



Optimalisasi jaringan tunnel menggunakan routeros untuk mendukung kelangsungan operasional PT. KLK Agriservindo di masa pandemik Covid-19

¹Syamsu Hidayat, ²Thomas Budiman *, ³Asih Septia Rini

^{1,2,3}Sistem Informasi, Fakultas Ilmu Komputer, STMIK Jayakarta

Jl. Salemba Raya No.24, Jakarta Pusat, Indonesia

e-mail: syamsuhi3009@gmail.com, thomas@stmik.jayakarta.ac.id,

asihseptiarini@stmik.jayakarta.ac.id

Received: December 27, 2021, **Revised:** January 7, 2022, **Accepted:** January 10, 2022

Abstrak

PT. KLK Agriservindo merupakan *Subsidiary company* dari Kuala Lumpur Kepong Berhad, Malaysia. Perusahaan ini bergerak dalam bidang perkebunan kelapa sawit yang menghasilkan CPO (*Crude Palm Oil*) dan turunannya. Pangsa pasar produksinya adalah ekspor ke berbagai negara-negara di Asia. Sejak awal Januari 2020 dunia Internasional mengalami hal yang sangat mengejutkan dengan mewabahnya jenis virus Sars Cov-2 yang menyerang sistem pernapasan manusia yang berakibat fatal hingga menyebabkan kematian. Adapun hal yang menjadi kebijakan pemerintah Indonesia adalah dengan menerapkan Pembatasan kegiatan Masyarakat, yang berimbas pada berbagai sektor kehidupan, tidak terkecuali sektor dunia usaha. Untuk menghadapi kebijakan ini maka perusahaan menerapkan kebijakan pembatasan kehadiran karyawan ke kantor, memperbolehkan karyawan bekerja dari rumah. Adapun masalah yang muncul kemudian adalah karyawan tidak bisa mengakses resource yang berada di lingkungan kantor, karena kebijakan keamanan Informasi perusahaan mengharuskan akses melalui jalur private atau LAN. Dalam penelitian ini menggunakan metode *Network Development Life Cycle* kemudian Department Informasi melakukan inovasi dengan mengoptimalkan *RouterOS* yang dimiliki perusahaan agar dapat menjadi Jaringan Tunnel yang dapat menjembatani komunikasi data antara jaringan publik (*internet*) dengan Jaringan LAN kantor, sehingga karyawan dapat mengakses resource kantor tanpa Batasan ruang dan waktu.

Kata kunci: KLK, Sars Cov2, LAN, Tunnel, *Network Development Life Cycle*

Abstract

PT. KLK Agriservindo is a subsidiary of Kuala Lumpur Kepong Berhad, Malaysia. This company is engaged in oil palm plantations that produce CPO (Crude Palm Oil) and its derivatives. Its production market share is exports to various countries in Asia. Since the beginning of January 2020, the international community has experienced something very surprising with the outbreak of the Sars Cov-2 virus which attacks the human respiratory system which is fatal to cause death. The Indonesian government's policy is to impose restrictions on community activities, which have an impact on various sectors of life, including the business sector. To deal with this policy, the company implemented a policy of limiting employee attendance at the office, allowing employees to work from home. The problem that arises then is that employees cannot access resources in the office environment, because the company's information security policies require access through private channels or LAN. In this study using the Network Development Life Cycle method, the Information



DOI : 10.54593/jstekwid.v1i1.44

Jurnal Sains dan Teknologi Widyadoka This work is licensed under a [Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License](https://creativecommons.org/licenses/by-nc-sa/4.0/).



Department innovates by optimizing the company's RouterOS so that it can become a Tunnel Network that can bridge data communication between the public network (internet) and the office LAN network, so that employees can access office resources without space restrictions. and time.

Keywords: *KLK, Sars Cov2, LAN, Tunnel, Network Development Life Cycle*

1 Pendahuluan

Penyebaran virus Sars Cov-2 atau lebih dikenal dengan nama Corona Virus Disease 19 ke seluruh dunia tidak terkecuali Indonesia telah mengakibatkan banyak korban jiwa. Penyebaran secara masif ini tidak terlepas dari kebijakan pemerintah Indonesia dengan tidak menutup masuk kedatangan internasional sehingga ditemukan sejumlah kasus positif di berbagai bidang, tidak terkecuali karyawan PT. KLK Agriservindo dan menjadikan area kantor menjadi zona merah penyebaran virus Covid-19. Sesuai dengan kebijakan pemerintah Indonesia yang pada akhirnya menetapkan peraturan pemerintah dalam hal pembatasan kegiatan masyarakat, hal ini menjadi acuan perusahaan dalam membuat kebijakan bekerja dari rumah atau *Work From Home* agar operasional perusahaan tetap berjalan. Ada beberapa aplikasi perusahaan yang hanya bisa diakses melalui jaringan Local Area Network kantor, beberapa karyawan diantaranya memanfaatkan penggunaan aplikasi remote dengan versi trial untuk dapat tetap mengakses aplikasi kantor dengan cara melakukan remote komputer kerja yang ada di kantor, dikarenakan aplikasi yang digunakan adakan dengan versi trial maka terdapat limitasi dalam penggunaannya, dengan rentang waktu penggunaan aplikasi ini maka akan terputus otomatis, sehingga menjadi masalah.

Tujuan dari kegiatan penelitian ini adalah untuk melakukan optimalisasi jaringan tunnel agar para karyawan sebagai end-user dapat mengakses aplikasi yang berada di kantor tanpa harus melakukan kegiatan remote ke komputer mereka. Pemanfaatan fitur yang ada pada RouterOS Mikrotik yakni Virtual Private Network sebagai jalur private tunnel yang dapat menghubungkan antara jaringan public internet dengan jaringan private Local Area Network.

2 Tinjauan Literatur

Dalam penelitian ini, penulis menggunakan beberapa penelitian sebelumnya sebagai bahan literatur untuk dapat menambah wawasan keilmuan penulis. Berikut adalah beberapa penelitian yang penulis jadikan sebagai bahan literatur.

Penelitian yang dilakukan oleh Elly Mufida, Dedi Irawan, Giatika Chrisnawati, menjelaskan tentang implementasi perangkat jaringan VPN dengan menggunakan *Router Mikrotik* untuk pengambilan data base transaksi keuangan pada aplikasi *Excellent*, dengan hasil bahwa proses pengambilan data sudah tidak lagi diambil dengan cara manual ataupun email, tetapi sudah memanfaatkan jaringan VPN yang sudah terintegrasi menjadi jaringan *Tunnel* antara kantor Yayasan dan sekolah (Mufida et al., 2017).

Penelitian yang dilakukan oleh Ikhwan Ruslianto, Uray Ristian, menjelaskan penerapan SSTP pada *Mikrotik* merupakan sebuah metode dalam membuat jaringan privat di Fakultas MIPA Universitas Tanjungpura menggunakan koneksi internet, membuat pengguna dapat mengakses jaringan kampus tanpa harus berada pada jaringan *private* (LAN) (Ruslianto, 2019).

Penelitian yang dilakukan oleh Rian Septian Anwar, Nani Agustina, menjelaskan penggunaan OpenVPN dapat memberikan akses keamanan data yang lebih baik. *Open VPN* dapat bekerja dengan baik disaat melakukan koneksi *virtual* (*Tunnel*) dalam mengakses jaringan interkoneksi (Anwar & Agustina, 2020).



DOI : 10.54593/jstekwid.v1i1.44

Jurnal Sains dan Teknologi WidyaloKa This work is licensed under a [Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License](https://creativecommons.org/licenses/by-nc-sa/4.0/).



Penelitian yang dilakukan oleh Jabal Nur, La raufun, Muhtita Afifa, menjelaskan mengenai implementasi VPN *Mikrotik* dengan Metode SSTP sehingga dapat menghubungkan dan mengkomunikasikan kampus Palagimata dan kampus Istana Ilmiah Unidayan Baubau (Nur et al., 2021).

Penelitian yang dilakukan oleh Riana Febrianti, Sidik, Susafa'ati, Esron Rikardo Nainggolan, Ummu Radiyah, menjelaskan mengenai penggunaan Virtual Private Network Point to Point Tunneling Protocol (PPTP) sebagai protocol yang dimanfaatkan untuk menghubungkan komunikasi data antara Gedung A dan Gedung B di SMK Pejuang Negeri Haurgeulis Indramayu, dapat terkoneksi dengan aman walau dengan menggunakan jaringan public (Febrianti et al., 2021).

Penelitian yang dilakukan oleh Arnita Arnita, Muhammad Farid, menjelaskan mengenai kinerja jaringan *Virtual Private Network* membuat transmisi data lebih cepat dan efisien dalam penggunaannya, dengan menggunakan teknologi *Multi Protocol Label Switching* sesuai dengan kebutuhan untuk pengembangan komunikasi interkoneksi data dan juga kualitas jaringannya baik (Arnita & Farid, 2020).

Penelitian yang dilakukan oleh Sidik, Ade Sudaryana, Rame Santoso, menjelaskan mengenai pemanfaatan *EoIP Tunnel* untuk mengakses *file server* yang dilakukan dari kantor cabang Citereup ke kantor Pusat lebih cepat, terdapat peningkatan kecepatan sebesar 48% dalam proses *transfer data* (Sidik et al., 2020).

Penelitian yang dilakukan oleh Sari Dewi, Fajar Riyadi, Tita Suwastitaratu, Noer Hikmah, menjelaskan mengenai penggunaan metode *Tunneling Protocol PPTP (Point To-Point Tunneling Protocol)* pada Kantor Desa Kertaraharja sangat bermanfaat untuk komunikasi data, pekerjaan dan pertukaran informasi jadi lebih fleksibel, cepat kemudian administrator jaringan dapat melakukan pekerjaan dengan cara remote (Dewi, 2020).

Penelitian yang dilakukan oleh Haekal Alief Syawaludin, Ahmad Fauzi, Susy Rosyida, menjelaskan mengenai tentang adanya *Tunneling PPTP VPN* pengiriman informasi dan data antar instansi pusat dan cabang tidak lagi menggunakan aplikasi pihak ke 3 dan keamanan data lebih terjamin (Haekal Alief Syawaludin, Ahmad Fauzi, 2010).

Penelitian yang dilakukan oleh Muhammad Husni Zarkasyi, Agus Ganda Permana, Heru Christian Dilak, menjelaskan mengenai VPN *Server* memiliki kemampuan lebih baik dalam melayani akses data dan juga dengan VPN *Server* dapat mengakses jaringan local perusahaan dari luar jaringan kantor yang telah *diforward* ke jaringan *internet* (Zarkasyi et al., 2018).

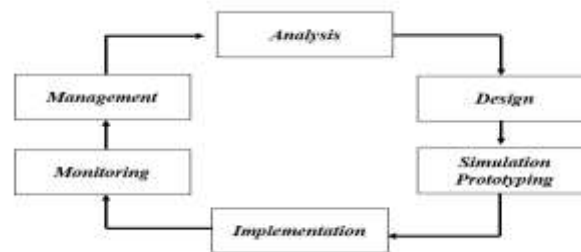
Penelitian yang dilakukan oleh Sari Masshitah, Fikri Divac Puzian, menjelaskan mengenai bahwa dalam evaluasi keamanan jaringan terbukti bahwa menggunakan VPN dengan protocol PPTP terdapat kompres data, enkapsulasi dan enkripsi sehingga komunikasi data menjadi lebih aman (Hendra, 2016).

Adapun yang membedakan penelitian ini dengan penelitian sebelumnya adalah penggunaan SSL Sertifikat terverifikasi baik di perangkat Mikrotik maupun perangkat komputer pengguna, sehingga keamanan *transfer data* menjadi aman, dan juga penempatan perangkat *Mikrotik* sebagai VPN *Tunnel* dibelakang *Firewall*. Selain daripada penelitian sebelumnya, peneliti juga menggunakan beberapa sumber lain diantaranya buku dan juga artikel online sebagai literatur penelitian

3 Metode Penelitian

Pada penelitian ini penulis menggunakan metode Network Development Life Cycle sebagai sebuah metode perancangan yang dibuat berdasarkan rancangan yang sudah ada sebelumnya (Wirainformatika, 2019).





Gambar 1. Diagram Network Development Life Cycle

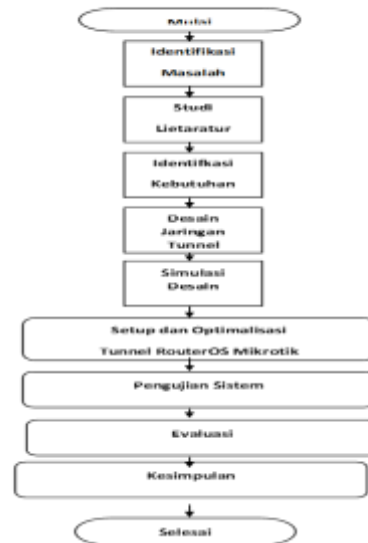
Sebagai objek penelitian adalah optimalisasi pemanfaatan jaringan Tunnel dengan menggunakan RouterOS Mikrotik untuk menjembatani komunikasi data antara jaringan public dengan jaringan LAN dikantor. Sedangkan sebagai subjek penelitian adalah para karyawan untuk mendapatkan tingkat kepuasan karyawan dalam hal pengimplemtasian jaringan VPN Ini untuk mendukung kegiatan work from home

Dalam menganalisa data penulis menggunakan teknik analisa data dengan model interaftif Miles dan Huberman, yang dimulai dari mengumpulkan beberapa data mentah (Raw Data) , kemudian menampilkan data, dan dilanjutkan dengan mereduksi data hingga proses verifikasi dan kesimpulan data yang diperoleh.

Tahapan yang dilakukan dalam penelitian ini adalah sebagai berikut:

1. Tahap pertama dalam penelitian ini adalah dengan melakukan observasi dan wawancara terhadap karyawan PT. KLK Agriservindo untuk mengidentifkasi masalah atas kendala yang dihadapi saat melakukan kegiatan bekerja dari rumah (WFH).
2. Melakukan Studi Literatur untuk mendukung penelitian ini dalam bidang keilmuan dengan menggunakan beberapa jurnal penelitian yang sudah terbit dan juga bebeapa buku pengetahuan.
3. berdasarkan data yang diperoleh dari kegiatan observasi dan wawancara dan juga didukung oleh kegiatan studi literatur penelitian, kemudian dilakukan desain optimaliasi jaringan *Tunnel*.
4. Melakukan simulasi dari desain optimalisasi jaringan *Tunnel* untuk menjadi bahan pertimbangan sebelum diimplementasikan kedalam jaringan yang real. Pada tahap ini menggambarkan secara simulasi atau dilakukan uji coba pada jaringan
5. Melakukan Implementasi jaringan *Tunnel* dengan menggunakan *RouterOS mikrotik* agar dapat memenuhi kebutuhan pengguna dalam hal ini karyawan dan manajemen perusahaan untuk dapat mengakses *resources* yang berada di Local Area Kantor dengan memanfaatkan jalur *Tunnel Virtual Private Network* dengan metode *Secure Socket Transfer Protocol*.
6. Melakukan evaluasi atas sistem yang sudah berjalan
7. Memberikan kesimpulan atas penelitian yang telah dilakukan.





Gambar 2. Kerangka Pemikiran

4 Hasil dan Pembahasan

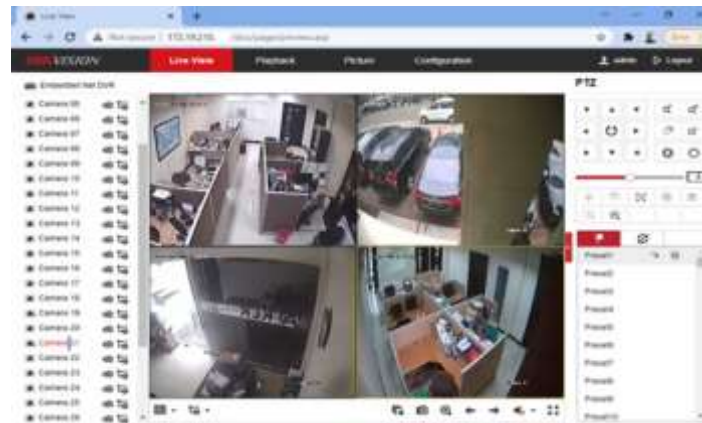
Sebelum implementasi jaringan Tunnel, karyawan menggunakan beberapa aplikasi berbayar dengan versi Trial untuk melakukan remote, diantaranya adalah TeamViewer dan Anydesk, dikarenakan yang digunakan adalah versi trial maka ada limitasi penggunaan aplikasi tersebut sehingga mengakibatkan koneksi remote terputus otomatis

Setelah dilakukan implementasi optimalisasi jaringan tunnel maka karyawan kembali dapat mengakses aplikasi dan resources data yang berada pada jaringan lokal kantor PT. KLK Agriservindo dengan baik dan tidak terkendala dengan limitasi waktu penggunaan

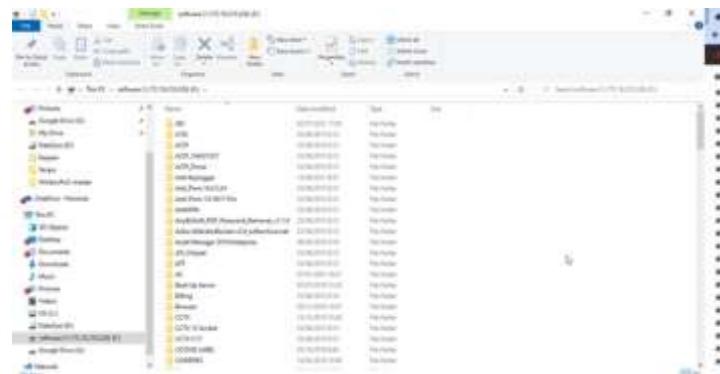


Gambar 3. Akses aplikasi web purchasing





Gambar 4. Monitoring CCTV System



Gambar 5. Map Network Drive

Infrastruktur jaringan informasi di PT. KLIK Agriservindo sebelum dan sesudah memasuki masa pandemik *Covid-19* masih hanya sebatas lalu lintas data dengan pemanfaatan koneksi internet untuk beberapa kegiatan seperti berikut :

1. *Email*.
2. *Browsing*.
3. *Share data* dengan menggunakan free online storage (*Google drive, Microsoft One Drive*).
4. Mengakses aplikasi internal baik *desktop* maupun *web*.
5. Melakukan troubleshooting secara *remote* menggunakan aplikasi *remote* dengan lisensi percobaan (*trial*) contohnya aplikasi *Teamviewer* dan *Anydesk*.



DOI : 10.54593/jstekwid.v1i1.44

Jurnal Sains dan Teknologi WidyaloKa This work is licensed under a [Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License](https://creativecommons.org/licenses/by-nc-sa/4.0/).



Gambar 6. Topologi sebelum optimalisasi jaringan Tunnel

Untuk menyelesaikan permasalahan yang dihadapi dalam penerapan kebijakan bekerja dari rumah (*Work From Home*). Dengan melakukan implementasi berupa optimalisasi penggunaan *RouterOS* sebagai Jaringan Tunnel, memberikan hasil dan manfaat bagi para karyawan PT. KLIK Agriservindo sehingga dapat mengakses beberapa *resources* yang berada di jaringan *local area network* kantor tanpa harus berada dilokasi kantor



Gambar 7. Topologi setelah implementasi jaringan tunnel

Routerboard Mikrotik sudah *built-in* dengan *operating systemnya*, yakni *RouterOS*. Tahap selanjutnya adalah melakukan instalasi aplikasi *winbox* untuk dapat melakukan konfigurasi terhadap *Routerboard Mikrotik*. Aplikasi *winbox* ini dapat didownload di *website Mikrotik* dengan alamat <https://mikrotik.com/download> pilih versi *winbox* yang akan didownload.

Beberapa konfigurasi yang dilakukan pada perangkat Mikrotik adalah sebagai berikut :

1. Pengaturan *Ip Address*
2. Pengaturan *Gateway*
3. Pengaturan *DNS*
4. Pembuatan *IP Pool*
5. *Setup VPN Tunnel dengan Metode Secure Socket Transfer Protocol*
6. Instalasi *SSL Sertifikat* Terverifikasi kedalam perangkat Mikrotik





Gambar 8. Setup SSTP Server di Mikrotik

Dikarenakan perangkat Mikrotik sebagai *VPN Tunnel* berada dibelakang Perangkat *Load Balancer* dan juga *firewall*, maka dibutuhkan setup *policy* dikedua perangkat tersebut. Berikut adalah beberapa konfigurasi yang dilakukan di perangkat *Juniper Firewall* agar *traffic* dari luar dapat mengakses perangkat *Mikrotik Tunnel*:

1. Membuat *Virtual IP* yang dapat memapping IP menuju ke perangkat *Mikrotik*
2. Membuat *Policy* yang mengijinkan *traffic* dari *port 443* menuju ke perangkat *Mikrotik*

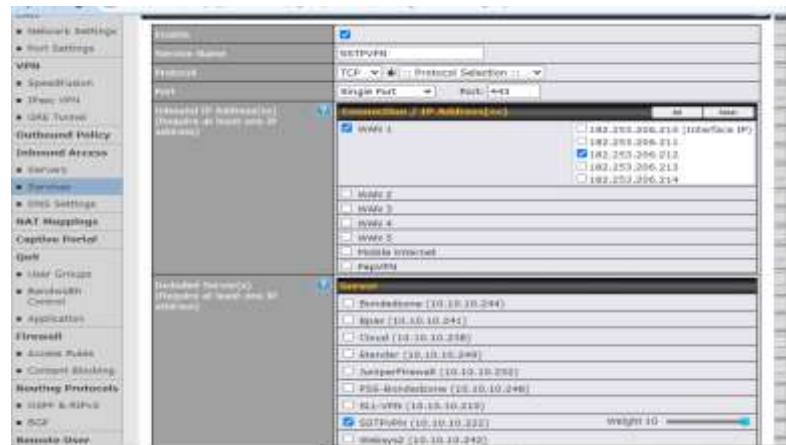


Gambar 9. Allow Traffic port 443 ke perangkat Mikrotik

Kemudian dilakukan juga beberapa konfigurasi pada perangkat *Peplink* sebagai perangkat yang dari dan menuju ke jaringan *public (Internet)* agar *traffic* yang menggunakan *port 443* dapat diakses dari jaringan *public*:

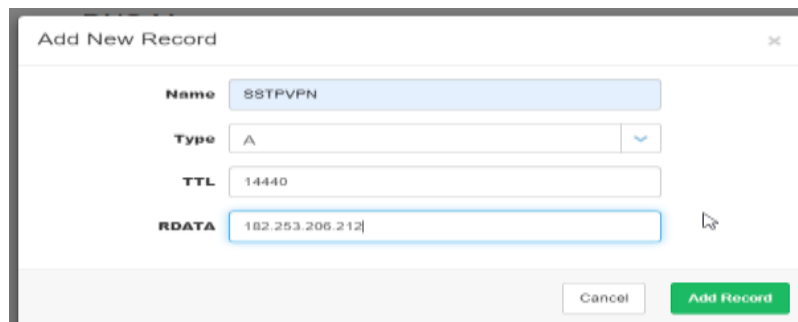
1. Membuat *Virtual IP* Yang mengarah ke perangkat *Juniper* yang sudah di Mapping ke perangkat *Mikrotik*.
2. Membuat *Policy* agar *traffic* dari *public* dapat mengakses prangkat *Mikrotik* dengan *port 443*.
3. Kemudian menentukan link internet mana yang akan digunakan dan dipointing untuk *traffic Tunnel Secure Socket Transfer Protocol (SSTP)*.





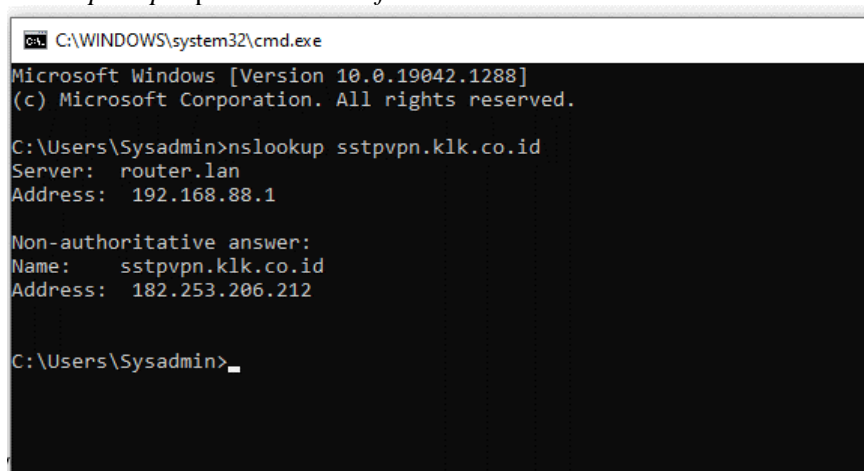
Gambar 10. Pointing IP Public SSTP VPN

Untuk memudahkan dalam mengakses SSTP VPN Tunnel, kemudian melakukan *pointing domain* di hosting dengan mengarahkan *nameserver* `sstp.vpn.klk.co.id` ke alamat *IP Public* yang sudah ditentukan.



Gambar 11. Pointing Domain Name

Kemudian lakukan pengecekan apakah *sub-domain* tersebut sudah *resolve* atau belum dengan menggunakan *command prompt* aplikasi *Microsoft Windows*.



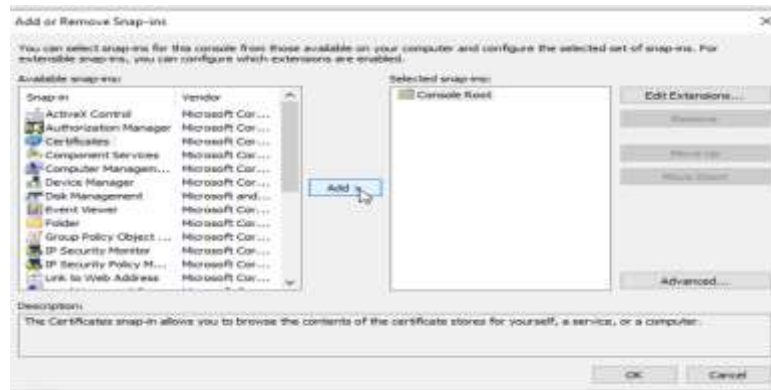
Gambar 12. Hasil Pengecekan Domain Name





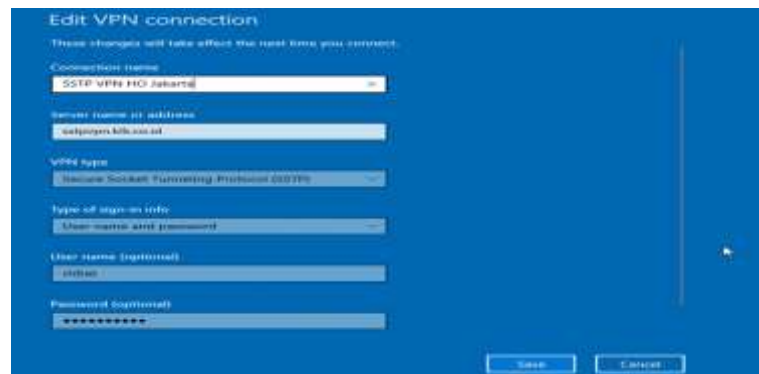
Kemudian untuk dapat terhubung antara komputer pengguna ke jaringan private kantor PT. KLK Agriservindo dilakukan beberapa konfigurasi pada perangkat komputer pengguna :

1. Melakukan import SSL terverifikasi kedalam perangkat komputer



Gambar 13. Import Sertifikat SSL ke Komputer Pengguna

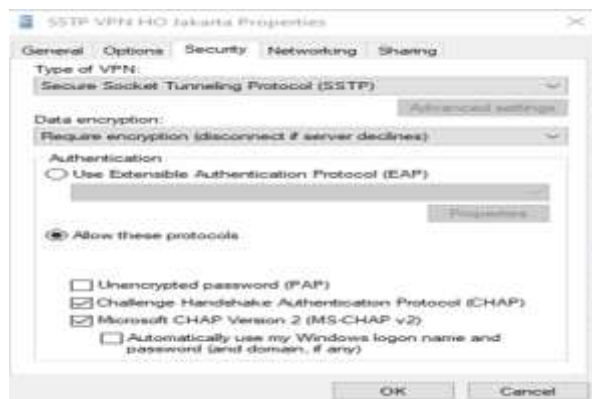
Kemudian membuat sebuah koneksi baru yang mengarah ke jaringan *tunnel* PT. KLK Agriservindo.



Gambar 14. Membuat Koneksi VPN di Perangkat Pengguna

Agar koneksi antara perangkat pengguna dengan jaringan tunnel aman maka dilakukan beberapa konfigurasi seperti berikut :





Gambar 15. Setup Security VPN Di Client

Setelah proses konfigurasi keamanan VPN diperangkat komputer pengguna kemudian lakukan koneksi ke jaringan *tunnel* dengan mengklik *connect* pada koneksi VPN yang telah kita buat sebelumnya.

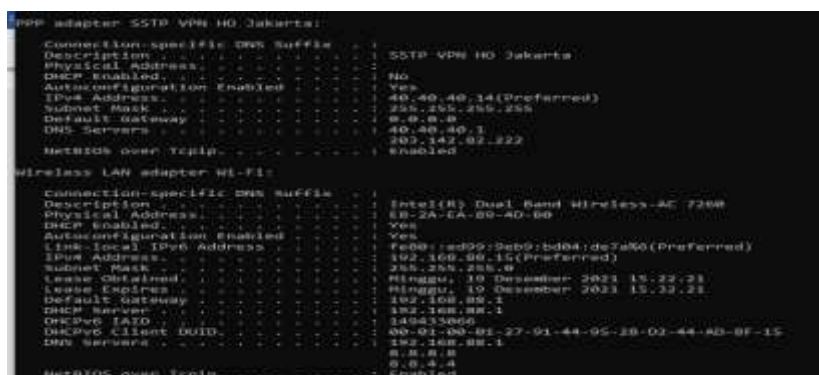


Gambar 16. Tampilan Menu *Connect*



Gambar 17. Tampilan SSL VPN sudah Terkoneksi

Setelah terkoneksi ke jaringan *tunnel* PT. KLK Agriservindo lakukan beberapa pengecekan untuk memastikan bahwa perangkat komputer pengguna sudah terkoneksi dengan jaringan *tunnel*.



Gambar 18. Hasi Test Cek Ip Address

Kemudian lakukan tes koneksi dengan menggunakan tools ping dan *tracert* ke arah komputer *host* yang berada di jarnngan *private* kantor PT. KLK Agriservindo.





```
C:\Users\Sysadmin>ping 172.19.210.226

Pinging 172.19.210.226 with 32 bytes of data:
Reply from 172.19.210.226: bytes=32 time=5ms TTL=127
Reply from 172.19.210.226: bytes=32 time=7ms TTL=127
Reply from 172.19.210.226: bytes=32 time=8ms TTL=127
Reply from 172.19.210.226: bytes=32 time=6ms TTL=127

Ping statistics for 172.19.210.226:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 5ms, Maximum = 8ms, Average = 6ms

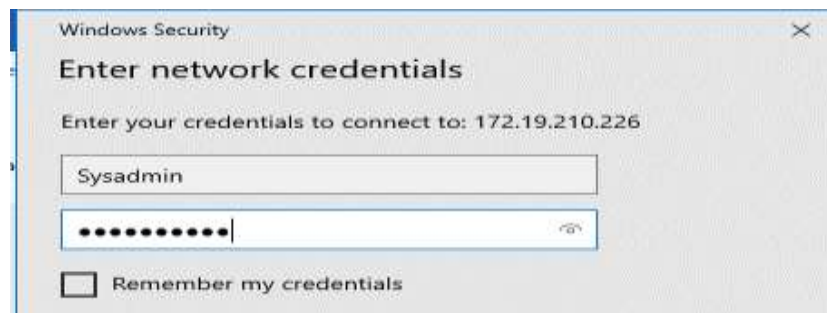
C:\Users\Sysadmin>tracert 172.19.210.226

Tracing route to HPSWITCH [172.19.210.226]
over a maximum of 30 hops:
  0  7 ms    7 ms    6 ms  40.40.40.1
  1  8 ms    7 ms    6 ms  HPSWITCH [172.19.210.226]

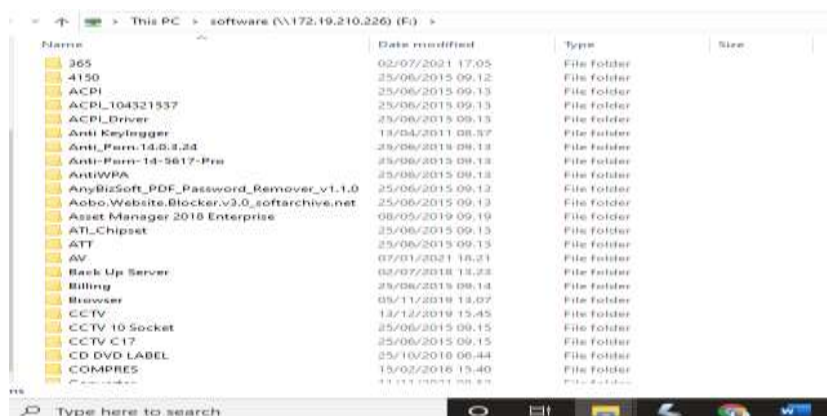
Trace complete.
```

Gambar 19. Hasil Ping dan Tracert

Kemudian lakukan percobaan *Map Network Drive* kearah *host* 172.19.210.226



Gambar 20. Memasukan *Credential Host* 172.19.210.226



Gambar 21. Tampilan *Map Network Drive Host* 172.19.210.226

Pada pelaksanaan implementasi Optimalisasi jaringan Tunnel dengan menggunakan *RouterOS*, tidak ditemukan kendala yang menjadi penyebab hambatan dari penelitian ini, semua berjalan dengan baik, adapun untuk hasil akses ke aplikasi server yang berada di *Local Area Network* kantor PT. KLK Agriservindo itu sangat tergantung dari *Bandwith Internet* dan kestabilan koneksi yang dimiliki oleh *internet* pengguna dan juga *internet* di kantor PT. KLKA. Berdasarkan hal tersebut penulis memberikan analisa bahwa koneksi *Tunnel* bergantung kepada *bandwith internet* yang dimiliki.



DOI : 10.54593/jstekwid.v1i1.44

Jurnal Sains dan Teknologi Widyalyoka This work is licensed under a [Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License](https://creativecommons.org/licenses/by-nc-sa/4.0/).



5 Kesimpulan

Berdasarkan hasil dari implementasi jaringan *tunnel* yang diterapkan di PT. KLK Agriservindo pada penelitian ini, penulis mendapatkan kesimpulan bahwa :

1. Dengan pengimplementasian jaringan tunnel menggunakan *RouterOS Mikrotik* para karyawan dapat kembali mengakses beberapa resources aplikasi berbasis jaringan yang berada di *Local Area Network* kantor PT. KLK Agriservindo tanpa harus berada dilokasi kantor dan batasan waktu akses.
2. Dengan penerapan *Secure Socket Layer* menggunakan SSL sertifikat terverifikasi proses *transfer* data menjadi lebih aman.
3. Penggunaan *RouterOS Mikrotik* sebagai *router device* untuk menjalankan service *Virtual Private Network* dengan metode *Secure Socket Transfer Protocol* menggunakan port 443 menghindari kemungkinan layanan service terblokir atau terisolasi oleh Provider Internet, dikarenakan menggunakan port yang sama dengan browser menggunakan *HTTPS (Hypertext Transfer Protocol Secure)*.
4. Dengan harga yang lebih murah dibandingkan produk manufaktur lainnya, penggunaan *RouterOS Mikrotik* dapat menekan biaya pengeluaran, walaupun lebih murah dibanding produk manufaktur lainnya akan tetapi fungsi dari fitur-fitur yang ada pada *RouterOS Mikrotik* cukup handal.

Referensi

- [1] Anwar, R. S., & Agustina, N. (2020). *Implementasi dan Analisa Kinerja Jaringan Wide Area Network dengan Open VPN-Access Server*. 4(2), 143–152.
- [2] Arnita, A., & Farid, M. (2020). *Implementasi jaringan virtual private network dengan teknologi Multi Protocol Label Switching (MPLS)*. 5(2), 28–39.
- [3] Dewi, S. (2020). *Keamanan Jaringan Menggunakan VPN (Virtual Private Network) Dengan Metode PPTP (Point To Point Tunneling Protocol) Pada Kantor Desa Kertaraharja Ciamis*. *EVOLUSI: Jurnal Sains Dan Manajemen*, 8(1), 128–139. <https://doi.org/10.31294/evolusi.v8i1.7658>
- [4] Haekal Alief Syawaludin, Ahmad fauzi, S. R. (2010). *Jurnal Edik Informatika Jurnal Edik Informatika*. 7(1), 9–18.
- [5] Hendra, S. (2016). *Implementasi Remote Site Pada Virtual Private Network Berbasis Mikrotik*. *Bina Insani ICT Journal*, 3(1), 85–98.
- [6] Mufida, E., Irawan, D., & Chrisnawati, G. (2017). *Remote Site Mikrotik VPN Dengan Point To Point Tunneling Protocol (PPTP) Studi Kasus pada Yayasan Teratai Global Jakarta*. *Jurnal Matrik*, 16(2), 9. <https://doi.org/10.30812/matrik.v16i2.7>
- [7] Nur, J., Raufun, L., & Afifa, M. (2021). *SIMULASI VIRTUAL PRIVATE NETWORK (VPN) MENGGUNAKAN SECURE SOCKET TUNNELING PROTOCOL (SSTP) PADA JARINGAN KAMPUS UNIDAYAN BAUBAU SIMULATION OF VIRTUAL PRIVATE NETWORK (VPN) USING SECURE SOCKET TUNNELING PROTOCOL (SSTP) ON UNIDAYAN BAUBAU CAMPUS NET*. 10(1), 85–92.
- [8] Ruslianto, I. (2019). *Perancangan dan Implementasi Virtual Private Network (VPN) menggunakan Protokol SSTP (Secure Socket Tunneling Protocol) Mikrotik di Fakultas MIPA Universitas Tanjungpura*. *Computer Engineering, Science and System Journal*, 4(1), 74. <https://doi.org/10.24114/cess.v4i1.11792>
- [9] Sidik, 1, Sudaryana, A., 2, Santoso, R., & 3. (2020). *Implementasi Virtual Interface Menggunakan Metode EOIP Tunnel Pada Jaringan WAN PT. Indo Matra Lestari*. VI(1), 2550–



DOI : 10.54593/jstekwid.v1i1.44

Jurnal Sains dan Teknologi Widyadoka This work is licensed under a [Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License](https://creativecommons.org/licenses/by-nc-sa/4.0/).



0120. <https://doi.org/10.31294/jtk.v4i2>

- [10] Wirainformatika. (2019). *NETWORK DEVELOPMENT LIFE CYCLE (NDLC)*. <https://www.wirainformatika.com/2019/08/28/network-development-lifecycle-ndlc/>
- [11] Zarkasyi, M. H., Agus, I., Permana, G., Dillak, H. C., & Kom, S. (2018). Implementasi Virtual Private Network (Vpn) Server Dengan Menggunakan Mikrotik Os Di Pt . Charisma Persada Nusantara Implementation of Virtual Private Network (Vpn) Server Using Mikrotik Os in Pt . Charisma Persada Nusantara. *Implementasi Virtual Private Network(VPN) Server Dengan Menggunakan Mikrotik Os Di Pt. Charisma Persada Nusantara*, 4(3), 2463–2474.



DOI : 10.54593/jstekwid.v1i1.44

Jurnal Sains dan Teknologi WidyaloKa This work is licensed under a [Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License](https://creativecommons.org/licenses/by-nc-sa/4.0/).