UNIVERSITAS BUDI LUHUR
FAKULTAS TEKNOLOGI INFORMASI
KAMPUS PUSAT : Jl. Raya Ciledug, Petukangan Utara, Jakarta Selatan 12260
Telp : (021) 5853753 (Hunting), (021) 7371164, Fax : (021) 5853753
Website : http://www.budiluhur.ac.id

KEPUTUSAN DEKAN FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS BUDI LUHUR

NOMOR : K/UBL/FTI/000/004/09/22

TENTANG:
PENUGASAN KEGIATAN TRI DHARMA & PENUNJANG BAGI DOSEN
FAKULTAS TEKNOLOGI INFORMASI UNIVERSITAS BUDI LUHUR
SEMESTER GASAL TAHUN AKADEMIK 2022/2023

DEKAN FAKULTAS TEKNOLOGI INFORMASI UNIVERSITAS BUDI LUHUR

Menimbang :

1) Bahwa Dosen adalah pendidik profesional dan ilmu dengan tugas utama mentrans-formasikan, mengembangkan, dan menyebarluaskan ilmu pengetahuan, teknologi, dan seni melalui pendidikan/pengajaran penelitian & karya ilmiah, dan Pengabdian pada masyarakat yang dikenal dengan istilah Tri Dharma Perguruan Tinggi;
2) Bahwa untuk meningkatkan profesionalitas dan kompetensi sebagai pendidik profesional maka dipandang perlu untuk memberikan tugas-tugas tambahan/penunjang dalam lingkup kegiatan penunjang Tri Dharma;

Mengingat :

1) Undang – undang Republik Indonesia Nomor 12 Tahun 2012 tentang Pendidikan Tinggi;
2) Peraturan Pemerintah Republik Indonesia Nomor 17 Tahun 2010 tentang Pengelolaan dan Penyelenggaraan Pendidikan;
3) Peraturan Menteri Riset, Teknologi, dan Pendidikan Tinggi Republik Indonesia Nomor 44 Tahun 2015 tentang Standar Nasional Pendidikan Tinggi;
4) Peraturan Menteri Riset, Teknologi dan Pendidikan Tinggi Republik Indonesia Nomor 15 Tahun 2017 tentang Penamaan Program Studi Pada Perguruan Tinggi;
5) Akta Yayasan Pendidikan Budi Luhur Tanggal 23 Desember 1991;
6) Peraturan Pengurus Yayasan Pendidikan Budi Luhur Cakti Nomor: K/YBLC/KEP/000/389/08/17 tanggal 24 Agustus 2017 tentang Statuta Universitas Budi Luhur;

M E M U T U S K A N

Menetapkan :

PERTAMA : Menugaskan dosen-dosen Fakultas Teknologi Informasi Universitas Budi Luhur untuk melaksanakan kegiatan **Tri Dharma Perguruan Tinggi dan penunjangnya** pada Semester Gasal Tahun Akademik 2022/2023 yang meliputi:

a. **Kegiatan partisipasi aktif** dalam Pertemuan Ilmiah sebagai Ketua/Anggota/Peserta/Pembicara/Penulis/Narasumber pada kegiatan Seminar, Workshop, Konferensi, Pelatihan, Simposium, Lokakarya, Forum Diskusi, Sarasehan dan sejenisnya;
b. **Publikasi Ilmiah** pada Prosiding, Jurnal/majalah/surat kabar dan sejenisnya;
c. **Partisipasi dalam organisasi** profesi, organisasi keilmuan dan/atau organisasi lain yang menunjang kegiatan Tri Dharma Pendidikan Tinggi;

d. **Pengabdian Kepada Masyarakat (PPM)**, dalam kegiatan terprogram, terjadwal atau insidental;

KEDUA : Dosen-dosen yang melaksanakan penugasan wajib membuat Laporan Kegiatan, dengan mengikuti pedoman dari Fakultas/Program Studi, sebagai pertanggungjawaban atas kegiatan yang diikuti;

KETIGA : Kegiatan Tri Dharma yang tidak termasuk dalam surat keputusan ini akan memiliki penugasan tersendiri;

KEEMPAT : Keputusan ini berlaku sejak tanggal ditetapkan dan akan diubah sebagaimana mestinya apabila di kemudian hari terdapat kekeliruan.

Ditetapkan di : Jakarta
Pada Tanggal : 1 September 2022
==========
Dekan Fakultas Teknologi Informasi

Dr. Ir. Deni Mahdiana, S.Kom., M.M., M.Kom

LAMPIRAN KEPUTUSAN DEKAN FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS BUDI LUHUR

NOMOR : K/UBL/FTI/000/004/09/22

TENTANG:
PENUGASAN KEGIATAN TRI DHARMA & PENUNJANG BAGI DOSEN
FAKULTAS TEKNOLOGI INFORMASI UNIVERSITAS BUDI LUHUR
SEMESTER GASAL TAHUN AKADEMIK 2022/2023

NO	NIDN	NAMA DOSEN	PROGRAM STUDI
1	0305068201	ACHMAD SOLICHIN	Ilmu Komputer
2	0312127303	ANTON SATRIA PRABUWONO	Ilmu Komputer
3	0311127802	ARIF BRAMANTORO	Ilmu Komputer
4	0319097803	DARMAWAN BAGINDA NAPITUPULU	Ilmu Komputer
5	0324127901	DENNI KURNIAWAN	Ilmu Komputer
6	0324028005	DWI PEBRIANTI	Ilmu Komputer
7	0318068702	INDRA NUGRAHA ABDULLAH	Ilmu Komputer
8	0325117805	LUHUR BAYUAJI	Ilmu Komputer
9	8833923420	MOEDJIONO	Ilmu Komputer
10	0316097401	MOHAMMAD SYAFRULLAH	Ilmu Komputer
11	0314126304	MUHAMAD SADLY	Ilmu Komputer
12	0303097901	RUSDAH	Ilmu Komputer
13	0412017103	SAMIDI	Ilmu Komputer
14	0326086304	SETYAWAN WIDYARTO	Ilmu Komputer
15	0306067506	SOFIAN LUSA	Ilmu Komputer
16	0318016801	YAN RIYANTO	Ilmu Komputer
17	0324107203	ABDUL MUIS SOBRI	Teknik Informatika
18	0302068001	ACHMAD ADITYA AU	Teknik Informatika
19	0305118901	ACHMAD ARDIANSYAH	Teknik Informatika
20	0320038303	AGUNG SAPUTRA	Teknik Informatika
21	0304039102	AHMAD PUDOLI	Teknik Informatika
22	0315018603	ALEXANDER J.P. SIBARANI	Teknik Informatika
23	0301098202	ANDRI SUNANDAR	Teknik Informatika
24	8848870018	ANDY RIO HANDOKO	Teknik Informatika
25	0314038803	ANGGA KUSUMA NUGRAHA	Teknik Informatika
26	0303129401	ANWAR RIFA'I	Teknik Informatika

27	0328079201	AQMAL MAULANA	Teknik Informatika
28	0330087506	ARMAN YUSUF	Teknik Informatika
29	0301027501	ARSANTO NARENDRO	Teknik Informatika
30	0301048101	BASUKI HARI PRASETYO	Teknik Informatika
31	0318068503	CHANDRA JATNIKA	Teknik Informatika
32	0311098901	DOLLY VIRGIAN SHAKA YUDHA SAKTI	Teknik Informatika
33	0328028503	DWI PUSPITA ANGGRAENI	Teknik Informatika
34	0315058201	FERNANDO SITINDAON	Teknik Informatika
35	0305026801	GUNAWAN PRIA UTAMA	Teknik Informatika
36	0308048501	HADIDTYO WISNU WARDANI	Teknik Informatika
37	0306058502	HARIS MUNANDAR	Teknik Informatika
38	0320038704	HILLMAN AKHYAR DAMANIK	Teknik Informatika
39	0302018604	IKA SUSANTI	Teknik Informatika
40	0317069301	IKHSAN RAHDIANA	Teknik Informatika
41	0309069301	IMAN PERMANA	Teknik Informatika
42	0005017601	IMELDA	Teknik Informatika
43	0322038603	INDRA	Teknik Informatika
44	0322118705	INDRA HERTANTO	Teknik Informatika
45	0325128504	IWAN SAPUTRA	Teknik Informatika
46	0305076701	KRISNA ADIYARTA	Teknik Informatika
47	0327118903	KUS ANDRIADI	Teknik Informatika
48	0328017702	LESTARI MARGATAMA	Teknik Informatika
49	0308128901	MEPA KURNIASIH	Teknik Informatika
50	0330127502	MERRY ANGGRAENI	Teknik Informatika
51	0321117001	MOHAMMAD ANIF	Teknik Informatika
52	0329067903	MUFTI	Teknik Informatika
53	0329068201	MUHAMMAD AINUR RONY	Teknik Informatika
54	0305126805	NANO PRAMONO SOERYONEGORO	Teknik Informatika
55	0312128002	NURUL JAMAL	Teknik Informatika
56	0322028201	PIPIN FARIDA ARIYANI	Teknik Informatika
57	0319087801	PURWANTO	Teknik Informatika

58	0308029102	PUTRI HAYATI	Teknik Informatika
59	0330108801	RAHMAT OKTAVIAN	Teknik Informatika
60	0317068301	REVA RAGAM SANTIKA	Teknik Informatika
61	0328036602	RIRIT ROESWIDIAH	Teknik Informatika
62	0313048901	RISKIANA WULAN	Teknik Informatika
63	0327068604	RIZKA TIAHARYADINI	Teknik Informatika
64	0311068001	RIZKY TAHARA SHITA	Teknik Informatika
65	0322027501	SAFRINA AMINI	Teknik Informatika
66	0305068203	SEJATI WALUYO	Teknik Informatika
67	0330016701	SISWANTO	Teknik Informatika
68	0312067402	SUBANDI	Teknik Informatika
69	0314097004	SUBANDI	Teknik Informatika
70	0302106002	SUDARMADI	Teknik Informatika
71	0305068605	SYAMSUDIN ZUBAIR	Teknik Informatika
72	0315117302	UTOMO BUDIYANTO	Teknik Informatika
73	0323108902	WILLIAM FRADO PATTIPEILOHY	Teknik Informatika
74	0317048601	WINDARTO	Teknik Informatika
75	0322058003	WINDHY WIDHYANTY	Teknik Informatika
76	0213068501	YUDI WIHARTO	Teknik Informatika
77	0320069003	ZAQI KURNIAWAN	Teknik Informatika
78	0318017504	ACEP MARDIYANA	Teknik Informatika
79	0312096401	ADY WIDJAJA	Sistem Informasi
80	0322018502	AGNES ARYASANTI	Sistem Informasi
81	0315065602	AGUNG PRIHARTONO	Sistem Informasi
82	0309088302	AGUS UMAR HAMDANI	Sistem Informasi
83	0316068301	ANITA DIANA	Sistem Informasi
84	0316079202	ANUGRAH BAGUS SUSILO	Sistem Informasi
85	0007097901	ARIEF WIBOWO	Sistem Informasi
86	0319097906	ASEP ABDUL ROHMAN	Sistem Informasi
87	0312017102	BAGUS TRI PRABAWA	Sistem Informasi
88	0319027202	BRURI TRYA SARTANA	Sistem Informasi

89	0323126401	BULLION DRAGON ANDAH L	Sistem Informasi
90	0325067402	CHANDRA SUNJAYA	Sistem Informasi
91	0311118201	COUDRY BERNADETH	Sistem Informasi
92	0328127303	DENI MAHDIANA	Sistem Informasi
93	0303129201	DEVIT SETIONO	Sistem Informasi
94	0310128401	DEWI KUSUMANINGSIH	Sistem Informasi
95	0322018301	DIAN ANUBHAKTI	Sistem Informasi
96	0305036302	DJATI KUSDIARTO	Sistem Informasi
97	0321117301	FX BIMA CAHYA PUTRA	Sistem Informasi
98	0306027701	GANDUNG TRIYONO	Sistem Informasi
99	0324096902	GOENAWAN BROTOSAPUTRO	Sistem Informasi
100	0325058101	Hendri Irawan	Sistem Informasi
101	9903260690	HESTYA PATRIE	Sistem Informasi
102	0308087105	HIMAWAN SETIADI	Sistem Informasi
103	0312078106	HIRTY PANCA SARI	Sistem Informasi
104	0303048001	HUMISAR HASUGIAN	Sistem Informasi
105	0314049302	INDAH PUSPASARI HANDAYANI	Sistem Informasi
106	0303118201	ITA NOVITA	Sistem Informasi
107	0312069205	JEREMY JONATHAN	Sistem Informasi
108	0303067601	JOKO SUTRISNO	Sistem Informasi
109	0307079301	JULAIHA PROBO ANGGRAINI	Sistem Informasi
110	0319059103	KUKUH HARSANTO	Sistem Informasi
111	0317057603	LIHIN	Sistem Informasi
112	0422036901	MARDI HARDJIANTO	Sistem Informasi
113	0307038703	MARINI	Sistem Informasi
114	0328116903	MAYANTI	Sistem Informasi
115	0311038203	MOTIKA DIAN ANGGRAENI	Sistem Informasi
116	0324078202	MUHAMAD FITRA SYAWALL	Sistem Informasi
117	0317077905	NAWINDAH	Sistem Informasi
118	0318077601	NIDYA KUSUMAWARDHANY	Sistem Informasi
119	0315028502	NOFIYANI	Sistem Informasi

120	0305078002	NONI JULIASARI	Sistem Informasi
121	0302077805	NURMANSYAH	Sistem Informasi
122	0315057803	NURWATI	Sistem Informasi
123	0302057901	PAINEM	Sistem Informasi
124	0315069301	RATNA KUSUMAWARDANI	Sistem Informasi
125	0305128107	RATNA UJIAN DARI	Sistem Informasi
126	0324038006	RETNO WULANDARI	Sistem Informasi
127	0326039202	RIZA ALAMSYAH	Sistem Informasi
128	0324118802	RIZKY PRADANA	Sistem Informasi
129	0317098201	SAFITRI JUANITA	Sistem Informasi
130	0329098202	SAMSINAR	Sistem Informasi
131	0309097401	SRI MULYATI	Sistem Informasi
132	0407127201	TEJA ENDRA ENG TJU	Sistem Informasi
133	0320127901	TITIN FATIMAH	Sistem Informasi
134	0317018702	TRI IKA JAYA KUSUMAWATI	Sistem Informasi
135	0320096102	WENDI USINO	Sistem Informasi
136	0326047001	WIWIN WINDIHASTUTY	Sistem Informasi
137	0325098802	WULANDARI	Sistem Informasi
138	0316068702	YESI PUSPITA DEWI	Sistem Informasi
139	0316017201	YUDI SANTOSO	Sistem Informasi
140	0325078803	YULIANAWATI	Sistem Informasi
141	0329077501	YULIAZMI	Sistem Informasi
142	0004105902	DWI ACHADIANI	Sistem Informasi
143	0411076603	GATOT PURWANTO	Sistem Komputer
144	0314056902	HARI SOETANTO	Sistem Komputer
145	0305027401	IRAWAN	Sistem Komputer
146	0302046501	JAN EVERHARD RIWUROHI	Sistem Komputer
147	0311118107	RIRI IRAWATI	Sistem Komputer
148	0317025801	TATANG WIRAWAN WISNUADJI	Sistem Komputer
149	0331057703	YANI PRABOWO	Sistem Komputer
150	0315038601	ARI SAPUTRO	Sistem Komputer

151	0320048401	ATIK ARIESTA	Manajemen Informatika
152	0330118001	DYAH RETNO UTARI	Manajemen Informatika
153	0324118302	JOKO CHRISTIAN CHANDRA	Manajemen Informatika
154	0301108606	MUHAMAD SALMAN ALFARISI	Manajemen Informatika
155	0307038501	WAHYU PRAMUSINTO	Manajemen Informatika
156	0323088401	FERDIANSYAH	Manajemen Informatika
157	0319047501	GRACE GATA	Komputerisasi Akuntansi
158	0317058106	LIS SURYADI	Komputerisasi Akuntansi
159	0303027601	SOVAN DIANARTO	Komputerisasi Akuntansi

Ditetapkan di : Jakarta
Pada Tanggal : 1 September 2022
==========
Dekan Fakultas Teknologi Informasi

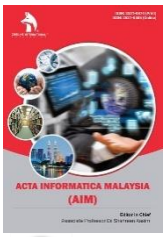
Dr. Ir. Deni Mahdiana, S.Kom., M.M., M.Kom

ZIBELINE INTERNATIONAL™ PUBLISHING

ISSN: 2521-0874 (Print)
ISSN: 2521-0505 (Online)
CODEN: AIMCCO

Acta Informatica Malaysia (AIM)

DOI: http://doi.org/10.26480/aim.01.2022.01.06



RESEARCH ARTICLE

SECURING DATA NETWORK FOR GROWING BUSINESS VPN ARCHITECTURES CELLULAR NETWORK CONNECTIVITY

Hillman Akhyar Damanik

Faculty of Information Technology Budi Luhur University, Jakarta, Indonesia.
****Corresponding Author Email: hillman.akhyardamanik@budiluhur.ac.id***

ARTICLE DETAILS

Article History:

Received 07 December 2021
Accepted 10 January 2022
Available online 17 January 2022

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 Level Agreement.

1. INTRODUCTION AND RESEARCH OBJECTIVES

In today's digital world, the scope of corporate networks in developing business wings is no longer challenging. Every organization sets up corporate offices, small offices, operations centers, production plants and sales offices all over the world and needs them to be connected via computer networks. This research will discuss small business network connectivity solutions and provide secure remote connectivity to business networks to enable remote connections and let them have access to servers, applications and file sharing as they are used to (Yamaguchi and Ida, 2016; Figueiredo and Subratie, 2020; Zhao and Deng, 2012). 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 (Nair and Nair, 2016; Pavlicek and Sudzina, 2018).

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 (Jones et al., 2019; Narayan et al., 2015). In this study, 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 (Jahan et al., 2017). 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 System).

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 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-

Quick Response Code	Access this article online	
	Website: www.actainformaticamalaysia.com	**DOI:** 10.26480/aim.01.2022.01.06

Cite The Article: Hillman Akhyar Damanik (2022). Securing Data Network For Growing Business VPN Architectures Cellular Network Connectivity. *Acta Informatica Malaysia , 6(1): 01-06.*

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. This is because of their relatively low cost and ease of deployment, VPNs also allow the flexibility for staff to be able to access network resources in a secure manner from anywhere in the world. 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 customers 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) (Damanik et al., 2020).

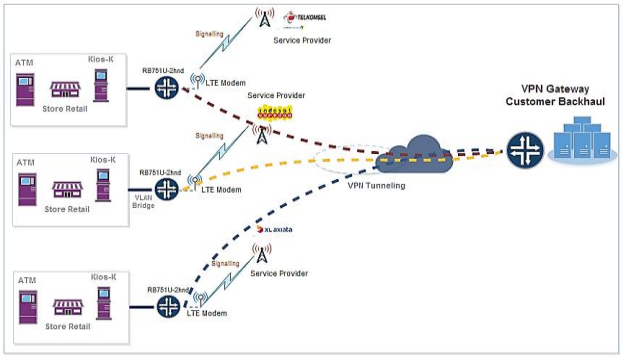


Figure 1: Securing Data Network for Growing Business VPN architectures Cellular Network Connectivity

2. Literature Review

2.1 Ethernet over IP (EoIP) with IP Security (IPSec)

Ethernet over IP (EoIP) Tunneling allows tunneling by encapsulating Ethernet frames in IP packets and forwarding them to other routers. Ethernet over IP (EoIP) creates an Ethernet tunnel over the IP connection between two routers. All Ethernet traffic will be bridged, just as if there was a physical interface (Usino et al., 2019; Aung and Thein, 2020). The design and implementation that will be carried out in this research, tunneling that will be used is Ethernet over IP with parameters to enable IPSec.

This protocol will be used as transmission over the network to carry packets and traffic from remote to backhaul customer site. Network setups with EoIP interfaces:

- Possibility to bridge interface port on-premises over the Internet
- Possibility to bridge interface port on-premises over encrypted tunnels
- Possibility to bridge interface port on-premises over 802.11b

2.2 Point to Point Tunnel Protocol (PPTP) Concept

The "point-to-point" part of the term focuses on the connection made by PPTP. This allows one point (remote site) to access another specified point (remote network) over the global Internet. The "tunneling" part of the term refers to the way one protocol is encapsulated within another protocol (Jain and Trivedi, 2016). In PPTP, the point-to-point protocol (PPP) is wrapped inside the TCP/IP protocol, which can provide an Internet connection. Therefore, even if a connection is established over the Internet, a PPTP connection mimics a direct link between two different locations and allows a secure connection. PPTP traffic through service port TCP 1723 and IP protocol GRE (Generic Routing Encapsulation (GRE), IP Protocol/47) (Rybin et al., 2018). PPTP (Point to Point Tunneling Protocol) is implemented at the data link layer of the OSI model to develop a secure tunnel for data exchange and can be used for routing processes. Strongly strengthened authentication method is implemented to increase VPN reliability & security with PPTP protocol apart from conventional username and password technique.

2.3 Secure Socket Tunnel Protocol (SSTP) Concept

SSTP protocol is as secure as Hypertext Transfer Protocol Secure (HTTPS) and Secure Socket Layer (SSL) encryption systems which have higher layer security protocol services for encryption and encapsulation (Lawas et al., 2016). Additionally, it has minimal proxy issues as it connects to TCP port 443 which is open by default. When the device used in this paper is the RB751U-2hnd as a remote site router, it is initially connected to the SSL VPN customer backhaul server (gateway) and will authenticate each other via digital certificates generated from Open SSL. SSTP serves to encapsulate Point-to-Point protocol (PPP) traffic over SSL channels of the HTTPS protocol. PPP supports strong authentication system and will be enabled for MS-CHAPv2. During encapsulation, PPP frames and IP datagrams are encapsulated for transmission of data communications over the network (Lawas et al., 2016). During encryption, messages are encrypted with an SSL channel from HTTPS.

3. Research Method Configuration and Schema

This research is in the form of an application and technical analysis with network availability and utilizing dynamic IP obtained 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. This method takes advantage of the LTE features found on the RB751U-2hnd and then integrates Huawei Mobile Broadband LTE. Several stages of testing carried out with the concepts mentioned above are:

- Configuring VPN architectures on the cellular network connectivity that is created is 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 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.
- 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 implement, 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, including network reachable, round-trip time, and throughput. 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 terms 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

Ethernet over IP (EoIP) Tunneling to create an port interface tunnel between two routers over an IP connection from a remote site to a backhaul customer. This EoIP tunnel will run on top of the PPTP and SSTP tunnels that will be deployed. When the router's linking function is enabled, all Ethernet traffic (all port interface protocols) will be bridged as if there was a physical and wired port interface between two routers (with linking enabled). This protocol allows several network schemes that can later be applied to both data link and network layer protocols. Figure 2 match conditions and actions to apply to match EoIP tunnel remote site. The main thing in implementing Ethernet over IP (EoIP) is the tunnel-id which is a method to identify the tunnel above the internet network obtained from the service provider. Tunnel-id on remote site and backhaul integer value is 972. The bridging router will be configured to be enabled, so that all Ethernet traffic will be bridged as if there was a physical Ethernet and wired interface between the remote to the backhaul (with bridging enabled). This protocol allows multiple network schemes between remote and backhaul.

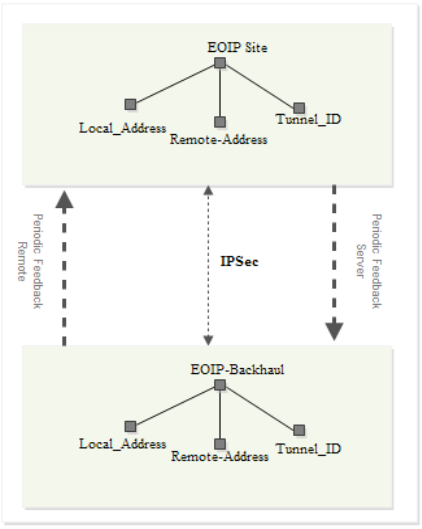


Figure 2: Proposed Ethernet over IP Remote Site

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

The Point to Point Tunneling Protocol (PPTP) in this paper is for remote access tunneling techniques 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. PPTP is a layer two tunneling protocol that extending the standard Point to Point Protocol (PPP) with dial-up networking techniques. The concept this protocol works first PPTP encapsulates the packet inside the PPP packet, it is encapsulated with GRE and finally wrapped in IP head. PPTP remote and backhaul customer site setup as shown in Figure 3. This tunneling technique works in client-server architecture and PPTP ensures authentication and encryption. Permit and allow authentication using PAP, CHAP and MSCHAP.

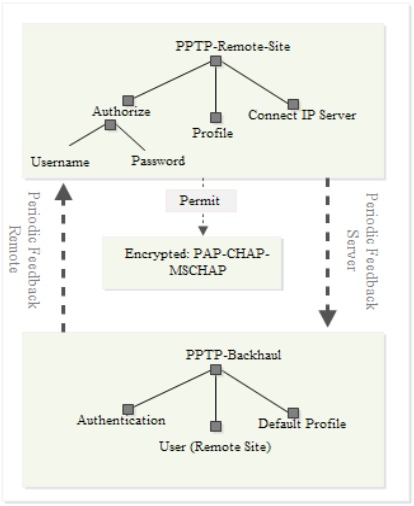


Figure 3: Proposed Setup Point to Point Tunnel Protocol (PPTP) method Remote Site and Server

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.

Procedure: match conditions and actions to apply to match SSTP remote site and customer backhaul site:

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.

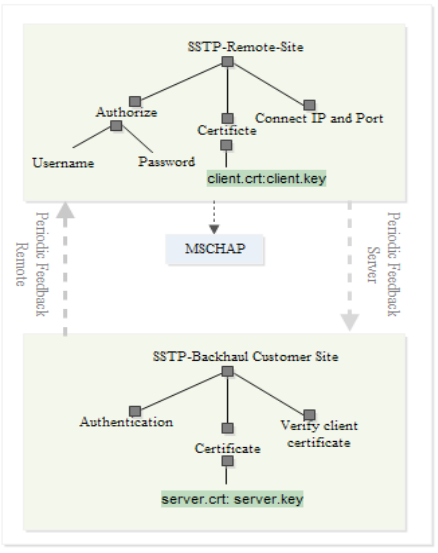


Figure 4: Proposed Setup Secure Socket Tunnel Protocol (SSTP) method Remote Site and Server

4. 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 3 (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. Configuring and modeling VPN Tunneling Protocol rules, using the EoIP with IP Sec 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.

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:

$$Rx_{bps} = Rx_2\text{-}Rx_1 \quad (1)$$

$$Tx_{bps} = Tx_2\text{-}Tx_1 \quad (2)$$

$$Parameter = \frac{Rxbps+Txbps}{RTT} \quad (3)$$

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 Bandwidth Utilization

- Bits sent is the maximum number of bits per second a network element can transfer (upload).
- Bits receive is the maximum number of bits per second a network element can transfer (download)
- Utilization (U) is the percentage of the capacity on a link or path currently being consumed by aggregated traffic
- Formula Bandwidth Utilization:

$$\frac{\sum total\ bytes\ receive\ (bps) + total\ bytes\ sent(bps)}{\sum Bandwidth\ Capacity\ (kbps)}$$

$$\frac{\sum total\ bytes\ receive\ (kbps) + total\ bytes\ sent(kbps)}{\sum Bandwidth\ Capacity\ (kbps)}$$

4.1.3 Index Service Level Agreement (SLA)

Each customer node in each node will have a status. SLA status is calculated according to the selected algorithm based on up and down time. 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 for 1 week period of the implemented connectivity.

Parameter	Description
Service times	By default the service operates 24x7x365 with the formula: *Acceptable SLA x Number of Days in 1 Month x 24 Hours*
New service time	Service times:
	Uptime - service uptime
	Downtime - Service status (Status State) in this period affect SLA.
Acceptable SLA (%)	99.5
SLA (%)	100

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 will downtime.

SLA Service Customer	
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.

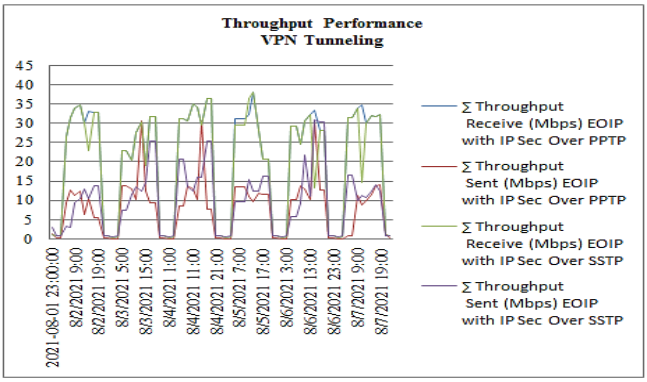


Figure 5: Index Throughput Performance VPN Tunneling (Provider TSEL)

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 Celluler (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

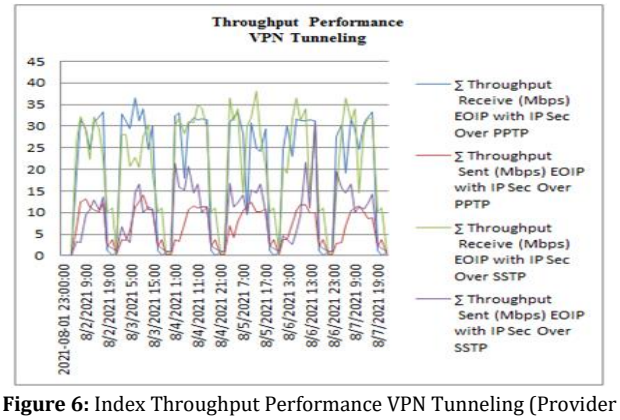


Figure 6: Index Throughput Performance VPN Tunneling (Provider ISAT)

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.

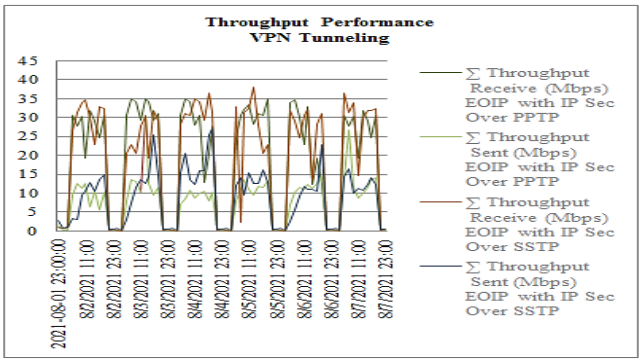


Figure 7: Index Throughput Performance VPN Tunneling (Provider XL)

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.

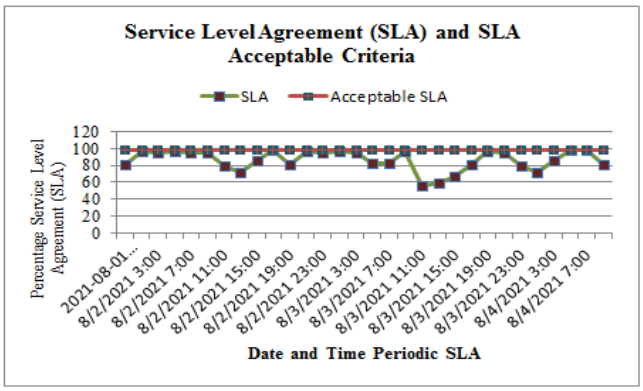


Figure 8: Service Level Agreement (SLA) Performance VPN Tunneling (Provider TSEL)

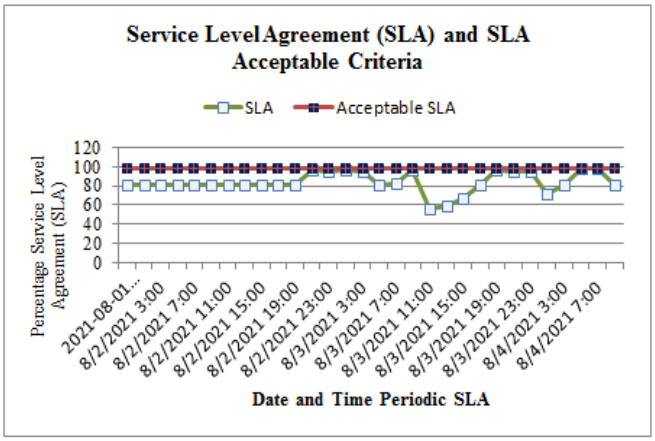


Figure 9: Service Level Agreement (SLA) Performance VPN Tunneling (Provider ISAT)

In this paper, the applied SLA or acceptable SLA for remote site 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 91.8% 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).

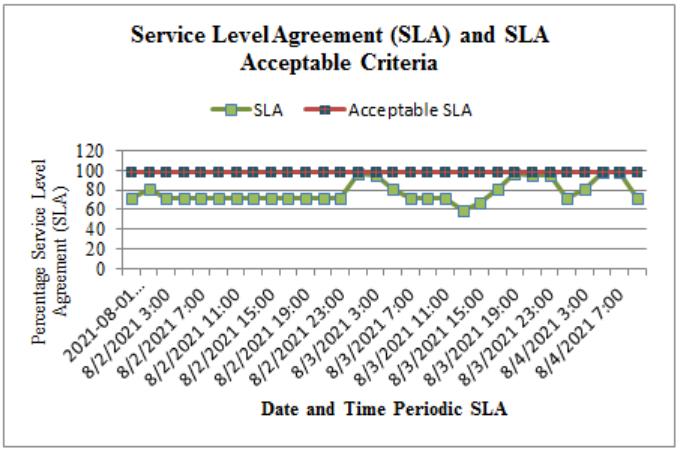


Figure 10: Service Level Agreement (SLA) Performance VPN Tunneling (Provider XL)

Service Level Agreement (SLA) acceptable criteria with long distance customers is 98.5%. In the Zabbix monitoring system designed, the sampling period is 1 month and the daily average for the SLA value to customers is met with an average SLA of 91.8%. By knowing the parameters of this SLA value, it is hoped that the level of service and also the minimum level will allow customers to use the maximum service from the Service Provider (SP).

5. 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, including network reachable, round-trip time, and throughput. Some of these aspects are then computed to produce a parameter that is used as a guide for network selection. 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 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 the minimum level, customers can use the maximum service from the Service Provider (SP).

REFERENCES

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

Damanik, Akhyar, H., and Anggraeni, M., 2020. Implementation Scheme SLA and Network Availability Mechanism for Customer Service Provider. Jurnal Penelitian Pos dan Informatika.

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

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

Jain, R.K., and Trivedi, P., 2016. 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), Pp. 442-445.

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

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

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

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

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

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

Wendi, U., Hillman, D., Merry, A., 2019. A Satellite LTE Delay Tolerant Capabilities Tunnelling: Design and Performance Evaluation. Journal of Physics: Conference Series. Pp. 1192. 012047.

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

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