MJRICT 2022;5(1) : (43-52)
MJRICT : Musamus Journal Of Research Information and Communication Technology
ISSN 2655-5735 (Online) | ISSN 2654-4083 (Cetak)
https://ejournal.unmus.ac.id/index.php/mjrict

# ANALISIS DAN OPTIMALISASI KEAMANAN JARINGAN MENGGUNAKAN PROTOKOL IPSec

Chalimatus Solikhah[*1], Nugroho Adhi Santoso[2], Rifki Dwi Kurniawan[3]
Program Studi Teknik Informatika STMIK YMI Tegal[1]
Program Studi Sistem Informasi STMIK YMI Tegal[23]
[1]chalimah23imeh@gmail.com, [2]nugrohoadhisantoso29@gmail.com, [3]rifki.dk@gmail.com

***Abstrak***

*IPSec terdiri dari beberapa protokol untuk melindungi jaringan menggunakan otentikasi dan proses enkripsi berbasis IP. IPSec memungkinkan sistem untuk memilih protokol keamanan, algoritma enkripsi, dan kunci keamanan untuk digunakan. IPSec adalah perlindungan keamanan berupa kontrol akses, perlindungan integritas, dan kerahasiaan. Koneksi antar jaringan komputer sangat diperlukan untuk pengembangan sistem pendidikan yang masih menggunakan fitur email dan whatsapp khususnya pada Mi Miftahul Huda di Tegal. Selain memungkinkan pihak yang tidak aman dan tidak bertanggung jawab untuk meretas, kehadiran IPSec dapat mendukung berbagai aktivitas, meningkatkan keamanan pengiriman, dan terjadi saat mengirim data melalui jaringan. dapat mengurangi kemungkinan ancaman tertentu.*

***Kata kunci****— Keamanan jaringan, Keamanan data, dan IPSec.*

***Abstract***

*IPSec consists of several protocols to protect the network using IP-based authentication and encryption processes. IPSec allows the system to choose the security protocol, encryption algorithm, and security key to use. IPSec is security protection in the form of access control, integrity protection, and confidentiality. Connections between computer networks are very necessary for the development of an education system that still uses email and whatsapp features, especially at Mi Miftahul Huda in Tegal. In addition to allowing insecure and irresponsible parties to hack, the presence of IPSec can support various activities, increase delivery security, and occur when sending data over the network. can reduce the likelihood of certain threats*

***Keywords—*** *Network security, Data security and IPSec*

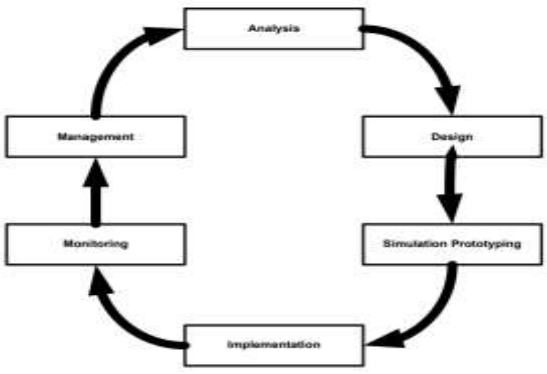
## 1. PENDAHULUAN

Kebutuhan ketersediaan jaringan komunikasi dan *internet* sangat meningkat dengan ketergantungan manusia akan peran teknologi informasi dan mempunyai dampak yang diperlukan adanya sistem penyediaan layanan *internet* yang efisien, canggih namun tetap ekonomis dan aman. Kemajuan teknologi khususnya teknologi jaringan memudahkan dunia pendidikan sekolah agar lebih berkembang dan menghadapi tantangan serta menemukan hal-hal baru. Di Mi Miftahul Huda Kota Tegal Pengamanan data masih menjadi suatu hal yang dirasa kurang penting dari pengguna komputer keamanan data masih dianggap sulit untuk diterapkan, sehingga keamanan data dianggap penting jika terjadi serangan atau pencurian data. [1]

Memasang *firewall* adalah wajib karena jaringan terhubung ke Internet dan pihak eksternal yang menggunakan *firewall* hanya dapat mengakses jaringan internal dengan izin. *Firewall* ini secara efektif mencegah pencurian data dan penyusup dari membobol sistem jaringan Anda. Namun, *firewall* tidak mencegah penyadapan data oleh pihak-pihak di dalam jaringan itu sendiri. Cara lain untuk meningkatkan keamanan data Anda adalah dengan mengenkripsi data yang dikirim. Jika data yang dikirim dalam format *file, file* tersebut dienkripsi dan tidak dapat dibaca kembali dengan cara biasa, tetapi untuk membuat data file sehat kembali, diperlukan pengembalian (*decode*) *enkripsi.* diperlukan. Untuk melakukan ini, pengirim harus melakukan prosedur enkripsi dan mengambil tindakan sebelum mengirim *file.* Demikian pula, penerima harus mendekripsi agar berhasil mengakses file yang diterima. Di Mi Miftahul Huda di kota Tegal, hal ini sering terlihat menjengkelkan karena pengirim tidak mengenkripsi *file* yang dikirim. Hal ini memudahkan pihak yang tidak diinginkan untuk mengakses bila file tersebut diambil oleh pihak yang tidak bertanggung jawab. Pengiriman *e-mail (e-mail)* dapat dilindungi dengan tanda tangan digital. Namun, jika mengharuskan untuk menyadari penerapan tanda tangan digital dalam email yang dikirim oleh pengirim *email*. Hal ini sering diabaikan. Beberapa untuk menyelesaiakan masalah yang muncul dari penerapan skema keamanan tersebut adalah dengan menggunakan *IPSec. IPSec* merupakan salah satu bagaimana meningkatkan keamanan transmisi data terutama pada jaringan komputer yang menggunakan protokol TCP/IP. *seletivitas* logika mengurangi kedua jumlah padam dan durasi jaringan distribusi IEC 61850 dapat diterapkan standar *logic Selectivity* dimana pesan Generik berorientasi Objek acara Subjek (*GOOSE*) pertukaran antara perangkat lapangan cerdas melalui internet. Namun keamanan informasi dan otomasi dicatat untuk memastikan pengoprasian seleksif yang aman dan akurat integrasi data dan kerahasiaan melalui *IPSec.* [2]

## 2. METODE PENELITIAN

Metode yang digunakan dalam penelitian ini adalah *metode Network Development Life Cycle (NDLC),* dengan beberapa tahapan-tahapan yaitu: Analisis dan *Design,* Simulasi, Implemetasi, Manajemen dan Monitoring**.** [3] Gambar *Network Development Life Cycle* ditunjukan pada gambar 1 sebagai berikut:




Gambar 1 *Network Development Life Cycle*

*IPSec* diimplementasikan lapisan transport dalam *OSI Reference* melindungi protokol IP dan protokol yang lebih tinggi dengan beberapa keamanan yang dapat dikonfigurasikan untuk memenuhi keamanan pengguna.

Metode yang dilakukan adalah sebagai berikut :

a. Penelitian Lapangan
   Penelitian ini dilakukan dengan mewancarai kepala sekolah dan guru mengajuakan pertanyaan dan menganalisis masalah.
b. Perpustakaan penelitian

Penelitian kepustakaan ini dengan cara membaca jurnal, buku, internet yang membahas tentang jaringan komputer, *IPSec* yang berkaitan dengan analisis dan optimalisasi keamanan jaringan. Sehingga dapat digunakan sebagai dasar penelitian selanjutnya. [4]

## 3. TINJAUAN PUSTAKA

**1. *L2TP/IPSec***

*L2TP* digunakan untuk autentikasi untuk dapat memenuhi keamanan jaringan makan disertai dengan mengimplementasikan keamanan dengan menggunakan *IPSec* antara *server* dan *client* lebih aman, dan terdapat perlindungan ganda pada jarinagan yang pertama dengan *point-to-point protocol* sedangkan perlindungan yang kedua dengan enkripsi untuk keamanan yang dimiliki *IPSec*. [5]

**2. *Multi-Layer IPSec***

*IPSec multi-layer* di mana proses enkripsi dan otentikasi *IPSec* diterapkan ke *payload* datagram IP atau header IP sebagai unit IPSec *multi-layer*, diagram IP dibagi menjadi beberapa zona, setiap zona memiliki satu asosiasi keamanan, akses pribadi Menentukan node mana memiliki zona dengan kunci. Bagian zona diagram IP dengan skema perlindungan keamanan. [6]

**3. TCP/IP *(Transmission Control Protocol/Internet Protocol)***

Suatu standar komunikasi data yang digunakan serangkaian internet dengan proses tukar menukar data dengan satu komputer ke komputer lainya disuatu jaringan, pembagian pada TCP/IP menjadi *protocol* komunikasi data yang diterapkan dengan mudah dan fleksibel disetiap komputer sebagian besar isi kumpulan *protocol* tidak spesifik terhadap satu komputer atau jaringan tertentu. [7]

Dalam pengembangan Internet tidak dapat dipisahkan dari kebutuhan perangkat *software*, *hardware*, dan protokol. Protokol standar yang diterapkan pada Internet adalah *TCP/IP*, dan implementasinya sangat penting dan mempengaruhi sistem kerja pada router. [8]

**4. *IP address***

*IP Address* merupakan pengenal numerik yang ditetapkan untuk perangkat seperti komputer, *router*, atau printer dalam jaringan komputer yang menggunakan Protokol Internet sebagai sarana komunikasi. [9]

*Subnetting* dalam Alamat *IP* versi 4 dari sistem teknik pengalamatan membantu mengurangi jumlah Alamat *host* di jaringan. Hasil yang didapat dari perhitungan *Subnetting, yaitu subnet mask, subnet, Jumlah host di setiap subnet, broadcast, Range IP, Network id* jaringan, dan jangkauan Setiap kelas IP. [10]

**5. *Network Address Translator (NAT)***

*NAT* membuat sekelompok komputer di jaringan tampil seolah-olah adalah satu komputer dengan satu alamat *IP*. Kondisi ini berguna ketika kumpulan alamat *IP* terbatas. walaupun terlihat menguntungkan di satu sisi, tetapi hanya yang sesuai dengan konsep komunikasi klien dari *server*. *Server* memiliki alamat global dan klien memiliki alamat *private*. [11]

Tujuan lain menggunakan *NAT* adalah untuk menyimpan alamat *IP* publik dan keamanan. Ini memungkinkan komputer yang terhubung ke jaringan *private (loca*l) untuk terhubung ke Jaringan Internet hanya dengan menggunakan alamat *IP private*. [12]

**6. Jaringan Komputer**

Jaringan komputer merupakan kumpulan dari komputer yang saling terhubung dan bekerja sama secara otomatis melalui media transmisi sebagai jalur koneksi. Pengguna jaringan komputer dapat bertukar dokumen dan data melalui kabel atau nirkabel dan berbagi perangkat keras atau perangkat lunak terhubung ke jaringan yang sama. [13]

Keamanan jaringan keamanan sistem suatu perlindungan yang diberikan untuk menjaga kerahasiaan, integritas, dan ketersediaan layanan data dan informasi. Beberapa yang digunakan

untuk membangun sistem Keamanan berarti aman. Yaitu,

1. Kerahasiaan yaitu orang yang memiliki hak dapat bisa mengetahui atau mengubah data suatu informasi),
2. Integritas yaitu Menjaminnya keaslian dan keakuratan dari data suatu informasi
   Ketersediaan yaitu Ketersediaan data informasi jika di akses oleh pengguna. [14]

**7. Sistem Operasi**

Sistem operasi adalah komponen penting dalam *hardware* seperti laptop atau komputer. Sistem operasi yang ada Hari ini adalah hasil dari perubahan sangat dipengaruhi oleh perkembangan teknologi komputer selama bertahun-tahun. *Windows* salah satu dari banyak sistem Operasi sedang berlangsung. Windows memiliki mengalami banyak perkembangan untuk membangun sistem. Beberapa versi Windows Saat ini digunakan yaitu *Windows 7*, *Windows 8* dan *Windows 10*. [15]

## 4. HASIL DAN PEMBAHASAN

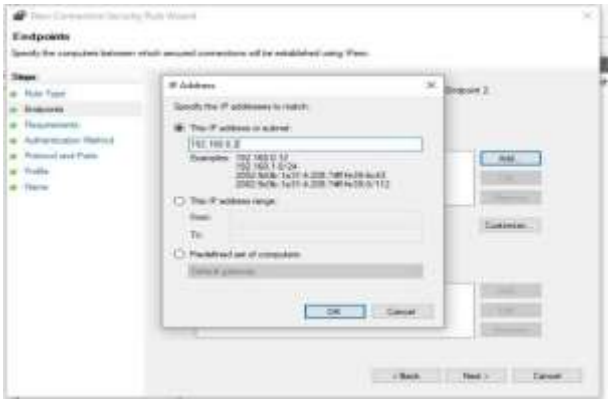
Ada beberapa yang perlu diketahui saat mengimplementasikan *IPSec*. Artinya, keseimbangan antara melindungi data Anda dari pengguna yang tidak sah dan memberikan akses kepada pengguna yang memiliki akses ke jaringan Anda. Ini harus dilakukan untuk menghindari analisis risiko jaringan. Tingkat keamanan yang diperlukan. Penting juga untuk menentukan jenis implementasi dan kebijakan keamanan terbaik untuk memastikan bahwa tidak ada masalah teknis atau administratif untuk mengidentifikasi informasi yang harus dilindungi dari serangan pada jaringan. Berikan akses kepada pengguna sehingga mereka dapat mengaksesnya dengan aman dan efisien hanya dalam kepentingan mereka. Beberapa langkah-langkah dalam mengimplementasikan *IPSec* di komputer *server Microsoft Windows* terlihat seperti ini :

1. Buka *Control panel* lalu pilih *Sistem & Security* kemudian *Windows Defender Firewall With Advanced Security*
2. Kemudian klik *New Connection Security Rules*
3. Pilih *Custom* di *rule type* lalu lanjutkan (*Next)*.

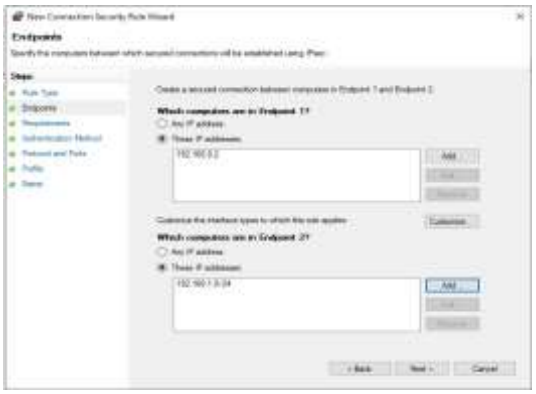
Pada gambar *New connection Security Rule Wizard* ditunjukan pada gambar 2 sebagai berikut:

Gambar 2 New connection Security *Rule Wizard*

4. Lalu masukan IP pada alamat *Endpoin1* dan IP client bagian alamat *Endpoint2*. IP boleh menggunakan range atau bisa *subnet*. Kemudian klik *Next* untuk melanjutkan, pada gambar *Enpoints* pada *IPSec* ditunjukan pada gambar 3 dan gambar 4 sebagai berikut:

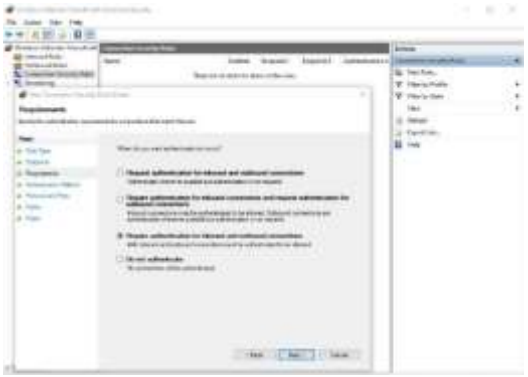


Gambar 3 Memasukan IP *Enpoint* di *IPSec*



Gambar 4 memasukan *IP Enpoint*

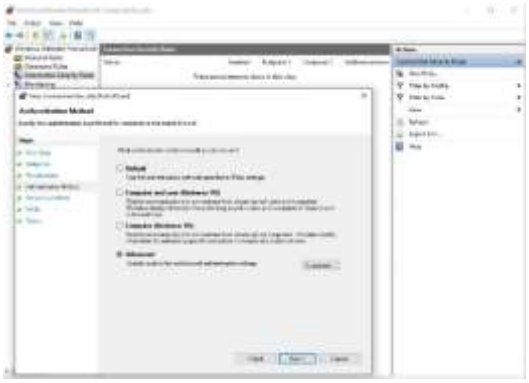
5. Kemudian memilih *Require aunthentication for inbound and outbound connections* lalu



Next, gambar *aunthentication* pada *IPSec* ditunjukan pada gambar 5 sebagai berikut:

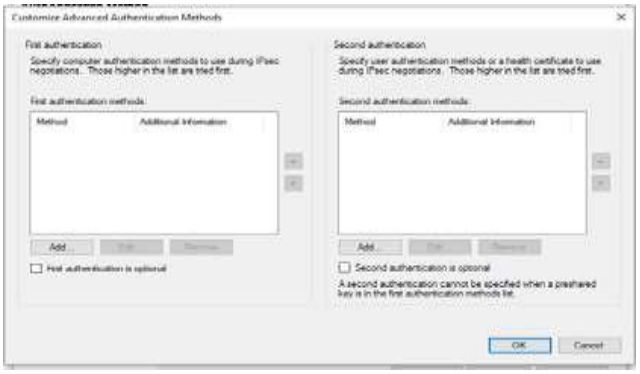
Gambar 5 aunthentication *IPSec*

6. Kemudian pilih *Advanced* lalu klik *customize* gambar metode otentikasi ditunjukan pada gambar 6 sebagai berikut



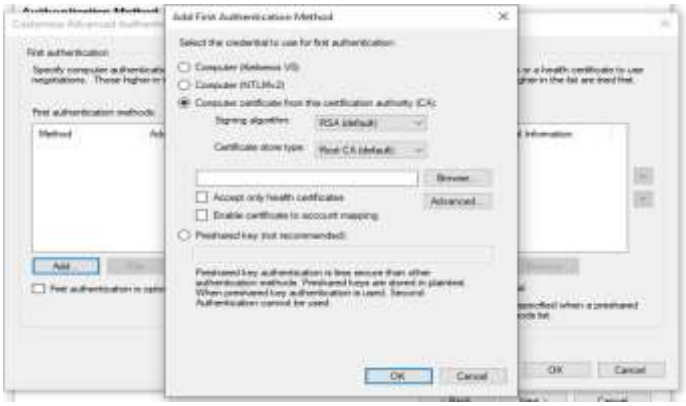
Gambar 6 Metode Otentikasi

Pada *First Aunthentication* lalu klik *Add* gambar *customize advanced Aunthentication methods* ditunjukan pada gambar 7 sebagai berikut:



Gambar 7 *customize advancedAunthentication methods*

7. Setelah memilih CA, kemudian *browse* untuk memilih CA, memilih metode otentikasi ditunjukan pada gambar 8 sebagai berikut:



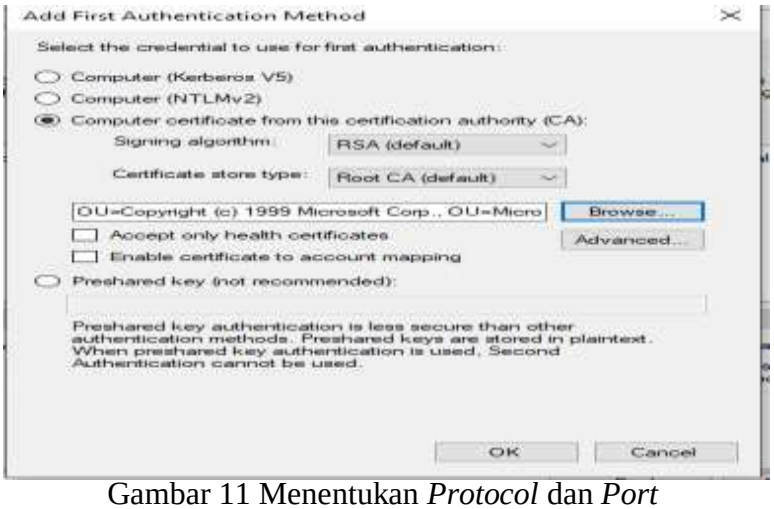
Gambar 8 Memilih Metode otentikasi

8. Kemudian ok lalu *Next*, gambar untuk memilih *Certificate authority* ditunjukan pada gambar 9 sebagai berikut:


Gambar 9 Memilih *Certificate authority*

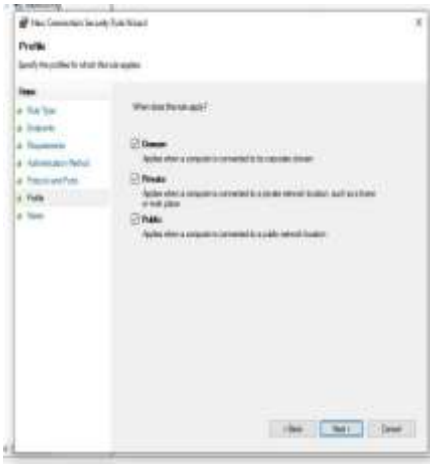
9. Menentukan *Protocol* dan *Port* gambar untuk menentukan *Protocol* dan *Port* ditunjukan pada gambar 10 dan gambar 11 sebagai berikut:


Gambar 10 Menentukan *Protocol* dan *Port*




Gambar 11 Menentukan *Protocol* dan *Port*

10. Ceklis semua pada profil lalu *Next*, gambar memilih *Profile Rule* ditunjukan pada gambar 12 sebagai berikut:

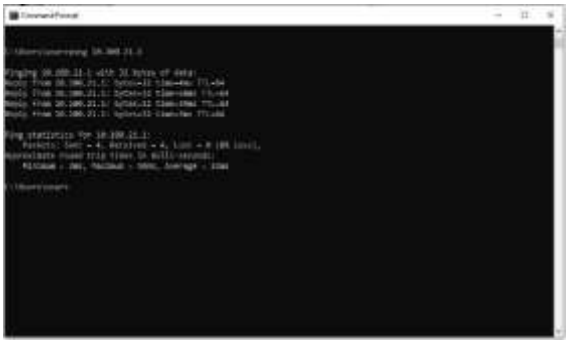


Gambar 12 Memilih Profile *Rule*

11. Masukan name pada *description rule* yang dibuat, kemudian klik *Finish* untuk menyelesaikan langkah konfigurasi, gambar menentukan *name* dan *descriptions rule* ditujukan pada gambar 13 sebagai berikut:

Gambar 13 Menentukan *name* dan *descriptions*

12. Kemudian, setelah menyelesaikan *fase* implementasi *IPSec*, gunakan prosedur yang sama untuk mengkonfigurasi komputer klien. Untuk memverifikasi bahwa *IPSec* berjalan dengan benar, gunakan perintah ping untuk memverifikasi komunikasi.. Gambar untuk menentukan koneksi jaringan ditunjukan pada gambar 14 sebagai berikut:



Gambar 14 Koneksi Jaringan

## 5. KESIMPULAN

Penelitian ini berfokus pada menganalisa serta mengeksplorasi sebuah fitur keamanan jaringan di *Microsoft Windows*. Persyaratan sistem, Microsoft Windows, lebih efisien dan tidak memerlukan penggunaan sebuah aplikasi pada desain keamanan jaringan karena dapat mengimplementasikan *IPSec* tanpa perangkat lunak tambahan. *IPSec* meningkatkan keamanan jaringan komputer dengan mengenkripsi data yang dikirim oleh *IPSec*. Jaringan komunikasi. Jika terjadi penyadapan, tidak bisa menampikan data asli tanpa menggunakan kunci *encripsi*. *IPSec* secara otomatis melindungi data. Seperti disebutkan di atas, model jaringan *client-server* dapat digunakan untuk mengimplementasikan *IPSec* dalam berbagai kasus. Atau model jaringan *point-to-point* dengan kemampuan tunneling IPSec. .

## DAFTAR PUSTAKA


[1] M. Maryanto, M. Maisyaroh, dan B. Santoso, "Metode Internet Protocol Security (IPSec) Dengan Virtual Private Network (VPN) Untuk Komunikasi Data," *PIKSEL Penelit. Ilmu Komput. Sist. Embed. Log.*, vol. 6, no. 2, hal. 179–188, 2018, doi: 10.33558/piksel.v6i2.1508.

[2] T. Rahman dan A. I. Haris, "Rancang Bangun Jaringan Virtual Private Network ( VPN ) Berbasis IPSec Pada PT . INNER CITY MANAGEMENT," *Simp. Nas. Ilmu Pengetah. dan Teknol. 2017*, 2017.

[3] F. Sjafrina, "Rancang Bangun Jaringan VPN Berbasis IPSEC Menggunakan Mikrotik Routerboard Pada PT. Zahir Internasional," *Proc. Semin. Nas. Teknol. Inf. dan Komun. STI&K (SeNTIK 2019)*, vol. 3, hal. 211–217, 2019.

[4] Prayogi Wicaksana, F. Hadi, dan Aulia Fitrul Hadi, "Perancangan Implementasi VPN Server Menggunakan Protokol L2TP dan IPSec Sebagai Keamanan Jaringan," *J. KomtekInfo*, vol. 8, no. 3, hal. 169–175, 2021, doi: 10.35134/komtekinfo.v8i3.128.

[5] J. Safira, P. Teknologi, R. Jaringan, J. T. Elektro, dan P. N. Lhokseumawe, "Implementasi Jaringan Vpn L2Tp / Ipsec Menggunakan Linux Di," vol. 5, no. 1, hal. 59–63, 2021.

[6] M. M. Ipsec, S. Efendi, dan Z. Situmorang, "Analisis Pengamanan Jaringan Pada Protokol IPv6," *Query J. Inf. …*, vol. 5341, no. October, hal. 10–23, 2019, [Daring]. Tersedia pada: http://jurnal.uinsu.ac.id/index.php/query/article/view/6362.

[7] I. F. Anshori, "Implementasi Socket Tcp/Ip Untuk Mengirim Dan Memasukan File Text Kedalam Database," *Responsif*, vol. Vol 1 No 1, no. 1, hal. 1–5, 2019.

[8] L. Z. A. Mardedi dan K. Marzuki, "Network Rancang Bangun Jaringan Komputer LAN Berdasarkan Perbandingan Kinerja Routing Protokol EIGRP dan Routing Protokol OSPF," *MATRIK J. Manajemen, Tek. Inform. dan Rekayasa Komput.*, vol. 18, no. 2, hal. 202–210, 2019, doi: 10.30812/matrik.v18i2.372.

[9] Y. Adi, "Perancangan Manajemen Bandwidth Dan Block Access Website Berdasarkan User Di Mikrotik Pada Ananda Islamic School," *KERNEL J. Ris. Inov. Bid. Inform. dan Pendidik. Inform.*, vol. 1, no. 2, hal. 94–101, 2020, doi: 10.31284/j.kernel.2020.v1i2.1196.

[10] S. Hidayatulloh, P. M. Ilham, dan M. Lase, "Calculation Application for Subnetting IPv4 Address on Android," *J. Informatics Telecommun. Eng.*, vol. 4, no. 1, hal. 112–118, 2020, doi: 10.31289/jite.v4i1.3827.

[11] R. Asmara dan D. Saputra, "Jurnal J – Click Jurnal J – Click," *J-Click*, vol. 6, no. 2, hal. 201–207, 2019.

[12] U. U. Indonesia *et al.*, "Analisa Dan Perancangan Public Cloud Storage Dengan Memanfaatkan Fitur Forwarding Network Address Translation Melalui Virtual Private Network Server Menggunakan Mikrotik Public Cloud Storage Analysis and Design By Using the Forwarding Network Address Tran," vol. 7, no. 2, hal. 56–67, 2021.

[13] S. Sumarna dan A. Maulana, "Implementasi Virtual Private Network Menggunakan L2TP/IPsec pada BBPK Jakarta," *Expert J. Manaj. Sist. Inf. dan Teknol.*, vol. 11, no. 2, hal.

90, 2021, doi: 10.36448/expert.v11i2.1829.

[14] D. F. S. Astri Saraun, Arie S.M. Lumenta, "An Analysis of WLAN Security at the Minahasa Regency Office of Educational Affairs," *J. Tek. Inform. unsrat*, vol. 17, no. 1, hal. 19–26, 2021.

[15] D. Nur Sulistyowati, I. Budiawan, dan D. Arum Ningtyas, "Sistem Pendukung Keputusan Pemilihan Sistem Operasi Windows Pada Dekstop Dengan Menggunakan Metode Analytical Hierarchy Process," *J. Ilmu Pengetah. Dan Teknol. Komput.*, vol. 3, no. 2, hal. 175–180, 2018, [Daring]. Tersedia pada: http://www.nusamandiri.ac.id.