Implementasi Jaringan VPN Menggunakan L2TP Dengan IP Sec Pada PT Datindo Infonet Prima

Farizal Triyansa[1], Irwan Agus Sobari[2]

[1,2]Program Studi Informatika, Fakultas Teknologi Informasi, Universitas Nusa Mandiri
Jl. Jatiwaringin No. 2, Cipinang Melayu, Makasar, Jakarta Timur - 13620, Indonesia

e-mail: [1] 12207063@nusamandiri.ac.id, [2] irwan.igb@nusamandiri.ac.id

Artikel Info : Diterima : 28-04-2022 | Direvisi : 30-05-2022 | Disetujui : 15-06-2022

Abstrak - Perancangan ini berlatar belakang oleh adanya kebutuhan suatu jaringan yang mengkhususkan user untuk kerja di rumah (WFH) dikarena masalah pandemi covid-19 oleh peraturan pemerintah PPKM level 3. Tepatnya teknologi VPN sangat berperan penting dalam dunia komunikasi sekarang ini, dikarenakan VPN mampu membuat jaringan lokal dengan menggunakan fasilitas publik. Dengan adanya VPN perusahaan bisa menjalin suatu koneksi data yang mudah dan bersifat aman. VPN dapat memungkinkan untuk terbentuknya suatu jaringan data privasi yang dapat di akses melalui jaringan publik yaitu internet, Hanya yang mendapatkan otoritas sajalah yang dapat mengakses VPN tersebut. L2TP (Layer 2 Tunneling Protocol) menawarkan solusi keamanan yang cukup baik dengan cara membuat tunnel (terowongan) pada jaringan publik. Penggunaan L2TP itu sendiri tidak lepas dengan pengaruh sistem keamanan yang makin berkembang pesat, Oleh karenanya dengan menambahkan proses L2TP dengan IPsec diharapkan mampu menangani kasus masalah dari sistem kemanan jaringan. Dengan akses VPN para pekerja dapat bekerja di dalam rumah (WFH) tanpa harus ke kantor.

Kata Kunci : VPN, L2TP, IPsec.

Abstracts *- This design is based on the need for a network that specializes in users for working at home (WFH) due to the covid-19 pandemic problem by PPKM level 3 government regulations. using public facilities. With a VPN, companies can establish an easy and secure data connection. VPN can allow for the formation of a private data network that can be accessed through a public network, namely the internet, only those who have the authority can access the VPN. L2TP (Layer 2 Tunneling Protocol) offers a fairly good security solution by creating a tunnel on a public network. The use of L2TP itself cannot be separated from the influence of the security system which is growing rapidly. Therefore, by adding the L2TP process with IPsec, it is hoped that it will be able to handle problem cases from the network security system. With VPN access, workers can work from home (WFH) without having to go to the office..*

Keywords : VPN, L2TP, IPsec

PENDAHULUAN

Pada dasarnya setiap perusahaan selalu menginginkan kemudahan, keamanan dan kecepatan dalam pertukaran data. Karena hal tersebut merupakan salah satu aspek pendukung dalam berjalannya operasional suatu perusahaan. Jika ke tiga aspek tersebut tidak terpenuhi, Maka pasti akan terjadi hambatan dalam proses operasional dalam suatu perusahaan. Terlebih lagi di zaman Pandemi covid-19 ini para Perusahaan banyak yang menerapkan sistem *Work From Home* (WFH) untuk menjamin kesehatan para karyawannya (Idris, 2021) . Oleh sebab itu dibutuhkan komunikasi antar jaringan, Sehingga semua karyawan yang menjalani *Work From Home* (WFH) masih dapat menjalankan aktifitas pekerjaanya meskipun tidak berada di kantor.

Selain dari pada itu komunikasi data pada internet dapat melibatkan masalah keamanan, kemudahan dan kecepatan transfer. Hal ini yang harus diperhatikan oleh pemilik sistem informasi suatu perusahaan dalam melakukan berbagai kegiatan di dunia internet. Sehingga kerahasiaan informasi suatu perusahaan dapat terjaga dengan baik serta kecepatan pertukaran data dapat di terapkan meskipun dari jarak jauh sehingga dapat menghemat

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

waktu dan biaya pada perusahaan tersebut. Penggunaan VPN L2TP sangat disarankan untuk menjaga keamanan data yang mengenkapsulasi ganda jika dibandingan dengan PPTP.

Virtual Private Network (VPN) yang menggunakan RB1100X2AH menjadikan penggunanya terhubung langsung ke jaringan kantor seperti halnya jaringan lokal atau LAN dengan membuat tunneling pada jaringan internet, Menjadikan komputer yang lokasi- nya jauh dapat saling terhubung ke jaringan lokal atau LAN (Huda, 2019). VPN juga merupakan salah satu teknogi termurah untuk membantu menghubungkan 2 jaringan yang berbeda (Prayogi Wicaksana et al., 2021). Dengan menggunakan IP Sec pada VPN sehingga lebih aman karena terenkripsi (Sari et al., 2020). Sehingga proses transaksi dan manajemen tetap berjalan di masa pandemi dengan akses dari VPN tersebut (Zuhri & Sobari, 2017). Beberapa protokol yang bisa diterapkan dalam membuat VPN diantaranya PPTP dan L2TP (Dahnial, 2019).

Oleh sebab itu perlunya manajemen jaringan yang baik untuk memfasilitasi seluruh karyawan (Nalendra, 2020). Sehingga jaringan VPN yang terbentuk menjadi lebih baik dan stabil digunakan saat WFH (Supriadi et al., 2021). Penggunaan VPN juga mampu memangkas pemakaian bandwidth menjadi lebih kecil (Firmansyah et al., 2019). Teknologi VPN ialah *tunneling* dimana merupakan salah satu dasar untuk membuat jaringan private melalui jaringan publik (Sidik et al., 2020). Untuk itu dibangun sebuah jaringan private dari kantor pusat dengan berbagai tempat disesuaikan dengan user client sehingga dengan adanya hal tersebut dapat memudahkan para karyawan menyelesaikan pekerjaannya tanpa harus terkendala waktu dan tempat (Syawaludin et al., 2020). Hal ini dapat membawa dampak baik pada kinerja dan hasil pekerjaan sesuai yang diharapkan.

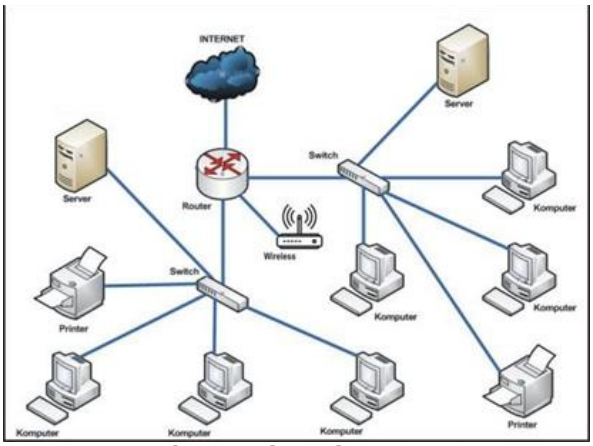
METODE PENELITIAN

Beberapa metode yang dilakukan penulis dalam melakukan penelitian sebagai berikut:

1. Observasi, penulis melakukan peninjauan secara langsung ke PT Datindo Infonet Prima untuk melihat langsung jaringan yang telah ditarapkan.
2. Wawancara, Penulis melakukan wawancara dengan Ibu Windri Anggraini sebagai Admin Marketing, Ibu Yulli sebagai *Staff Payroll* yang terkendala pekerjaan ketika *Work From Home* (WFH).
3. Studi Pustaka, penulis mempelajari beberapa artikel ilmiah dan buku dan mengambil sebagai sumber referensi.

HASIL DAN PEMBAHASAN

PT. Datindo Infonet Prima mempunyai koneksi internet bersumber dari ISP yaitu Biznet dengan kecepatan speed download Up To 40 Mbps dan Upload Up To 40 Mbps.Koneksi internet yang didapat dialirkan ke router mikrotik, lalu ke switch1 dan switch2 kemudian ke komputer server, wireless router, absensi dan ke 45 komputer atau laptop user. IP Address yang digunakan adalah IP Address kelas C

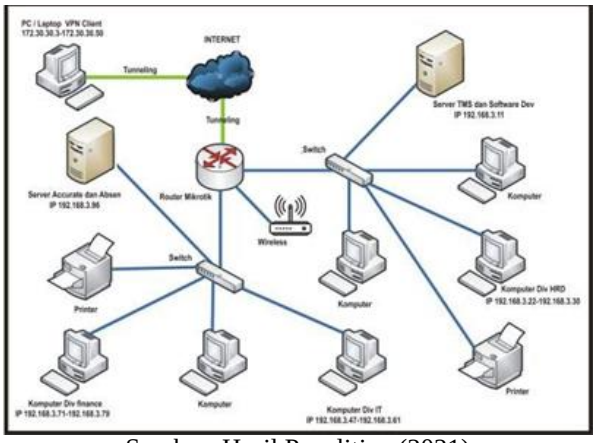


Sumber: Hasil Penelitian (2021)
Gambar1. Skema Jaringan Datindo Infonet Prima

1. Jaringan usulan

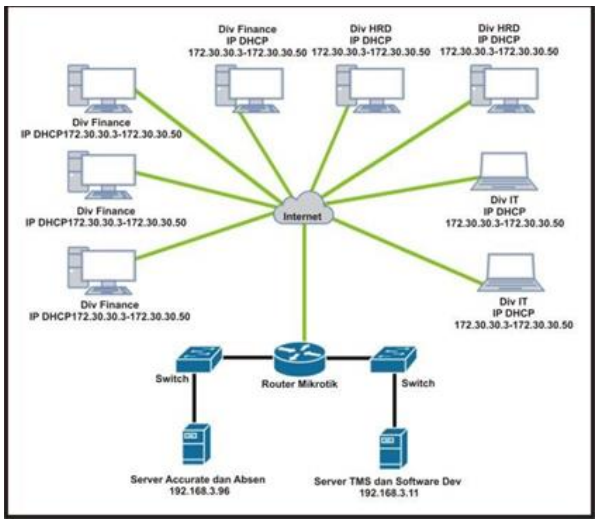
Jaringan VPN yang diusulkan yaitu dengan menggunakan remote access untuk menghubungkan client ke jaringan lokal perusahaan dari berbagai macam lokasi yang jauh dari perusahaan. Dengan harapan dapat mempermudah client dalam hal ini ialah karyawan PT. Datindo Infonet Prima yang sedang menjalani WFH atau pekerja yang sedang WFO, Tapi sedang berada dilapangan yakni para engineer, IT Software Suppot, Network engineer dan lain sebagainya untuk tetap bisa terhubung ke jaringan perusahaan, Tentunya dengan network yang

aman, Serta bisa juga digunakan untuk menghubungkan antara kantor pusat dan juga kantor cabang.



Sumber: Hasil Penelitian (2021)
Gambar3. Skema Jaringan Usulan

Berdasarkan skema jaringan tersebut, Hanya beberapa divisi yang akan dapat akses untuk VPN, Di karenakan membutuhkan data yang ada pada server. Seperti divisi finance membutuhkan akses ke jaringan lokal kantor untuk terkoneksi dengan aplikasi accurate server yang berada di server dengan IP 192.168.3.96, Terdapat 4 karyawan finance yang membutuhkan akses tersebut. Kemudian dari divisi HRD terdapat 2 karyawan yang membutuhkan akses ke jaringan lokal kantor, Untuk menarik absen para tim engineer, Tim repair, Dan karyawan lainnya yang sedang WFO (Work From Office), Dan yang terakhir divisi IT untuk memonitoring server 192.168.3.11 yang berada dikantor, Agar dapat melihat aplikasi TMS (Terminal Managament System) berjalan normal atau tidak. Berikut gambaran skema jaringan ketika client terkoneksi jaringan melalui jaringan VPN L2TP IpSec.



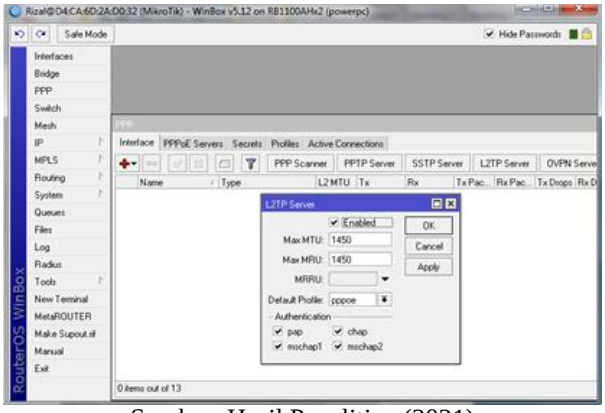
Sumber: Hasil Penelitian (2021)
Gambar4. Skema Jaringan Client VPN

Sedikit penjelasan dari skema diatas, VPN Client menggunakan internet dari luar kantor atau dirumah masing-masing karyawan dengan PC atau Laptop, Kemudian login dengan menggunakan VPN L2TP yang sudah dibuat dengan cara memasukan IP Publik kantor yaitu 117.102.94.74 kemudian memasukan username dan password yang sudah ditentukan. Ketika VPN berhasil terkoneksi maka PC atau Laptop client sudah terkoneksi langsung dengan jaringan lokal dikantor, Melalui mikrotik yang akan memberikan rute ke setiap server.

2. Implementasi

a. Konfigurasi L2TP Server

Masuk ke aplikasi winbox pilih menu PPP maka akan tampil jendela PPP, selajutnya pilih L2TP Server,dan pada jendela L2TP Server checklist pada checkbox enable. Gunakan profile “Default-encryption” agar jalur VPN terenkripsi.

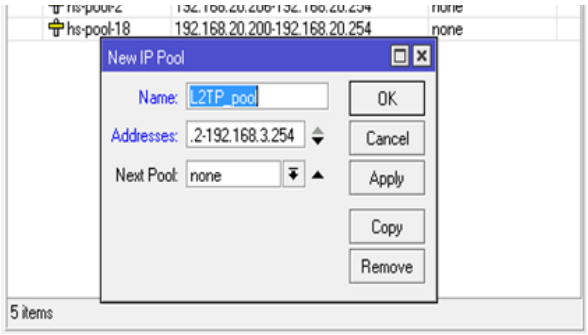


Sumber: Hasil Penelitian (2021)
Gambar5. Konfigurasi L2TP Server

b. Konfigurasi IP Poll

Kemudian kita buat L2TP Pool yang berfungsi untuk menentukan range IP VPN yang di dapat oleh VPN Client. Kita klik IP => Pool => klik tanda +, maka akan muncul jendela “New IP Pool”. Berikut fungsi dan form yang harus diisi:

1) Name adalah form untuk memasukan nama dari IP Pool yang ingin kita buat.
2) Addresses adalah form untuk memasukkan range IP yang akan kita setting di VPN Client kita isi dengan 10.63.3.30-10.63.3.35

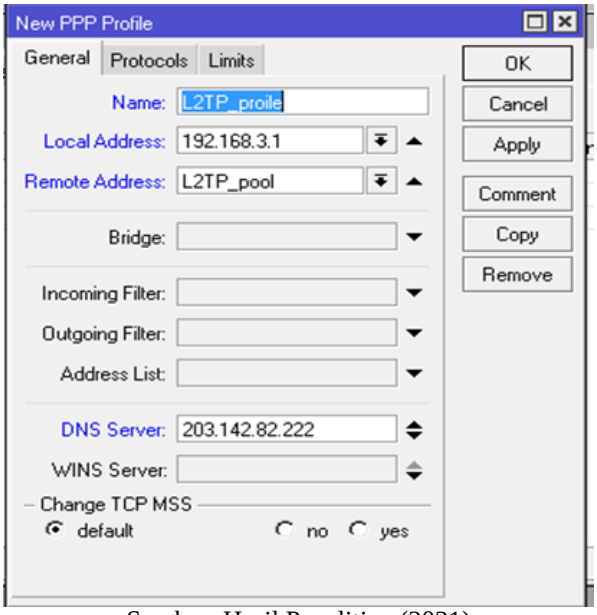


Sumber: Hasil Penelitian (2021)
Gambar6. IP Pool

c. Konfigurasi PPP Profile

pilih menu PPP => Profiles => klik tanda +, maka akan muncul jendela “PPP Profile”. Berikut fungsi dan form yang harus diisi:

1) Name adalah form untuk memasukan namaprofile yang akan kita buat.
2) Local Address adalah form untuk memasukkan gateway IP pada jaringa lokal. Masukkan 10.62.1.1.
3) Remote Address pilih L2TP_pool yang sudah kita buat tadi. DNS Server kita isi saja 8.8.8.8

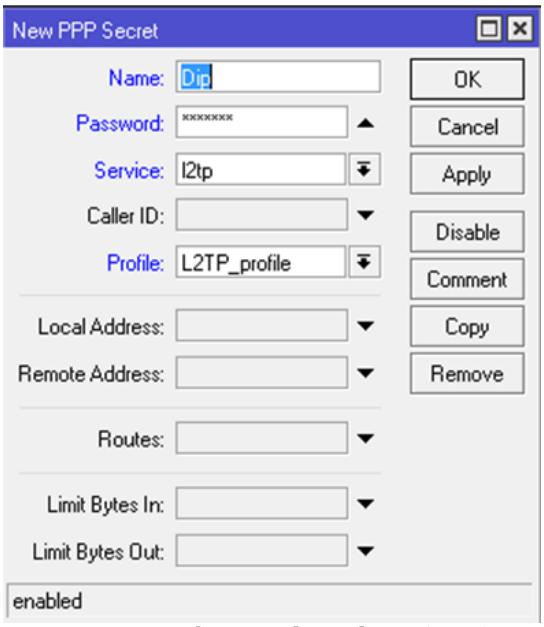


Sumber: Hasil Penelitian (2021)
Gambar7. Konfigurasi PPP Profile

d. Konfigurasi PPP Secret

Pada tahap ini, kita akan menentukan username dan password untuk proses autentikasi client yang akan terkoneksi ke L2TP Server. Penggunaan huruf besar dan kecil akan berpengaruh. Pilih menu PPP => secret => klik tanda +, maka akan muncul jendela PPP Secret. Berikut fungsi dan form yang harus diisi:

1) Name adalah form untuk memasukkan username dari client. Penggunaan huruf besar dan kecil akan berpengaruh.
2) Password adalah form untuk memasukkan password dari client. Penggunaan huruf besar dan kecil akan berpengaruh.
3) Service pilih L2TP, karena kita mensetting client L2TP.
4) Profile pilih L2TP_profile, dalam hal ini kita pilih menggunakan enkripsi yang sudah kita tambah sebelumnya.



Sumber: Hasil Penelitian (2021)
Gambar8. Konfigurasi PPP Secret

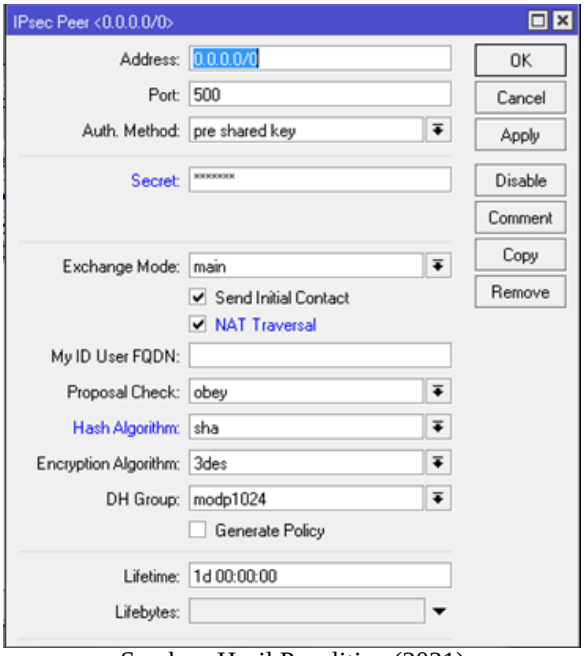
e. Konfigurasi IPsec

Tahap yang terakhir ini adalah kita akan konfigure IPsec untuk sistem keamana VPN. Berikut fungsi dan form yang harus diisi:

1) Secret adalah form untuk memasukkan password dari client. Penggunaan huruf besar dan kecil akan

berpengaruh.

2) Checklist pada checkbox NAT Traversal.
3) Hast Algorithm ubah sha



Sumber: Hasil Penelitian (2021)
Gambar9. Konfigurasi PPP Secret

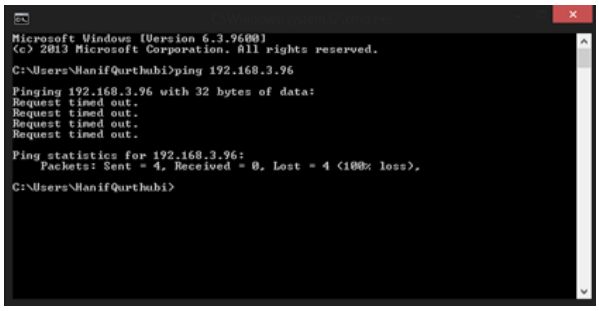
3. Pengujian

Tujuan pengujian jaringan ini agar melihat perbedaan antara jaringan awal dan jaringan akhir yang di usulkan penulis.

a. Pengujian awal

Pengujian jaringan awal akan dilakukan dengan melakukan ping dan mengakses file sharing server dari network luar ke network lokal perusahaan.

1) Ujicoba ping dari network luar ke ip lokal perusahaan, disini kita mencoba ping ke server perusahaan dengan IP tujuan 192.168.3.96, Terlihat pada gambar Gambar dari 4 paket yang dikirim, keseluruhan mengasilkan 100% Loss.



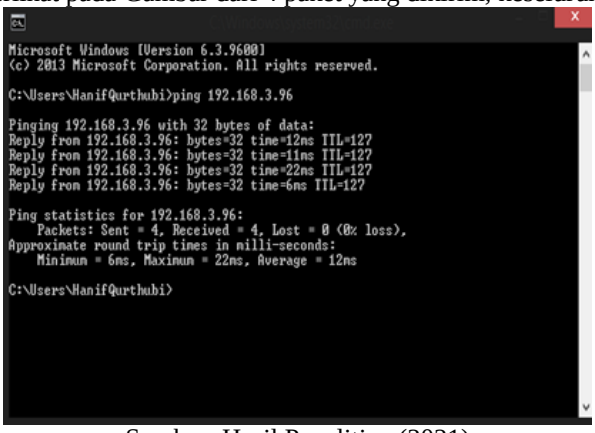
Sumber: Hasil Penelitian (2021)
Gambar10. Tes PING dari *network client* ke *network local.*

2) Ujicoba selajutnya yaitu membuka file sharing komputer server dari luar network perusahaan dengan alamat tujuan 192.168.3.96, Terlihat pada Gambar muncul pesan Network Error.

Sumber: Hasil Penelitian (2021)
Gambar11. Error saat mengakses directory folder server

b. Pengujian akhir

1) Ujicoba ping dari network luar ke ip lokal perusahaan, disini kita mencoba ping ke server perusahaan dengan ip tujuan 192.168.3.96. Terlihat pada Gambar dari 4 paket yang dikirim, keseluruhan berhasil dan 0% Loss.



Sumber: Hasil Penelitian (2021)
Gambar12. PING Jaringan Server dari client VPN.

2) Ujicoba selajutnya yaitu membuka file sharing komputer server dari luar network perusahaan dengan alamat tujuan 192.168.3.96. Terlihat pada Gambar file sharing dapat di akses.

Sumber: Hasil Penelitian (2021)
Gambar13. Client VPN mengakses directory local server.

KESIMPULAN

Pada penelitian serta penerapan, terdapat kesimpulan yang di ambil diantaranya, Bahwa dengan hasil konfigurasi melalui Remote Access pada windows dengan L2TP diperoleh hasil VPN Client dapat dikonfigurasikan dengan L2TP dan IPsec, Penerapan L2TP dan IPsec ini akan melakukan enkripsi terhadap proses transfer data dari VPN Client menuju Server, Begitu juga sebaliknya, Dan penggunaan VPN L2TP dan IPsec dapat memberikan kemudahan kepada karyawan yang sedang bekerja dari rumah WFH (*Work From Home*) untuk mengakses data yang ada pada perusahaan, tanpa harus datang ke perusahaannya, dan memberikan mekanisme keamanan yang baik.

REFERENSI

Dahnial, D. (2019). Analisa Perbandingan Quality Of Service Antara Protokol PPTP dan L2TP Pada Virtual Private Network Berbasis Router Mikrotik. *Jurnal Ilmiah Informatika Global*, *10*(2), 107–113. https://doi.org/10.36982/jig.v10i2.858

Firmansyah, F., Wahyudi, M., & Purnama, R. A. (2019). Analisis Performa Site to Site IP Security Virtual Private Network (VPN) Menggunakan Algoritma Enkripsi ISAKMP. *JUITA : Jurnal Informatika*, *7*(2), 129. https://doi.org/10.30595/juita.v7i2.4491

Huda, M. (2019). *Teknologi Komputer*. Bisakimia. https://www.google.co.id/books/edition%0A/Teknologi_Komputer/2DmnDwAAQBAJ%0A?hl=id&gbpv=0%0A

Idris, M. (2021). Mulai 24 Desember 2021, PPKM Level 3 Diterapkan di Seluruh Indonesia. *https://www.kompas.com*. https://www.kompas.com/wiken/read/2021/11/21/194144181/mulai-24-desember-2021-ppkm-level-3-diterapkan-di-seluruh-indonesia?page=all

Nalendra, K. A. (2020). *Manajemen Jaringan Komputer*. Pusaka Akademi Komunitas Indonesia. https://openlibrary.telkomuniversity.ac.id/pustaka/167243/manajemen-jaringan-komputer.html

Prayogi Wicaksana, Hadi, F., & Aulia Fitrul Hadi. (2021). Perancangan Implementasi VPN Server Menggunakan Protokol L2TP dan IPSec Sebagai Keamanan Jaringan. *Jurnal KomtekInfo*, *8*(3), 169–175. https://doi.org/10.35134/komtekinfo.v8i3.128

Sari, A. P., Sulistiyono, & Kemala, N. (2020). Perancangan Jaringan Virtual Private Network Berbasis IP Security Menggunakan Router Mikrotik. *Jurnal PROSISKO*, *7*(2), 150–164. https://e-jurnal.lppmunsera.org/index.php/PROSISKO/article/view/2523/1463

Sidik, Sudaryana, A., & Santoso, R. (2020). *Implementasi Virtual Interface Menggunakan Metode EOIP Tunnel Pada Jaringan WAN PT. Indo Matra Lestari*. *VI*(1), 103–110. https://doi.org/10.31294/jtk.v4i2

Supriadi, Y., Sobari, I. A., & Amir, R. F. (2021). Optimalisasi Jaringan Komputer Menggunakan Vpn Concentrator Dengan Bonding Pada Pt Maxindo Mitra Solusi Jakarta. *Jurnal Infortech*, *3*(1), 65–72. https://doi.org/10.31294/infortech.v3i1.10493

Syawaludin, H. A., Fauzi, A., & Rosyida, S. (2020). PERANCANGAN DAN IMPLEMENTASI JARINGAN TUNNEL DENGAN METODE PPTP PADA YAYASAN PENDIDIKAN BINA PUTERA INDONESIA. *Oktober*, *7*(1). http://dx.doi.org/10.22202/ei.2020.v7i1.4346

Zuhri, M., & Sobari, I. A. (2017). Optimalisasi Jaringan Wide Area Network Dengan Teknik Multiprotocol Label Switching. *Prosiding SIMNASIPTEK*, 190–194. http://seminar.bsi.ac.id/simnasiptek/index.php/simnasiptek-2017/article/view/140