JITET (Jurnal Informatika dan Teknik Elektro Terapan)
Vol. 12 No. 2, pISSN: 2303-0577 eISSN: 2830-7062 http://dx.doi.org/10.23960/jitet.v12i2.4230

IMPLEMENTASI VPN DAN LOAD BALANCING DUA LINE ISP BERBEDA PADA PT. ASURANSI BINAGRIYA UPAKARA

Rizky Waldiyan[1], Irwan Agus Sobari[2*]

[1,2] Universitas Nusa Mandiri Jakarta; Jl. Kramat Raya, Senen, Jakarta Pusat, Jawa Barat, Telp.(021)3190857

Riwayat artikel:

Received: 25 Maret 2024
Accepted: 30 Maret 2024
Published: 2 April 2024

Keywords:
VPN, Load Balancing, PPTP

Corespondent Email:
irwan.igb@nusamandiri.ac.id

Abstrak. Revolusi industri 4.0, penggunaan komputer dan internet menjadi sangat penting dalam menjalankan berbagai pekerjaan, termasuk pertukaran data. PT Asuransi Binagriya Upakara, sebuah perusahaan asuransi dengan beberapa cabang di Indonesia, mengandalkan jaringan komputer sebagai sarana utama untuk pertukaran dan pengontrolan data dalam pekerjaan serta operasional kantor. Saat ini, sistem pertukaran data internal di PT Asuransi Binagriya Upakara masih menggunakan email sebagai media pengiriman data. Namun, dalam keadaan daring (online), diperlukan keamanan data yang tinggi untuk melindungi jaringan dari ancaman keamanan. Untuk mengatasi hal ini, penulis telah memutuskan untuk menggunakan jaringan VPN (*Virtual Private Network*) dan *Load balancing* dua line ISP berbeda sebagai solusi untuk menjaga keamanan privasi data internal dan menjaga koneksi internet agar tetap stabil. Penerapan VPN, hanya diberikan kepada beberapa staf yag berwenang. Hal ini memastikan bahwa data tetap aman dan hanya dapat diakses oleh pihak yang berwenang serta menhubungkan kantor pusat dan kantor cabang.. Dengan adanya konfigurasi VPN dan Load balancing dua line ISP, membuat jaringan komputer stabil dan aman.

Abstract. *Industrial revolution 4.0, the use of computers and the internet has become very important in carrying out various jobs, including exchanging data. PT Asuransi Binagriya Upakara, an insurance company with several branches in Indonesia, relies on computer networks as the main means for exchanging and controlling data in work and office operations. Currently, the internal data exchange system at PT Asuransi Binagriya Upakara still uses email as a data delivery medium. However, in online situations, high data security is required to protect the network from security threats. To overcome this, the author has decided to use a VPN (Virtual Private Network) network and load balancing two different ISP lines as a solution to maintain internal data privacy security and keep the internet connection stable. VPN implementation is only given to a few authorized staff. This ensures that data remains safe and can only be accessed by authorized parties and connects the head office and branch offices. With VPN configuration and two ISP line load balancing, the computer network is stable and secure..*

1. PENDAHULUAN

Dalam era perkembangan teknologi informasi yang cepat ini, penggunaan komputer dan jaringan internet telah menjadi kebutuhan penting dalam mendukung aktivitas pekerjaan. Karena itulah, perusahaan membutuhkan sistem cerdas untuk memfasilitasi pertukaran data dan informasi melalui jaringan komputer. Sama seperti halnya, penulis melakukan penelitian di PT. Asuransi Binagriya Upakara tentang sistem jaringan komputer yang digunakan di kantor pusat perusahaan tersebut. Jaringan komputer yang diterapkan oleh PT. Asuransi Binagriya Upakara adalah *Wide Area Network (WAN).*

Jaringan komputer di PT. Asuransi Binagriya Upakara mengimplementasikan *WAN (Wide Area Network)* sebagai sarana penghubung antara jaringan lokal *LAN (Local Area Network)* yang ada di kantor

pusat dan beberapa daerah terpisah, dengan tujuan menghemat biaya dan meningkatkan efisiensi. Namun, *WAN* pada PT. Asuransi Binagriya Upakara masih memiliki beberapa kelemahan dalam hal keamanan jaringan komputer. Salah satu kelemahan utamanya adalah ketiadaan jaringan privat yang hanya dapat diakses oleh manajer khusus dan beberapa karyawan dengan akses tertentu di kantor pusat maupun cabang. Akibatnya, terdapat beberapa kendala dalam melaksanakan pekerjaan saat berada di kantor cabang tanpa harus berkunjung ke kantor pusat.

Untuk mengatasi masalah ini, diperlukan pendirian jaringan komputer privat bagi para karyawan untuk memudahkan pekerjaan tanpa mengalami kendala terkait jarak dan waktu. Salah satu solusinya adalah dengan merancang jaringan *VPN (Virtual Private Network)*. *VPN* adalah suatu jaringan lokal yang terhubung melalui infrastruktur jaringan publik[1].

Virtual Private Network (VPN) diciptakan oleh *National Institute of Standards and Technology (NIST)*, merupakan organisasi yang mengkhususkan diri dalam teknologi dan standar nasional di Amerika Serikat. VPN memberikan perlindungan terhadap data, menjaga kerahasiaan data selama proses transmisi, memastikan integritas data, otentikasi sumber data, melindungi dari replay attack, dan mengontrol akses selama proses transmisi melalui jaringan komputer publik[2].

Pemanfaatan PPTP (*Point to Point Tunneling Protocol*) dalam perancangan jaringan memperbolehkan instansi untuk membuka cabang di berbagai lokasi tanpa perlu membangun infrastruktur milik perusahaan sendiri[3]. Dengan menggunakan *load balance*, kecepatan internet dan kestabilan jaringan internet akan terjaga. Beban trafik bisa dibagi menjadi dua menjadi lebih seimbang dapat berjalan optimal, memaksimalkan *throughput* sehingga dapat meningkatkan kinerja dan omset perusahaan tersebut[4].

2. TINJAUAN PUSTAKA

Jaringan komputer merujuk pada koneksi antara minimal dua komputer yang saling terhubung melalui media transmisi, baik itu menggunakan kabel atau teknologi nirkabel. Dalam konteks ini, dua perangkat komputer dianggap terhubung apabila keduanya dapat menukar informasi atau data, berpartisipasi dalam penggunaan sumber daya yang sama, dan menggunakan software dan hardware yang terkoneksi dalam jaringan yang sama[5].

Jaringan MAN terdiri dari beberapa sistem LAN. Jangkauan jaringan MAN biasanya berkisar antara 10 hingga 50 km, sehingga sangat cocok untuk memperluas jaringan antar kantor di dalam satu kota, menghubungkan instansi cabang dengan kantor pusat yang berada dalam wilayah cakupannya [6].

MikroTik adalah sebuah platform perangkat lunak dan sistem operasi yang memungkinkan komputer berfungsi sebagai router jaringan yang andal. Platform ini menawarkan beragam fitur yang dirancang khusus untuk jaringan IP dan jaringan nirkabel. MikroTik sangat cocok digunakan oleh penyedia layanan internet (ISP), penyedia hotspot, dan warung internet (warnet). Dengan memanfaatkan MikroTik, pengguna dapat efisien dalam mengelola jaringan dan mengoptimalkan pengalaman konektivitas para pengguna dengan berbagai fungsi yang tersedia.[7]

Router berfungsi untuk mengambil paket data yang diterima dari satu jaringan atau sumber, lalu meneruskannya ke jaringan atau tujuan yang sesuai dengan alamat tujuan yang terkandung dalam paket tersebut[8].

Winbox memberikan antarmuka grafis (GUI) yang memudahkan tampilan dan pengaturan Mikrotik, yang biasanya diakses melalui protokol telnet atau SSH yang menggunakan baris perintah (*command line*). Hal ini dapat menyulitkan bagi pemula saat melakukan pengaturan Mikrotik, tetapi dengan adanya Winbox, proses tersebut menjadi lebih mudah dan sederhana[9].

Load balancing merupakan teknik untuk memisahkan antar dua atau banyak network link agar beban traffic dibagi menjadi seimbang sehingga jaringan dapat berjalan optimal[10].

VPN merupakan sebuah jalur komunikasi yang baru secara private dan aman, VPN ini menghubungkan antara client dengan server yang berada pada jaringan internet dengan jaringan lokal agar dapat saling berkomunikasi[11]. Penggunaan jaringan VPN bisa menjadi alternatif lain yang lebih singkat serta efisiensi waktu dalam kegiatan transmisi data dan efisiensi biaya[12].

3. METODE PENELITIAN

Penulis melakukan pengamatan secara langsung ke PT. Asuransi Binagriya Upakara dan mengevaluasi hasil pengamatan yang kemudian dijadikan sebagai pertimbangan dalam mengambil keputusan. Berikut beberapa tindakan yang mencakup sebagai berikut:

A. Analisis Kebutuhan

Analisa kebutuhan adalah sebuah cara untuk mendapatkan informasi, spesifikasi, model mengenai software/hardware yang dibutuhkan PT. Asuransi Binagriya Upakara. Analisa kebutuhan dilangsungkan sebelum dimulainya implementasi jaringan yang akan dibangun.

B. Desain

adalah tahapan berikutnya dari tahapan analisa kebutuhan. Desain menggambarkan bagaimana perangkat hardware dalam jaringan di PT. Asuransi Binagriya Upakara bisa saling terhubung, dalam hal ini penulis menggunakan Microsoft Visio untuk

menggambarkan topologi desain dari kebutuhan yang ada

C. Testing

Ini adalah fase pengujian terhadap jaringan yang telah diusulkan dan direncanakan. Di sini, saya akan melakukan uji coba awal dan uji coba akhir pada router untuk melakukan tes ping dan menguji konfigurasi ke beberapa perangkat menggunakan Aplikasi Winbox untuk membuktikan bahwa jaringan yang saya usulkan dapat beroperasi sesuai dengan solusi yang diharapkan.

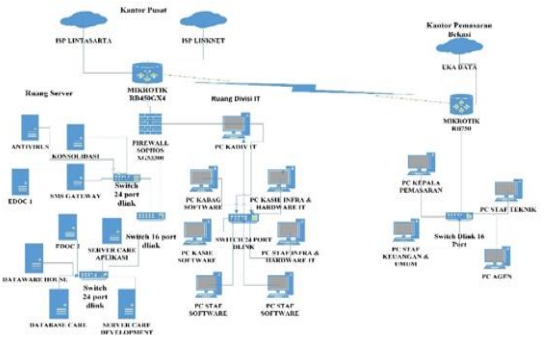
D. Implementasi

Dalam tahap ini penulis mengimplementasikan jaringan Virtual Private Network pada jaringan komputer PT. Asuransi Binagriya Upakara menggunakan perangkat mikrotik routerboard RB941-2ND sebagai media penerapannya

4. HASIL DAN PEMBAHASAN

4.1 Skema Jaringan

Sesuai dengan pengamatan secara langsung pada PT. Asuransi Binagriya Upakara. Jaringan PT. Asuransi Binagriya Upakara pada kantor pusat menggunakan 2 sumber ISP (*Internet Service Provider*) yaitu Lintasarta dan Linknet keduanya digunakan untuk Lintasarta sebagai primary dan Linknet sebagai Backup, selain itu pada kantor cabang menggunakan 1 Internet Service Provider yaitu Ekadata yang difungsikan sebagai sumber internet untuk router Mikrotik dan beberapa Pc client pada kantor cabang.

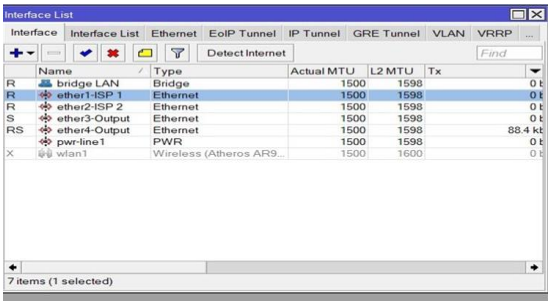


Gambar 1 Skema Jaringan

Dari gambar 1 penulis memaksimalkan fitur dari mikrotik yaitu tunnelling (VPN) unuk membuat jalur private yang menghubungkan kantor pusat dengan kantor cabang dan memaksimalkan internet yang tersedia dikantor pusat dengan load balancing agar traffic bisa dibagi merata dan internet lebih stabil.

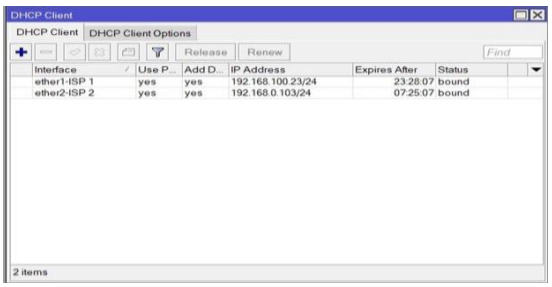
4.2 Implementasi Jaringan

Dalam implementasi ini penulis menggunakan load balancing dan VPN untuk mengatasi masalah yang ada pada PT. Asuransi Binagriya Upakara.

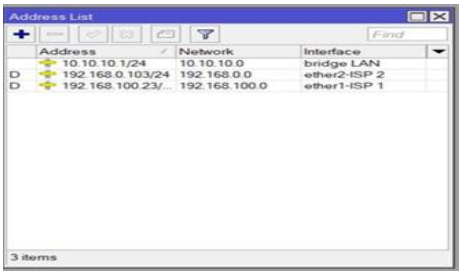


Gambar 2 Interface Mikrotik Kantor Pusat

Pada gambar 2 dapat dilihat kantor pusat mempunyai 2 ISP yang berbeda, ISP 1 50 Mbps dan ISP2 30 Mbps.



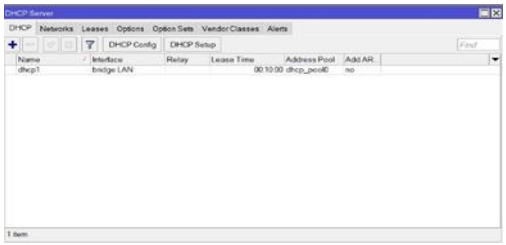
Gambar 3 Dhcp Client Mikrotik



Gambar 4 Konfigurasi Ip Address Mikrotik

pada gambar 4 merupakan elemen kunci yang diperlukan untuk mengaktifkan fungsi router. Saat ini, MikroTik hanya menggunakann protokol IPv4.

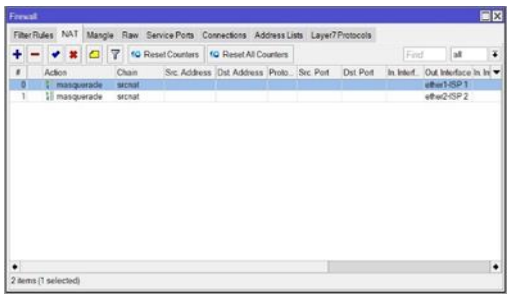
Gambar 5 Setting Bridge Local Area Network



Gambar 6 Dhcp Server

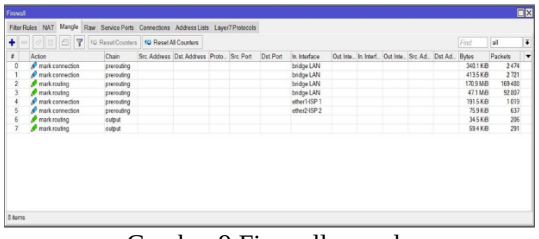
Gambar 7 Setting DNS

DNS berperan dalam mengaitkan nama host atau domain di Internet menjadi alamat IP yang sesuai. Dalam gambaran ini, dijelaskan bahwa Domain Name Server menggunakan Server Dinamis dari penyedia layanan internet (ISP) yang tengah digunakan dan juga menggunakan Domain Name Server.



Gambar 8 Konfigurasi Firewall

Network Address Translation (NAT) merupakan komponen firewall yang berperan dalam mengubah alamat IP pengirim dalam paket data. Dalam praktiknya, NAT akan memodifikasi paket data yang dikeluarkan oleh komputer pengguna agar tampak seolah-olah berasal dari router itu sendiri.

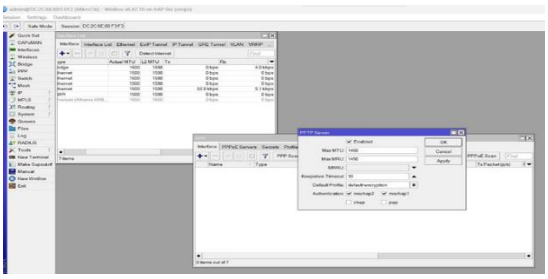


Gambar 9 Firewall mangle

Pada gambar 9, penulis akan memanfaatkan fitur yang dikenal sebagai PCC (*Per Connection Classifier*). Melalui PCC, penulis dapat mengelompokkan lalu lintas koneksi yang melewati atau bergerak melalui router menjadi beberapa kelompok. Pengelompokan ini mampu dibedakan berdasarkan alamat sumber (*src-address*), alamat tujuan (*dst-address*), port sumber (*src-port*), dan/atau port tujuan (*dst-port*). Router akan menyimpan informasi tentang jalur gateway yang digunakan oleh koneksi pada awalnya, sehingga pada paket-paket berikutnya yang terkait dengan koneksi asal akan diteruskan melalui jalur gateway yang sama.

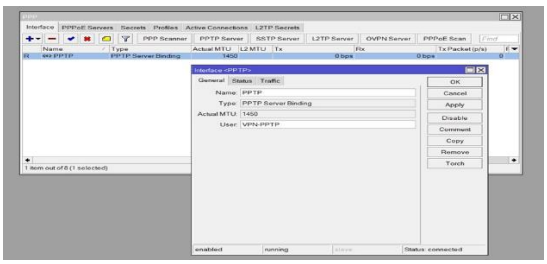
Gambar 10 Setting Routes Load balancing PCC

Pada gambar 10 yang membagi traffic agar berjalan seimbang dan tidak overload disalah satu isp jaringan sehingga kenerja jaringan internet lebih stabil dan efisien.

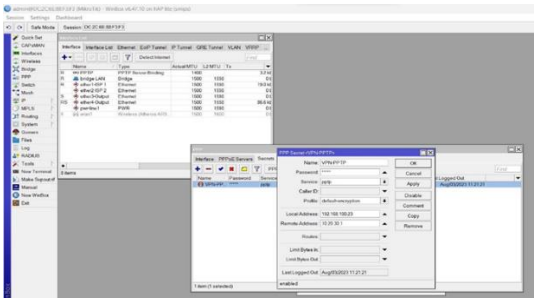


Gambar 11 Konfigurasi PPTP Server

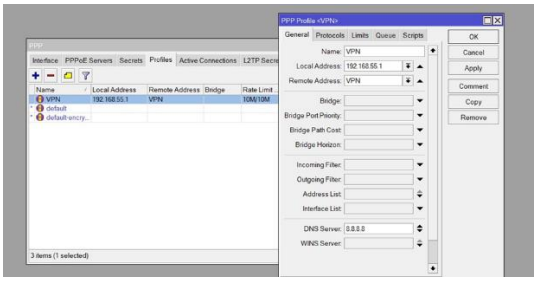
Gamar 11 Penulis melakukan konfigurasi PPTP untuk jalur tunnelling (VPN) yang menghubungkan kantor pusat dan kantor cabang.



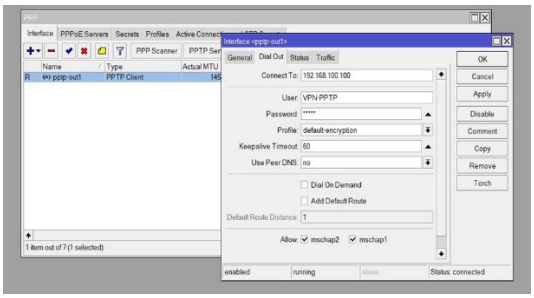
Gambar 12 Konfigurasi Interface Point to Point Tunneling Protocol



Gambar 13 Konfigurasi Secrets PPTP

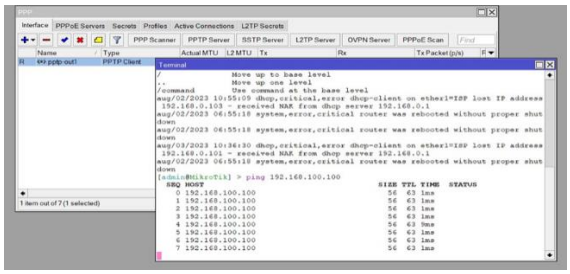


Gambar 14 Konfigurasi Profil PPTP



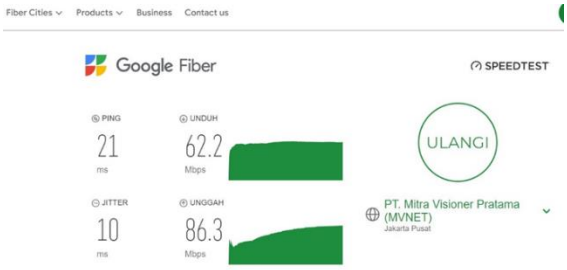
Gambar 15 Konfigurasi PPTP Client

Pada gambar 15 penulis melakukan konfigurasai pada router kantor cabang.



Gambar 16 Test Koneksi jaringan PPTP Client

Pada gambar 16 dapat dilihat hasil ping dari kantor cabang ke kantor pusat sudah terhubung.



Gambar 17 Uji coba kecepatan internet setelah Load balancing aktif

Pada gambar 17 koneksi pada komputer client terlihat lebih stabil dari proses download dan uploadnya sehingga kinerja internet bisa maksimal.

5. KESIMPULAN

Berdasarkan uraian yang diatas dapat disimpulkan bahwa penerapan metode *Virtual Private Network* (VPN) dan metode Load balancing pada PT. Asuransi Binagriya Upakara memberikan dampak positif, yang dapat dijelaskan sebagai berikut:

1. Penggunaan keamanan jaringan komputer melalui VPN menggunakan metode PPTP dapat menghubungkan kantor pusat dan kantor cabang serta mempermudah tim IT dalam mengendalikan dan menangani permasalahan jaringan di perusahaan dari lokasi yang jauh, tanpa harus hadir secara fisik di lokasi tersebut.
2. Dengan mengatur load balancing pada 2 ISP melalui perangkat MikroTik, koneksi internet di kantor pusat menjadi lebih optimal dan stabil. Sehingga meningkatkan kinerja karyawan dan efisiensi perusahaan.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada kedua orang tua, bapak Irwan Agus Sobari yang telah membantu penelitian ini. Penulis juga mengucapkan banyak terima kasih pada Bapak pimpinan dan karyawan PT. Asuransi Binagriya Upakara.

DAFTAR PUSTAKA

[1] S. Dewi, “Keamanan Jaringan Menggunakan VPN (Virtual Private Network) Dengan Metode PPTP (Point To Point Tunneling Protocol) Pada Kantor Desa Kertaraharja Ciamis,” *EVOLUSI J. Sains dan Manaj.*, vol. 8, no. 1, pp. 128–139, 2020, doi: 10.31294/evolusi.v8i1.7658.

[2] D. A. Pangestu, A. S. Budiman, and S. Sartini, “Rancangan Site-To-Site Vpn Dengan Pptp Pada Interkoneksi Antar Kantor Pt. Indosis Integrasi,” *semanTIK*, vol. 8, no. 1, p. 1, 2022, doi: 10.55679/semantik.v8i1.9189.

[3] S. Sidik, S. Susafa’ati, E. R. Nainggolan, and

U. Radiyah, "Implementasi VPN Berbasis Point To Point Tunneling Protocol (PPTP) Menggunakan Mikrotik Router Board," *J. Infortech*, vol. 3, no. 1, pp. 46–51, 2021, doi: 10.31294/infortech.v3i1.10400.

[4] S. A. Haris, H. Suhartono, and H. Herlawati, "Menjaga Kestabilan Jaringan Load Balancing Nth Dengan Teknik Failover Pada PT. Jakarta Samudera Sentosa Jakarta," *PIKSEL Penelit. Ilmu Komput. Sist. Embed. Log.*, vol. 6, no. 1, pp. 49–60, 2018, doi: 10.33558/piksel.v6i1.1399.

[5] A. V. Mananggel, A. Mewengkang, and A. C. Djamen, "Perancangan Jaringan Komputer Di Smk Menggunakan Cisco Packet Tracer," *Edutik J. Pendidik. Teknol. Inf. dan Komun.*, vol. 1, no. 2, pp. 119–131, 2021, doi: 10.53682/edutik.v1i2.1124.

[6] M. J. N. Yudianto, "Jaringan Komputer dan Pengertiannya," *Ilmukomputer.Com*, vol. Vol.1, pp. 1–10, 2014.

[7] A. I. Ardhitya, "Pengertian dan Penjelasan Mikrotik Arse Irawhan Ardhitya," 20019.

[8] D. Gustina and D. Mutiara, "Sistem Penunjang Keputusan Pemilihan Router Mikrotik Dengan Menggunakan Metode Ahp (Analitycal Hierarchy Process)," *J. Ilm. FIFO*, vol. 9, no. 1, p. 68, 2017, doi: 10.22441/fifo.v9i1.1443.

[9] Https://zathco.com/, "Pengertian dan Fungsi Winbox."

[10] T. A. Andriyan and I. A. Sobari, "Implementasi Load Balancing Dan Failover Dua Line ISP Berbeda Pada PT Abhitrans Matra Indah," vol. 10, no. 1, pp. 20–25, 2024, doi: 10.31294/jtk.v.

[11] B. D. Oktavian and I. A. Sobari, "2. Implementasi Jaringan Terpusat Menggunakan Ospf Dan Vpn Dengan Failover Link DI PT. ADVANTAGE SCM," vol. 1, no. 3, 2022.

[12] N. I. Febriyanto and I. A. Sobari, "Perancangan Jaringan Vpn Menggunakan Protokol L2Tp+Ipsec Sebagai Media Transmisi Data Pada Yayasan Sirajul Falah Indonesia," *J. Inform. dan Tek. Elektro Terap.*, vol. 12, no. 1, pp. 275–281, 2024, doi: 10.23960/jitet.v12i1.3703.