Implementasi *Failover Link Backup VPN* Menggunakan *Fortinet* Untuk *ATM* Pada PT. Aplikanusa Lintasarta Denpasar

Andre[1)], Cania Andri Nur Saputra[2)], Shofwan Hanief[3)], I Made Ari Santosa[4)]
Program Studi Sistem Informasi[1),2),3)], Program Studi Sistem Komputer[4)]
Institut Teknologi dan Bisnis STIKOM Bali
Denpasar, Indonesia
e-mail: 220030070@stikom-bali.ac.id[1)], 220030738@stikom-bali.ac.id[2)], hanief@stikom-bali.ac.id[3)], arisantosamade@gmail.com[4)]

Abstrak

Teknologi informasi dan komunikasi yang memanfaatkan jaringan internet dimana semua paket data yang diolah masuk dalam jaringan internet, tidak memperdulikan dari mana, siapa, dan kapan seseorang akan mencoba masuk ke dalam jaringan kita. Dalam sebuah perusahaan perbankan jaringan Virtual Private Network (VPN) yang sangat dibutuhkan sebagai layanan transaksi data ke pusat data (data center) sehingga user dapat bekerja secara aman, dibandingkan menggunakan jaringan internet yang semua IP Public dapat dilacak dari berbagai tempat di dunia. Sebuah perbankan akan menjalin kerjasama dengan mitra untuk layanan komunikasi yang secure. Sebagai salah satu mitra perusahaan Internet Servive Provider (ISP) yaitu PT. Aplikanusa Lintasarta memberikan layanan Virtual Private Network (VPN) pada setiap pelanggannya, salah satu pelanggan yang sering di jumpai yaitu komunikasi data pada mesin ATM, dimana access yang di gunakan untuk komunikasi datanya menggunakan perangkat antena VSAT (very small aperture terminal). Lintasarta menawarkan tingkat ketersediaan (availability) Tier III dengan Service Level Agreement (SLA) sebesar 99,982%. Dengan demikian, diperlukan sebuah implementasi failover link backup untuk atm dengan menggunakan lebih dari satu uplink. Adanya lebih dari satu uplink memungkinkan kita untuk melakukan failover dimana salah satu link dijadikan sebagai main link dan yang lain menjadi link backup, maka router fortinet bisa menjadi solusi yang handal untuk memberikan layanan failover dengan menggunakan fitur IPSec Tunnel pada fortinet dan memberikan layanan data yang secure untuk atm sehingga meminmalisir waktu downtime dan KPI perusahaan tercapai terkait maintain to repair, sehingga diharapkan para pelanggan Lintasarta tidak mengalami gangguan operasional yang terlalu lama pada layanan atau transaksinya.

Kata kunci: *Implementasi, Failover, VPN, VSAT, Fortinet*

1. Pendahuluan

Secara umum *Virtual Private Network (VPN)* merupakan suatu jaringan komunikasi lokal yang terhubung melalui media jaringan internet yang dapat digunakan sebagai teknologi alternatif untuk menghubungkan jaringan lokal yang luas dengan biaya yang relatif murah [1]. Dalam sebuah perusahaan perbankan, jaringan *VPN* sangat dibutuhkan sebagai layanan transaksi data ke pusat data *(data center)* sehingga *user* dapat bekerja secara aman [2], dibandingkan menggunakan jaringan internet yang semua *IP Public* dapat dilacak dari berbagai tempat di dunia.

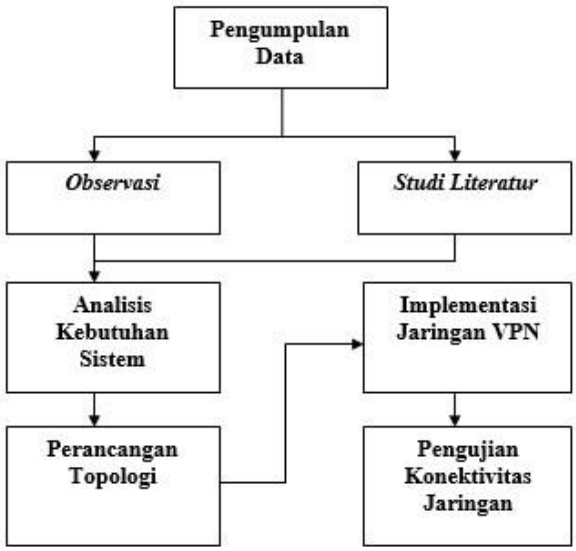
Sebagai salah satu mitra perusahaan *Internet Servive Provider (ISP)* yaitu PT. Aplikanusa Lintasarta memberikan layanan *Virtual Private Network (VPN)* pada setiap pelanggannya, salah satu pelanggan yang sering di jumpai yaitu komunikasi data pada mesin *ATM*, dimana akses yang di gunakan untuk komunikasi datanya menggunakan perangkat antena *VSAT (Very Small Aperture Terminal)* dan antena *BWA (Broadband Wireless Access)*. Lintasarta menawarkan tingkat ketersediaan *(availability) Tier III* dengan *Service Level Agreement (SLA)* sebesar 99,982%. Dengan adanya *SLA* sebesar 99,982% PT. Aplikanusa Lintasarta dituntut memberikan ketersediaan layanan pusat data dengan waktu *uptime* yang tinggi. Dimana estimasi maksimal gangguan yang dapat ditolerir oleh pelanggan Lintasarta dan menjadi acuan kontrak awal adalah empat jam, diatas itu dihitung menjadi gangguan yang sangat lama [3].

Perlu adanya sebuah implementasi *failover link backup* untuk *atm* dengan menggunakan lebih dari satu *uplink*. Adanya lebih dari satu *uplink* memungkinkan kita untuk melakukan *failover* dimana salah satu *link* bisa dijadikan sebagai *main link* dan yang lain menjadi *link backup* [4]. Dalam hal ini, *Router Fortinet* dapat digunakan sebagai salah satu alat penunjang dan penyedia *service failover* tersebut [5]. Berdasarkan dari permasalahan tersebut, penulis ingin membuat sebuah implementasi *failover link backup virtual private*

network menggunakan *fortinet* untuk *atm* pada PT Aplikanusa Lintasarta Denpasar untuk membantu meminimalisir waktu *downtime* pada mesin *atm*. Adanya implementasi *failover link backup virtual private network* diharapkan para pelanggan Lintasarta tidak mengalami gangguan operasional yang terlalu lama pada layanan atau transaksinya dan target *Service Level Agreement* dari perusahaan dapat tercapai.

2. Metode Penelitian

Bagan alur pemikiran metodologi yang digunakan yaitu metode pengamatan langsung *(Observasi)* dan studi *Literatur*, kemudian dilanjutkan menggunakan metode *Network Development Life Cycle (NDLC)*, terdiri dari analisis kebutuhan sistem, desain dan perancangan topologi, implementasi jaringan *vpn*, dan pengujian konektivitas jaringan [6] seperti yang diilustrasikan pada Gambar 1.



Gambar 1. Alur Ilustrasi Metode Penelitian

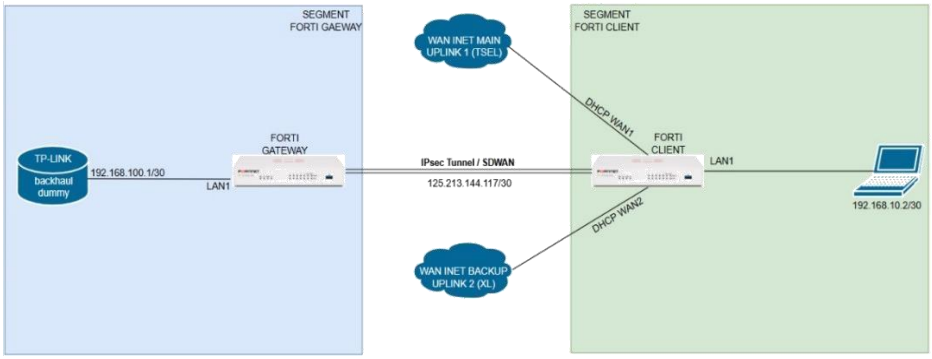
Pada tahap pertama adalah melakukan pengumpulan data melalui *observasi* dan studi *literatur*. *Observasi* merupakan teknik yang dilakukan melalui pengamatan langsung dengan menggunakan alat penunjang, sedangkan studi *literatur* adalah metode dengan cara membaca berbagai macam *literatur* yang berhubungan dengan penelitian [7]. Selanjutnya analisis kebutuhan sistem, yaitu tahap pengembangan sistem berisi rancangan analisa sistem yang akan dibuat. Lalu dalam perancangan ini akan digunakan kebutuhan fungsional seperti gambar topologi jaringan dan gambaran kebutuhan perangkat. Kemudian tahap berikutnya adalah tahap pembuatan sistem atau implementasi sistem. Pertama adalah menyiapkan *hardware* dan penunjang apa saja yang diperlukan serta pembuatan jalur koneksi *IPSec Gateway* dengan *MPLS* dan internet dari sistem, dan Modem Huawei sebagai penyedia layanan internet pada *Fortinet IPSec Client*. Pada implementasi ini digunakan sebagai *console* atau *setting* yaitu aplikasi melalui *Web Browser* atau *Command Line*. Setelah proses implementasi sistem selesai dilaksanakan, tahap terakhir adalah melakukan pengujian konektivitas jaringan.

3. Hasil dan Pembahasan

Pembahasan pada penelitian ini bertujuan untuk mengimplempentasikan *service failover vpn* pada *atm* menggunakan *fortinet 50E* agar meminimalisir waktu *downtime* yang terjadi. Artikel ini membahas berbagai aspek penting yang terkait dengan proses desain topologi, implementasi, pengaturan jaringan, pengujian jaringan, dan penerapan simulasi jaringan.

3.1 Desain Topologi Failover

Desain Topologi *Failover* akan dibuat seperti Gambar 2, dimana sebelumnya jaringan data melewati jalur akses antena *VSAT* kemudian akan dirubah atau di-*reroute* melewati jalur internet, namun pada dasarnya akan tetap masuk ke dalam jaringan *MPLS*-Lintasarta sebagai distribusi antar pelanggan yang saling terkoneksi.



Gambar 2. Topologi *Failover*

3.2 Tabel IP *Address*

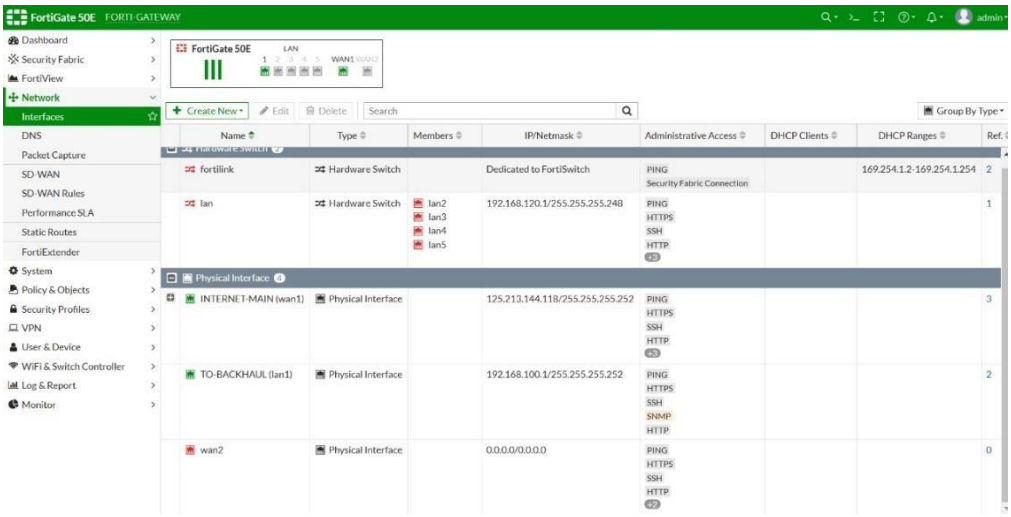
Berdasarkan topologi jaringan *failover* yang dibuat, maka diperoleh *IP Address* jaringan *failover* dengan melakukan simulasi serta melakukan pengujian langsung di lokasi penelitian yaitu pada PT Aplikanusa Lintasarta Denpasar seperti pada Tabel 1.

Tabel 1. *IP Address Jaringan Failover*

NO.	ITEM	*Address/Vlan/Usr*
1	*IP Backhoul* (Simulasi)	192.168.100.1/30
2	Koneksi *Forti Gateway* ke *Forti Client*	125.213.144.117/30
3	Koneksi *Forti Client* ke Internet	*IP DHCP* Sesuai *GSM*
4	*IP ATM* (Simulasi)	192.168.10.2/30

3.3 Implementasi

Langkah pertama ialah melakukan *routing* ke arah *IP Gateway* agar terkoneksi dengan internet. Konfigurasi *IP Routing*, masuk pada menu *Network -> Static Routes*, pilih *Create New*, masukkan *default route* yaitu *destination*: 0.0.0.0/0.0.0.0, *Gateway Address*: 125.213.144.117, lalu pilih *port Interface INTERNET-MAIN (wan1)*, ubah status jadi *enabled*, kemudian klik *OK*, secara otomatis jika koneksi kita benar, maka status warna *port* pada *interfaces* menjadi hijau sesuai pada Gambar 3.

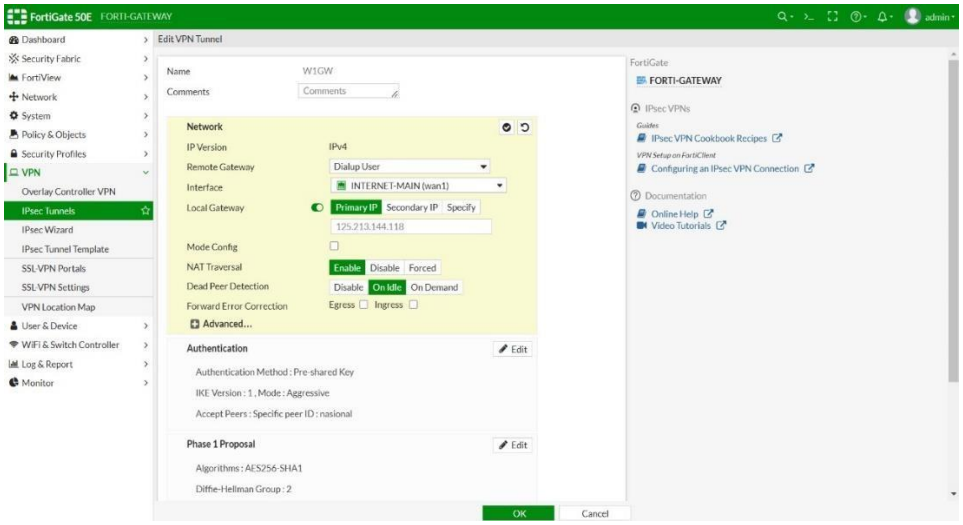


Gambar 3. *Setting IP Address*

3.4 Konfigurasi *IPSec Tunnel* Pada *Forti Gateway*

IPSec Tunnel pada *Forti Gateway* diakses oleh *client* melalui *IP Public* sesuai Gambar 4 yakni *IP Address* 125.213.144.118. Pada menu *VPN* pilih *IPSec Tunnel*, lalu *Create New IPSec Tunnel*. Pada menu

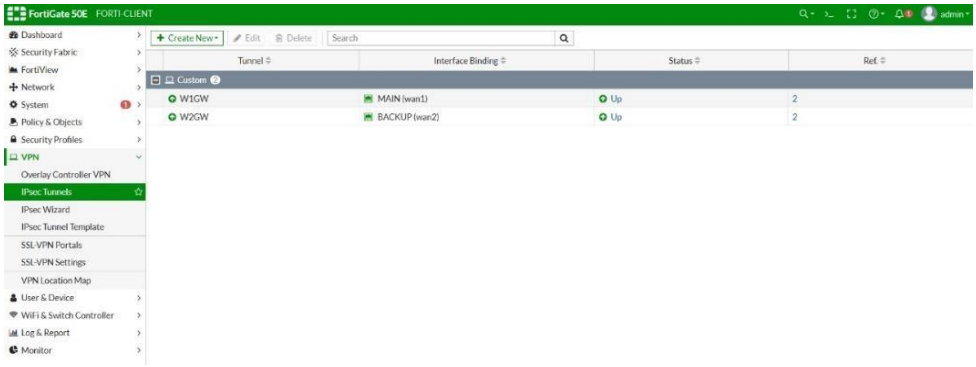
Remote Gateway pilih *Dialup User*, lalu diarahkan ke *Interface (INTERNET-MAIN (wan1))*, pilih *Enable* pada menu *NAT Traversal*, dan untuk menu *Dead Peer Detection* pilih *On Idle*, kemudian klik *OK*.



Gambar 4. *IPSec Tunnel Forti Gateway*

3.5 Konfigurasi *IPSec Tunnel* Pada *Forti Client*

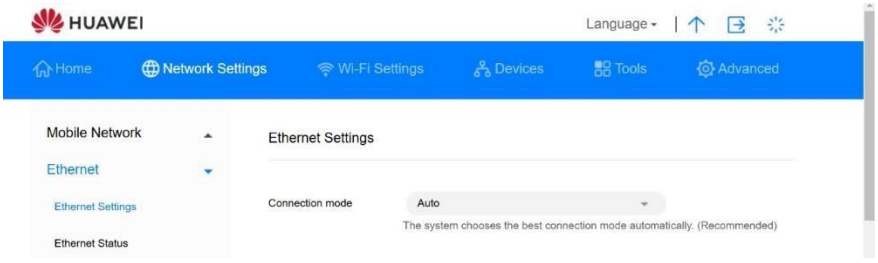
Pada *Forti Client* melalui port *WAN1* dan *WAN2*, dilakukan *DialUp* pada *IPSec Tunnel Main* dan *Backup* agar dapat terkoneksi dengan internet sesuai Gambar 5.



Gambar 5. *IPSec Tunnel Forti Client*

3.6 Konfigurasi *Ethernet* Modem Huawei *4G*

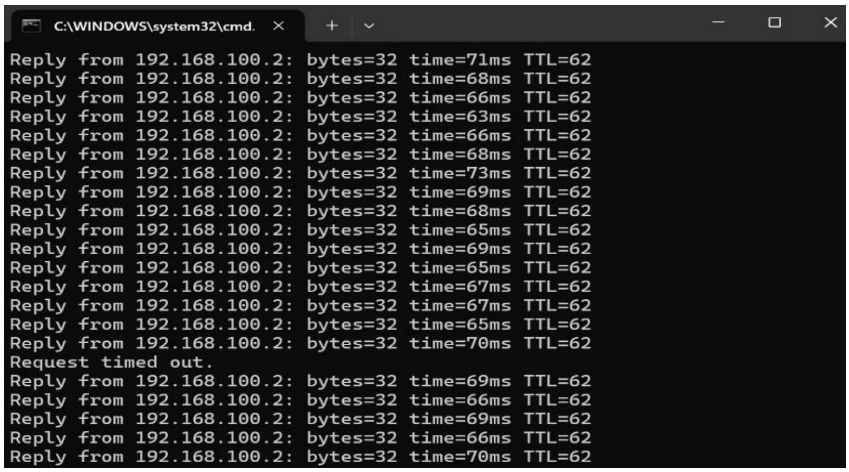
Setting Modem Huawei ialah masuk menu *Network Settings*, pilih *Ethernet Setting*, pada *Connection Mode->* pilih *Auto*, secara otomatis keluaran *port ethernet* Modem Huawei *4G* akan jadi *DHCP* sesuai pada Gambar 6.



Gambar 6. *Setting* Modem Huawei

3.7 Pengujian Jaringan *Failover*

Pengujian jaringan *failover* dilakukan melalui tes *ping* pengetesan dari *client (remote)* ke arah *router backhaul*. Tes *ping* ini digunakan untuk memastikan layanan *service VPN* berjalan dengan baik [8]. Proses ini juga melibatkan redudansi dan dapat dilakukan baik secara otomatis maupun manual, memungkinkan transisi yang mulus untuk menjaga kelangsungan sistem kritis tanpa keterlambatan atau gangguan yang terjadi. Berikut hasil tes pengujian sesuai Gambar 7.



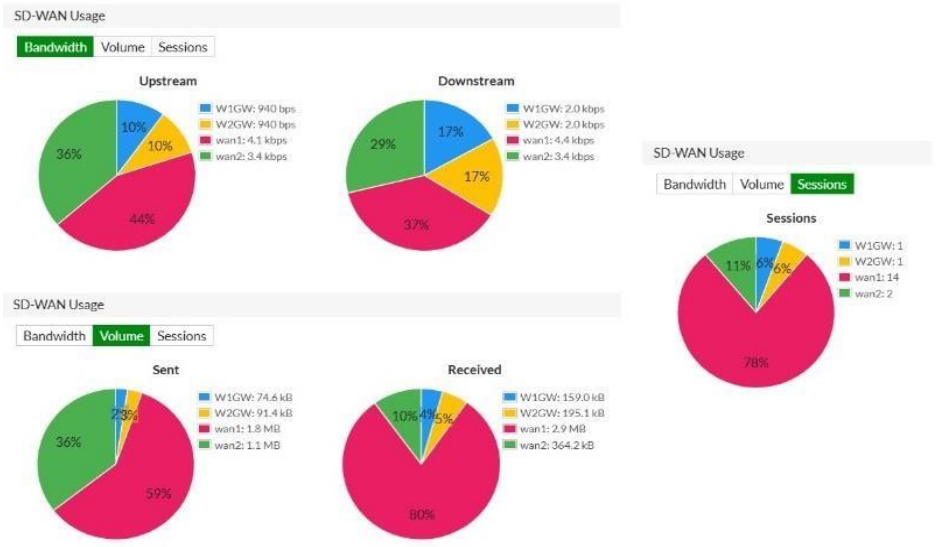
Gambar 7. Tes Pengujian Jaringan *Failover*

3.8 *Performance SLA* & *Dashboard SD-WAN Usage*

Performance SLA, dalam hal ini dilakukan untuk memastikan semua *service* berjalan dengan baik [9]. Berikut *dashboard performance SLA* untuk memonitoring *packet loss*, *latency*, dan *jitter* pada *tunneling VPN* sesuai Gambar 8.

Gambar 8. *Performance SLA*

Selain *Performance SLA*, ada juga dashboard *SD-WAN Usage*. *SD-WAN Usage* sendiri digunakan untuk memonitoring pergerakan data secara *upstream* dan *downstream* melalui menu *bandwith*, memonitoring jumlah pemakaian data yang digunakan sesuai Gambar 9.



Gambar 9. *SD-WAN Usage*

4. Kesimpulan

Kesimpulan yang di peroleh dari hasil implementasi *failover link backup virtual private network* menggunakan *fortinet* untuk *atm* pada PT Aplikanusa Lintasarta Denpasar, setelah melakukan analisa *observasi* pada media akses *existing* yaitu *VSAT (Very Small Aperture Terminal)* yang hanya menggunakan *single link* dan ketika terjadi *downtime, link* utama akan mati dan tidak ada *backup* [10]. Hal ini sangat berpengaruh terhadap pelayanan ke *customer* dari PT Aplikanusa Lintasarta. Dengan demikian, *router fortinet* mampu menjadi solusi yang handal untuk memberikan layanan *failover* secara otomatis dengan menggunakan fitur *IPSec Tunnel* pada *fortinet* dan memberikan layanan data yang *secure* untuk *atm* sehingga meminimalisir waktu *downtime* dan *KPI (Key Performance Indicator)* perusahaan tercapai terkait *maintain to repair*.

Daftar Pustaka

[1] P. Oktivasari, A. B. Utomo, "Analisa *Virtual Private Network* Menggunakan *Openvpn* dan *Point To Point Tunneling Protocol*," *Jurnal Penelitian Komunikasi dan Opini Publik*, vol. 20, no.2, pp. 185202, 2016.

[2] M. D. Andini, M. Amirulloh, H. N. Muchtar, "Penggunaan Aplikasi *Virtual Private Network (VPN) Point To Point Tunneling Protocol (PPTP)* Dalam Mengakses Situs Terblokir," *Supremasi Hukum: Jurnal Penelitian Hukum*, vol. 29, no. 2, pp 148-166, 2020.

[3] S. Darmaji, (2016, Aug). Lintasarta. Sebagai salah satu perusahaan telekomunikasi dan penyedia layanan pusat data terbesar di Indonesia [Online]. Available: https://www.lintasarta.net/.

[4] I. P. Suwandika, "Implementasi *Failover, Load Balancing* Dan *Warming System* Berbasis Mikrotik Studi Kasus Grand Istana Rama Hotel," 2020.

[5] Fortinet, *The Network Leader's Guide To Secure SD-WAN*, 372656-C-0-EN, 2021.

[6] P. Aditya, T. Informatika, S. Informasi, S. Widya Cipta Dharma, J. MYamin No, and S. Kalimantan Timur, "IMPLEMENTASI JARINGAN PPPOE DAN HOTSPOT SERVER RT/RW NET BERBASIS MIKROTIK DENGAN FITUR MIKHMON DI ADINET SAMARINDA SEBERANG," *Jurnal* INFORMATIKA, vol. 13, no. 1, 2023, doi: 10.46984/inf-wcd.2204.

[7] Sugiyono, "Metode Penelitian Kuantitatif, Kualitatif, dan R&D," 2018.

[8] S. Dewi, F. Riyadi, T. Suwastitaratu, N. Hikmah, "Keamanan Jaringan Menggunakan *VPN (Virtual Private Network)* Dengan Metode *PPTP (Point To Point Tunneling Protocol)* Pada Kantor Desa Kertarharja Ciamis," *Jurnal Sains dan Manajemen*, vol. 8, no. 1, 2020.

[9] R. D. Lisa, "Service Level Agreement (SLA)," 2014

[10] T. Rahman, F. A. Rahman, "Implementasi *Automatic Uplink Power Control* pada *VSAT Single Channel* per *Carrier*," *Jurnal Inovtek Polbeng – Seri Informatika*, vol. 5, no. 2, 2020.