INDONESIAN JOURNAL OF MULTIDISCIPLINARY SCIENCE

P-ISSN: 2808-5957
E-ISSN: 2808-6724
ijoms.internationaljournallabs.com

HIGH AVAILABILITY'S IMPLEMENTATION ON THE FORTIGATE FIREWALL USING SD-WAN ZONE AND HA CLUSTER ACTIVE-PASSIVE

Novandi Rizki Fattahillah[1], Farah Nurfadila[2], Yanto Setiawan[3*]
[1,2,3] *BINUS Online Learning, Bina Nusantara University, West Jakarta, DKI Jakarta, Indonesia*
[*] *yanto.setiawan@binus.ac.id*

ARTICLE INFO

Published: August 29th, 2023

Keywords: *FortiGate, High Availability, SD-WAN, Load balancing, Failover*

ABSTRACT

Networks that contain sensitive data or have high-security requirements require reliable and dependable network security solutions. FortiGate Firewall, as one of the popular network security solutions, provides High Availability (HA) features that ensure network availability and reliability. This study aims to analyze the implementation of HA on FortiGate Firewall in specific scenarios, such as networks with sensitive data or networks with high-security requirements. A real-world case study is applied to evaluate the effectiveness of HA implementation on FortiGate Firewall in enhancing network reliability and security. In this research, the implementation of HA on FortiGate Firewall at PT ABC was successfully built using the PPDIOO method and deploying SD-WAN load balancing and failover configurations, along with the utilization of a high-availability cluster mechanism. The HA implementation on FortiGate proves to be an effective solution, as demonstrated in the SD-WAN Zone testing of the Source-destination SD-WAN load balancing mode, which showed effectiveness in evenly and optimally distributing traffic among multiple available links, resulting in a 93.3% reduction in downtime. Furthermore, the testing of HA cluster mode in active-passive configuration achieved a 91.8% reduction in downtime compared to the pre-HA implementation state.

INTRODUCTION

Computer networks have become an integral part of business and organizational activities. Network security is crucial to protect important data and information from unauthorized access or attacks. However, networks must also be available and reliable at all times to ensure business productivity and efficiency (Sun, 2022). Network security is a system that functions to secure a network from various external threats that can disrupt the network and steal data within a company (Wicaksono & Widiasari, 2022).

Firewall is one of the network security solutions that can help protect the network from attacks and restrict unauthorized access. However, relying on a single firewall can pose security and network availability issues if the firewall experiences damage or disruptions (Wicaksono & Widiasari, 2022). Based on observations from the PT ABC case study on the existing network, the network security system is already robust. However, the network towards the internet only has a single gateway passing through a standalone FortiGate device, which creates a Single Point of Failure issue. This means that there is no backup in case the existing FortiGate experiences problems. If there is an issue with the FortiGate, the internet connection will be lost, resulting in the halt of the company's production operations. Please refer to Figure 1 for an illustration of the situation when the FortiGate device is down.

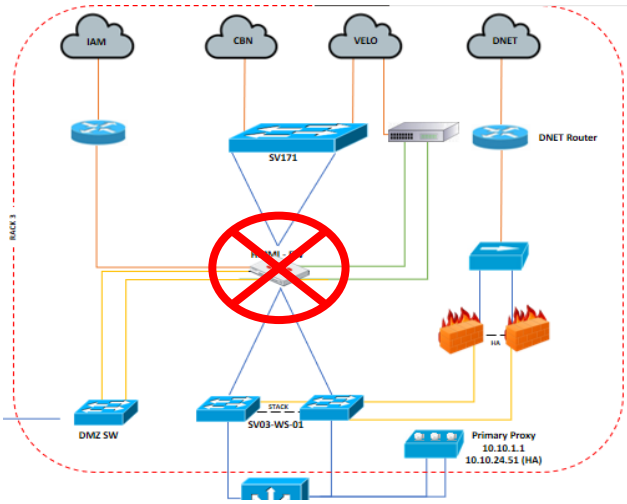

Figure 1. Illustration of an Inactive FortiGate Device

To address this issue, the High Availability (HA) solution can be employed to ensure network availability and reliability (Mukhopadhyay, 2020; Taresh & Zghair, 2023). FortiGate Firewall offers HA features that allow the configuration of multiple firewalls as a backup system, providing a failover solution that can automatically take over if the primary firewall encounters issues. Thus, this study has identified the problem statement to evaluate the implementation of HA on FortiGate Firewall in specific scenarios such as networks with sensitive data or networks with high-security requirements, and to assess the effectiveness of the HA solution in enhancing network reliability and security.

The significance of this research lies in ensuring high network availability with automatic recovery in case of primary device failure, which has proven to be effective when such failures occur. The objectives of this study are to establish the process and implementation methods of High Availability (HA) on FortiGate Firewall, as well as to test the effectiveness and reliability of HA implementation on FortiGate Firewall in specific scenarios.

The scope of this research encompasses several relevant aspects. Firstly, the analysis of the network system with HA implementation on FortiGate Firewall aims to determine the configuration that suits the network requirements. Subsequently, the HA configuration on FortiGate Firewall will be aligned with the official guidelines provided by the firewall manufacturer. Furthermore, the implementation of HA will undergo testing to evaluate its effectiveness and reliability.

A systematic literature review process is conducted within the context of High Availability to identify the approaches, techniques, and analyses used to implement high availability in FortiGate. The literature review has resulted in several relevant publications, which can be seen in Table 1.

Table 1. Literature Review

Researcher Name	*Neupane et al.*	*Zouini et al.*	*Peng et al.*	*Bahrul et al.*
Research Title	Next Generation Firewall for Network Security: ASurvey (Neupane et al., 2018)	Towards a Modern ISGA Institute Infrastructure Based on Fortinet SD-WAN Technology: Recommendations and Best Practices (Zouini et al., 2022)	A Load-Balancing and State-Sharing Algorithm for Fault-Tolerant Firewall Cluster (Peng et al., 2017)	Implementation of High Availability Message ISO 8583 using F5 Active-Passive Failover Method (Ilham & Setiawan, 2023)
Research result	A comparison of the current state of the technique and various NGFWs available in the market is provided highlighting their various parameters such as security functionality and performance such as FortiGate.	The results obtained show a considerable advantage that can be achieved with SD-WAN in terms of performance.	Research shows that load-balancing and state-sharing algorithms in cluster firewalls can effectively improve performance, and prevent single points of failure.	The main objective of this research is to measure the effectiveness of the Active Passive Failover method in performing High Availability using ISO 8583 message parameters and CPU Load, and to increase the level of Availability and reliability of the FDS Server.
Research Gaps	Only explained the comparison of NGFW firewall brands. There is no research that specifically implements FortiGate High Availability Firewall using the SDWAN and HA Cluster Active-Passive methods.	This research does not specifically discuss the implementation of FortiGate High Availability Firewall using SDWAN and HA Cluster Active-Passive methods.	This study does not incorporate the SDWAN method in implementing cluster firewalls. In addition, this study does not provide a specific focus on FortiGate devices as a firewall solution used in High Availability implementations.	The research does not directly compare the Active-Passive Failover method used with the FortiGate solution in the context of firewall implementation.

METHOD

The research methodology is the approach used to achieve a specific objective. In this study, a qualitative research methodology was employed to attain the research goals. This approach focuses more on theoretical aspects described in the theoretical framework and utilizes an analysis method based on the PPDIOO development model (Novianto et al., 2021) depicted in Fig.2.

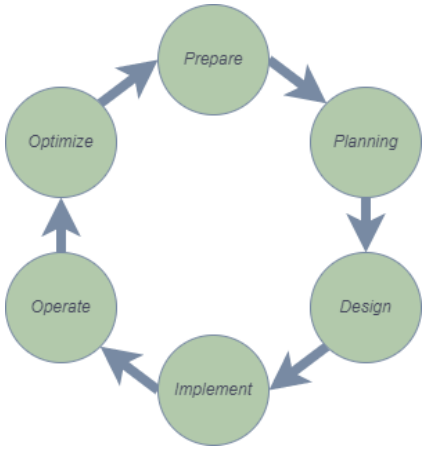

Figure 2. PPDIOO Development Model

Prepare

In the initial "prepare" phase, the researcher identified issues related to data exchange and network communication at PT. ABC. First, data collection was carried out through interviews with the Operation Manager responsible for network infrastructure, Subsequently, a literature review was conducted to search for references related to the identified issues. Furthermore, the researcher conducted direct field observations to gather additional information.

Plan

In the "plan" phase, the researcher analyzed the identified issues and created a plan related to those problems. One of the issues found was the lack of backup paths to replace the primary path in case of network failure. While the network security system was robust, the network towards the internet had only one gateway passing through a single FortiGate device with a standalone mechanism, resulting in a Single Point of Failure issue and no backup in case the existing FortiGate encountered problems. This problem was a consideration for the researcher in conducting research on the existing system.

Design

In the "design" phase, the researcher designed a new network after analyzing the identified issues. Considering the possibility of a single point of failure, we proposed a more secure HA mechanism to optimize network availability. The use of HA mechanism required two FortiGate devices, resulting in a change in the WAN direction topology. Fig. 3. depicts the implemented HA topology. Subsequently, the SD-WAN mechanism will be implemented as a failover and load balancing method to optimize network utilization (Sahoo et al., 2019). Fig. 4 illustrates the SD-WAN topology.

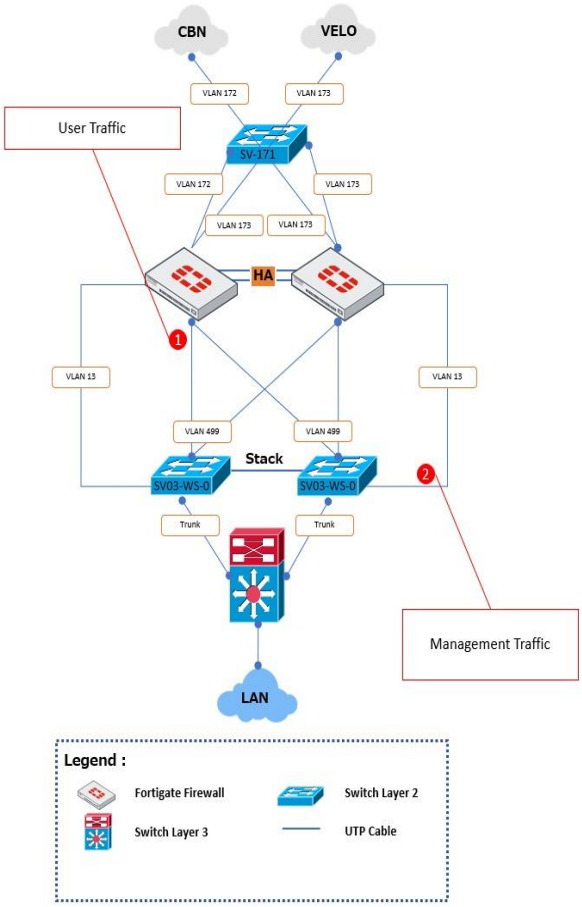

Figure 3. Topology of HA Implementation

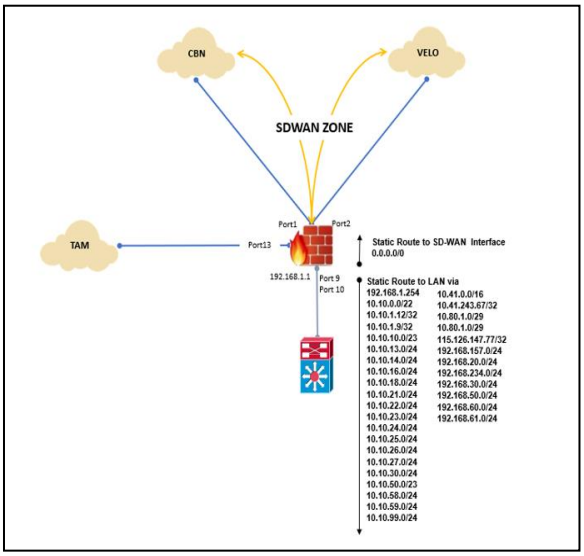

Figure 4. Topology of SD-WAN Implementation

Implement

In the "implement" phase, the researcher implemented a High Availability Cluster on two FortiGate devices using an active-passive mechanism. Additionally, the researcher implemented load balancing and failover as redundancy links using the Software-Defined Wide Area Network (SD-WAN) method. Fig. 5 represents the implementation process flow, utilizing FortiGate 601F, which will undergo testing of the SD-WAN and High Availability Cluster system.

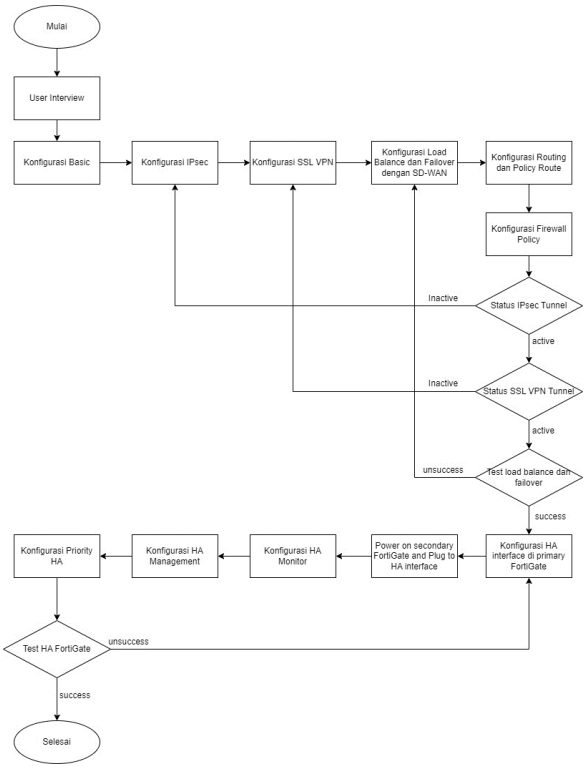

Figure 5. Implementation of HA FortiGate Firewall Flowchart

Operate and Optimize

In the "operate" phase, the researcher conducted experiments on the newly implemented system and performed tests according to the prepared scenarios. In the "optimize" phase, the researcher fine-tuned and adjusted the new system to integrate smoothly with the existing environment, ensuring optimal integration with other devices.

RESULT AND DISCUSSION

HA Load Balancing and Failover Configuration with SD-WAN Zone

SD-WAN Zone is a feature in SD-WAN technology that allows the simultaneous use of multiple internet connections to efficiently and effectively distribute data traffic (Du et al., 2022). SD-WAN Zone can be used to configure automatic load balancing and failover to enhance network performance and service availability (Fikri & Rifqi, 2023). Additionally, it can route traffic to appropriate networks to optimize costs by connecting physical paths through connections within a

single logical link (Bustamante & Avila-Pesantez, 2021). In the configuration of SD-WAN Zone, the available internet connections can be integrated and grouped into a zone. After the zone is formed, users can configure load balancing to evenly distribute data traffic across the available connections and leverage automatic failover features to remain connected to the internet even if one connection experiences disruptions (Ghama Wellyandi, 2022; Tanha et al., 2018). The configuration follows a topology similar to the one depicted in Fig. 3.

1) Global SD-WAN Zone Configuration: To utilize the SD-WAN Zone feature, it is necessary to enable the feature by setting the status to "enable." Additionally, to use load balancing in the SD-WAN Zone, it is important to define the load balancing technique to be employed. By utilizing load balancing techniques, the SD-WAN Zone can optimize network performance and accelerate data transfer by evenly distributing the load across the connections. In this case, the source-destination IP-based mode is used, where SD-WAN balances traffic evenly among member interfaces based on a hash algorithm using source and destination IP addresses. Here is the configuration for the SD-WAN Zone:

```
config system SD-WAN
    set status enable
    set load-balance-mode source-dest-ip-based
    config zone
        edit "virtual-wan-link"
        next
  end
```

2) Interface Member of SD-WAN Zone Configuration: In this step, two interfaces are configured and selected as member interfaces of the SD-WAN zone. The selection of two interfaces is based on the requirements for load balancing and failover to ensure network reliability. In this case, the chosen member interfaces are directed towards two ISPs, namely CBN and VELO, enabling High Availability links to the internet and WAN. The following is the configuration for the SD-WAN Zone member interfaces:

```
config members
        edit 1
            set interface "port1"
            set gateway ABC.ABC.ABC.129
        next
        edit 2
            set interface "port2"
            set gateway ABC.ABC.ABC.253
        next
    end
```

3) SD-WAN Zone Test: Initial testing in SD-WAN mode without load balancing showed that the traffic throughput without load balancing is dependent on the capacity and quality of the used links. Initial testing in SD-WAN Source-destination mode revealed a constraint in one link, causing slow internet performance, as shown in Fig. 6. The port towards CBN consumed excessive bandwidth, resulting in many users complaining about slow internet performance.

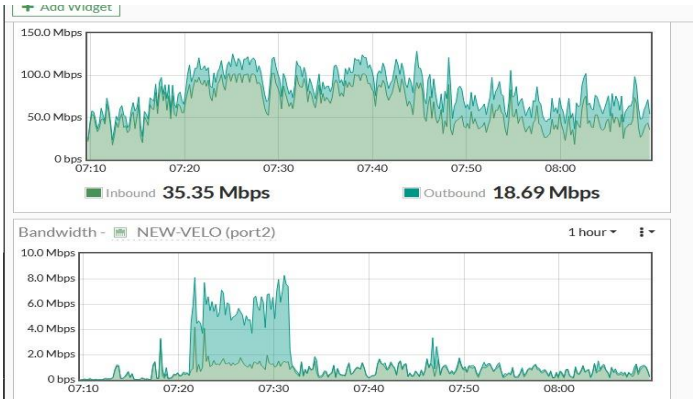

Figure 6. Before Implementation with Load Balancing Test Result

Subsequently, testing was conducted using SD-WAN load balancing in Source-destination mode. The SD-WAN Source-destination mode testing yielded positive results in enhancing overall network performance. During the load balancing testing, the researcher performed tests from local client users to access the internet with various destinations, allowing different ISP destinations based on the internet content accessed. Fig.7. depicts the results of the load balancing testing in Source-destination mode.

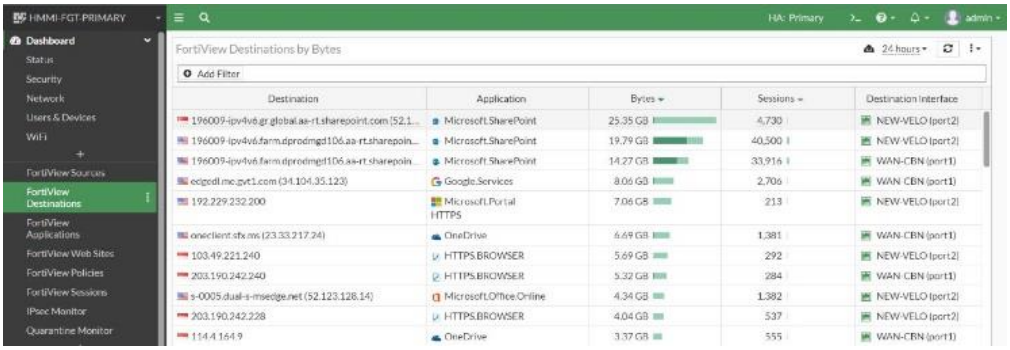

Figure 7. Load balancing Source-destination Mode Test Result

During the testing, the Source-destination mode successfully optimized bandwidth utilization and ensured faster and reliable packet delivery between the specified source and destination pairs. The implementation of Source-destination mode in SD-WAN can assist organizations in optimizing the utilization of existing network resources, improving service availability, and reducing downtime caused by network disruptions. Fig. 8. illustrates the bandwidth utilization of both ISP networks (VELO and CBN).

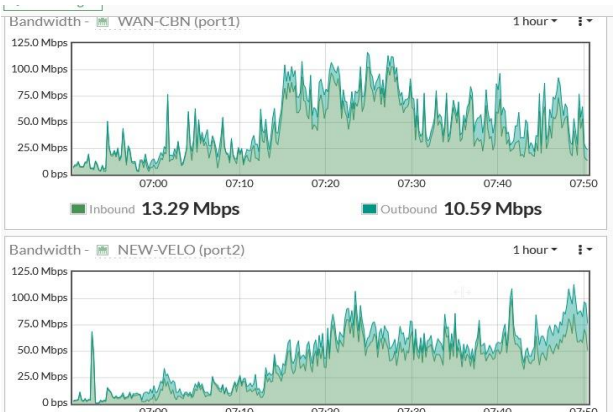

Figure 8. Bandwidth Utilization Result Test

The Source-destination mode SD-WAN testing with volume-based load balancing demonstrated its effectiveness in evenly and optimally distributing traffic among the available multiple links, as depicted in Fig. 9. This aligns with the theory (Golchi et al., 2019) that load balancing can evenly distribute traffic and workload across ISPs and resolve issues caused by unbalanced nodes (Devaraj et al., 2020; Yang et al., 2019).

Figure 9. Results of Traffic Distribution Volume of both ISPs

The SD-WAN failover testing yielded positive results in maintaining network service availability in the event of an ISP failure. The failover mechanism in SD-WAN proved to be effective in automatically and transparently redirecting traffic to backup paths with fast recovery times. During the testing, the SD-WAN failover mechanism optimized the utilization of multiple links by directing traffic to available and stable paths (Ouamri et al., 2023). Fig. 10 displays the public IP of the VELO network, where all traffic is routed to VELO when CBN is down.

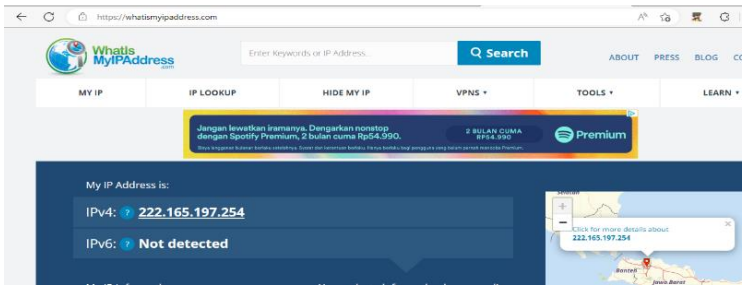

Figure 10. Failover through VELO

In the testing, the failover mechanism in SD-WAN demonstrated reliability and smoothly restored connections without significant disruptions for users and existing applications. Fig. 11 shows the results of the failover testing with CBN being down.

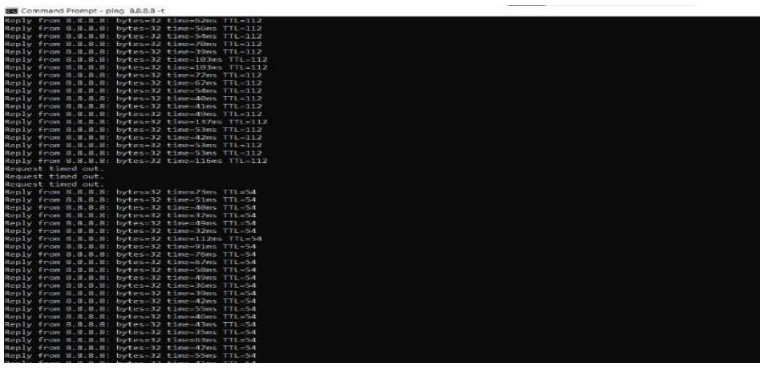

Figure 11. Failover Test Results When CBN is Off

By implementing SD-WAN technology in the failover system, a significant reduction in downtime of 93.3% was achieved based on the calculations obtained below. This percentage demonstrates the reliability of the system and its ability to restore connections smoothly without significant disruptions for users and applications.

$$Downtime\ percentage = \left(\frac{Successfully\ received\ ICMP\ packet}{Number\ of\ ICMP\ packets}\right) x100\% \quad (1)$$

$$Downtime\ percentage = \left(\frac{42}{45}\right) x100\% = 93.3\%$$

High Availability (HA) Cluster Configuration

In designing High Availability (HA) for FortiGate, the first step is to build a robust architecture that ensures continuous service availability. This can be seen in Fig. 3., which depicts the topology used in the High Availability Cluster mechanism.

1) High Availability Cluster Active-passive Mode: In this design, the active-passive mode will be implemented to achieve high availability on the FortiGate devices. This mode ensures that one device functions as the active primary unit, while the other device serves as the passive secondary unit, ready to take over in case of primary unit failure (Fiade et al., 2020). In the active-passive mode mechanism, it is necessary to establish priorities for both primary and secondary devices to determine the failover sequence. The priority settings determine which device will be the default primary unit and take over the tasks in the event of primary unit failure. The following is Table 2. Priority FortiGate.

Table 2. Priority FortiGate

No.	FortiGate Device	Interface	IP Address	Priority
1	Primary	Management	10.10.13.1	128
2	Secondary	Management	10.10.13.2	50

In this configuration, the primary FortiGate has a higher priority value (128) compared to the secondary FortiGate (50). This means that the primary FortiGate will be the active primary device by default. However, if a failure occurs on the primary device, the secondary FortiGate with the lower priority value will assume the role of the primary device.

2) Interface Monitoring: To ensure availability and optimal performance, in this design, the LOCAL interface, Port 11, and Port 12 will be monitored. Any changes or failures on these interfaces will be automatically detected by the system, triggering a fast and responsive failover process. The following Fig. 12. for the port configuration is done.

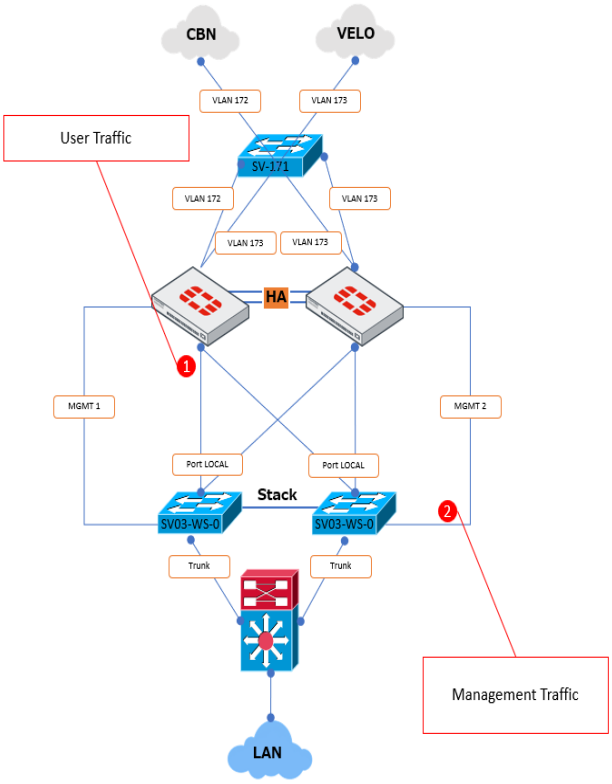

Figure 12. Port Configuration

3) Management Interface: In this design, the management interfaces on both FortiGate devices will be configured with unique IP addresses. This enables effective management and monitoring of both devices and facilitates access to the web-based GUI for configuration and monitoring purposes. The management interfaces will be configured based on Table 2.
4) Configuration Synchronization: In this design, configuration synchronization between the primary and secondary devices is required. This synchronization involves firewall policies, routing tables, and other necessary objects to maintain consistency and service availability during the failover process.

5) High Availability (HA) Testing: Prior to the HA configuration, as shown in Fig. 13, the security fabric relies on only one device. Therefore, if FGT-01 (FortiGate 500D) fails, the route to the internet or public network will be disrupted. This is due to the presence of a Single Point of Failure (SPOF) issue (Filali et al., 2020) and a single FortiGate device becomes a bottleneck due to the difficulty in handling traffic loads with complex policies (Hadjadj et al., 2022).

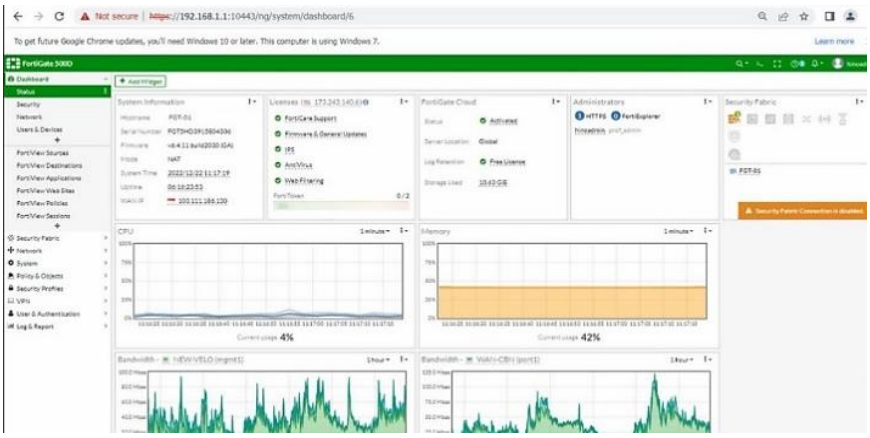

Figure 13. FortiGate Mechanism Without HA

Testing was conducted before implementing HA using the FortiGate 500D device. The HA active-passive testing on FortiGate demonstrated reliability and dependability in maintaining network availability. When one node experiences a failure, the passive node automatically takes over to ensure uninterrupted service (Bouizem et al., 2020; Pribadi et al., 2020). In the testing, the priorities assigned to the primary node (128) and secondary node (50) ensure that the primary node remains the preferred choice for handling normal traffic, while the secondary node is ready to take over when needed. Fig. 14. shows the scenario when the primary FortiGate is still operational, making it the primary device.

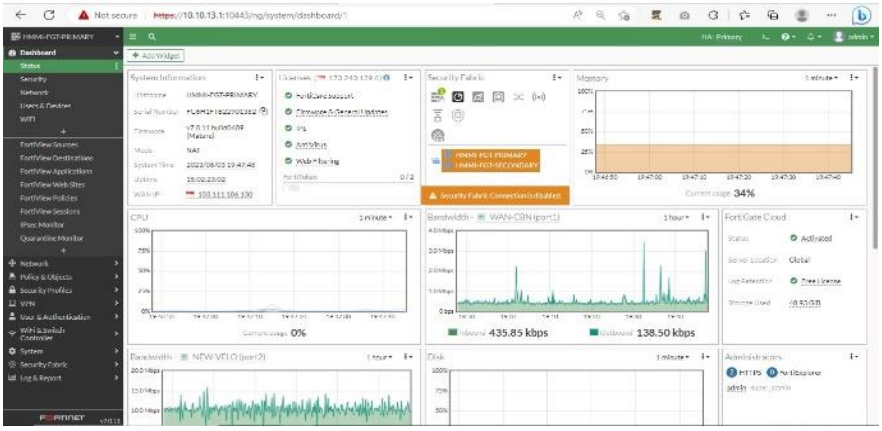

Figure 14. Display of FortiGate Primary when Power On

Next, the researchers conducted testing when the primary FortiGate device is down. In this case, the secondary FortiGate automatically becomes the primary device, as shown in Fig. 15. In the testing, the traffic transition from the primary FortiGate to the secondary FortiGate proved reliable and smoothly restored connections without significant disruptions for users and existing applications (Cheng et al., 2020). Fig. 16. displays the results of HA cluster testing with the primary FortiGate device being down.

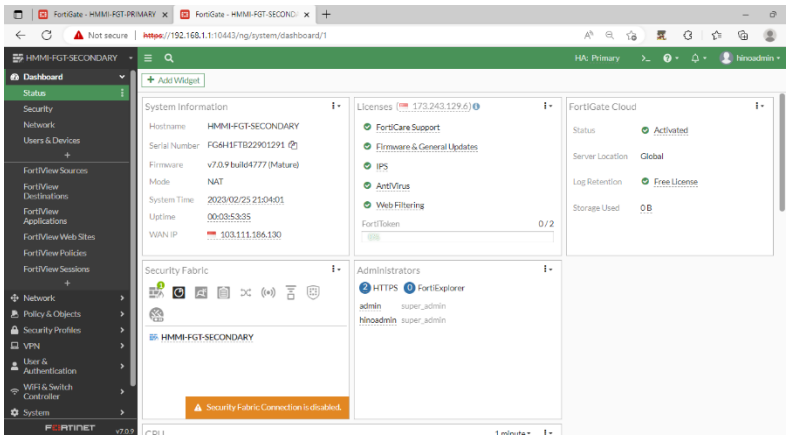

Figure 15. Display of FortiGate Primary When Power Off

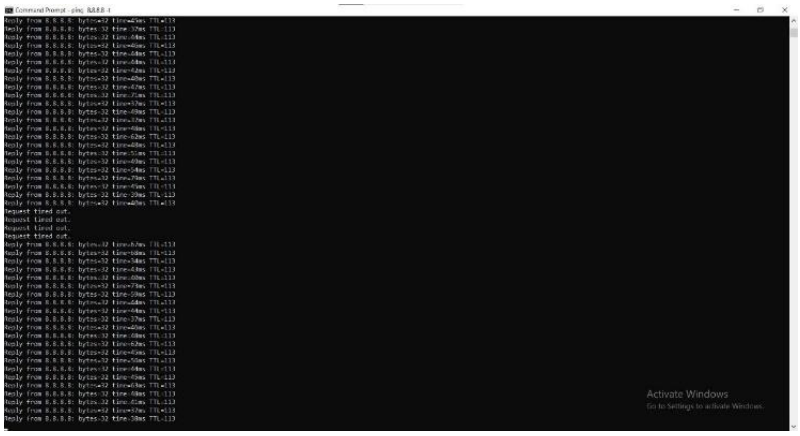

Figure 16. HA Cluster Test Results Primary Off

CONCLUSION

Based on the research, it can be concluded that the HA implementation has proven to be reliable and capable of restoring connections smoothly without significant disruptions for users and existing applications. This was evident in the SD-WAN Zone testing, where a 93.3% reduction in downtime was observed through load balancing and failover mechanisms.

The HA cluster testing with the active-passive mode resulted in a 91.8% reduction in downtime compared to the pre-HA implementation state. With automatic detection and failover capabilities, as well as the established priority mechanisms, the HA active-passive configuration can provide continuous service and minimize disruptions in network operations.

During testing, it was observed that without the HA mechanism, failures of the primary device could lead to downtime and service discontinuity. Therefore, implementing HA mechanisms in FortiGate ensures high network availability with automatic recovery in the event of primary device failure, proving to be effective in maintaining service continuity.

Based on the conclusions, the following recommendations are suggested for further research: conduct research on disaster recovery management using FortiGate HA mechanisms. Examine the system's ability to perform fast and effective recovery in the event of natural disasters or other unforeseen incidents.

REFERENCES

Bouizem, Y., Parlavantzas, N., DIb, D., & Morin, C. (2020). Active-Standby for High-Availability in FaaS. *WOSC 2020 - Proceedings of the 2020 6th International Workshop on Serverless Computing, Part of Middleware 2020*, 31–36. https://doi.org/10.1145/3429880.3430097

Bustamante, J. R., & Avila-Pesantez, D. (2021). Comparative analysis of Cybersecurity mechanisms in SD-WAN architectures: A preliminary results. *Proceedings of the 2021 IEEE Engineering International Research Conference, EIRCON 2021*. https://doi.org/10.1109/EIRCON52903.2021.9613418

Cheng, F. C., Liu, W. C., & Pan, T. J. (2020). *Fail recovery method and internet of things system and charging system using the same* (Patent U.S. Patent No. 10,805,147). Patent and Trademark Office.

Devaraj, A. F. S., Elhoseny, M., Dhanasekaran, S., Lydia, E. L., & Shankar, K. (2020). Hybridization of firefly and Improved Multi-Objective Particle Swarm Optimization algorithm for energy efficient load balancing in Cloud Computing environments. *Journal of Parallel and Distributed Computing*, *142*, 36–45. https://doi.org/10.1016/j.jpdc.2020.03.022

Du, C., Xiao, J., & Guo, W. (2022). Bandwidth constrained client selection and scheduling for federated learning over SD-WAN. *IET Communications*, *16*(2), 187–194. https://doi.org/10.1049/cmu2.12333

Fiade, A., Agustian, M. A., & Masruroh, S. U. (2020). Analysis of Failover Link System Performance in OSPF, EIGRP, RIPV2 Routing Protocol with BGP. *The 7th International Conference on Cyber and IT Service Management (CITSM 2019)*. https://doi.org/10.1109/CITSM47753.2019.8965373

Fikri, M., & Rifqi, M. (2023). Implementasi VPN Antar Cabang Menggunakan Teknologi Sdwan Dengan Metode Load Balance (Studi Kasus: PT. Mitra Solusi Infokom). *Jurnal Teknologi Informasi Dan Ilmu Komputer (JTIIK)*, *10*(1), 105–113. https://doi.org/10.25126/jtiik.2023105236

Filali, A., Mlika, Z., Cherkaoui, S., & Kobbane, A. (2020). Preemptive SDN Load Balancing with Machine Learning for Delay Sensitive Applications. *IEEE Transactions on Vehicular Technology*, *69*(12), 15947–15963. https://doi.org/10.1109/TVT.2020.3038918

Ghama Wellyandi. (2022). Implementation of Load Balancing and Failover Network Using Fortinet SDWAN Technology at PT. Lintasarta. *Ceddi Journal of Information System and Technology (JST)*, *1*(2), 8–13. https://doi.org/10.56134/jst.v1i2.20

Golchi, M. M., Saraeian, S., & Heydari, M. (2019). A hybrid of firefly and improved particle swarm optimization algorithms for load balancing in cloud environments: Performance evaluation. *Computer Networks*, *162*. https://doi.org/10.1016/j.comnet.2019.106860

Hadjadj, T. E., Bouhoula, A., Tebourbi, R., & Ksantini, R. (2022). Optimization of parallel firewalls filtering rules. *International Journal of Information Security*, *21*(2), 323–340. https://doi.org/10.1007/s10207-021-00557-4

Ilham, B., & Setiawan, Y. (2023). Implementation of High Availability Message ISO 8583 using F5 Active-Passive Failover Method. *International Journal of Engineering Trends and Technology*, *71*(4), 264–273. https://doi.org/10.14445/22315381/IJETT-V71I4P223

Mukhopadhyay, B. (2020). A Novel Approach to Load Balancing and Cloud Computing Security using SSL in IaaS Environment. *International Journal of Advanced Trends in Computer Science and Engineering*, *9*(2), 2362–2370. https://doi.org/10.30534/ijatcse/2020/221922020

Neupane, K., Haddad, R., & Chen, L. (2018). Next Generation Firewall for Network Security: A Survey. *In SoutheastCon IEEE*, 1–6.

Novianto, D., Setiawan Japriadi, Y., Luhur Pangkalpinang, A., Jenderal Sudirman, J., Selindung Baru, K., Gabek, K., & Pangkal Pinang, K. (2021). Comparative Analysis Of Performance Between Ecmp And Nth Methods In Implementation Of Microtic-Based Dual Link Load Balancing Techniques. *Jurnal TAM (Technology Acceptance Model)*, *12*(1), 80–88.

Ouamri, M. A., Barb, G., Singh, D., & Alexa, F. (2023). Load Balancing Optimization in Software-Defined Wide Area Networking (SD-WAN) using Deep Reinforcement Learning. *IEEE*, 1–6. https://doi.org/10.1109/isetc56213.2022.10010335

Peng, Z., Chen, D., & He, W. (2017). A load-balancing and state-sharing algorithm for fault-tolerant firewall cluster. *Proceedings - 2017 4th International Conference on Information Science and Control Engineering, ICISCE 2017*, 34–37. https://doi.org/10.1109/ICISCE.2017.17

Pribadi, Y., Putra Negara, A. B., & Irwansyah, M. A. (2020). Analisis Penggunaan Metode Failover Clustering untuk Mencapai High Availability pada Web Server (Studi Kasus: Gedung Jurusan Informatika). *Jurnal Sistem Dan Teknologi Informasi (Justin)*, *8*(2), 218. https://doi.org/10.26418/justin.v8i2.31965

Sahoo, K. S., Tiwary, M., Mishra, P., Reddy, S., Balusamy, B., & Gandomi, A. (2019). Improving End-Users Utility in Software-Defined Wide Area Network Systems. *IEEE Transactions on Network and Service Management*, *14*(8), 1–12. https://doi.org/10.1109/TNSM.2019.2953621

Sun, J. (2022). Computer Network Security Technology and Prevention Strategy Analysis. *Procedia Computer Science*, *208*, 570–576. https://doi.org/10.1016/j.procs.2022.10.079

Tanha, M., Sajjadi, D., Ruby, R., & Pan, J. (2018). Capacity-Aware and Delay-Guaranteed Resilient Controller Placement for Software-Defined WANs. *IEEE Transactions on Network and Service Management*, *15*(3), 991–1005. https://doi.org/10.1109/TNSM.2018.2829661

Taresh, A. A. R., & Zghair, N. A. K. (2023). Redesign of the communications network based on high availability of traffic management technologies to improve the communication. *Measurement: Sensors*, *27*. https://doi.org/10.1016/j.measen.2023.100776

Wicaksono, D., & Widiasari, I. R. (2022). Sistem Keamanan Jaringan Menggunakan Firewall Dengan Metode Port Blocking Dan Firewall Filtering. *Jurnal Teknik Informatika Dan Sistem Informasi*, *9*(2), 1380–1392. http://jurnal.mdp.ac.id

Yang, K., Guo, D., Zhang, B., & Zhao, B. (2019). Multi-Controller Placement for Load Balancing in SDWAN. *IEEE Access*, *7*, 167278–167289. https://doi.org/10.1109/ACCESS.2019.2953723

Zouini, M., Mantar, Z. El, Rouboa, N., Bensaoud, O., Outzourhit, A., & Bahnasse, A. (2022). Towards a Modern ISGA Institute Infrastructure Based on Fortinet SD-WAN Technology: Recommendations and Best Practices. *Procedia Computer Science*, *210*(C), 311–316. https://doi.org/10.1016/j.procs.2022.10.156