Ceddi Journal of Information System and Technology (JST) *ISSN: 2829-808X (print)*
Vol. 1 No. 2 December (2022) *ISSN: 2829-6575 (online)*
https://doi.org/10.56134/jst.v1i2.20

Implementation of Load Balancing and Failover Network Using Fortinet SDWAN Technology at PT. Lintasarta

Ghama Wellyandi

Department of Information Technology, Universitas Nusa Mandiri, Jakarta, indonesia

Abstract

An Internet Service Provider (ISP) is a company or entity that provides internet connection services and other related services. The complexity of distribution control from several ISPs causes problems, especially in the speed factor, which affects the costs that must be incurred by the company. Management company information is not only focused on price and speed, but also requires good security and data traffic management (Traffic Engineering/TE). One application that is able to meet these needs is Software Defined Wide Area Network (SD-WAN). SD-WAN is the latest technological network development paradigm, overcoming the challenges that exist in network mechanisms in TE. The results of this study can be used as a comparison of several ISPs so that it can be known which one is better or which one to choose. Based on the results of the data analysis, the following conclusions were obtained: 1) As for the jitter problem in the performance of SD-WAN technology, it has advantages over ordinary conventional networks that do not use sdwan technology; 2) Regarding the delay/latency of internet service providers, SD-WAN has advantages over ordinary conventional networks and 3) With respect to packet loss, SD-WAN internet service providers have an advantage over ordinary conventional networks.

Keywords: Software; Hardware; SD-WAN Fortinet; Load Balancing; Failover

Received: 10 August 2022 Revised: 15 August 2022 Accepted: 20 December 2022

Introduction

Currently, communication technology plays a very important role for everyone. Technological progress is also an indicator of the progress of human civilization at a certain time, and is the basis for future technological changes and developments (Bahtiar at al, 2018). With the increasing number of internet connection users, good infrastructure is also needed to maintain smooth internet access. Networking Infrastructure at PT. Lintasarta, as a network provider service to users, for example, already has a very good infrastructure, but the harshness of network technology users' demands that everything be done perfectly, therefore, in improving quality and quality at PT. Lintasarta. Lintasarta is currently developing Software Defined Wide Area Network (SD-WAN) technology (Yang et al., 2019). what exactly is it (SD-WAN)? Software Defined Networking – Wide Area Network (SDN-WAN) is a technology specification applied to WAN networks (Yadav, 2021); (Fares et al., 2022). WAN networks are used to connect networks between office branches with wide geographical distances. WAN also plays a role in connecting data centers at separate distances. The implementation of SDN-WAN helps to control the movement of network paths in the delivery of data packets with a software-based approach (Huddiniah et al., 2018).

Load balancing is a new technique that can streamline time by utilizing load sharing between internet service providers. Performance from the load balance is used to split the load into multiple paths (links). Load balancing is an important component in the distribution of computing technologies that attracts the attention of the world (Octavriana et al., 2021); (Devaraj et al., 2020). In this case, for example, bandwidth traffic entering from ISP-A and ISP-B gateways has long been used in online information systems, but there are often interruptions in internet connections due to the large number of users. One solution that can be taken is using graphing, which is a proprietary tool from the router (FortiNet), which can be useful in routers to test load sharing and the effect of failover in choosing a path automatically (Riffat Hasan Saputra et al., 2020).

*Corresponding author.
E-mail address: ghamawellyandi26@gmail.com (Ghama Wellyandi)

Method

In this case, the author collects data and information that is very supportive in the preparation of the thesis, including (i) Data Collection Methods, (ii) Research Analysis, (iii) Data Preparation, (iv) Implementation, (v) Function Test Results, and (vi) Deployment.

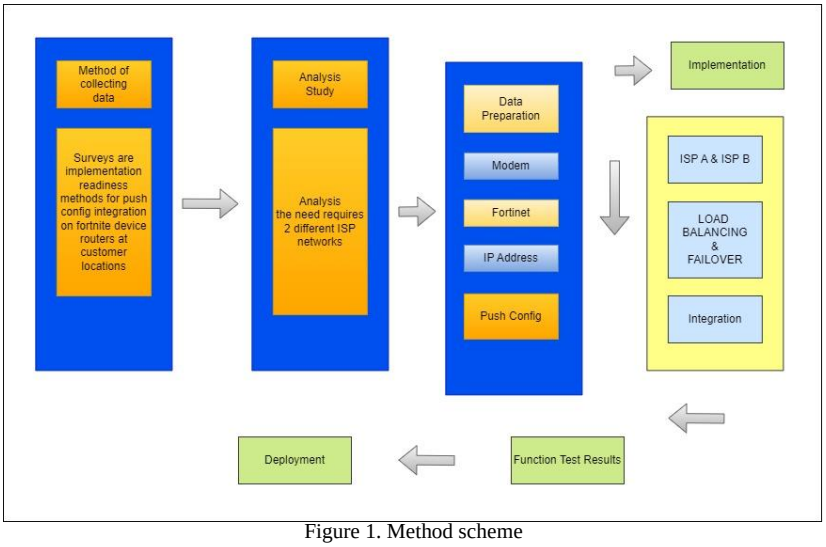

Figure 1. Method scheme

Data Collection Methods: The survey is a method of readiness implementation for the integration of push config on Fortinet device routers at customer locations.
Research Analysis: Needs analysis. The author needs 2 different ISP networks, one FortiNet CPE device managed by Lintasarta.
Data preparation: The data preparation phase includes all Activities to build the final dataset (data to be entered into modeling) from the initial raw data. Assignment Preparation data will be configured on the FortiNet device. In this case, the drafting techniques may include (i) Modem, (ii) FortiNet device, (iii) IP address, (iv) configuring the program into a GUI-shaped FortiManager language.
Implementation: So, each location in the server room contains SD-WAN technology devices that have been routed / configured; the device is a Fortinet device. It can be said that FortiNet is a router for controlling load balancing and failover. If the user experiences a network connection down at the same time on link one, it will automatically be directed to the backup link.
Function Test Results: The test is carried out using the respective modem from the ISP (Internet Service Provider), which will be connected/bypassed directly to the laptop for testing. In addition, to find out which network has been connected, I have not opened a command prompt by testing the ping test to the IP address, and speetest.net to find out whether the bandwidth speed is appropriate or not in accordance with the contract limit of the network lease.
Deployment: After the function test result stage is carried out, where the results of a network model are assessed in detail, the implementation of the entire network that has been built is carried out, followed by the monitoring stage.

Results and Discussion

Results

In analyzing the PT Lintasarta network with SD-WAN technology, the author tries to explain the computer network that is already running, which we already know above and below. To build an SD-WAN technology, we need equipment or devices connected to the network. The specifications for network devices that are needed are that ISPs must connect to the modem at the site using the Fiber optic cable line, a modem with an access point using Fiber optic, namely the

Raisecom brand, routers found on the site of each customer service, namely the Fortinet router trademark with type 50E (Wirawan & Jayadi, 2021).

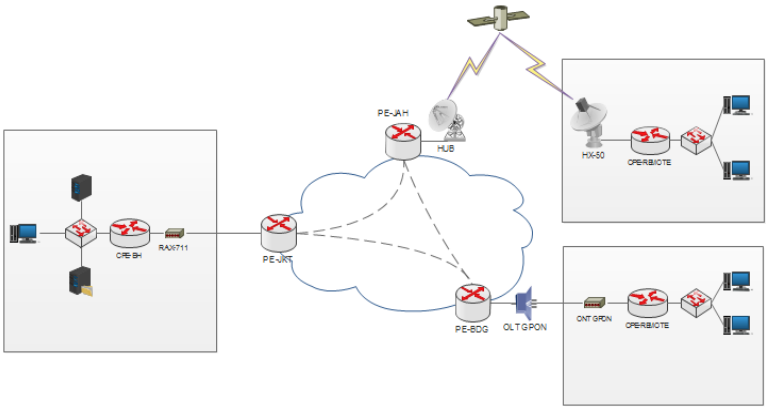

Figure 1. Mpls Topology

Figure 3. Fortinet Devices and Raisecom Modems

In this design, the author will create and implement load balancing that is able to divide network load based on speed on two ISPs, so that not only dividing but also choosing which ISP is the priority. This is obtained at the speed of each ISP, so that it can optimize existing resources. By using a router device (Fortinet 50 E), the author will configure the software FortiGate Manager. Here's an overview of the simple load-balancing topology design you want to configure.

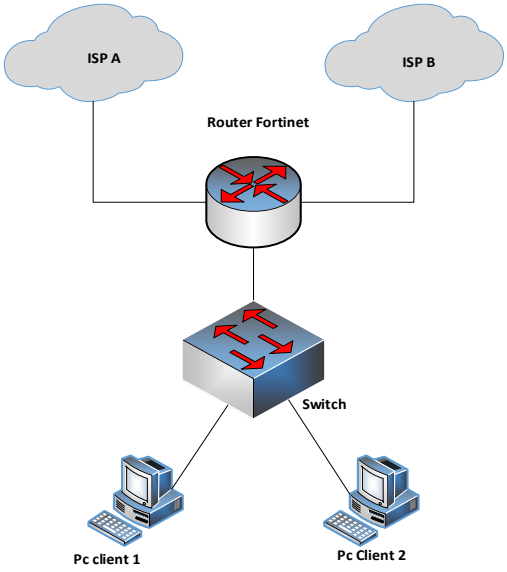

Figure 4. Application Design

In the table below, the configuration of load balancing and failover is applied, namely, configuring the IP Address. In the address list, add IP addresses for ISP A and ISP B. We just took an example for the implementation of the following site.

Table 1. IP Address Configuration ISP A

Ip public ISP A: 182.23.4.98/255.255.255.248			
DC_B	Tunnel Interface	1.1.5.32	255.255.255.255
DC_I	Tunnel Interface	1.1.1.32	255.255.255.255
DC_ME	Tunnel Interface	1.1.25.32	255.255.255.255
DR_B	Tunnel Interface	1.1.13.32	255.255.255.255
DR_I	Tunnel Interface	1.1.9.32	255.255.255.255
DR_ME	Tunnel Interface	1.1.33.32	255.255.255.255

Click the button (+), then fill in the IP Tunnel WAN Lintasarta ISP A and WAN Telkom for ISP B.

Table 2. IP Address Configuration ISP B

Ip public ISP B: 192.168.88.253/255.255.255.0			
DC_B	Tunnel Interface	1.1.5.32	255.255.255.255
DC_I	Tunnel Interface	1.1.1.32	255.255.255.255
DC_ME	Tunnel Interface	1.1.25.32	255.255.255.255
DR_B	Tunnel Interface	1.1.13.32	255.255.255.255
DR_I	Tunnel Interface	1.1.9.32	255.255.255.255
DR_ME	Tunnel Interface	1.1.33.32	255.255.255.255

In Network management, which will be implemented, it aims to help minimize the impact of a connection disruption to the first ISP in the company. The author proposes the application of load balancing techniques with SD-WAN technology so that if there is a connection interruption on the first ISP, the client PC still gets an internet connection because of the backup connection on the second ISP so that the internet connection becomes stable. And with the changes that the author makes, it is hoped that it can reduce the problems that occurred in the previous Network.

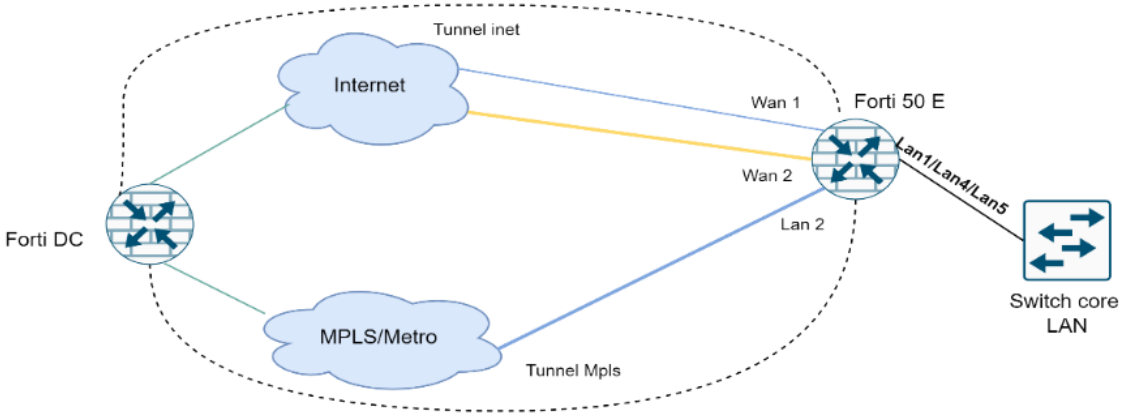

Figure 5. Proposed Network Topology

In this proposed network scheme, the author will describe the built-in monitoring of PT.lintasarta using Nagios. The author proposes and describes one B2B ISP (ISP B) with Indihome Provider and a ZTE modem as a link to the internet and as a backup for ISP A if at any time it experiences a disconnection. In this study, the author applies the load balancing technique following a picture of the proposed network scheme that will be described by distributing traffic:

Figure 6. Proposed Network Scheme

Discussion

The results of the final network test have implemented the proposed network that the author made and will be applied to the latest technology from Lintasarta, namely by adding one ISP (internet service provider), so that there are two ISPs running, as well as the implementation of load balancing and Failover. At this stage, ISP A is experiencing problems. It can be seen that ISP B immediately replaces the role of ISP A, and from the ping test results, it only requires a few moments to replace the internet connection (Yazdanmehr et al., 2022); (Yahiaoui et al., 2019). In the final network testing stage above, the results have been shown with the application of load balancing and failover techniques running well.

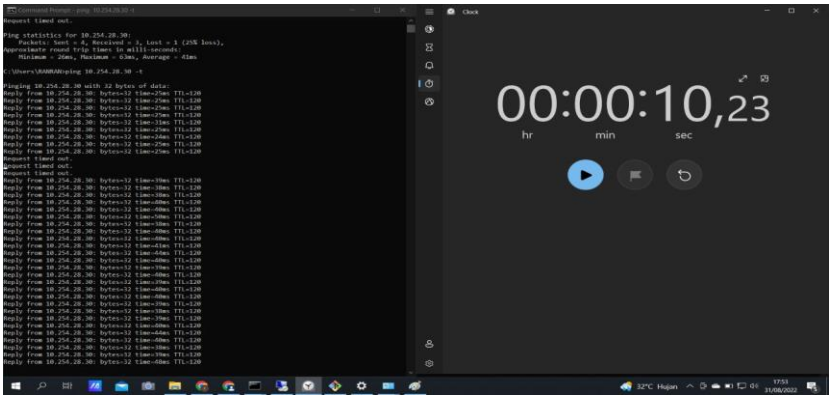

Figure 7. Failover results

Conclusions and Suggestions

Conclusions

Load Balancing is a solution on the network that can connect one internet line gateway to another. So that one network and another can be connected to each other. Load balancing is also useful as a method to keep internet functionality going because if one internet gateway dies, then the others can back each other up. From the picture, it can be seen that if one of the ISP connections dies, at that moment, it passes through the other ISP gateway.

Suggestion

There are a few suggestions that can be given to develop this research. The advice given is as follows**:**

1. Always back up the configuration after setting up the router, so as to avoid accidentally configuring it, and not to repeat the configuration again from the beginning.
2. We recommend changing the username and password on the router to be safe from interference from other irresponsible users, because the default router configuration generally has the same username and password
3. You should calculate the IP Address standings first before configuring the router to minimize misconfigurations

4. Disable unused router features so as not to consume a lot of router resources, and also minimize the crime of irresponsible people.
5. Load balancing using this PCC technique will run effectively and close to balanced if more connections (from clients) occur.

Acknowledgements
Thanks to Allah SWT, parents, wife, and family who pray so that this research can be completed on time

References

Bahtiar. (2018). Teknologi Komunikasi dan Informasi. *Al-Hikmah Media Dakwah, Komunikasi, Sosial Dan Kebudayaan*, *9*(1), 1–11. https://doi.org/10.32505/HIKMAH.V9I1.1722

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.

Fares, O., Dandoush, A., & Aitsaadi, N. (2022). SDN-based Platform Enabling Intelligent Routing within Transit Autonomous System Networks. *2022 IEEE 19th Annual Consumer Communications \& Networking Conference (CCNC)*, 909–912.

Huddiniah, E. R., Safitri, E. M., Priyambada, S. A., Nasrullah, M., & Angresti, N. D. (2018). Optimasi Rute Untuk Software Defined Networking-Wide Area Network (SDN-WAN) Dengan Openflow Protocol. *Informatika Mulawarman : Jurnal Ilmiah Ilmu Komputer*, *13*(1), 7. https://doi.org/10.30872/jim.v13i1.1006

Octavriana, T., Joni, K., & Ibadillah, A. F. (2021). Optimalisasi Jaringan Internet Dengan Load Balancing Pada High Traffic Network. *Jurnal Teknik Informatika*, *14*(1), 28–39. https://doi.org/10.15408/jti.v14i1.15018

Riffat Hasan Saputra, A. S. (2020). Pengaruh Failover Pada Jaringan Software-Defined Network dan Konvensional. *Jurnal of Internet and Software Engineering (JISE)*, *1*(1), 149–153.

Wirawan, E. D. I. Y., & Jayadi, R. (2021). Business Study of Network Provider Development in XYZ Industry Area With NNI Modeling (Network to Network Interface) as A Stage Towards Smart Industrial Park. *Journal of Theoretical and Applied Information Technology*, *99*(6).

Yadav, S. (2021). *SD-WAN Service Analysis, Solution, and its Applications*.

Yahiaoui, L., Horgan, J., Deegan, B., Yogamani, S., Hughes, C., & Denny, P. (2019). Overview and empirical analysis of isp parameter tuning for visual perception in autonomous driving. *Journal of Imaging*, *5*(10), 78.

Yang, Z., Cui, Y., Li, B., Liu, Y., & Xu, Y. (2019). Software-defined wide area network (SD-WAN): Architecture, advances and opportunities. *2019 28th International Conference on Computer Communication and Networks (ICCCN)*, 1–9.

Yazdanmehr, A., Li, Y., & Wang, J. (2022). Does stress reduce violation intention? Insights from eustress and distress processes on employee reaction to information security policies. *European Journal of Information Systems*, 1–19.