ANALISIS PENERAPAN TEKNOLOGI VIRTUAL PRIVATE NETWORK (VPN) SEBAGAI SOLUSI KEAMANAN DATA DI JARINGAN PUBLIK

Harry Pribadi Fitrian, Nanda Alia Destiara, Neng Elsa Destianti, Gilan Maddanil Khowat
Manajemen Informatika, Universitas Teknologi Digital
Jln. Cibogo indah III Bodogol, Jawa Barat, Indonesia
harrypribadi@digitechuniversity.ac.id

ABSTRAK

Di era perkembangan teknologi yang semakin pesat, pertukaran data dan komunikasi melalui jaringan publik juga semakin meningkat. Namun, ancaman keamanan seperti penyadapan (*sniffing*), peretasan dan serangan *man-in-the-middle* semakin sering terjadi yang sangat berpotensi mengakibatkan kebocoran data sensitif. Penelitian ini bertujuan untuk menganalisis penerapan teknologi *Virtual Private Network* (VPN) sebagai solusi untuk meningkatkan keamanan data pada jaringan publik. Metode yang digunakan adalah studi literatur, dengan pengumpulan data, pemilihan artikel dan analisis serta indentifikasi jurnal-jurnal terkait permasalahan. Hasil penelitian ini menunjukan bahwa penggunaan *Virtual Private Network* (VPN), terutama dengaan protokol L2TP/IPSec, dapat memberikan perlindungan data yang optimal melalui mekanisme enkripsi dan *tunneling*. Pengujian QOS pada protokol ini menunjukan hasil yang sangat baik dengan nilai *packet loss* mendekati nol, *delay* dan *jitter* dalam kategori sangat bagus, serta troughput yang tinggi. Kesimpulan dari penelitian ini menegaskan bahwa *Virtual Private Network* (VPN) merupakan solusi efektif untuk keamanan data, terutama pada jaringan publik dengan risiko yang tinggi.

Kata kunci : *keamanan data, sniffing, Virtual Private Network (VPN), protokol L2TP/IPSec, jaringan publik.*

1. PENDAHULUAN

Semakin berkembangnya teknologi membuat pertukaran informasi dan data menjadi lebih efektif dan efisien. Dimana setiap orang membutuhkan informasi dalam waktu yang cepat, singkat dan akurat. Dengan adanya internet membuat jarak bukan lagi sebagai kendala dalam hal berkomunikasi atau berbagi data.

Namun, kemajuan teknologi ini juga diiringi dengan meningkatnya ancaman keamanan selama proses pertukaran informasi dan data tersebut. Ancaman yang paling umum adalah peretasan, penyadapan (*sniffing*) dan serangan yang dilakukan *hacker* untuk menyusup terhadap komunikasi antara dua pihak dan memantau serta mengubah data yang dikirimkan oleh dua pihak tersebut (*man-in-the-middle*). Hal ini dapat berdampak serius, seperti kebocoran informasi sensitif, kemudian kerugian finansial, hingga ancaman terhadap privasi individu dan organisasi

Sebagai respons terhadap tantangan ini, diperlukan solusi yang dapat menjamin keamanan data selama proses transmisi. Salah satu teknologi yang menjadi andalan dalam mengatasi permasalahan ini adalah *Vitual Private Network* (VPN). *Virtual Private Network* (VPN) merupakan teknologi pengamanan jaringan yang menciptakan terowongan (*tunnel*) untuk memungkinkan jaringan yang valid terhubung ke jaringan eksternal melalui internet. *Virtual Private Network* (VPN) memanfaatkan jaringan internet yang bekerja berdasar TCP/IP sebagai media internet sehingga jangkauannya menjadi luas tanpa investasi yang besar. Standar utama *Virtual Private Network* (VPN) selalu menyertakan fitur utama enskripsi dan *tunneling* untuk keamanan data dan kerahasian transmisi data dari akses yang tidak berhak dalam transmisinya.

Bedasarkan permasalahan dan ancaman yang telah di uraikan di atas maka solusi yang relevan dan penting untuk mengatasi ancaman keamanan dalam pertukaran informasi dan data pada jaringan publik. Penelitian ini akan mengkaji lebih dalam mengenai penggunaan dan implementasi *Virtual Private Network* (VPN) sebagai solusi dalam mengatasi permasalahan dan ancaman dalam keamanan data jaringan publik.

2. TINJAUAN PUSTAKA

2.1. Ancaman Keamanan data

a. *Sniffing*
Sniffing bisa disebut sebuah bentuk *cyber-crime* yang memantau atau memegang kendali data pengguna secara ilegal dengan cara memanfaatkan jaringan internet. Pelaku *sniffing* akan melakukan penipuan mengatasnamakan korban dan merusak/menghapus data milik korban. Pelaku *sniffing* kerap kali melancarkan aksinya dengan program *sniffer* yang berfungsi sebagai penganalisis jaringan dan bekerja untuk memantau jaringan pada komputer [1].

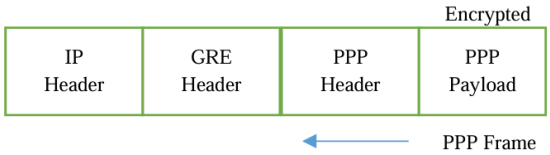
b. *Man-in-the-middle*
Serangan *man-in-the-middle* merupakan serangan yang memanfaatkan celah dalam jaringan untuk memantau, mencuri atau mengubah data yang dikirimkan antara dua pihak yang berkomunikasi [2]. Pelaku *man-in-the-middle* menyusup dalam aliran komunikasi dan meniru salah satu pihak, sehingga mereka dapat memperoleh akses tidak sah ke informasi yang *sensitive*.

2.2. Analisis Protokol VPN Dan Definisi Tunneling

VPN merupakan suatu jaringan private yang menghubungkan satu jaringan ke jaringan yang lain dengan memanfaatkan jaringan internet. Data yang dikirimkan dalam proses pertukaran data di enkapsulasi dan dienkripsi agar data tersebut terjaga kerahasiaannya [3].

Agar antar pengguna dapat terhubung pada komunikasi VPN maka dibutuhkan suatu protokol VPN. Ada tiga protokol VPN yang paling sering digunakan dan paling populer, yaitu ada *Point To Point Protocol* (PPTP), *Layer Two Tunneling Protocols* (L2TP), serta yang ketiga ada *Internet Protocol Security* (IPSec). Ketiga protokol tersebut akan dianalisis untuk menemukan metode mana yang paling baik dan aman digunakan dengan kajian studi kasus yang sudah ada sebelumnya.

a. *Point To Point Protocol* (PPTP)
   Pada protokol PPTP memungkinkan jalur lintas multi-protokol yang dienskripsi dan dirumuskan pada header ip yang nantinya dikirimkan melalui IP organisasi atau IP public seperti internet. PPTP mengimplementasikan teknik encapsulasi untuk mengintegrasikan frame PPP ke dalam datagram IP, memungkinkan transmisi data yang cepat dan aman melalui jaringan IP [4].



Gambar 1. Struktur paket pptp ip diagram

b. *Layer 2 Tunneling Protocol* (L2TP)
   Layer 2 Tunneling Protocol atau disingkat L2TP adalah salah satu protokol VPN yang merupakan hasil pengembangan dari protokol PPTP atau juga sering disebut sebagai protokol *dial-up virtual*. L2TP ini sendiri memperluas seni *dial-up* dari PPP menggunakan jaringan *public*. L2TP memiliki metode pengamanan jaringan yang dimiliki sedikit lebih baik dibandingkan PPTP yang dimana hanya menggunakan MPPE [5]. Namun, kekurangan yang dimiliki L2TP ini yaitu tidak memiliki enskripsi, sehingga protokol ini masih memerlukan layanan tambahan untuk menciptakan kemananan yang lebih tinggi lagi seperti protokol IPSec sebagai *layer* 3 untuk meningkatkan keamanan privasi.
c. *Internet Protocol Security* (IPSec)
   IPSec merupakan protokol yang dipakai untuk mengamankan transmisi datagram pada jaringan yang berbasis TCP/IP. IPSec bisa juga dikenal dengan rangkaian protokol yang dapat menambahkan keamanan komunikasi pada tingkat *Internet Protocol* (IP). IPSec memiliki 3 layanan inti, yaitu autentikasi dan integritas data, kerahasiaan, serta manajemen kunci [5]. IPSec ini juga menyediakan enkripsi *end-to-end* untuk data yang dikirimkan melalui *tunneling* L2TP.
d. *Tunneling*
   Tunneling merupakan sebuah teknologi yang menangani dan menyediakan koneksi *point to point* dari sumber sampai ke tujuannya dalam membangun koneksi jaringan sendiri di dalam jaringan umum yang dilaluinya, sehingga hanya dapat dilalui secara *private* oleh si pembuat koneksi. *Tunneling* adalah metode pengiriman data yang memanfaatkan proses enkapsulasi paket *multicast* menjadi *unicast*, sehingga data dapat dikirimkan dari satu jaringan ke jaringan lainnya dengan memanfaatkan jalur tersembunyi [6]

3. METODE PENELITIAN

Metode yang digunakan dalam penelitian ini adalah pengumpulan data berdasarkan studi literatur dengan menggali informasi pada jurnal-jurmal penelitian yang terkait dengan topik "Analisis Penerapan Teknologi *Virtual Private Network* (VPN) Sebagai Solusi Keamanan Data Di Jaringan Publik" yang bertujuan untuk mengidentifikasi kesenjangan penelitian yang signifikan.

Langkah yang akan dilakukan diantaranya:

a. Pengumpulan data
   Pada tahap ini adalah proses pengumpulan data sebagai bahan pengembangan sistem yang dilakukan dengan cara observasi dan studi pustaka mencari sumber dari jurnal-jurnal yang membahas tentang keamanan jaringan [7]
b. Pemilihan artikel
   Pada tahap ini adalah proses pemilihan artikel yang sesuai dengan topik untuk mengumpulkan informasi tentang keamanan jaringan
c. Analisis dan identifikasi
   Pada tahap ini dilakukan analisis dan identifikasi data dari berbagai aspek yang berkaitan dengan topik keamanan jaringan menggunakan *Virtual Private Network*. Pada tahapan ini mencakup analisis risiko keamanan, pemilihan solusi dan identifikasi kebutuhan keamanan data.

4. HASIL DAN PEMBAHASAN

Pada bagian ini terdapat pemaparan analisis studi literatur dari hasil penelitian-penelitian terdahulu.

4.1 Studi Kasus Implementasi VPN

Penelitian terkait *Virtual Private Network* (VPN) sebagai implementasi jaringan komputer ini telah banyak dilakukan oleh para peneliti sebelumnya, termasuk dalam penerapan sebagai solusi atas keamanan jaringan internet pada perusahan-perusahan. Pemilihan VPN sebagai alternatif atau solusi ini di dasari karena banyaknya terjadi pencurian, penyadapan dan peretasan pada beberapa data akibat kurangnya keamanan ketika dilakukannya pertukaran atau transmisi data. Oleh karena itu adanya teknologi jaringan seperti VPN yang menawarkan keamanan

data yang tinggi ini akhirnya menjadi salah satu pilihan yang baik.

4.2 Analisis QOS Dalam Jaringan VPN L2TP/IPSEC Pada Butik Bimba Y Lola

Pada sebuah penelitian yang dilakukan oleh Wadih & Desi Ramayanti (2023) yang menguji penerapan VPN L2TP/IPSEC pada Butik Bimba Y Lola menggunakan pengukuran QOS (*Quality of Service*) terhadap kualitas jaringan internet dengan mengukur *packet loss, delay, jitter dan throughput* yang mengacu pada standar TIPHON atau *Telecommunications and Internet Protocol Harmonization Over Network* [8]. Dan dari hasil pengujian yang telah dilakukan menunjukkan kualitas jaringan internet yang bagus pada butik Bimba Y Lola dengan nilai *packet loss* sebesar 0,5% yang berarti data hilang mendekati nol atau tidak ada, ini menandakan tingkat keamanan data yang sangat baik, kemudian *delay* sebesar 7,8 ms dengan nilai sangat bagus, selanjutnya *jitter* sebesar 0,1 ms dengan indeks 4 atau berarti bagus dan yang terakhir ada *throughput* dengan nilai 177/*kbits*/s yang termasuk dalam kategori sangat bagus. Berdasarkan hasil penelitian yang telah di dapat penulis menyimpulkan bahwa implementasi protokol VPN L2TP/IPSec memberikan proteksi terhadap keamanan jaringan tanpa mengurangi kualitas jaringan tersebut.

4.3 Implementasi Dan Perbandingan Keamanan Virtual Private Network (VPN) Menggunakan PPTP Dan L2TP

Dalam studi kasus lain yang juga telah melakukan pengujian perbandingan keamanan pada PPTP dan L2TP/IPsec VPN menggunakan QOS oleh Muhammad Alvin Gunawan dan Sukma Wardhana (2023) memperoleh hasil yang baik. Data yang dikirim melalui jaringan VPN dienkripsi, sehingga tidak dapat dibaca oleh pihak luar yang berusaha mengaksesnya, yang sudah di uji melalui teknik *sniffing* oleh penulis sebelumnya. Sementara itu, pada jaringan tanpa VPN, data yang dikirim cenderung lebih rentan terhadap akses pihak luar karena tidak terlindungi oleh enkripsi. Pengujian *Sniffing* pada Protokol VPN L2TP/IPsec didapatkan hasil yang baik bahwa Informasi yang terkandung dalam pesan *signaling* tidak dapat diketahui karena telah dienkapsulasi oleh *header* ESP. Hal ini menunjukkan tingkat keamanan jaringan tersebut tinggi karena menggunakan lapisan enkripsi ganda [9].

4.4 Analisis Quality Of Service Jaringan Virtual Private Network (VPN) di STMIK STIKOM Indonesia

Selanjutnya pada penelitian yang dilakukan oleh I Kadek Susila Satwika & I Made Sukafona (2020) mengenai "Analisis *Quality Of Service* Jaringan *Virtual Private Network* (VPN) di STMIK STIKOM Indonesia" juga memperoleh hasil yang baik, pengukuran menggunakan parameter QOS berupa *delay, jitter, throughput,* dan *packet loss* memperoleh nilai sangat bagus. Untuk pengujian menggunakan *file* video dengan tahapan pengujian pertama melalui cara *upload file* dan pengujian kedua melalui download *file*, didapatkan hasil QOS dengan indeks 3,75 yang jika dikonversikan pada standar TIPHON, jaringan VPN di STMIK STIKOM Indonesia mempunyai kualitas yang memuaskan [10].

4.5 Keamanan Jaringan Menggunakan VPN (Virtual Private Network) Dengan Metode PPTP Pada Kantor Desa Kertaharga Ciamis

Studi kasus selanjutnya yang dilakukan oleh Sari Dewi, Fajar Riyadi, Tika Suwastitaratu & Noer Hikmah (2020) mengenai "Keamanan Jaringan Menggunakan VPN *(Virtual Private Network)* Dengan Metode PPTP *(Point To Point Tunneling Protocol)* Pada Kantor Desa Kertaraharja Ciamis" memperoleh hasil yang positif, dengan menggunakan teknologi *Virtual Private Network* (VPN) dengan metode *tunneling protocol* PPTP *(Point-To-Point Tunneling Protocol)* yang diterapkan pada Desa Kertaraharja berdampak sangat positif karena dengan metode tersebut jaringan komputer antara kantor dapat saling berkomunikasi, dengan itu pekerjaan dan pertukaran informasi menjadi lebih fleksibel, cepat dan lebih aman. Serta administrator jaringan tidak perlu repot-repot melakukan kunjungan untuk me-*monitoring* jaringan yang sedang berjalan pada masing-masing kantor [11].

4.6 Penerapan Firewall Dan Protocol IPSec/L2TP Sebagai Solusi Keamanan Akses Jaringan Publik

Studi kasus selanjutnya yang dilakukan oleh Muhammad Ayub, Andry Maulana & Ahmad Fauzi (2021) mengenai "Penerapan *Firewall* Dan *Protocol* IPSec/L2TP Sebagai Solusi Keamanan Akses Jaringan Publik" memperoleh hasil yang positif. Tujuan penelitian ini tidak lain untuk mencegah terjadinya jenis serangan malware yang terdapat pada situs yang beredar di jaringan publik dengan menyaring penggunaan *firewall*. Pada perusahaan PT Neu Indonesia memiliki sebuah wilayah pusat dan Solo yang dapat menerapkan keamanan jaringan komputer dengan menggunakan jaringan *Wide Area Network*. Perusahaan PT Neu memanfaatkan fitur internet *firewall* yang sebelumnya hanya menggunakan keamanan bawaan dari *windows* sehingga mempermudah seseorang dalam merampas data internal maupun eksternal jaringan sehingga diterapkan *firewall* pada *router* yang berfungsi mengawasi adanya ancaman *malware* ataupun bahaya. Maka dari itu sebuah situs yang menerapkan *firewall* pada komputer memiliki keunggulan terutama untuk mendeteksi hadirnya *malware* dari kunjungan kita ke berbagai macam situs. Karena kebutuhan PT Neu dalam meningkatkan keamanan jaringan pada perusahaan, akhirnya diterapkan *firewall* yang peka terhadap kesalahan konfigurasi dan kegagalan.

Kemudian untuk melakukan pertukaran data dan infromasi kini dapat menggunakan sebuah metode protokol IPSec/L2TP yang aman. *Virtual Private Network (VPN)* ini diterapkan agar hubungan antara cabang pusat dengan solo mempunyai jaringan *private* yang aman dan ter-enskripsi dengan memanfaatkan internet [12].

4.7 Penerapan Sistem Keamanan Jaringan Menggunakan VPN Dengan Metode PPTP Pada PT Hinoka Sinergi Tanyo

Studi kasus selanjutnya yang dilakukan oleh Berliana Syela Fajrin, Priatno & Muhammad Ridwan Effendi (2024) mengenai "Penerapan Sistem Keamanan Jaringan Menggunakan VPN Dengan Metode PPTP Pada PT Hinoka Sinergi Tanyo" memperoleh hasil yang baik. Pada penerapan sistem keamanan jaringan dengan VPN PPTP ini dapat memberikan akses pada server secara *private*, serta menyediakan kemudahan untuk teknisi IT dalam mengelola dan memperbaiki permasalahan pada server perusahaan secara *remote* dengan aman. Hal yang dilakukan perusahaan adalah dengan memberikan pemahaman terkait kebijakan dalam keamanan VPN kepada user dan memberikan pelatihan terkait penggunaan yang aman untuk tidak memberikan kunci akses VPN kepada orang lain dan memastikan user dapat memahami pentingnya keamanan pada saat menggunakan VPN, Kemudian penggunaan VPN L2TP/IPSec untuk tingkat keamanan yang lebih baik dan mengoptimalkan *white list* IP *Address* untuk memblokir IP *Address* yang tidak dikenali oleh server [13].

4.8 Penerapan Teknologi Jaringan VPN IP Berbasis IPSec

Studi kasus lain yang dilakukan oleh Hari Suryanto, Adi Sopian dan Dartono mengenai "Penerapan Teknologi *Fortigate* Dalam Pembangunan Jaringan VPN-IP Berbasis IPSec" *FortiGate* merupakan sebuah pilihan terbaik dalam memeberikan perlindungan yang tinggi terhadap sebuah ancaman serta keamanan agar lebih dinamis dan menyederhanakan terhadap infrastruktur IT organisasi. Berdasarkan penelitian yang telah dilakukan di dapatkan hasil berupa sebuah jalur lintas komunikasi, dimana terjadi proses pertukaran data yang aman serta terpercaya (*secure and reliable*) antara kampus pusat ITB Swadharma Jakarta dengan kampus cabang. Adanya jalur VPN IPSec, di kampus ITB Swadharma Jakarta berguna menghemat biaya pengeluaran serta dapat mengubungkan secara *real time* antara kampus cabang dengan kampus pusat. Dari pengujian konektivitas jaringan VPN IPSec di dapatkan hasil yang menunjukan persentase *packet loss* sebesar 0%, *round trip time* dengan besar 10000 *bytes*, 5000 *bytes*, dan 10000 *bytes* melalui tes selama 100 kali. kemudian *Round trip* minimum 1000 *bytes*, ialah 1.18 *milisecond* dan ukuran maksimumnya sebesar 11.95 *bytes*, *round trip times* minimum 5000 *bytes* yaitu 1.90 *milisecond* dengan maksimum 21.84 *milisecond*, *round trip time* minimum 10000 *bytes* yaitu 2.72 *milisecond* dengan ukuran maksimal 22.20 *milisecond*, semakin besar ukuran paket menjadikan *round trip time* sampai ke tujuan semakin lama. Dilakukan juga pengetesan melalui transfer *file* dari kampus pusat ke kampus cabang menggunakan besar *size* paket 10,1 MB, 20,2 MB, dan 24,9 MB. Untuk transfer *file* berukuran 10,1 MB diperlukan waktu sekitar 20 detik [14].

5. KESIMPULAN DAN SARAN

Berdasarkan hasil penelitian dari analisis literatur yang telah penulis lakukan bahwa penggunaan *Virtual Private Network* (VPN) untuk keamanan data jaringan publik merupakan solusi yang sangat baik untuk meningkatkan keamanan data pada jaringan publik, terutama dalam menghadapi ancaman serangan seperti sniffing, peretasan, dan serangan man-in-the-middle. Dilihat dari studi-studi kasus penelitian serupa yang telah melakukan pengujian terhadap VPN, terutama dengan protokol L2TP/IPSec, mampu memberikan tingkat perlindungan data yang tinggi melalui enkripsi dan tunneling tanpa mengurangi kualitas jaringan secra signifikan, seperti yang dibuktikan oleh pengujian QOS dengan parameter seperti packet loss, delay, jitter, dan troughput yang memenuhi standar TIPHON. VPN juga terbukti meningkatkan efisiensi operasional, yang memungkinkan akses jarak jauh yang aman, serta mendukung konektivitas antar lokasi dengan biaya yang lebih rendah. Terdapat saran yang bisa dilakukan untuk penelitian selanjutnya yaitu melakukan pengujian langsung menggunakan objek penelitian sehingga ke akuratan implementasi VPN dapat terlihat secara nyata dengan hasil data pengujian yang telah dilakukan penulis.

DAFTAR PUSTAKA

[1] A. Novenzo Ihsana and A. Maslan, "ANALISIS KEAMANAN JARINGAN DARI SERANGAN PAKET DATA SNIFFING DI PT RADEN SYAID KANTOR POS PIAYU KOTA BATAM," 2020.

[2] D. Firmansyah, "PENERAPAN TEKNOLOGI BLOCKCHAIN UNTUK MENGATASI SERANGAN MAN IN THE MIDDLE," 2023.

[3] H. Afifi Al-Atsari and I. Suharjo, "Integrasi Server On-Premise dengan Server Cloud Menggunakan Cloud VPN dan Mikrotik Ipsec Untuk Peningkatan Keamanan Koneksi," *Jurnal Syntax Admiration*, vol. 4, no. 11, pp. 1977–1996, Nov. 2023, doi: 10.46799/jsa.v4i11.757.

[4] M. Ocka Dharma Putra, A. Rahman, A. Azhari, and D. Redaksi, "4,5 PT. Semen Baturaja (Persero) TBK. Indonesia 1,2,3 Jl. Ki Ratu Penghulu Karang Sari No. 02301 Baturaja," *JURNAL INTECH*, vol. 3, no. 1, pp. 17–21.

[5] Prayogi Wicaksana, F. Hadi, and Aulia Fitrul Hadi, "Perancangan Implementasi VPN Server

Menggunakan Protokol L2TP dan IPSec Sebagai Keamanan Jaringan," *Jurnal KomtekInfo*, pp. 169–175, Aug. 2021, doi: 10.35134/komtekinfo.v8i3.128.

[6] T. Ariyadi, M. Agung Prabowo, D. Palembang, J. Ahmad Yani No, and P. Palembang Sumatera Selatan, "Perbandingan Kinerja Virtual Private Network Antara Vpn Tunnel Dan Internet Protocols Security," vol. 6, no. 1, p. 2021.

[7] N. Bayu and A. Susila, "Penerapan Teknologi Fortigate Dalam Pembangunan Jaringan VPN Berbasis SSL-VPN (Studi Kasus: Kementerian PANRB)," *Jurnal Ilmu Komputer dan Pendidikan*, vol. 2, no. 1, 2023, [Online]. Available: https://journal.mediapublikasi.id/index.php/logic

[8] B. Bimba, L. Wadih, and D. Ramayanti, "Analisis QOS Dalam Jaringan VPN L2TP/IPSEC Pada," 2023. [Online]. Available: http://jurnal.mdp.ac.idjatisi@mdp.ac.id;

[9] M. A. Gunawan and S. Wardhana, "Implementasi dan Perbandingan Keamanan PPTP dan L2TP/IPsec VPN (Virtual Private Network)," vol. 6, no. 1.

[10] I. Kadek, S. Satwika, and M. Sukafona, "Analisis Quality Of Service Jaringan Virtual Private Network (VPN) di STMIK STIKOM Indonesia."

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

[12] M. Ayub, A. Maulana, and A. Fauzi, "Penerapan Firewall Dan Protokol IpSec/L2TP Sebagai Solusi Keamanan Akses Jaringan Publik." [Online]. Available: http://jurnal.bsi.ac.id/index.php/co-science

[13] B. Syela Fajrin and M. Ridwan Effendi, "PENERAPAN SISTEM KEAMANAN JARINGAN MENGGUNAKAN VPN DENGAN METODE PPTP PADA PT HINOKA SINERGI TANYO."

[14] "558233-penerapan-teknologi-fortigate-dalam-pemb-c9672952".