 ms and 0.371 ms were lower than those from the General Access PC, indicating higher network connection stability. The absence of packet loss in this session further reinforces the reliability and consistency of the device's connection.

The Asset Supervisor PC testing showed comparable results, with a data transfer of 1.25 MBytes and a steady bitrate of 1.05 Mbits/sec in both test sessions. The recorded jitter values of 0.628 ms and 0.495 ms were in the moderate range when compared to the other two devices. Nonetheless, these values still demonstrate stable network performance. The absence of packet loss (0/906) indicates that the network remained responsive and capable of transmitting data effectively throughout the entire testing sequence.

CONCLUSION

Based on the results of the conducted study, the implementation of SD-WAN technology with the Maximize Bandwidth (SLA) method and firewall policies on the NGFW Fortigate has successfully improved network performance and security at XYZ Institution. The integration of two ISP providers through the SD-WAN approach enables more optimal bandwidth distribution, preventing disruptions in internet connectivity even during traffic spikes on one floor. This is especially crucial in maintaining consistent operational performance, as the institution relies heavily on network availability for day-to-day activities. Additionally, the network segmentation applied through the firewall policies ensures that access between floors can be restricted according to each floor's role, significantly enhancing security levels. With this segmentation, unauthorized access between different divisions and departments is effectively minimized, helping to safeguard sensitive data and improve the institution's overall cybersecurity posture. The testing results show that all tested devices were able to communicate effectively without packet loss, and network performance remained stable despite high traffic fluctuations. This highlights the robustness and reliability of the SD-WAN implementation in a dynamic network environment. Furthermore, this implementation not only addresses bandwidth limitations but also prevents unauthorized access between divisions, thereby improving operational efficiency and reducing the risk of data breaches. With these results, this study makes a significant contribution to the development of network infrastructure in similar institutions facing comparable challenges in connectivity, security, and operational continuity. The findings provide valuable insights into optimizing network resources and enhancing network security in a rapidly evolving digital landscape.

REFERENCES

[1] W. Pratiwi and D. Gunawan, "Design and Strategy Deployment of SD-WAN Technology : In Indonesia (Case Study: PT.XYZ)," in 2021 International Conference on Green Energy, Computing and Sustainable Technology (GECOST), Jul. 2021, pp. 1–6. doi: 10.1109/GECOST52368.2021.9538796.

[2] G. K. Soejantono, M. I. Nashiruddin, S. N. Hertiana, and M. A. Nugraha, "Performance Evaluation of SD-WAN Deployment for XYZ Enterprise Company in Indonesia," in 2021 IEEE 12th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Oct. 2021, pp. 0311–0316. doi: 10.1109/IEMCON53756.2021.9623170.

[3] B. V Jadhav R Gosavi, M. D. Pawar, and A. Professor, "Software-Defined Wide-Area Network (SD-WAN) Implementation in Service Provider Network," | *An ISO*, vol. 9001, p. 14541, 2021, doi: 10.15680/IJIRSET.2021.1011081.

[4] A. Botta, R. Canonico, A. Navarro, G. Stanco, and G. Ventre, "Adaptive overlay selection at the SD-WAN edges: A reinforcement learning approach with networked agents," *Computer Networks*, vol. 243, Apr. 2024, doi: 10.1016/j.comnet.2024.110310.

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 7, Nomor 1, September 2025
e-ISSN 2685-998X
DOI : 10.30865/json.v7i1.9012

[5] M. KholilRomadhoni, L. S. Kenanga, D. R. Akbi, and D. Risqiwati, "Performance Evaluation of Outgoing Interface Selection Method on Fortigate SD-WAN for Network Optimization," *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control*, May 2025, doi: 10.22219/kinetik.v10i2.2120.
[6] M. Muchlisin and B. Yuliadi, "Improving Network Performance of Headquarters and Branches Using Software-Defined Network WAN (SD-WAN)," *PIKSEL : Penelitian Ilmu Komputer Sistem Embedded and Logic*, vol. 12, no. 1, pp. 23–34, Mar. 2024, doi: 10.33558/piksel.v12i1.8115.
[7] Z. Qin, "SD-WAN for Bandwidth and Delay Improvements on the Internet," *SHS Web of Conferences*, vol. 144, p. 02004, 2022, doi: 10.1051/shsconf/202214402004.
[8] "Internal Segmentation Firewall." Accessed: Jun. 09, 2025 [Online]. Available: https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-isf-security-where-you-need-it-w hen-you-need-it.pdf
[9] "Secure End-to-End Segmentation at Scale." Accessed: Jun. 09, 2025 [Online]. Available: https://www.cisco.com/c/dam/en/us/products/collateral/security/sdwan-seg-scale-sol-brief1.pdf
[10] A. S. George, A. S. Hovan George, and T. Baskar, "SD-WAN Security Threats, Bandwidth Issues, SLA, and Flaws: An InDepth Analysis of FTTH, 4G, 5G, and Broadband Technologies," *Partners Universal International Innovation Journal*, 2023, doi: 10.5281/zenodo.8057014.
[11] P. T. Anh Quang, S. Martin, J. Leguay, X. Gong, and F. Zeng, "Intent-based policy optimization in SD-WAN," in *Proceedings of the 2021 SIGCOMM 2021 Poster and Demo Sessions, Part of SIGCOMM 2021*, Association for Computing Machinery, Inc, Aug. 2021, pp. 74–75. doi: 10.1145/3472716.3472858.
[12] Fortinet Document Library, "Maximize bandwidth (SLA) strategy," Fortinet. Accessed: Jun. 09, 2025. [Online].Available:https://docs.fortinet.com/document/fortigate/7.0.4/administrationguide/708464/maximize-bandwidth-sl a-strategy
[13] Jordan Pioth, "How SD-WAN Helps with Bandwidth Aggregation," COEO. Accessed: Jun. 09, 2025. [Online]. Available: https://www.coeosolutions.com/news/sd-wan-helps-bandwidth-aggregation
[14] "SD-WAN Traffic Optimization," 2025. Accessed: Jun. 09, 2025. [Online]. Available: https://docs.versa-networks.com/Solutions/SD-WAN_Design/09_SD-WAN_Traffic_Optimization
[15] D. Prima Jaya, H. Aspriyono, and E. Suryana, "Implementasi Keamanan Jaringan Komputer Menggunakan Fortigate Sebagai Firewall pada Lab Komputer IAIN Bengkulu Implementation of Computer Network Security Using Fortigate as a Firewall at the Computer Lab of IAIN Bengkulu," *Print) Gatotkaca Journal*, vol. 2, no. 1, doi: 10.37638/gatotkaca.2.1.31-38.
[16] Fortinet Document Library, "SD-WAN rules - maximize bandwidth (SLA)," Fortinet. Accessed: Jun. 09, 2025. [Online]. Available: https://docs.fortinet.com/document/fortigate/6.2.16/cookbook/708464/sd-wan-rules-maximize-bandwidt h-sla
[17] Fortinet Document Library, "Securing OT with Network Microsegmentation." Accessed: Jun. 09, 2025. [Online]. Available:https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-securing-ot-networks-with-micr osegmentation.pdf
[18] V. V. Baligodugula, A. Ghimire, and F. Amsaad, "An Overview of Secure Network Segmentation in Connected IIoT Environments," *Computing&AI Connect*, vol. 1, Aug. 2024, doi: 10.69709/caic.2024.193182.
[19] SolarWinds Worldwide, LLC., "Graphical Network Simulator 3," Graphical Network Simulator 3". Accessed: Jun. 09, 2025. [Online]. Available: gns3.com