Improving Network Performance of Headquarters and Branches Using Software-Defined Network WAN (SD-WAN)

Muchlisin 1, Boy Yuliadi 1,*

* Correspondence Author: e-mail: boy.yuliadi@dosen.undira.ac.id

1 Informatics Engineering; Computer Science Faculty; Universitas Dian Nusantara; Jl. Tj. Duren Barat. 2 No.1, Kota Jakarta Barat, Daerah Khusus Ibukota Jakarta 11470, Indonesia; 0812-8770-2769; e-mail: 411192131@mahasiswa.undira.ac.id; e-mail: boy.yuliadi@dosen.undira.ac.id

Submitted : 09/12/2023
Revised : 22/12/2023
Accepted : 24/01/2024
Published : 30/03/2024

Abstract

Information Technology has developed quickly, where private companies are trying to expand their business, especially in the field of information technology. Small to medium companies also need a stable and safe internet network so that the company can grow. Companies that have branch offices in geographically separated locations must use a Wide Area Network (WAN) to be connected. SD-WAN is a special software from Software-Defined Network (SDN) technology, which is used on WAN (wide area network) connections. This research aims to provide solutions to small and medium companies to increase the SLA (Zero Downtime) of their connectivity. Currently, by implementing SD-WAN to improve the performance of head office and branch networks with a low budget. Using the PPDIOO method which is Cisco's life cycle network design approach to support computer network development. The PPDIOO method is an abbreviation of the research design used, namely Prepare, Plan, Design, Implement, Operate and Optimize. After implementing SD-WAN, this becomes a solution that can replace the function of the Juniper router currently used and reduce the burden of internet subscription costs due to its implementation. This SD-WAN simply uses 1 internet link and 1 MPLS link.

Keywords: SD-WAN, Network, PPDIOO, Load Balance

1. Introduction

The rapid progress in information technology (IT) is driving numerous private companies to expand their operations, especially within the domain of IT, (Syahrani & Yuliadi, 2023). In a technical context, information technology is defined as a set of infrastructure that supports information management. The processes of collecting, storing, searching, disseminating and reusing information are included in this category (Yuliad & Nugroho, 2016). With the increasingly rapid progress and development of data information technology, the need for communication is increasing (Syahrani & Yuliadi, 2023).

Small to medium companies also need a stable and safe internet network so that the company can develop (Fikri & Rifqi, 2023). However, a limited budget sometimes becomes an obstacle for a company to get a stable and safe internet network from threats such as malware, trojans and others (Riduan & Sadikin, 2021).

Small to medium companies sometimes also have separate branch offices in various regions (Hidayat & Akbar, 2023). Companies that have a lot of branch offices in various regions will sometimes face the problem of connecting journeys from office to office. This makes it necessary for a company to have a stable and safe network so that the company can grow. However, a limited budget sometimes becomes an obstacle for a company to get a stable and safe internet network from threats such as malware, trojans and others (Riduan & Sadikin, 2021).
geographically separated locations must use a Wide Area Network (WAN) to be connected. There are many problems with communication, including speed, bandwidth, delay, and redundancy of communication lines (Fikri & Rifqi, 2023).

Small and medium-sized enterprises (SMEs) with branches require a stable internet service to support their operations. However, SMEs often face challenges in terms of budget constraints and limited resources. Due to these issues, the author aims to address this research by exploring the use of SD-WAN (Software-Defined Wide Area Network) technology.

From the problem statements, the author formulates the problem as follows "How to Implement SD-WAN to Improve Head Office and Branch Network Performance (Case Study of Small & Medium Enterprise Companies)?"

This research aims to provide solutions to small and medium companies to improve SLA (Zero Downtime) from the current connectivity by implementing SD-WAN to improve the performance of the head office and branch networks by budget low (Sumbawa, 2020).

2. Research Method

In this research the author used the PPDIOO method. PPDIOO is a Cisco life cycle network design approach to support computer network development (Fikri & Rifqi, 2023). The PPDIOO method is an abbreviation of the research design used, namely Prepare, Plan, Design, Implement, Operate and Optimize (Sumbawa, 2020):

![PPDIOO Method](Fikri & Rifqi, 2023)

1) Prepare phase

The Prepare Phase, determines company and business needs, develops a network strategy, and proposes a high-level architectural concept to support a strategy, which is supported by the budget capabilities of the company or company (Saputra et al., 2019).

2) Plan Phase

This phase identifies network requirements based on goals, facilities, and user needs. This phase also describes the characteristics of the network with the aim of assessing the network by conducting a gap analysis on the best architectural design by looking at how it behaves in the operating environment (Saputra et al., 2019). Project planning helps manage tasks, responsible parties, stepping stones, and resources required for design and implementation (Saputra et al., 2019).
3) Design Phase
The technical and business requirements of the previous situation shape the network design. To meet today's technical and business requirements, network design specifications are comprehensive and detailed designs. The network must ensure performance, scalability, reliability, security, and availability (Saputra et al., 2019).

4) Implement Phase
In this phase, new equipment is installed and configured, according to design specifications. These new devices will replace or augment existing infrastructure. During this phase, project planning must also be considered, if there are changes they must be communicated in meetings by reaching agreement (Saputra et al., 2019).

5) Operate Phase
Operate phase, maintains the integrity of daily operational network activities, such as managing and monitoring network components, maintaining routing, managing upgrade activities, managing performance, identifying and correcting network errors. During the operation period, network management must monitor network performance and stability (Saputra et al., 2019).

6) Optimize Phase
The Optimize phase, involves network managers being proactive in identifying and resolving issues before they impact the network. Optimize phase, it is possible to change the network design if network problems become too numerous, to fix performance problems or solve application problems (Saputra et al., 2019).

3. Results and Analysis
3.1. Discussion
In this research we get a problem from an SME (small medium enterprise) company which operates in retail sales and has 7 branch stores. Currently using 2 ISPs with dedicated internet services and one Metro-e service. The device currently used is Juniper as a VPN Tunneling router. Apart from that, to maintain data communication between the Head Office and the Store, we currently use two different ISPs. The following is the existing topology:

The existing topology causes the costs for network procurement to be large and the additional use of Juniper device licenses means that currently existing devices have to be upgraded, of course this requires large costs. Seeing this problem, a redesign of the existing topology and ongoing traffic flow was carried out. In the form of eliminating internet (ISP 2) services, as well as using site-to-site IP Security VPN communication on 1 existing line and the MPLS line will be coated with site-to-site IP Security VPN as well, so that data communication between the head office and branch offices will be better. safe. Then, managing the redundancy for the load balance of the 2 lanes will be handled with SD-WAN. And it has also been updated with a Traffic Steering feature which helps traffic to direct apps or other traffic based on the best path, so that the function of the currently installed Juniper device will be replaced by SD-WAN.
3.2.3. Proposed Network Topology Design

In the proposed topology, the author designs a system using Juniper devices with SD-WAN technology. SD-WAN (Software Defined Wide Area Network) is a solution to this problem by managing network traffic using many available internet connections, so that if one connection fails, the traffic will be automatically diverted to another connection. And with fairly affordable costs for SD-WAN devices, SME companies can get a stable and secure network at an affordable cost.

The following is the proposed network topology:

Source: Research's Result (2023)

Figure 3. Proposed Network Topology

3.4. System Configuration
3.4.1. Interface

SD-WAN interface configuration must be enabled and member interfaces must be selected. This can be a physical interface, aggregate, VLAN, IPsec, or anything else. For firewall policies and static routes, the SD-WAN interface is shown as a GUI after configuration.
3.4.2. Setting DNS (Domain Name System)

DNS is a system that can resolve a domain into an IP address. DNS can be configured in the FortiManager menu. It can be configured in the System → DNS menu.

3.4.3 Routing

Routing is a process where packets traverse a network from one network to another. For the SD-WAN interface, the author must configure the default route. The default gateway for each SD-WAN member interface does not need to be defined in a static route table. On FortiGate to implement the AND function requires iBGP and ADVPN configuration for automation of routing between devices and ADVPN shortcuts. The author uses Static Route as an IP configuration to make it more secure.
3.4.4. VPN Tunnel

VPN Tunnel makes it easier to manage and monitor data center networks and is more secure and centralized to increase security. Fortinet SD-WAN uses the Dial Up method which acts as a responder on the Hub side to respond to requests to establish VPN tunnels from Spoke (branch) devices. VPN Tunnel can be configured in the VPN à IPsec Phase 1 and IPsec Phase 2 menu.
3.4.5. System Admin Settings
The default web admin access for FortiGate devices uses the HTTPS service with port 443. To make it more secure, the access port has been changed to another port. For example, on FortiGate devices the default HTTPS port is changed to port 49155. HTTPS port can be configured in the System → Admin menu.

3.4.6. System Log Settings
Logging Configuration The device has been pointed to FortiAnalyzer.

3.5. Testing
3.5.1. Failover Testing
For this failover test the author will carry out 2 scenarios to prove that the two links can backup each other.
a. Scenario 1: Shutdown MPLS Link and traffic running via internet (ISP 1)
The first scenario test was carried out by pinging the server at DC I then deactivating the MPLS interface and observing the ping connection. This aims to verify the solution with failover, namely being able to automatically change the path to the internet link when the MPLS link is down.
Figure 13. Disabled MPLS (1)

Source: Research’s Result (2023)

Figure 14. Disabled MPLS (2)

Source: Research’s Result (2023)

Figure 15. Test Ping

Source: Research’s Result (2023)
b. Scenario 2: Internet shutdown (ISP 1) and traffic running via MPLS
The second scenario test was carried out by pinging the server at DCI then deactivating the internet interface (ISP 1) then observing the ping connection. This aims to verify the solution with failover, namely being able to automatically change the path to the internet link when the internet link (ISP 1) is down.

Source: Research’s Result (2023)
Figure 16. Disabled ISP 1 (1)

Source: Research’s Result (2023)
Figure 17. Disabled ISP 1 (2)
3.5.2. Load balance testing

aims to prove that traffic can use both links, namely MPLS and the Internet. Both links will be active simultaneously and the existing traffic load will be distributed evenly so that there is no overload on either link. And the second IP hop for MPLS is 10.200.201.1 and the second IP hop for the internet (ISP 1) is 10.200.200.1.
Improving Network Performance of Headquarters and Branches Using Software-Defined Network WAN (SD-WAN)

4. Conclusion

From the research that has been carried out by the author, the results show that SME companies currently use Juniper routers with an end of life license issue and use 3 active links (internet+internet+MPLS) which initially aims to maintain link availability (SLA), but the impact on the costs that must be incurred by the company becomes greater. Small to medium companies also need a stable and safe internet network so that the company can grow. However, a limited budget sometimes becomes an obstacle for a company to get a stable and safe internet network. After implementing SD-WAN, this became a solution that could replace the function of the Juniper router and reduce the burden of internet subscription costs because implementing SD-WAN simply uses 1 internet link and 1 MPLS link.

Acknowledgements

The author understands that this research will be difficult to complete without support and guidance from various parties. Therefore, the author would like to express his gratitude to the presence of Allah SWT who always gives grace, grace and grace to the researchers while carrying out this research. The author's parents always provide love, support in the form of material and encouragement. To the author's supervisor, Mr. Boy Yuliadi S.T., M.Kom, for the author's life motivation in completing the author's research and always providing input and completing this research report. This award will be given to the person who guided the author. And the author would like to thank the Piksel Journal editorial team for giving us the opportunity to submit and evaluate the journal entitled “Improving Head Office and Branch Network Performance Using SD-WAN (Small Business Case Study)”. The author hopes that this journal can be useful for all readers, especially those studying computer science engineering.

Author Contributions

Muchlisin raised the topic; Muchlisin and Boy Yuliadi compiled the model and designed the experiment; Muchlisin and Boy Yuliadi implemented of SD-WAN to Improve Network Performance of Headquarters and Branches (Case Study Of Small & Medium Enterprise Companies); Muchlisin and Boy Yuliadi analyzed the results.

Conflicts of Interest

There is no conflict of interest for the author.

PIKSEL status is accredited by the Directorate General of Research Strengthening and Development No. 225/E/KPT/2022 with Indonesian Scientific Index (SINTA) journal-level of S3, starting from Volume 10 (1) 2022 to Volume 14 (2) 2026.
References


