INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2024, VOL. 70, NO. 1, PP. 5-11
Manuscript received July 27, 2023; revised March, 2024. doi: 10.24425/ijet.2024.149540

Implementation of auto failover on SD-WAN technology with BGP routing method on Fortigate routers at XYZ company

Lukman Medriavin Silalahi, Vahira Amaada, Setiyo Budiyanto,
Imelda Uli Vistalina Simanjuntak, and Agus Dendi Rochendi

***Abstract*—The current technological development is SD-WAN (Software-Defined Wide Area Network) which provides high-performance access for users located far from the head office so as to allow faster network connections and has been facilitated automation techniques for branch offices. This research solves the problem of XYZ company because it is known that the company requires network connectivity with a high SLA (Service Level Agreement) and no downtime in the information exchange process. This research hypothesis assumes that using SD-WAN would be ideal and the problems with XYZ company were resolved. The purpose of this research is the implementation of a WAN network using SD-WAN technology against two ISPs on the FortiGate router, as well as testing QoS (Quality of Service) that has been configured using the BGP (Border Gateway Protocol) routing method. This research plan consists of ISP-A using IP-VPN (Internet Protocol-Virtual Private Network) and ISP-B using broadband Internet. The test scenario was carried out using 3 methods, namely Full Service Scenario, Fail Over Scenario-1 when the IP VPN service is down and Fail Over Scenario-2 when the broadband Internet service is down. The final results of the research have obtained "Satisfactory" results for both services, including the average index on ISP-A and ISP-B of 3.7.**

***Keywords*—BGP; SD-WAN; IP-VPN; QoS; Fail Over; ISPs**

I. INTRODUCTION

THE rapid development of technology has a broad impact on the process of exchanging information that is getting faster. In long-distance communication, it also has a data rate that contains information [3, 2, 8, 26]. SDN (Software Defined Network) is a technology that has advantages in wide area coverage based on references [14] that have been carried out by IHS Markit showing that 74% of companies are conducting SD-WAN (Software Defined-Wide Area Network) trials, and more of these companies have implemented SD-WAN technology today [12, 25]. XYZ Company is an Indonesia Company engaged in electronics and has branch offices throughout Indonesia, so the Company requires network connectivity with high SLA (Service Level Aggreements) so as not to downtime in the information exchange process.

In order for this solution to be achieved, it requires setting up auto-failover so that the process of meeting the needs of the above. Auto failover functions as an automatic and dynamic setting in the event of a failure on the main network, so it can automatically move to the backup network. To support the auto-failover scheme in this research using the dynamic BGP (Border Gateway Protocol) routing method to ISPs (Internet Service Providers) who have subscribed [1, 21]. BGP is a routing protocol that is able to maintain, organize and distribute routing information between networks that follows every network change dynamically [10, 13, 17, 18].

After reviewing several studies, there is literature that correlates with the research done. First research based on references (14, 22] contains about the proposed converged SD-WAN architecture due to the lack of flexibility of the existing SD-WAN architecture. The architecture in question adapts SDN as the core of the SD-WAN suite and distributes to the company's headquarters. Different from other SDN solutions, this integrated SD-WAN architecture uses CPE (Customer Premise Equipment) as the main device for data transmission [4, 16, 19, 27].

The second research based on references [15] explains solutions and innovations regarding the constant development in the world of information technology that has an impact on application and service makers because it requires automatic and invividual deployment of resources on the network, especially for traditional infrastructure. Therefore there are alternative solutions that efficiently manage existing resources. This study proposes the application of an SD-WAN Network to connect two data centers that guarantee QoS (Quality of Service) and traffic prioritization.

The third study based on reference [7, 21] discusses three main problems, namely delays in data transmission due to network failures, high data transfer throughput caused by incorrect path selection using BGP, and efficient data distribution (Load balancing and scalability). All three issues introduce scalability, load balancing and failover issues with respect to network architecture. Next based on reference [11] presents the design of the MMS (multipath multi-WAN-hop SD WAN) system to realize an overlay network on top of the internet. MMS includes SSC (SD-WAN System Control) and Gateway MMS. The SSC is responsible for the configuration of the routing path for the entire system. MMSG uses networks

The first, third, fourth and fifh, authors are with Universitas Mercu Buana, Indonesia (email: {lukman.medriavin, sbudiyanto, imelda.simanjuntak, agusdendi}@mercubuana.ac.id).

The second author is with PT Aplikanusa Lintasarta Indonesia, Indonesia (email: vamaada@gmail.com).

The fifth author is with Badan Riset dan Inovasi Nasional Republik Indonesia, Indonesia (email: agus105@brin.go.id).

such as PON, xDSL, PLC, modem, and cellular networks to access the internet.

Next based on reference [9, 23] aims to increase knowledge about the application of agile project management to IT Infrastructure. This research uses case studies and Design Science Research Methodologies on pharmaceutical companies that transform IT network infrastructure for branch offices from conventional WAN topologies to SD-WAN topologies, managed by Lean and Kanban agile project management. As a contribution, the study proposes a project management model for agile adoption of IT Infrastructure inspired by Kanban and Lean agile project management frameworks to implement Network transformation. From the literature review that has been stated, this research has a hypothesis that the implementation of BGP in network systems by adapting SD-WAN technology and using double ISPs can provide high scalability, minimize downtime, increase SLAs adjusted to the agreement between customers and ISPs. The contribution of this research is to provide solutions to the complexity of PT XYZ's network where it has distributed branches throughout Indonesia.

II. Research Method

This research method describes the stages of the network topology design process at XYZ Company, routing protocol selection and failover scenarios. The topological design in this study as shown in Fig. 1 [5, 24].

A. Network Topology Design

The initial step is the design of the complex network topology shown on the Fig. 2, using the Hub-and-Spoke model where the Hub is placed in the Head Office and the Spoke is placed on the side of the Branch office which is Low Level Design (LLD) on the Hub side (Head Office) and on the Spoke side (Branch Office).

In the Hub network there are several parts, namely:

1. 2-two PE (Provider Edge), 1-one PE for IP VPN service and 1-one PE for Dedicated Internet service where the configuration in it has been set by the ISP-A provider.
2. In addition, there is also a 1-one Cisco device as an edge router connecting PE and the Fortigate SD-WAN router.
3. And there is a 1-one Fortigate as an SD-WAN router on the Hub side.

In the Spoke network there are several parts, namely:

1. 2- two PE, 1-one PE for IP VPN service provided by ISP-A and 1-one PE for broadband Internet service provided by ISP-B, where the configuration in it has been set by each provider.
2. And there is a 1-one Fortigate as an SD-WAN router on the Spoke side.
3. And there is a 1-one Switch Layer 2 owned by XYZ Company which is used as a LAN-Spoke.

1) IP Address Allocation

The allocation of an IP address on the network must be planned properly in order to connect devices in the network within the company. In this XYZ Company network, it uses IPv4 type IP Addresses for all IP Address allocations on each device. Furthermore, Table I will explain the IP address of each device.

2) Underlay – ISP Network Provisioning

The underlay stage is the stage of provisioning an ISP network consisting of 2-two ISPs to support network design. ISP-A operates on a VPN IP Hub, Internet Hub and Spoke IP VPN network. ISP-B operates on an Internet Spoke network.

3) IP Address Configuration

The next stage is the configuration of the IP address on the PE side of each router shown in Table I, except for the IP configuration on the ISP side, carried out by the ISP concerned.

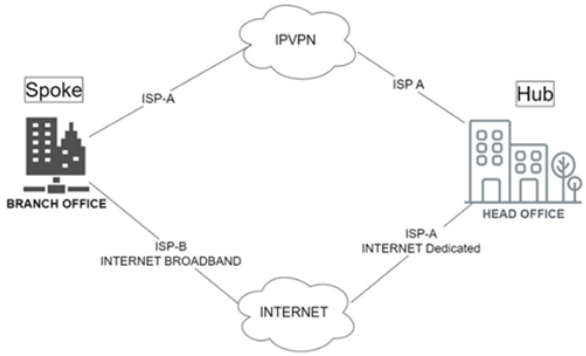
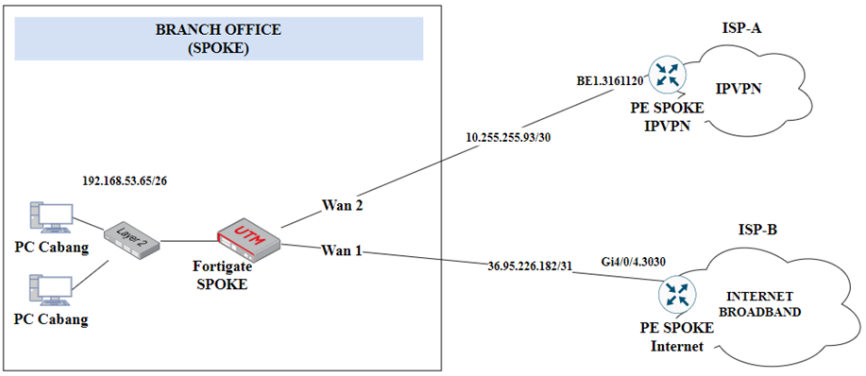
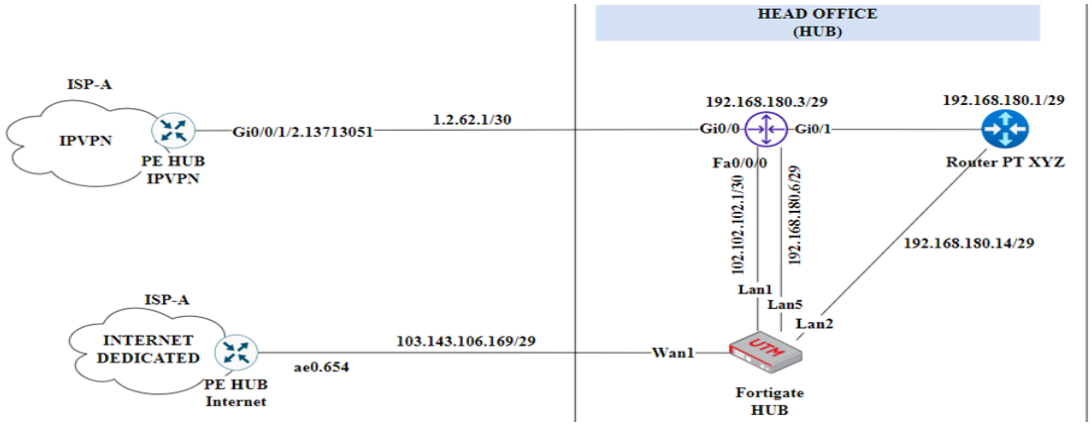


Fig. 1. Research block diagram



(a)



(b)

Fig. 2. LLD (Low Level Design) (a) Spoke topology (Branch Office) (b) Head office topology

4) Overlay – Configure IPsec and IP Tunnel on the Hub and Spoke side

After the underlay stage has been completed, the next step is the overlay stage where IPSec configuration is required [6]. In the IPSec configuration, there are 2 (two) phases that will describe the destination of the tunnel. Tunnel IP configurations need to be made in 2 forms for each Hub and Spoke, namely for VPN and Internet IP services according to the IP allocation in Table I.

.

TABLE I
TUNNEL IP CONFIGURATIONS

Service	Interface	IP Address	Description
ISP – A (Hub)	Gi0/0/1/2.13713051	1.2.62.1/30	PE IPVPN connected to CPE Cisco
ISP-A (Hub)	ae0.654	103.143.106.169/29	PE Internet Dedicated connected to FortiGate Hub
ISP-A (Spoke)	Bundle-Ether1.3161120	10.255.255.93/30	PE IPVPN connected to FortiGate Spoke
ISP-B (Spoke)	Gi4/0/4.3030	36.95.226.182/31	PE Internet Broadband connected to FortiGate Spoke
CPE Cisco (Hub)	Gi0/0	1.2.62.2/30	Edge Router connected to PE IPVPN
CPE Cisco (Hub)	Fa0/0/0	102.102.102.1/30	Edge Router connected to FortiGate Hub
CPE Cisco (Hub)	Gi0/1	192.168.180.3/29	Edge Router connected to FotiGate dan ke router XYZ Company
SD-WAN Router (Hub)	Port-1	102.102.102.2/30	Connect to CPE Cisco for IPVPN service
SD-WAN Router (Hub)		169.254.253.254/24	As Gateway IPSec for IPVPN
SD-WAN Router (Hub)	WAN-1	103.143.106.170/29	Connect to ISP-A: Internet Dedicated
SD-WAN Router (Hub)		169.254.253.254/24	Connect to Gateway IPSec for Internet
SD-WAN Router (Hub)	Port-5	192.168.180.6/29	Connect to CPE Cisco for SD-WAN gateway SD-WAN and XYZ Company router
SD-WAN Router (Hub)	Port-2	192.168.180.14 /29	Connect to LAN PT XYZ
Router PT XYZ (Hub)		192.168.180.1/29	Connect to CPE Cisco and SD-WAN gateway router (FortiGate)
SD-WAN Router (Spoke)		192.168.180.14/29	
SD-WAN Router (Spoke)	WAN-2	10.255.255.5/30	Connect to IP VPN ISP-A service
IP FortiGate Spoke-side		169.254.254.1/24	works as a Spoke side Tunnel IP for VPN IP
SD-WAN Router (Spoke)	WAN-1	36.95.226.183/31	Connect to ISP-B: Internet Broadband
IP FortiGate Spoke-side	V3	169.254.253.1/24	Serves as a Spoke side IP Tunnel for broadband Internet
SD-WAN Router (Spoke)	Port-1	192.168.53.65/26	connected to Layer 2-switch belongs to XYZ Company's Spoke-side

5) Routing configuration on the Hub side and Spoke side

After the overlay stage has been completed, then the Routing settings. Routing configuration using BGP. The implementation of the FortiGate router for BGP routing has several stages until the BGP configuration is met. The first step is to set up a community list. On the XYZ Company network, it uses ASN at tags 65530:2 for Hub and 65530:1 for Spoke. Then, create a route-map configuration as a traffic flow controller on the Hub side. If the route-map has been formed, then the neighbour BGP configuration uses the rules that have been created on the community-list and route-map.

6) Configure Firewall Policy (Security) on the Hub and Spoke side

After the routing stage has been completed, then add a Firewall policy configuration on the Hub side. This firewall policy is a set of policies that control where traffic goes, how it is processed, whether it is processed, and whether it is allowed to pass through FortiGate or not. When the Firewall receives a packet, it analyzes the source address, destination address, and services (based on port). In addition, it is necessary to register the incoming interface, outgoing interface used and schedule in a day.

7) SD-WAN Rules Spoke Configuration

On the Spoke side, SD-WAN rules are needed because based on the design provided by Fortinet to achieve the Zero-Touch-Provisioning nature of the Hub configuration, the SD-WAN zone is only configured on the Spoke side and the Hub will learn based on what is listed on the Spoke side through calling the Tunnel Hub IP when adding the SD-WAN configuration on the Spoke side.

B. Verify Hub and Spoke Configuration

TABLE II
CONFIGURATION VERIFICATION RESULTS

Service Verification	IP Result	Status
IPSec on the Hub side for the Internet	36.95.156.123	Up
IPSec on the Hub side for IP VPN	10.255.255.5	Up
IPSec on the Spoke side for the Internet	103.143.106.170	Up
IPSec on the Spoke side for IP VPN	102.102.102.2	Up
BGP on the Hub side for the Internet	169.254.253.1	Established/ Up
BGP on the Hub side for IP VPN	169.254.254.1	Established/ Up
BGP on the Spoke side for Internet	169.254.253.254	Established/ Up
BGP on the Spoke side for IP VPN	169.254.254.254	Established/Up

After the series of configurations on the Hub side and on the Spoke-side have been completed, it is necessary to verify the configuration results on the Hub and Spoke side to prove that the configuration being done is appropriate and correct. Based on the routing used, namely BGP, to prove the Hub is monitored UP, Spoke is monitored UP and the two are connected to each other, verification is required using several command check methods. The verification results on the Hub side will show that the Spoke configuration has been read on the Hub side so that the IP that appears at the time of verification is the IP on the Spoke side, and vice versa the verification carried out on the Spoke side indicates that the Hub configuration has been read on the Spoke side so that the IP that appears at the time of verification is the IP on the Hub side. The results of configuration verification are shown in Table II.

C. Scenario Experiments

Fail-over testing relates to this research. The test scenario performed consists of 3-three scenarios.

First Scenario is a full service scenario, if both connections work properly, the application runs according to its connection needs, for example SAP applications that require a private connection will run through the IPVPN path and for public applications such as Web applications and Outlook email, it will run through the path to the Internet.

The second scenario is if the IPVPN service is down, applications that use private access can go through the internet link. In this condition, the private application will run on the Internet tunnel to support connectivity to continue running privately and securely.

The third scenario is if the Internet service goes down, the application can continue to run through the IPVPN connection. In this condition, the web application and email applications will run on the IPVPN tunnel which will then use the XYZ Company's proxy which has been set up on the core side of the XYZ Company router.

After that, analyze based on QoS parameters that refer to the TIPHON (Telecommunication and Internet Proocol Harmonization Over Network) standard, including packet loss, delay and jitter, each of which has an index value to determine its quality. Table III is the standard for packet loss parameters, Table IV is the standard for delay parameters and Table V is the standard for jitter parameters.

TABLE III
PACKET LOSS CATEGORY

Category	Value (%)	Index
Very Good	0-2	4
Good	3 – 15	3
Fair	15 – 24	2
Bad	>25	1

TABLE IV
DELAY CATEGORY

Category	Value (ms)	Index
Very Good	< 150	4
Good	150 – 300	3
Fair	300 – 450	2
Bad	>450	1

TABLE V
JITTER CATEGORY

Category	Value (ms)	Index
Very Good	0	4
Good	0 – 75	3
Fair	75 – 125	2
Bad	>125	1

III. RESULT AND DISCUSSION

After the research design has been completed, this chapter discusses auto failover testing with the BGP method for later analysis of the test results. This test uses a traceroute system with one source IP LAN Spoke heading to 3 (three) Application

IP destinations, namely SAP (10.144.107.20), web application defined using google DNS (8.8.8.8) and email application (10.144.160.17). The QoS (Quality of Service) parameters used for analysis are Packet loss, Latency and Jitter.

The tests carried out, using the source options feature provided by FortiGate so that it makes it seem as if the FortiGate router on the Spoke side acts as a Spoke LAN.

A. Testing Full-Service Scenarios

Fig. 4 shows the traceroute result to the SAP application and states that the result is as desired where the SAP application is running on a private connection.

Fig. 5 shows the results of the traceroute to Email IP test stating that the results are appropriate where the Email App is running on a private connection.

Fig. 6 shows the google dns traceroute test results stating that the traceroute results are appropriate where the connection towards the web app will be directly routed to the Internet via the Public Internet IP.

B. Testing Failover Scenarios when IPVPN is Down

The test results in this scenario are shown in Fig. 7 that the IPVPN service status is monitored down. The traceroute test results can be seen in Fig. 8 which shows the traceroute to the SAP application and states that the private application will run on the IPSec Internet tunnel with IP 169.254.253.254.

Fig. 9 shows a traceroute to the mail application and states that the private application will run on an IPSec Internet tunnel with an IP of 169.254.253.254.

Fig. 10 is the result of traceroute to google's DNS based on open public will still direct to Public Internet Broadband Spoke with IP 36.95.156.122.

```
2012003732-SHARP-SUR~AYA # exe traceroute-options source 192.168.53.65

2012003732-SHARP-SUR~AYA # exe traceroute 10.144.107.20
traceroute to 10.144.107.20 (10.144.107.20), 32 hops max, 3 probe packets
 1  169.254.254.254  19.875 ms  18.885 ms  21.215 ms
 2  192.168.180.1  20.946 ms  21.564 ms  26.386 ms
 3  192      4.179  19.935 ms  21.046 ms  19.681 ms
 4  172     .93.133  20.917 ms  21.174 ms  19.915 ms
 5  192      8.250  89.397 ms *  91.729 ms
 6  192      8.249  85.015 ms  85.713 ms  93.934 ms
13  10.      .9  126.796 ms  127.792 ms  127.224 ms
14  10.      .41  129.815 ms  130.707 ms  132.289 ms
15  10.144.0.210  132.498 ms  131.764 ms  129.120 ms
16  10.144.107.20 <skaap930.gs.sharp-global.com>  127.951 ms  126.607 ms
```

Fig. 4. [Full Service] Traceroute to SAP apps

```
2012003732-SHARP-SUR~AYA # exe traceroute 10.144.160.17
traceroute to 10.144.160.17 (10.144.160.17), 32 hops max,
 1  169.254.254.254  20.225 ms  21.086 ms  19.769 ms
 2  192.168.180.1  24.172 ms  23.629 ms  23.079 ms
 3  192.     4.187  21.982 ms  22.194 ms  20.522 ms
 4  172.     93.133  23.377 ms  22.621 ms  22.285 ms
 5  192.     8.250  90.038 ms  87.607 ms  91.594 ms
11  10.1     42  127.585 ms  128.303 ms  128.993 ms
12  10.1     23  127.186 ms  143.651 ms  127.787 ms
13  10.1     .9  131.037 ms  127.765 ms  129.259 ms
14  10.1     .41  130.103 ms  130.885 ms  129.549 ms
15  10.144.160.17  130.830 ms  131.791 ms  129.143 ms
```

Fig. 5. [Full Service] Traceroute to Email

```
2012003732-SHARP-SUR~AYA # exe traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 32 hops max, 3 probe packets
 1  36.95.156.122  7.298 ms  9.700 ms  9.700 ms
 2  180.240.190.77  20.434 ms  20.978 ms  21.097 ms
 3  180.240.190.77  20.294 ms  19.919 ms  20.060 ms
 4  180.240.205.80  22.016 ms  21.935 ms  22.175 ms
 5  72.14.223.88  23.068 ms  21.728 ms  21.970 ms
 6  108.170.240.225  25.170 ms  25.339 ms  24.951 ms
 7  142.251.52.49  22.231 ms  22.205 ms  21.994 ms
 8  8.8.8.8 <dns.google>  24.348 ms  24.831 ms  24.993 ms
```

Fig. 6. [Full Service] Traceroute to DNS Google

```
2012003732-SHARP-SUR~AYA # get sys interface physical
== [onboard]
        ==[wan1]
                mode: static
                ip: 10.255.255.5 255.255.255.252
                ipv6: ::/0
                status: down
                speed: n/a
        ==[wan2]
                mode: static
                ip: 36.95.156.123 255.255.255.254
                ipv6: ::/0
                status: up
                speed: 1000Mbps (Duplex: full)
```

Fig. 7. Interface IPVPN (WAN-1) Down

```
2012003732-SHARP-SUR~AYA # exe traceroute 10.144.107.20
traceroute to 10.144.107.20 (10.144.107.20), 32 hops max,
 1  169.254.253.254  18.705 ms  19.061 ms  18.083 ms
 2  192.168.180.1  18.669 ms  19.375 ms  20.054 ms
 3  192      4.179  17.780 ms  17.991 ms  17.975 ms
 4  172     93.133  18.464 ms  17.891 ms  18.146 ms
 5  192      8.250  84.723 ms  86.993 ms  90.774 ms
13  10.      .9  124.570 ms  124.030 ms  132.287 ms
14  10.      .41  125.917 ms  126.416 ms  128.502 ms
15  10.144.0.210  126.458 ms  125.712 ms  130.008 ms
16  10.144.107.20 <skaap930.gs.sharp-global.com>  127.902 ms
```

Fig. 8. [Failover-1 Scenario] Traceroute to SAP

```
2012003732-SHARP-SUR~AYA # exe traceroute 10.144.160.17
traceroute to 10.144.160.17 (10.144.160.17), 32 hops max,
 1  169.254.254.254  20.225 ms  21.086 ms  19.769 ms
 2  192.168.180.1  24.172 ms  23.629 ms  23.079 ms
 3  192.     4.187  21.982 ms  22.194 ms  20.522 ms
 4  172.     93.133  23.377 ms  22.621 ms  22.285 ms
 5  192.     8.250  90.038 ms  87.607 ms  91.594 ms
11  10.1     42  127.585 ms  128.303 ms  128.993 ms
12  10.1     23  127.186 ms  143.651 ms  127.787 ms
13  10.1     .9  131.037 ms  127.765 ms  129.259 ms
14  10.1     .41  130.103 ms  130.885 ms  129.549 ms
15  10.144.160.17  130.830 ms  131.791 ms  129.143 ms
```

Fig. 9. [Failover-1 Scenario] Traceroute to Email

```
2012003732-SHARP-SUR~AYA # exe traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 32 hops max, 3 probe packets
 1  36.95.156.122  5.179 ms  2.723 ms  10.021 ms
 2  180.240.190.77  20.823 ms  21.442 ms  20.689 ms
 3  180.240.190.77  20.542 ms  19.867 ms  19.906 ms
 4  180.240.205.80  21.994 ms  22.679 ms  22.086 ms
 5  72.14.223.88  21.302 ms  24.452 ms  21.345 ms
 6  108.170.240.225  25.449 ms  25.119 ms  24.897 ms
 7  142.251.52.49  22.314 ms  21.889 ms  21.942 ms
 8  8.8.8.8 <dns.google>  24.349 ms  24.739 ms  23.953 ms
```

Fig. 10. [Failover-1 Scenario] Traceroute to DNS google

C. *Testing Failover Scenarios when the Internet is Down*

Fig. 11 shows that the status of the Internet service is monitored down. Fig. 12 shows the results of testing traceroute to SAP application and states that the private application will run on IPSec tunnel IP VPN with IP 169.254.254.254. Fig. 13 shows the traceroute to the mail application and states that the private application will run on the IPSec tunnel IP VPN with IP 169.254.254.254.

Fig. 14 is the result of traceroute to google DNS based on open public will first go through IPSec tunnel IP VPN with IP 169.254.254.254 then directed to Internet Hub with IP gateway Public Internet Hub 103.143.106.169 to get access to the Internet through the Hub.

```
2012003732-SHARP-SUR~AYA # get sys interface physical
== [onboard]
        ==[wan1]
                mode: static
                ip: 10.255.255.5 255.255.255.252
                ipv6: ::/0
                status: up
                speed: 1000Mbps (Duplex: full)
        ==[wan2]
                mode: static
                ip: 36.95.156.123 255.255.255.254
                ipv6: ::/0
                status: down
                speed: n/a
```

Fig. 11. Interface Internet (WAN-2) down

```
2012003732-SHARP-SUR~AYA # exe traceroute 10.144.107.20
traceroute to 10.144.107.20 (10.144.107.20), 32 hops max,
 1  169.254.254.254  17.791 ms  17.816 ms  17.877 ms
 2  192.168.180.1  18.511 ms  21.661 ms  21.452 ms
 3  192.      .179  18.391 ms  18.379 ms  19.302 ms
 4  172.      3.133  22.124 ms  19.076 ms  18.399 ms
 5  192.      .250  225.326 ms  209.306 ms  204.179 ms
12  10.:      3  235.383 ms  217.375 ms  231.005 ms
13  10.:      9  251.978 ms  237.379 ms  242.178 ms
14  10.:      41  229.909 ms  224.625 ms  213.538 ms
15  10.144.0.210  221.987 ms  214.570 ms  205.086 ms
16  10.144.107.20 <skaap930.gs.sharp-global.com>  207.243 ms
```

Fig. 12. [Failover-2 Scenario] Traceroute to SAP apps

```
2012003732-SHARP-SUR~AYA # exe traceroute 10.144.160.17
traceroute to 10.144.160.17 (10.144.160.17), 32 hops max,
 1  169.254.254.254  17.782 ms  17.926 ms  18.118 ms
 2  192.168.180.1  18.220 ms  20.345 ms  19.031 ms
 3  192.      1.187  18.236 ms  18.491 ms  17.817 ms
 4  172.      3.133  18.622 ms  19.040 ms  18.783 ms
 5  192.      1.246  82.304 ms  85.368 ms  81.160 ms
11  10.1      12  123.274 ms  124.633 ms  123.465 ms
12  10.1      13  132.381 ms  131.391 ms  137.458 ms
13  10.1       9  126.386 ms  132.578 ms  129.060 ms
14  10.144.0.41  132.268 ms  139.415 ms  136.354 ms
15  10.144.160.17  124.935 ms  125.803 ms  124.725 ms
```

Fig. 13. [Failover-2 Scenario] Traceroute tp Email

```
2012003732-SHARP-SUR~AYA # exe traceroute 8.8.8.8

traceroute to 8.8.8.8 (8.8.8.8), 32 hops max, 3 probe packets
 1  169.254.254.254  21.837 ms  20.807 ms  21.020 ms
 2  103.143.106.169  28.576 ms  26.238 ms  24.388 ms
 3  36.37.77.38  32.937 ms  25.206 ms  25.264 ms
 4  36.37.77.43  37.566 ms  37.704 ms  37.568 ms
 5  202.152.0.226  36.704 ms  35.547 ms  38.628 ms
 6  142.250.238.121  38.507 ms  36.736 ms  37.536 ms
 7  209.85.245.51  36.275 ms  36.713 ms  37.390 ms
 8  8.8.8.8 <dns.google>  36.288 ms  36.223 ms  37.402 ms
```

Fig. 14. [Failover-2 Scenario] Traceroute to DNS Google

D. *QoS Parameter Analysis*

This analysis is based on data generated from the FortiGate SD-WAN router through the Fortimanager tool as a network analyzer which is a feature of the FortiGate router.

Table VI shows the results of the analysis of packet loss parameters which states that the causality of the two services is "Excellent" with an index of 4.

TABLE VI
PACKET LOSS ANALYSIS

Time (s)	Full Service		Scenario-1		Scenario-2	
	IP VPN	Internet	IP VPN	Internet	IP VPN	Internet
60	0	0	100	0	0	100
120	0	0	100	0	1	100
180	0	0	100	0	0	100
240	0	0	100	0	1	100
300	0	0	100	0	0	100
$\bar{X}$	0	0	100	0	0,4	100
Index	4	4	-	4	4	-

Table VII shows the results of the delay parameter analysis which states that the causality of the two services is "Excellent" with index 4

TABLE VII
DELAY ANALYSIS

Time (s)	Full Service		Scenario-1		Scenario-2	
	IP VPN	Internet	IP VPN	Internet	IP VPN	Internet
60	23,4	16,4	N/A	16,5	21,5	N/A
120	21,8	16,3	N/A	16,5	20,8	N/A
180	22,5	16,5	N/A	16,6	22,7	N/A
240	21,9	16,6	N/A	16,5	21	N/A
300	22,8	16,6	N/A	16,5	21,1	N/A
$\bar{X}$	22,5	16,5	N/A	16,53	21,4	N/A
Index	4	4	-	4	4	-

Table VIII shows the results of the jitter parameter stating that the top quality of both services is "Good" with an index of 3.

TABLE VIII
JITTER ANALYSIS

Time (s)	Full Service		Scenario-1		Scenario-2	
	IP VPN	Internet	IP VPN	Internet	IP VPN	Internet
60	1,7	0,2	N/A	0,1	2	N/A
120	1,4	0,2	N/A	0,2	1,3	N/A
180	1,4	0,2	N/A	0,6	1,8	N/A
240	2,8	0,7	N/A	0,4	1,3	N/A
300	3,1	0,1	N/A	0,2	1	N/A
$\bar{X}$	**2,08**	**0,28**	**N/A**	**0,3**	**1,48**	**N/A**
Index	**3**	**3**	**N/A**	**3**	**3**	**N/A**

CONCLUSION

This research has successfully designed and implemented a WAN network by utilizing SD-WAN technology using two ISPs on the FortiGate router device to support the network at XYZ Company. This research also provides test results of Failover scenarios with 3 conditions and obtained test results that are expected that when one of the services experiences a network failure, the application can automatically move to a normal service. Based on data retrieval using the FortiManager

feature of the FortiGate router, it was found that the quality of the two services was "Satisfactory" with an Index value for IPVPN services provided by ISP-A and broadband Internet provided by ISP-B of 3.7 with the category "Satisfactory". The advice that can be given is that it is hoped that further research can be developed for failover systems with more complex network schemes with other types of dynamic routing to prove the flexibility of SD-WAN technology against many routing protocols. As well as to prove that other dynamic routing protocols can also provide automation of complex networks.

ACKNOWLEDGEMENTS

We would like to thank Universitas Mercu Buana and Beijing Institut of Technology for the foreign co-operation research, hopefully this article will be published and become a consumption for scholars.

REFERENCES

[1] Budiyanto, S., Aprihansah, C. S., Silalahi, L. M., Vistalina Simanjuntak, I. U., Silaban, F. A., & Rochendi, A. D. (2022). Auto Discover Virtual Private Network Using Border Gateway Protocol Route Reflector. *2022 IEEE International Conference on Communication, Networks and Satellite (COMNETSAT)*, 123–129. doi:10.1109/COMNETSAT56033.2022.9994439

[2] Budiyanto, S., & Pratama, I. (2020). Classification of Network Status in Academic Information Systems using Naive Bayes Algorithm Method. *2020 2nd International Conference on Broadband Communications, Wireless Sensors and Powering (BCWSP)*, 107–112. doi:10.1109/BCWSP50066.2020.9249398

[3] Budiyanto, S., Silalahi, L. M., Silaban, F. A., Dewi, R. K., & Fajar Rahayu, I. M. (2020). Techno-Economics on Implementation of FTTH Network for Broadband Services. *2020 IEEE International Conference on Communication, Networks and Satellite, Comnetsat 2020 - Proceedings*. doi:10.1109/Comnetsat50391.2020.9328977

[4] Bustamante, J. R., & Avila-Pesantez, D. (2021). Comparative analysis of Cybersecurity mechanisms in SD-WAN architectures: A preliminary results. *2021 IEEE Engineering International Research Conference (EIRCON)*, 1–4. doi:10.1109/EIRCON52903.2021.9613418

[5] Charisma, A., Setiawan, A. D., Megiyanto Rahmatullah, G., & Hidayat, M. R. (2019). Analysis Quality of Service (QoS) on 4G Telkomsel Networks In Soreang. *2019 IEEE 13th International Conference on Telecommunication Systems, Services, and Applications (TSSA)*, 145–148. doi:10.1109/TSSA48701.2019.8985489

[6] Darmawan, E., Budiyanto, S., & Silalahi, L. M. (2022). QoS Analysis on VoIP with VPN using SSL and L2TP IPSec Method. *2022 IEEE International Conference on Communication, Networks and Satellite (COMNETSAT)*, 130–136. doi:10.1109/COMNETSAT56033.2022.9994572

[7] Demaku, N., & Dermaku, A. (2022). Improving Load Balancing and Scalability by Implementing Path Selection on BGP Using Multi SD-WAN. *J. Commun.*, *17*(4), 250–259.

[8] Fakhrurrasi, T. R., Adriansyah, A., Budiyanto, S., Andika, J., Haryanti, S., & Rachmawati, U. A. (2021). Load balance optimization in peer classifier robin method as hybrid from peer connection classifier and round robin methods. *Journal of Engineering Science and Technology*, *16*(3), 2528–2543.

[9] Fitriani, A. N., Raharjo, T., Hardian, B., & Prasetyo, A. (2021). IT Infrastructure Agile Adoption for SD-WAN Project Implementation in Pharmaceutical Industry: Case Study of an Indonesian Company. *2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)*, 1–6. doi:10.1109/IEMTRONICS52119.2021.9422650

[10] Gaur, K., Kalla, A., Grover, J., Borhani, M., Gurtov, A., & Liyanage, M. (2021). A Survey of Virtual Private LAN Services (VPLS): Past, Present and Future. *Computer Networks*, *196*, 108245. doi:10.1016/j.comnet.2021.108245

[11] Lee, S., Chan, K.-Y., & Chen, T.-Y. (2020). *Design and implementation of an sd-wan vpn system to support multipath and multi-wan-hop routing in the public internet*.

[12] Medriavin Silalahi, L., Uli Vistalina Simanjuntak, I., Artadima Silaban, F., Budiyanto, S., Heryanto, & Ikhsan, M. (2020). Integration of opencv raspberry pi 3b+ and camera sensor in access control of vehicleignition key system. *IOP Conference Series: Materials Science and Engineering*, *909*(1), 12002. doi:10.1088/1757-899x/909/1/012002

[13] Mehraban, S., Vora, K. B., & Upadhyay, D. (2018). Deploy Multi Protocol Label Switching (MPLS) Using Virtual Routing and Forwarding (VRF). *2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI)*, 543–548. doi:10.1109/ICOEI.2018.8553949

[14] Mine, G., Hai, J., Jin, L., & Huiying, Z. (2020). A design of SD-WAN-oriented wide area network access. *2020 International Conference on Computer Communication and Network Security (CCNS)*, 174–177. doi:10.1109/CCNS50731.2020.00046

[15] Mora-Huiracocha, R. E., Gallegos-Segovia, P. L., Vintimilla-Tapia, P. E., Bravo-Torres, J. F., Cedillo-Elias, E. J., & Larios-Rosillo, V. M. (2019). Implementation of a SD-WAN for the interconnection of two software defined data centers. *2019 IEEE Colombian Conference on Communications and Computing (COLCOM)*, 1–6. doi:10.1109/ColComCon.2019.8809153

[16] Ouamri, M. A., Barb, G., Singh, D., & Alexa, F. (2022). Load Balancing Optimization in Software-Defined Wide Area Networking (SD-WAN) using Deep Reinforcement Learning. *2022 International Symposium on Electronics and Telecommunications (ISETC)*, 1–6. doi:10.1109/ISETC56213.2022.10010335

[17] Previdi, S., Filsfils, C., Lindem, A., Sreekantiah, A., & Gredler, H. (2019). Segment Routing Prefix Segment Identifier Extensions for BGP. In *IETF RFC 8669*. IETF.

[18] Ramadhan, E., Firdausi, A., & Budiyanto, S. (2017). Design and analysis QoS VoIP using routing Border Gateway Protocol (BGP). *2017 International Conference on Broadband Communication, Wireless Sensors and Powering (BCWSP)*, 1–4. doi:10.1109/BCWSP.2017.8272556

[19] Segeč, P., Moravčik, M., Uratmová, J., Papán, J., & Yeremenko, O. (2020). SD-WAN - architecture, functions and benefits. *2020 18th International Conference on Emerging ELearning Technologies and Applications (ICETA)*, 593–599. doi:10.1109/ICETA51985.2020.9379257

[20] Silalahi, L. M., Budiyanto, S., Silaban, F. A., Sitorus, H. B. H., Rochendi, A. D., & Ismail, M. F. (2021). Analysis of the effectiveness of online electronic learning system using data traffic network performance management to succeed merdeka learning--Merdeka campus during the Covid-19 pandemic. *International Journal of Electronics and Telecommunications*, *67*(4), 595–601.

[21] Silalahi, L. M., Budiyanto, S., Simanjuntak, I. U. V., Effendi, R. A., Rochendi, A. D., Kampono, I., & others. (2023). Application of MPLS Tunnel Service L2TP-VPN Optimization Concept with Traffic Engineering Method for Looping-Protection Service Analysis. *International Journal of Electronics and Telecommunications*, 115–120.

[22] Silalahi, L. M., Budiyanto, S., Simanjuntak, I. U. V., Silaban, F. A., Sulissetyo, N. G., & Rochendi, A. D. (2020). Bandpass Filter Design using the Square Loop Resonator on 3 GHz Frequency for Radar Applications. *2020 IEEE International Conference on Communication, Networks and Satellite, Comnetsat 2020 - Proceedings*. doi:10.1109/Comnetsat50391.2020.9328928

[23] Silalahi, L. M., Ikhsan, M., Budiyanto, S., Vistalina Simanjuntak, I. U., Osman, G., & Rochendi, A. D. (2022). Designing a Thief Detection Prototype using Banana Pi M2+ Based Image Visual Capture Method and Email Notifications. *2022 5th International Conference of Computer and Informatics Engineering (IC2IE)*, 293–296. doi:10.1109/IC2IE56416.2022.9970065

[24] Silalahi, L. M., Jatikusumo, D., Budiyanto, S., Silaban, F. A., Simanjuntak, I. U. V., & Rochendi, A. D. (2022). Internet of things implementation and analysis of fuzzy Tsukamoto in prototype irrigation of rice. *International Journal of Electrical and Computer Engineering*, *12*(6), 6022.

[25] Toy, M., & Toy, A. (2021). Overall Network and Service Architecture. In M. Toy (Ed.), *Future Networks, Services and Management: Underlay and Overlay, Edge, Applications, Slicing, Cloud, Space, AI/ML, and Quantum Computing* (pp. 93–155). Springer International Publishing. doi:10.1007/978-3-030-81961-3

[26] Ubedilah, Budiyanto, S., & Silalahi, L. M. (2022). Analysis QoS VoIP using GRE + IPSec Tunnel and IPIP Based on Session Initiation Protocol. *2022 5th International Conference of Computer and Informatics Engineering (IC2IE)*, 47–54. doi:10.1109/IC2IE56416.2022.9970120

[27] Wang, J., & Zheng, L. (2022). SD-WAN: Edge Cloud Network Acceleration at Australia Hybrid Data Center. In L. Barolli, F. Hussain, & T. Enokido (Eds.), *Advanced Information Networking and Applications* (pp. 659–670). Springer International Publishing.