Available online at: https://proceeding.researchsynergypress.com/index.php/cset
RSF Conference Series: Engineering and Technology
ISSN 2809-6843 (Online) | 2809-6878 (Print)
Volume 1 Number 2 (2021): 14 - 20

Securing Data Network for Growing Business VPN Architectures Cellular Network Connectivity

Hillman Akhyar Damanik[1]
[1] Faculty of Information Technology Budi Luhur University, Jakarta, Indonesia

Abstract

Private networks allow organizations to leverage, customize and dedicate LTE network capabilities to their own service needs. These networks are controlled and managed locally and can be optimized for specific network services and applications. Often they are used because there may be gaps in coverage where there is no cellular connectivity. Enterprises and businesses running on light application systems, using small bandwidth and requiring fast deployment such as ATMs, vending machines, digital signage kiosks and small store branches We propose a method and concept and implementation, in the form of a Data Network Security Configuration For Business Growth VPN architecture Mobile Network Connectivity for various businesses. By implementing products and services by developing the configuration and model of VPN Tunneling Protocol rules, using the EOIP Protocol and SSTP Protocol methods and virtualization schemes using the VLAN Bridging method on Wide Area Network (WAN) network connectivity. This method takes advantage of the LTE features found on the RB751U-2hnd and then integrates Huawei Mobile Broadband LTE. We also present a general Service Level Agreement (SLA) and an open source tools-based SLA network system Zabbix. Then configure the VPN Tunneling Protocol and its features on the RB751U-2hnd using Paramiko Network Automation. The focus of the results of this research is that by utilizing the available tools we will build a VPN with system monitoring facilities with the results achieved are network performance and availability and show that the design we build can be used for private connections for growing businesses. the results obtained from testing for 1 month for the 3 providers used, for the average throughput value with VPN tunneling applied TSEL 14.2 Mbps, ISAT 13.9 Mbps and XL 13.5 Mbps. The SLA value obtained is based on acceptable criteria, TSEL 91.5%, ISAT 91.8% and XL 90.6%.
Keywords: *VPN, SSTP, PPTP, EoIP, Network Automation, Zabbix, Service Leve Agreement.*

INTRODUCTION

The VPN is a tunnel that provides security connection to a remote resource. Data link layer and network layer design is used to implement cloud connectivity. Network virtualization using a combination of technology and methodologies that uses a well understood network design for both service providers and cloud users [1] [2] [3] [4] [5].

The Personal Point-to-Point Protocol (PPTP) Virtual Private Network is widely used in small, medium and corporate businesses in the telecommunications sector for their customers [6] [7]. In this paper, we apply and propose implementation methods and concepts, in the form of real configurations on security data networks for business growth VPN architecture mobile network connectivity for various businesses. By implementing a product and service by developing a VPN tunneling protocol configuration and rule model, using the tunneling bridge EoIP over PPTP and SSTP Protocol methods and virtualization schemes using the VLAN Bridging method on Wide Area Network (WAN) network connectivity [8]. This method takes advantage of the LTE features found on the RB751U-2hnd and then integrates Huawei Mobile Broadband LTE. We also present Network Availability and an open source tools-based SLA network system Zabbix. Zabbix will be used to monitor Network Availability and SLA network system in the form of usage traffic that is monitored for 1 month and ICMP packets. Then configure PPTP and SSTP

Corresponding author
hillman.akhyardamanik@budiluhur.ac.id
DOI: 10.31098/cset.v1i2.470

Protocol and their features on the RB751U-2hnd using Paramiko Network Automation. The result of this research is that by utilizing the RB751U-2hnd device and then integrating the available Huawei Mobile Broadband LTE. We will build a VPN with system monitoring facilities with the results achieved are network performance and availability and show that the design we built can be used for private connections for growing businesses. Figure 1 the implementation concept that will be applied, with the aim that later on on-premises or on endpoint devices, various concepts can be applied because we present VLAN Bridging to customer backhaul, so that later on such as routing protocols and virtualization can be applied. The VPN method can also secure data communications across untrusted networks link. This is because of their relatively low cost and ease of deployment, VPNs also allow the flexibility for administrator to be able to access network resources in a secure manner from anywhere in the global internet. This paper covers functionality testing and performance testing in terms of Service Level Agreement (SLA), which will be explained in each of the sub-sections below. This SLA value parameter will be a guarantee value for the quality of link availability for customer that has been agreed with the Service Provider (SP). The SLA functionality applied to customers at remote sites is 98.5%. After knowing the parameters of this SLA value, it is hoped that at the service level and also the minimum level, customers can use the maximum service from the Service Provider (SP) [9].

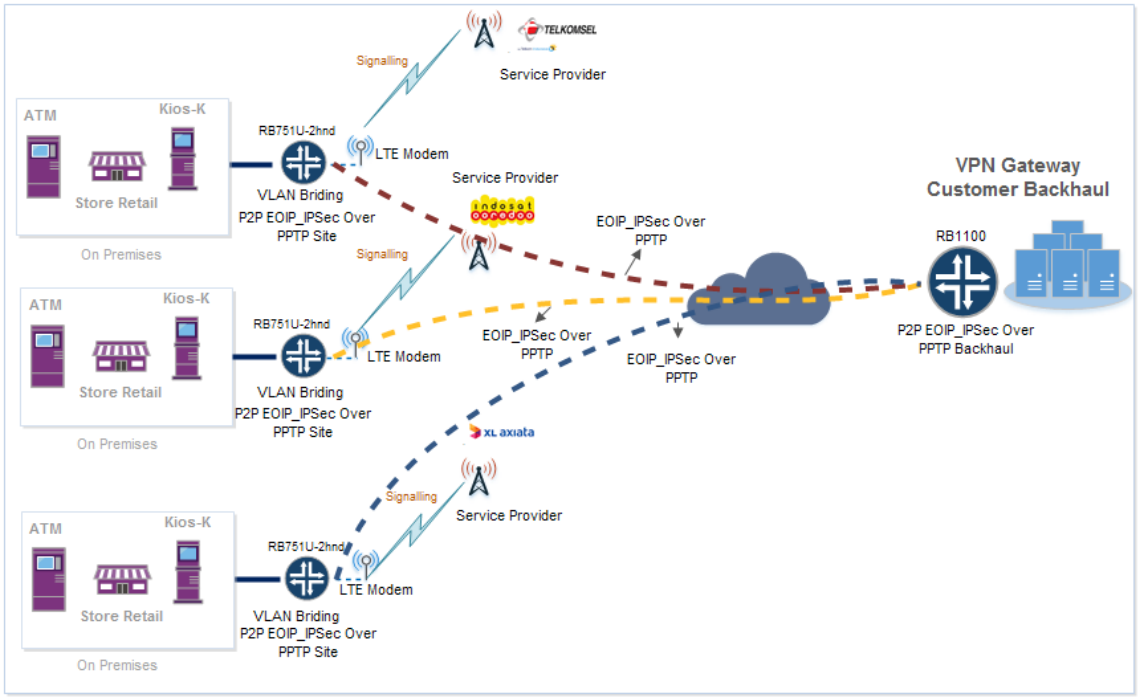

Figure1. Securing Data Network For Growing Business VPN architectures Cellular Network Connectivity

RESEARCH METHOD CONFIGURATION AND SHEME

This research is in the form of an application and technical analysis with SLA from cellular providers and based on the reliability of access media using VPN Protocol, EOIP Protocol with IPSec and SSTP Protocol methods and virtualization scheme from remote site to customer backhaul configuring VPN architectures on the cellular network connectivity is created expected to adapt to unstable network conditions, especially cellular networks.

- In general, the implementation will use 4 Huawei Mobile Broadband LTE modems as connection lines. Based on the 3 modem devices, the best connection will be taken based on the throughput quality generated by each connection per second.
- Each throughput data is then sent to Zabbix with trap and get SNMP to modify the port throughput table (Tx and Rx) in the port table of each RB751U-2hnd device.
- The test will also be analyzed within a period of 1 month for the connectivity of 4 Huawei Mobile Broadband LTE modems to each BTS service provider connection.
- Configuring and modeling VPN Tunneling Protocol rules, using the EoIP Bridging over PPTP and SSTP Protocol methods and virtualization schemes with setup and testing of data link layer (VLAN) and network layer protocol static routes and OSPF with Network Automation using Paramiko tools.

In the implementation process, several hardware used to meet needs system. Device specifications will be described in table 1 below.

Hardware Instrumentation Design and Specifications		
Hardware	**Quantity**	**Device Function**
RB751U-2hnd	4	Router VPN Tunneling: - Dial-Up Internet - SSTP Protocol Setup - PPTP Protocol Setup - VLAN Bridging - Routing Protocol
Huawei Mobile Broadband E3276	4	Dial Up Internet
Simcard (Tsel, Indosat and XL)	4	
Software Instrumentation Design and Specifications		
Linux Ubuntu Server 18.04.6 LTS (Bionic Beaver)		Operating System
Zabbix 5.4		Traffic Monitoring and Service Level Agreement (SLA)
Paramiko 3.4		Network Automation Tool

3.1 Evaluating and Configuring Scheme and Method

The design and modeling of the architectural system in this research paper uses real tools, which are intended to test dynamically with connectivity with Huawei Mobile Broadband LTE modem connections to the 3 tested providers. The selected provider is a provider that uses GSM link to considering several aspects. Some of these aspects are then computed to produce a parameter that is used as a guide for network selection. The signaling configuration of the RB751U-2hnd device will be built under a VPN connection with the aim of making the connection more secure and the main point is to build a VPN network by integrating EoIP bridging over PPTP and SSTP, this paper include functionality testing and performance testing in term of Service Level Agreement (SLA), which will be explained in each of the sub-sections below.

3.1.1 Evaluating and Setup Signalling Dial LTE

The dial-up process is a connecting process a device on the RB751U-2hnd LTE interface port with the internet through the cellular provider network to get internet via Dynamic IP. This dial-up process aims to provide access to internet from the host router RB751U-2hnd which is used as a gateway. After the host router has finished the dial-up process, it is tested by sending ICMP packets to an IP address on the global internet. The following table 7 shows test procedure for dial-up process from a modem on the host routers.

Procedure: match conditions and actions to apply to match dial-up:

- Add supported 4G LTE device modem
  - Direct-IP Interface only
  - QMI protocol mode coming in RB751U-2hnd
  - Verify SIM card activated with carrier provider
- Configuring APN in LTE port interface
- Enable LTE port interface
- Enable and configuring DHCP-Client on interface LTE and add default route
- Verify running LTE on port interface
- Configuring PPP interface and enabled advanced mode
- Configuring data channel & info channel
- Enable port interface PPP.

3.1.2 Evaluating and Setup Ethernet over IP (EOIP) method

The main thing in implementing Ethernet over IP is the tunnel-id which is a method to identify the tunnel above the internet network obtained from the service provider. Interface port traffic will be bridged as if there was a physical Ethernet and wired interface between the remote to the backhaul site with bridging enabled [10] [11]. This protocol allows multiple network schemes between remote site and backhaul site.

3.1.3 Evaluating and Setup Point to Point Tunnel Protocol (PPTP) method

The PPTP protocol in this paper is for remote access tunneling after being connected from a cellular service provider, then the PPP protocol is built to be able to connect between remote sites to

backhaul. This protocol allows organization network expansion using private tunneling method [12].

The concept this protocol works first PPTP encapsulates the packet inside the PPP packet, it is encapsulated with GRE and finally encapsulate in IP header [13]. PPTP remote and backhaul customer site setup as shown in Figure 3.

This tunneling technique works in remote-backhaul architecture and PPTP ensures authentication and encryption. Permit and allow authentication using PAP, CHAP and MSCHAP.

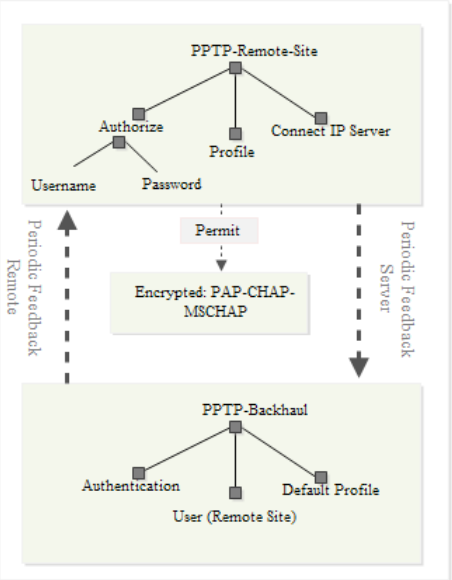

Figure3. Proposed setup PPTP method remote site and backhaul

3.1.4 Evaluating and Setup Secure Socket Tunnel Protocol (SSTP) method

The SSTP protocol in this paper is how we will connect with multiple networks through dynamic networks using SSTP. Here we will emphasize the creation of certificates with OpenSSL on the SSTP configuration both on the backhaul and remote sites.

Figure 4 shows the connection applied from the remote site to the backhaul customer site via an SSTP encrypted tunnel. The RB751U-2hnd device is connected to the internet via an LTE connection obtained from a cellular provider with a dynamic IP [14] [15].

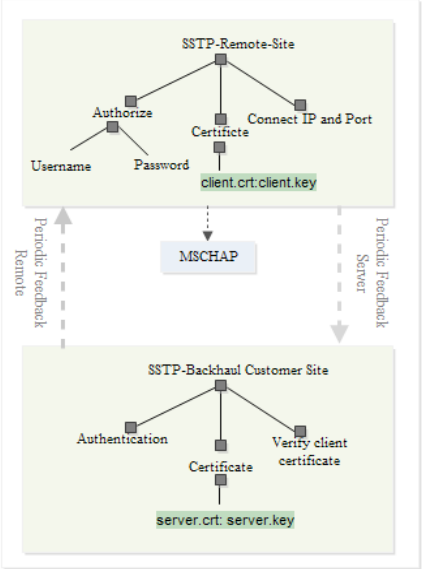

Figure 4. Proposed setup SSTP method remote site to backhaul

3. Design Integrate Data Network For Growing Business VPN architectures Cellular Network Connectivity

The implementation will use 4 Huawei Mobile Broadband LTE modems as connection lines. Based on the 4 (four) modem devices, the best connection will be taken based on the throughput quality generated by each connection per second. Each throughput data is then sent to zabbix with trap and get SNMP to modify the port throughput table (Tx and Rx) in the port table of each RB751U-2hnd device. The test will also be analyzed within a period of 1 month for the connectivity of 4 Huawei Mobile Broadband LTE modems to each BTS service provider connection.

4.1 Index Data Collection and analysis

4.1.1 Index Throughput After the throughput data is entered into the zabbix database then the zabbix application will determine for the service level agreement data from the time tested for 1 month.

$$Rx_{bps} = Rx_2\text{-}Rx_1 \quad (4.1)$$

$$Tx_{bps} = Tx_2\text{-}Tx_1 \quad (4.2)$$

$$Parameter = \frac{Rxbps+Txbps}{RTT} \quad (4.3)$$

R_{x1}= Number of packets received in the first second (bytes)

R_{x2}= Number of packets received in the second second (bytes)

T_{x1}= Number of packets sent in the first second (bytes)

T_{x2} = Number of packets sent in the second second (bytes)

Rx_{bps}= Packets received per second (bytes per second)

Tx_{bps}= Packets sent per second (bytes per second)

RTT= Round Trip Time (time required for a packets to return to sender) (milliseconds)

4.1.2 Index Service Level Agreement (SLA)

The Service Level Agreement (SLA) modeling concept will explain the calculations in detail as shown in table 2. In this paper, we assume the SLA is 99.5% which must be obtained during 1 week period of the implemented connectivity. SLA calculation in table 3, when sending ICMP Ping time is 1, then the SLA value will be calculation is up. When the ICMP Ping time value is 0, it will affect the SLA value because the remote site status is downtime.

SLA Service	
Description Customer	**Customer Service**
Status calculation algorithm	Problem, if all device have problems
Calculation SLA, Acceptable SLA (%)	99.5
Trigger	ICMP Ping Time (Unavailable Ping)
Period	Uptime

4.2 Test Performance Index Throughput

Performance testing on this system is carried out to find out how good the throughput quality is obtained by users using the VPN Tunneling mechanism with connectivity to the nearest cellular network BTS.The analysis results of throughput vary depending on the default protocol parameters and encryption method. For throughput measurement, zabbix is used to trap Tx and Rx traffic on the ether 2 router interface and different delay values of 20 milliseconds to 50 milliseconds when uploading and downloading from remote sites to backhaul customers.

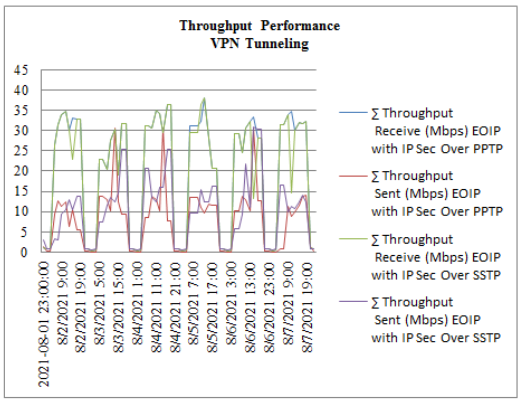

Figure 5. Index Throughput Performance VPN Tunneling (Provider TSEL)

Based on the data in the graph in Figure 5, the results of the download and upload throughput performance test results with the VPN tunneling use of real time 4G TSEL

Throughput Performance VPN (TSEL) Network Connectivity	
Index Throughput	Average (Mbps)
∑ Receive EOIP with IP Sec Over PPTP	20.11691591
∑ Sent EOIP with IP Sec Over PPTP	7.856867672
∑ Receive EOIP with IP Sec Over SSTP	19.40961971
∑ Sent EOIP with IP Sec Over SSTP	9.815818178

Table 4 shows the average test download, upload and use of real time 4G TSEL provider with the results of receiving and sending EOIP with IPSec over PPTP an average of 20.4 Mbps (receive) and 7.8 Mbps (sent) and EOIP with IPSec over SSTP an average of 19.4 Mbps (receive) and 9.8Mbps. Based on the data in the graph in Figure 6, the results of the download and upload throughput performance test results with the VPN tunneling use of real time 4G ISAT

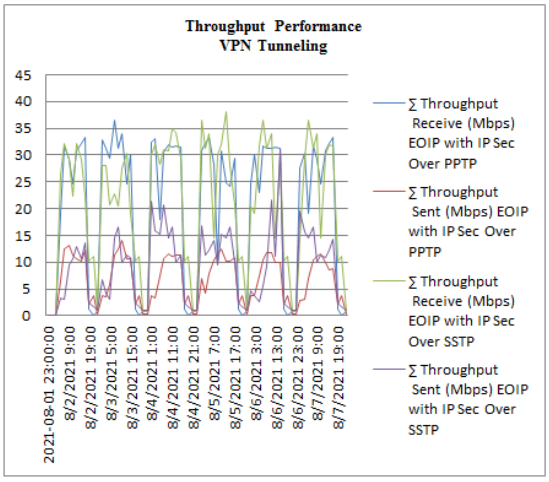

Figure 6. Index Throughput Performance VPN Tunneling (Provider ISAT)

Table 5 shows the average test download, upload and use of real time 4G ISAT provider with the results of receiving and sending EOIP with IPSec over PPTP an average of 19.7 Mbps (receive) and 6.6 Mbps (sent) and EOIP with IPSec over SSTP an average of 20.7 Mbps (receive) and 8.6Mbps.

Throughput Performance VPN Provider (ISAT) Network Connectivity	
Index Throughput	Average (Mbps)
∑ Receive EOIP with IP Sec Over PPTP	19.762458
∑ Sent EOIP with IP Sec Over PPTP	6.6326053
∑ Receive EOIP with IP Sec Over SSTP	20.728309
∑ Sent EOIP with IP Sec Over SSTP	8.6712368

Based on the data in the graph in Figure 7, the results of the download and upload throughput performance test results with the VPN tunneling use of real time 4G XL

The graph in Figure 7 shows the results of the download and upload throughput performance test results with the VPN tunneling use of real time 4G XL an average of 28.7 Mbps (receive) and 15.2Mbps (sent) taken in a period of 1 week.

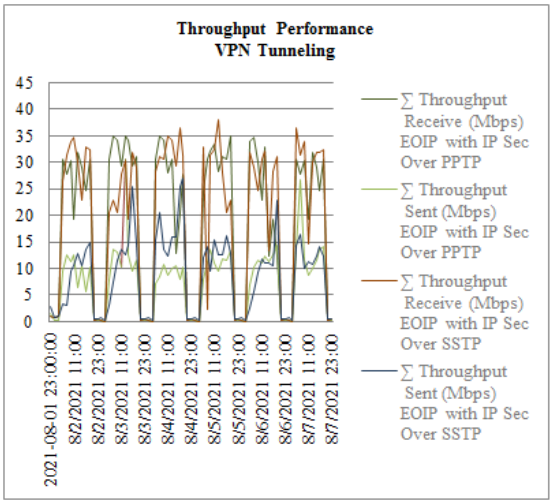

Figure 7. Index Throughput Performance VPN Tunneling (Provider XL)

Throughput Performance VPN Provider (XL) Network Connectivity	
Index Throughput	Average (Mbps)
∑ Receive EOIP with IP Sec Over PPTP	18.87187435
∑ Sent EOIP with IP Sec Over PPTP	7.671841366
∑ Receive EOIP with IP Sec Over SSTP	18.94041443
∑ Sent EOIP with IP Sec Over SSTP	8.674071554

Table 6 shows the average test download, upload and use of real time 4G XL provider with the results of receiving and sending EOIP with IPSec over PPTP and EOIP with IPSec over SSTP.

4.3 Test Performance Index Service Level Agreement (SLA)

The results of this SLA, are the quality assurance value of the availability of links from remote customer sites to customer backhaul. This SLA value is also a guarantee of the quality of link availability for customers which has been agreed with the Service Provider (SP). In this study, the SLA value from the remote site to the core backhaul using the device used will be seen in the presentation of the SLA obtained within 1 month. Knowing the value of this SLA parameter, can provide an overview to the user to be able to implement the system that is being implemented.

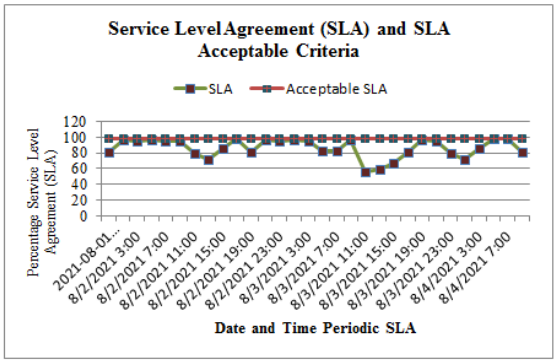

Figure 8. SLA Performance VPN Tunneling (Provider TSEL)

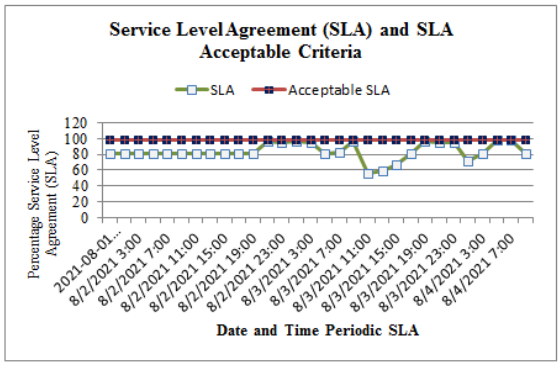

Figure 9. SLA Performance VPN Tunneling (Provider ISAT)

In this paper, the applied SLA or acceptable SLA for remote subscribers is 98.5%. Table 4.12 will describe each SLA value at each provider, within 1 month, the SLA value to customers is not fulfilled but can approach the SLA with a maximum average SLA of 91.5%, the parameter value of the SLA on the Telkomsel service provider is 91.8 %, ISAT provider 9.8% and XL 90.6%. This SLA value parameter is expected at the service level and also the minimum level, customers can use the maximum service from the Service Provider (SP).

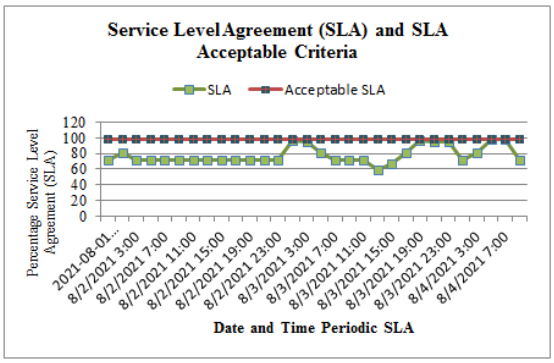

Figure 10. SLA Performance VPN Tunneling (Provider XL)

CONCLUSION

The design and modeling of the architectural system in this research paper uses real tools, which are intended to test dynamically with connectivity with Huawei Mobile Broadband LTE modem connections to the 3 tested providers. The selected provider is a provider that uses GSM frequencies by considering several aspects and include network reachable and unreachable, round trip and time and throughput. We also present a general Service Level Agreement (SLA) and an open source tools-based SLA network system Zabbix. Then configure the VPN Tunneling Protocol and its features on the RB751U-2hnd using Paramiko Network Automation. The results obtained from testing for 1 month for the 3 providers used, for the average throughput value with VPN tunneling applied TSEL 14.2 Mbps, ISAT 13.9 Mbps and XL 13.5 Mbps. The SLA value obtained is based on acceptable criteria, TSEL 91.5%, ISAT 91.8% and XL 90.6%. After

knowing the parameters of this throughput and SLA value, it is hoped that at the service level and also the minimum level, customers can use the maximum service from the Service Provider (SP).

REFERENCES

H. Yamaguchi and M. Ida, "SaaS virtualization method and its application," 2016 International Conference on Information Networking (ICOIN), 2016, pp. 238-243.

R. Figueiredo and K. Subratie, "Demo: EdgeVPN.io: Open-source Virtual Private Network for Seamless Edge Computing with Kubernetes," 2020 IEEE/ACM Symposium on Edge Computing (SEC), 2020, pp. 190-192.

Y. Zhao and Z. Deng, "A Design of WAN Architecture for Large Enterprise Group Based on MPLS VPN," 2012 International Conference on Computing, Measurement, Control and Sensor Network, 2012, pp. 340-342.

S. J. A. Nair and T. R. G. Nair, "Resource extension techniques in enterprise architectures through cloud connectivity," 2016 International Conference on Inventive Computation Technologies (ICICT), 2016, pp. 1-4.

A. Pavlicek and F. Sudzina, "Use of virtual private networks (VPN) and proxy servers: Impact of personality and demographics," 2018 Thirteenth International Conference on Digital Information Management (ICDIM), 2018, pp. 108-111.

J. Jones, H. Wimmer and R. J. Haddad, "PPTP VPN: An Analysis of the Effects of a DDoS Attack," 2019 SoutheastCon, 2019, pp. 1-6.

S. Narayan, C. J. Williams, D. K. Hart and M. W. Qualtrough, "Network performance comparison of VPN protocols on wired and wireless networks," 2015 International Conference on Computer Communication and Informatics (ICCCI), 2015, pp. 1-7.

Jahan, S., Rahman, M. S., & Saha, S. (2017). Application specific tunneling protocol selection for Virtual Private Networks. 2017 International Conference on Networking, Systems and Security (NSysS).

Damanik, Hillman Akhyar and merry anggraeni. "Implementation Scheme SLA and Network Availability Mechanism for Customer Service Provider." Jurnal Penelitian Pos dan Informatika (2020).

Usino, Wendi & Damanik, Hillman & Anggraeni, Merry. (2019). A Satellite LTE Delay Tolerant Capabilities Tunnelling: Design and Performance Evaluation. Journal of Physics: Conference Series. 1192. 012047.

S. T. Aung and T. Thein, "Comparative Analysis of Site-to-Site Layer 2 Virtual Private Networks," 2020 IEEE Conference on Computer Applications(ICCA), 2020, pp. 1-5.

R. K. Jain and P. Trivedi, "OSSEC Based Authentication Process with Minimum Encryption and Decryption Time for Virtual Private Network," 2016 8th International Conference on Computational Intelligence and Communication Networks (CICN), 2016, pp. 442-445.

D. Rybin, K. Piliugina and P. Piliugin, "Investigation of the applicability of SSL/TLS protocol for VPN in APCS," 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), 2018, pp. 1318-1321.

J. B. R. Lawas, A. C. Vivero and A. Sharma, "Network performance evaluation of VPN protocols (SSTP and IKEv2)," 2016 Thirteenth International Conference on Wireless and Optical Communications Networks (WOCN), 2016, pp. 1-5.

J. B. R. Lawas, A. C. Vivero and A. Sharma, "Network performance evaluation of VPN protocols (SSTP and IKEv2)," 2016 Thirteenth International Conference on Wireless and Optical Communications Networks (WOCN), 2016, pp. 1-5.