

Implementasi VPN dengan Metode IPSEC Site-To-Site Menggunakan Perangkat Fortigate dan Mikrotik pada PT. Adi Mitra Solusi

Dewita Dyan S¹, Herman Kuswanto²

^{1,2}Program Studi Informatika, Universitas Nusa Mandiri
dewitadyansulistiyani@gmail.com¹, herman.hko@nusamandiri.ac.id²

Abstract

The development of information technology provides great benefits for companies, especially in the security and efficiency of data exchange. PT. Adi Mitra Solusi, which is engaged in the service sector. The company is facing constraints on network usage on the SAP system used as the company's core ERP, the application cannot be accessed from branch offices, data delivery can only be done via email, which causes high data traffic loads, latency, and security risks. This study aims to implement a Virtual Private Network (VPN) network with the IPsec Site-to-Site method using Fortigate and Mikrotik devices as a connecting medium for the head office and branch networks, so that the SAP system can be accessed safely and efficiently from all branches. The research method is a descriptive case study, with stages starting from needs analysis, design design, testing and implementation. The results of the study showed that VPN IPsec Site-to-Site successfully connected the SAP system, the SAP system can be connected directly from the branch office to the head office. In conclusion, the use of Fortigate and Mikrotik devices in the implementation of VPN IPsec Site-to-Site effectively improves the performance and security of the company's network, where this implementation is a strategic step to modernize the network infrastructure of PT. Adi Mitra Solusi, supports operational integration, and improves overall business efficiency.

Keywords: VPN, IPsec Site-to-Site, Fortigate, Mikrotik, Network Security

Abstrak

Perkembangan teknologi informasi memberikan keuntungan besar bagi perusahaan, terutama dalam keamanan dan efisiensi pertukaran data. PT. Adi Mitra Solusi, yang bergerak di bidang jasa. Perusahaan sedang menghadapi kendala penggunaan jaringan pada sistem SAP yang digunakan sebagai core ERP perusahaan, aplikasi tersebut tidak bisa di akses dari kantor cabang, pengiriman data hanya dapat dilakukan melalui email, yang menyebabkan beban lalu lintas data tinggi, latensi, dan risiko keamanan. Penelitian ini bertujuan mengimplementasikan jaringan Virtual Private Network (VPN) dengan metode IPsec Site-to-Site dengan menggunakan perangkat Fortigate dan Mikrotik sebagai media penghubung jaringan kantor pusat dan cabang, sehingga sistem SAP dapat diakses dengan aman dan efisien dari semua cabang. Metode penelitian berupa studi kasus deskriptif, dengan tahapan mulai dari analisa kebutuhan, perancangan desain, pengujian dan implementasi. Hasil penelitian menunjukkan bahwa VPN IPsec Site-to-Site berhasil menghubungkan sistem SAP, sistem SAP dapat terkoneksi secara langsung dari kantor cabang ke kantor pusat. Kesimpulannya, penggunaan perangkat Fortigate dan Mikrotik dalam implementasi VPN IPsec Site-to-Site efektif meningkatkan kinerja dan keamanan jaringan perusahaan, dimana implementasi ini merupakan langkah strategis untuk modernisasi infrastruktur jaringan PT. Adi Mitra Solusi, mendukung integrasi operasional, dan meningkatkan efisiensi bisnis secara keseluruhan.

Kata kunci: VPN, IPsec Site-to-Site, Fortigate, Mikrotik, Keamanan Jaringan

I. PENDAHULUAN

Perkembangan teknologi, terutama dalam bidang informasi, memberikan keuntungan besar bagi perusahaan yang mengadopsinya. Dengan teknologi yang mutakhir, perusahaan dengan banyak cabang dapat dengan aman, dan lancar bertukar data dan informasi. Ini membuka peluang untuk meningkatkan kinerja dan performa perusahaan secara keseluruhan, mendukung proses bisnis yang berjalan[5]. Bahkan dengan jarak yang jauh, termasuk antar pulau dan antar provinsi di seluruh Indonesia, perusahaan dapat tetap terhubung dan berkolaborasi tanpa hambatan. Hal ini membantu dalam

memperkuat integrasi operasional, mempercepat pengambilan keputusan, dan meningkatkan efisiensi secara keseluruhan[1]. Dengan demikian, teknologi informasi tidak hanya menjadi alat tambahan, tetapi menjadi fondasi penting dalam strategi bisnis modern yang berorientasi pada kinerja dan inovasi[3].

PT. Adi Mitra Solusi, adalah perusahaan yang bergerak pada penyediaan solusi pengadaan barang atau jasa dimana perusahaan ini memiliki beberapa cabang yang tersebar diseluruh wilayah Indonesia. Infrastruktur jaringan saat ini pada PT. Adi Mitra Solusi yaitu ketika melakukan pengiriman data-data perusahaan harus menggunakan email yang dikirim ke kantor pusat untuk

diinput kedalam sistem SAP (Systems Applications and Products in Data Processing)[2] dimana sistem SAP digunakan oleh perusahaan untuk pengelolaan berbagai aspek operasional mencakup manajemen keuangan, pengelolaan rantai pasokan, serta pengelolaan sumber daya manusia[9]. Untuk saat ini sistem SAP sendiri hanya dapat diakses dikantor pusat, dikarenakan banyaknya data-data dan informasi penting perusahaan yang tidak boleh diakses oleh orang yang tidak berkepentingan pada perusahaan tersebut.

Namun, kendala muncul ketika manajemen jaringan menjadi lebih rumit, pengaturan manual yang kompleks tanpa jaminan keamanan dan performa yang memadai, menghambat operasional dan efisiensi bisnis[6]. Hal ini terjadi karena pertumbuhan perusahaan yang pesat, menyebabkan beban lalu lintas data yang semakin tinggi dan menghasilkan latensi yang mengganggu kinerja sistem SAP. Dan permasalahan muncul meliputi, Sistem SAP sebagai core ERP perusahaan tidak bisa di akses dari site di Kalimantan, untuk bisa di akses dari site diperlukan koneksi jaringan yang dapat menghubungkan antara kantor pusat dan kantor cabang.

Untuk itu diperlukan koneksi VPN-IPsec yang dapat menghubungkan antar jaringan site-to-site, agar sistem SAP dapat diakses pada kantor pusat dan seluruh kantor cabang[14] PT. AMS. Dimana dengan menghubungkan VPN metode IPsec site-to-site dianggap sebagai langkah strategis yang diperlukan untuk meningkatkan efisiensi operasional yang merupakan tulang punggung proses bisnis[10]. Penggunaan VPN-IPsec sebagai tambahan lapisan keamanan menjadi penting[8]. Dengan VPN-IPsec, PT. Adi Mitra Solusi dapat mengenkripsi data yang dikirim, sehingga mengurangi risiko pencurian atau penyusupan data oleh pihak yang tidak sah[15]. Penggunaan infrastruktur jaringan VPN IPsec site-to-site pada perusahaan memungkinkan konektivitas yang aman dan andal antara berbagai kantor cabang yang tersebar secara geografis[11]. Perusahaan dapat menggunakan perangkat yang sudah berjalan pada kantor pusat dan kantor cabang seperti Fortigate dan Mikrotik untuk menerapkan VPN IPsec site to site dengan kewanaman yang lebih terjaga, dengan VPN-IPsec membantu mengurangi latensi dan gangguan konektivitas dengan menyediakan jalur komunikasi yang stabil dan teroptimasi[7].

Dengan implementasi yang dilakukan koneksi antar kantor pusat dan kantor cabang dapat terkoneksi secara realtime sehingga Sistem SAP sebagai core ERP perusahaan dapat diakses secara langsung dari kantor cabang, dengan kewanaman yang tetap terjaga, dari hasil tersebut diharapkan akan meningkatkan infrastuktur jaringan secara keseluruhan.

II. METODE PENELITIAN

2.1 Metode Pengumpulan Data

Dalam rangka memperoleh data yang dibutuhkan, penulis menerapkan pendekatan penelitian dengan observasi, wawancara dan setudi Pustaka[12], dengan tahapan sebagai berikut:

a. Observasi

Penulis melakukan pengamatan langsung serta meninjau proses kerja, terutama fokus pada jaringan LAN dan WAN di PT. Adi Mitra Solusi.

b. Wawancara

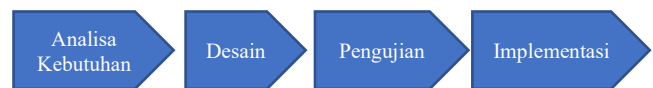
Penulis menghimpun data dan informasi melalui wawancara langsung kepala IT maupun dengan staf yang menggunakan jaringan komputer. Pendekatan ini dilakukan melalui dialog tanya jawab yang langsung dan teratur.

c.Studi Pustaka

Dalam rangka memperdalam isu-isu yang relevan dengan skripsi ini, penulis melakukan studi kepustakaan. Pendekatan ini melibatkan pengumpulan data teoritis dari berbagai sumber seperti buku, jurnal, penelusuran internet, dan literatur terkait. Tujuan dari studi ini adalah untuk memperoleh teori dan materi yang relevan dengan topik penelitian sebagai referensi tertulis.

2.2 Analisis Penelitian

Dalam penelitian ini, penulis melakukan analisis yang mencakup beberapa aspek, mulai dari analisa kebutuhan, desain, pengujian, dan implementasi[13], seperti dilihat pada gambar 1.



Gambar 1: Analisis Penelitian

a. Analisa Kebutuhan

Pada tahap ini, penulis melakukan identifikasi dan pemahaman kebutuhan bisnis dan teknis yang spesifik untuk menghubungkan jaringan kantor pusat dan kantor cabang melalui VPN-IPsec dengan menggunakan perangkat Fortigate dan Mikrotik.

b. Desain

Tahap ini dilakukan pengembangan arsitektur topologi jaringan yang sudah berjalan dengan penambahan konfigurasi VPN-IPsec pada perangkat FortiGate dan MikroTik untuk dapat diimplemetasikan Jaringan VPN pada PT. Adi Mitra Solusi.

c. Pengujian

Melakukan pengujian untuk memastikan bahwa jaringan VPN-IPsec berfungsi sesuai dengan spesifikasi dan kebutuhan.

d. Implementasi

Menerapkan konfigurasi jaringan yang telah dirancang untuk menghubungkan VPN-Ipsec Site-to-site pada kantor cabang.

III. HASIL PENELITIAN

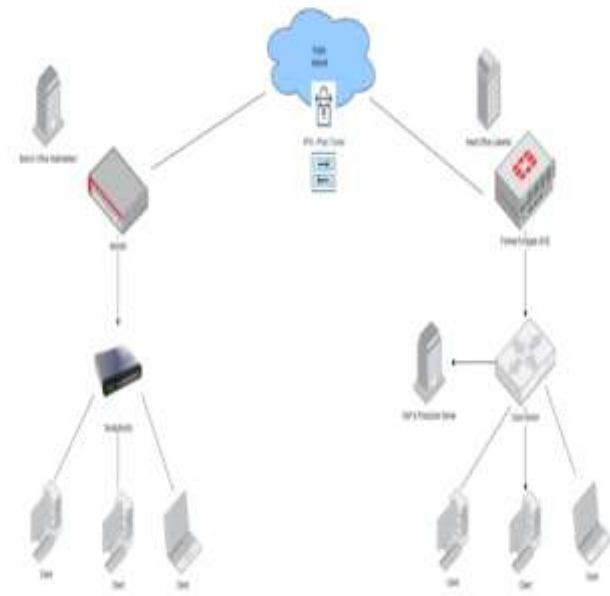
3.1 Hasil Analisis

Dari hasil penelitian dan riset yang penulis telah lakukan pada PT.AMS, terdapat permasalahan sebagai berikut :

1. Kendala sistem SAP sebagai core ERP perusahaan tidak bisa di akses dari site Kalimantan ke kantor Pusat.
2. Belum ada penerapan sistem keamanan untuk sharing (pertukaran) data antara kantor pusat dan kantor cabang.
3. Tidak adanya koneksi jaringan yang menghubungkan antara kantor pusat dan kantor cabang secara langsung.

3.2 Topologi Jaringan

Dengan menggunakan topologi yang sudah ada, akan ditambahkan konfigurasi untuk menghubungkan antara kantor cabang dan kantor pusat dengan menerapkan konfigurasi VPN-Ipsec Site to site, seperti pada gambar 2.



Gambar 2 : Rancangan Topologi VPN-Ipsec Site to site

3.3 Keamanan Jaringan

Keamanan jaringan pada PT. Adi Mitra Solusi menggunakan firewall yang terdapat pada FortiGate dan firewall pada Mikrotik. Firewall digunakan sebagai keamanan dari sisi internal dan external jaringan yang ada. Sedangkan untuk keamanan di sisi jaringan VPN digunakan security Ipsec.

3.3 Konfigurasi Usulan

Pada jaringan usulan ini, penulis merancang dan mengimplementasikan VPN-IPsec site-to-site untuk menghubungkan sistem SAP agar dapat terkoneksi antara kantor pusat Jakarta dan cabang yang berada di Kalimantan.

1. Konfigurasi Fortiget Kantor Pusat

a. Konfigurasi Phase 1 Ipsec

```
config vpn ipsec phase1-interface
edit "Jakarta-Kalimantan-VPN"
set interface "wan1"
set remote-gw 203.0.113.2 # IP publik
Mikrotik di Kalimantan
set psksecret "password123"
set proposal aes256-sha256
set ike-version 2
set dhgrp 14
end
```

b. Konfigurasi Phase 2 Ipsec

```
config vpn ipsec phase2-interface
edit "Jakarta-Kalimantan-VPN"
set phase1name "Jakarta-Kalimantan-VPN"
set proposal aes256-sha256
set dhgrp 14
set auto-negotiate enable
set src-subnet 192.168.21.0 255.255.255.0 # LAN Jakarta
set dst-subnet 10.10.10.0 255.255.255.0 # LAN Kalimantan
end
```

c. Konfigurasi Firewall

```
config firewall policy
edit 1
set srcintf "lan"
set dstintf "Jakarta-Kalimantan-VPN"
set srcaddr "Local_Network"
set dstaddr "Remote_Network"
set action accept
set schedule always
set service ALL
set logtraffic all
end
```

d. Konfigurasi Routing

```
config router static
edit 1
set dst 192.168.21.0/24
set gateway "Jakarta-Kalimantan-VPN"
end
```

2. Konfigurasi Mikrotik Kantor Cabang

a. Konfigurasi Phase 1

```
/ip ipsec profile add name=fortigate_profile hash-
algorithm=sha256 enc-algorithm=aes-256 dh-
group=modp2048
/ip ipsec peer add name=fortigate_peer
address=203.0.113.1 exchange-mode=ike2
profile=fortigate_profile send-initial-
contact=yes
```

b. Konfigurasi Pre-Shared Key

```
/ip ipsec identity add peer=fortigate_peer auth-
method=pre-shared-key secret="password123"
```

c. Konfigurasi Phase 2

```
/ip ipsec proposal add name=fortigate_proposal
auth-algorithms=sha256 enc-algorithms=aes-256-cbc
pfs-group=modp2048
/ip ipsec policy add src-address=192.168.21.0/24
dst-address=10.10.10.0/24 peer=fortigate_peer
tunnel=yes proposal=fortigate_proposal
```

d. Konfigurasi Routing

```
/ip route add dst-address=10.10.10.0/24
gateway=fortigate_peer
```

IV. PEMBAHASAN

Dari konfigurasi yang telah dilakukan sebelumnya, untuk memastikan konfigurasi berjalan sesuai dengan fungsinya maka dilakukan pengujian jaringan[4] pada VPN-IPSec site-to-site, pengujian dilakukan untuk memastikan konektivitas dan keamanan yang optimal,

dan memastikan bahwa semua sistem yang telah dibuat berfungsi dengan baik dan sesuai dengan rencana. Beberapa tahap pengujian akan dilakukan, termasuk pengujian awal tanpa VPN-IPsec dan pengujian akhir yang telah diimplementasikan VPN-IPsec.

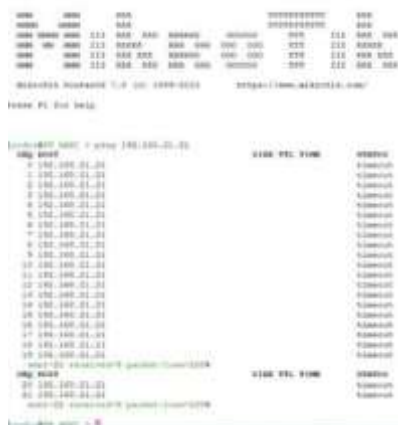
Konfigurasi VPN-IPSec site-to-site yang dilakukan bertujuan untuk memastikan bahwa semua sistem yang telah dikonfigurasi dapat berfungsi secara optimal dan sesuai dengan rencana. Pengujian jaringan merupakan langkah kritis dalam memastikan bahwa sistem yang dibangun dapat mengatasi segala kendala yang mungkin terjadi dalam jaringan dan memberikan hasil yang diharapkan, baik dari segi kinerja maupun keamanannya. Pengujian ini memiliki dua aspek utama yaitu konektivitas dan kemanan, dimana konektivitas untuk membuktikan apakah jaringan yang saling terhubung melalui VPN dapat saling berkomunikasi tanpa gangguan, dan kemanan untuk membuktikan bahwa koneksi antar cabang bisa terbentuk jika menggunakan pre share key yang sama.

Untuk pengujian dilakukan dengan dua tahapan, yaitu tahap pengujian awal tanpa VPN-Ipsec dan tahap pengujian akhir dengan VPN_Ipsec.

1. Pengujian Awal

Pengujian ini bertujuan untuk melihat kondisi dasar jaringan sebelum menerapkan VPN-IPSec. Tujuannya adalah untuk mengidentifikasi masalah yang mungkin ada dalam konektivitas dasar jaringan tanpa adanya enkripsi atau protokol keamanan tambahan. Pengujian ini memungkinkan untuk memperoleh baseline atau tolok ukur kinerja jaringan.

- Pengetesan dengan cara cek koneksi dari router Mikrotik cabang ke Ip address local pada kantor pusat, pada gambar 3, menunjukan bahwa dengan melakukan test ping hasilnya masih request time out atau pc yang dituju tidak dapat diakses, ditunjukan dengan adanya paket loss.



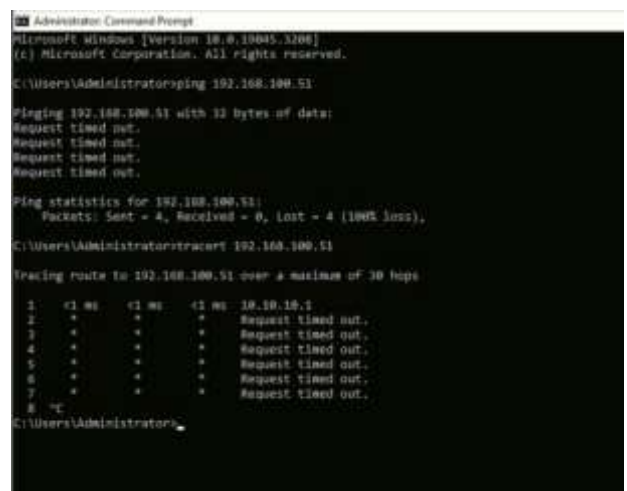
Gambar 3: Ping Mikrotik kantor cabang ke IP pc kantor pusat

- Pada gambar 4, dilakukan ujicoba koneksi dari router Fortiget ke ip address pda pc kantor cabang, untuk hasil ping masih tetap sama request time out atau pc tujuan tidak dapat dijangkau.



Gambar 4: Ping dari Fortigate kantor pusat ke ip PC kantor cabang

- Pada gambar 5, dilakukan tes koneksi langsung dari pc local cabang ke pc server SAP yang berada pada kantor pusat, untuk hasil ping terdapat paket loss dimana pc tujuan tidak ditemukan.



Gambar 5: Ping PC cabang ke server SAP

2. Pengujian Akhir

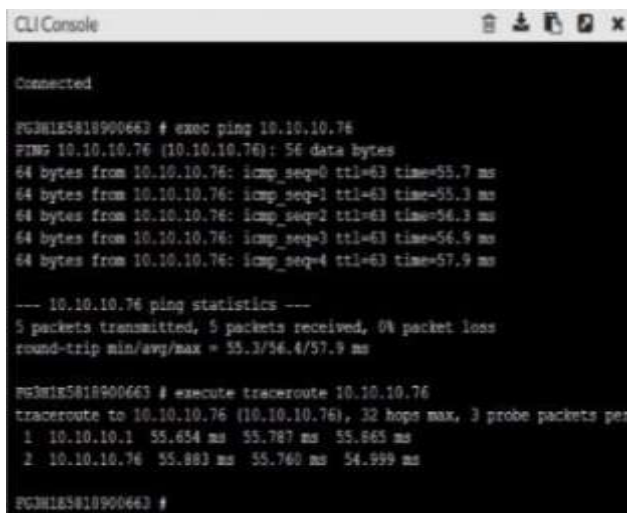
Setelah VPN-IPSec diterapkan, tahap kedua pengujian dilakukan untuk memastikan bahwa konektivitas dan keamanan terjamin setelah implementasi protokol enkripsi. Pengujian ini bertujuan untuk mengonfirmasi bahwa implementasi VPN tidak hanya meningkatkan keamanan tetapi juga tidak memengaruhi kinerja jaringan secara signifikan. Pada tahap ini, pengujian bertujuan memastikan bahwa dua titik jaringan yang terhubung melalui VPN-IPSec dapat saling berkomunikasi dengan lancar tanpa adanya gangguan.

- Pada gambar 6, menunjukan untuk pengujian koneksi dari kantor cabang ke ip address kantor pusat berjalan lancar, tidak terjadi paket loss atau pc kantor pusat bisa dijangkau dari kantor cabang



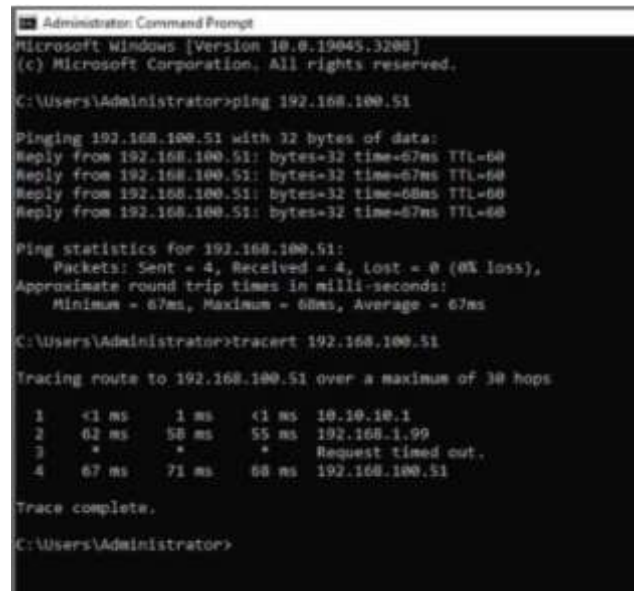
Gambar 6: Ping PC kantor cabang ke ip PC kantor pusat

b. Pada gambar 7, dilakukan uji koneksi dari router Fortiget ke router Mikrotik, hasilnya dari router Fortiget bisa menjangkau atau terkoneksi ke router Mikrotik yang ada di kantor cabang.



Gambar 7: Ping dari Fortigate kantor pusat ke mikrotik kantor cabang

c. Pada gambar 8, dilakukan uji koneksi dari pc yang berada pada kantor cabang ke Server SAP yang berada pada kantor pusat, dan hasilnya pc pada kantor cabang bisa menjangkau atau mengakses dengan lancar ke Server SAP.



Gambar 8: Ping PC kantor cabang ke Server SAP

V. KESIMPULAN

Beberapa kesimpulan dari hasil yang didapat penulis selama melakukan analisis dan implementasi jaringan pada PT Adi Mitra Solusi, adalah sebagai berikut:

1. Dengan Implementasi sistem jaringan VPN IPsec berhasil mengatasi masalah akses sistem SAP dari site Kalimantan ke kantor pusat. Dengan jaringan VPN IPsec, karyawan di Kalimantan dapat mengakses sistem SAP secara efisien dan tanpa hambatan, meningkatkan produktivitas dan operasional bisnis yang lancar.
2. Sebelum implementasi dilakukan, tidak ada sistem keamanan yang memadai untuk pertukaran data antara kantor pusat dan kantor cabang. Dengan penerapan VPN IPsec, keamanan pertukaran data telah ditingkatkan secara signifikan, melindungi informasi sensitif dari akses tidak sah.
3. Ketiadaan koneksi jaringan yang menghubungkan kantor pusat dan cabang sebelumnya menghambat komunikasi dan kolaborasi. Implementasi VPN IPsec telah menyediakan konektivitas yang andal dan stabil antara kantor pusat dan kantor cabang di Kalimantan, memungkinkan akses data yang cepat dan komunikasi yang lebih baik antar karyawan.
4. Penghematan biaya jaringan, Implementasi VPN-IPSec site-to-site dapat mengurangi biaya yang terkait dengan penyewaan jalur khusus (leased line) atau solusi jaringan lainnya yang lebih mahal. Dengan implementasi VPN-IPSec sehingga perusahaan dapat menghemat biaya tanpa mengorbankan keamanan dan kinerja jaringan.

VI. REFERENSI

- [1] Marisa Dika Andini, Muhamad Amirulloh, and Helitha Novianty Muchtar. 2020. PENGGUNAAN APLIKASI VIRTUAL PRIVATE NETWORK (VPN) POINT TO POINT TUNNELING PROTOCOL (PPTP) DALAM MENGAKSES SITUS TERBLOKIR. *Jurnal Penelitian Hukum* 29, 2 (August 2020), 148–166. Retrieved from <https://ditsti.itb.ac.id/layanan-vpn/>
- [2] Dessyana and Yola Yolanda. 2022. PENGARUH KUALITAS SISTEM DAN KUALITAS INFORMASI TERHADAP KEPUASAN PENGGUNA ENTERPRISE RESOURCE PLANNING-SYSTEM APPLICATION AND PRODUCT IN DATA PROCESSING (ERP-SAP) PADA PT. INALUM (PERSERO) SUMATERA UTARA. *Jurnal Ilmiah Mahasiswa Akuntansi Universitas Pendidikan Ganesha* 13, 1 (2022), 259–270.
- [3] Sari Dewi and Sulistiyah. 2022. Analisa Virtual Private Network (VPN) IP Multi Protocol Label Switching (MPLS) Untuk Jaringan Wide Area Network (WAN). *Journal of Information System, Applied, Management, Accounting and Research* 6, 1 (February 2022), 16–25. <https://doi.org/10.52362/jisamar.v6i1.662>
- [4] Ahmad Dandi Febrian and Redi Darmawan. 2022. Implementasi Jaringan Komputer Berbasis Virtual LAN untuk Layanan Iconnet VIP Pada Jaringan MPLS (Multi Protocol Label Switching): Studi Kasus di PT Indonesia Comnets Plus. *Scientia Sacra: Jurnal Sains, Teknologi dan Masyarakat* 2, 3 (September 2022), 466–480. Retrieved from <http://pijarpemikiran.com/index.php/Scientia>
- [5] Ahmad Firdausi and Hamam Wira Wardani. 2020. Simulasi dan Analisa QoS dalam Jaringan VPN Site To Site Berbasis IPsec dengan Routing Dynamic. *InComTech Jurnal Telekomunikasi dan Komputer* 10, 2 (August 2020), 49–56. <https://doi.org/10.22441/incomtech.v10i2.8131>
- [6] Harry Pribadi Fitriani, Nanda Alia Destiara, Neng Elsa Destianti, and Gilan Maddanil Khawat. 2025. ANALISIS PENERAPAN TEKNOLOGI VIRTUAL PRIVATE NETWORK (VPN) SEBAGAI SOLUSI KEAMANAN DATA DI JARINGAN PUBLIK. *JATI Jurnal Mahasiswa Teknik Informatika* 9, 1 (February 2025), 1559–1563.
- [7] Muhammad Gages Alvisyahri and Sidik. 2023. Perancangan dan Implementasi VPN Metode IPSEC Site to Site Menggunakan Fortigate Pada PT Linksindo Makmur. *Jurnal Jaringan Komputer dan Keamanan JJKK* 04, 03 (October 2023), 1–10.
- [8] Syarif Hidayatulloh. 2014. ANALISIS DAN OPTIMALISASI KEAMANAN JARINGAN MENGGUNAKAN PROTOKOL IPSEC. *Jurnal Informatika* I, 2 (September 2014), 93–104.
- [9] MUHAMMAD FAHREZA ISMAIL. 2021. SISTEM INFORMASI AKUNTANSI BERBASIS ERP-SAP DALAM MENINGKATKAN KUALITAS PENYAJIAN LAPORAN KEUANGAN (Studi pada PT PLN Persero UIKL SULAWESI). UNIVERSITAS ISLAM NEGERI ALAUDDIN MAKASSAR, Makasar.
- [10] Mark Lewis. 2006. *Comparing, Designing, and Deploying VPNs*. Cisco Press, Indianapolis, USA.
- [11] Ayu Purnama Sari, Sulistiyono, and Naga Kemala. 2020. PERANCANGAN JARINGAN VIRTUAL PRIVATE NETWORK BERBASIS IP SECURITY MENGGUNAKAN ROUTER MIKROTIK. *Journal PROSISKO* 7, 2 (September 2020), 150–164.
- [12] Niken Rahmasari, Fanny Adytia, and Herman Kuswanto. 2024. PEMANFAATAN SISTEM INFORMASI APOTEK BERBASIS WEB PADA POLIKLINIK PRATAMA BADAN KEPEGAWAIAN NEGARA. *JIKA* 8, 2 (April 2024), 163–170.
- [13] Andi Riyanto and Herman Kuswanto. 2024. Penerapan Teknologi Multi-Protocol Label Switching (MPLS) Dalam Optimasi Jaringan Backbone PT. Fiber Networks Indonesia. *Media Jurnal Informatika* 16, 2 (December 2024), 172. <https://doi.org/10.35194/mji.v16i2.3996>
- [14] Try Budi Septiandoko, Desmulyati, and Andi Taufik. 2021. Implementasi Jaringan Internet Site To Site VPN Dengan Metode IPsec Pada PT Telkom Akses. *Computer Science (CO-SCIENCE)* 1, 1 (January 2021), 18–26. Retrieved from <http://jurnal.bsi.ac.id/index.php/co-science>
- [15] Hari Suryantoro, Adi Sopian, and Dartono. 2021. PENERAPAN TEKNOLOGI FORTIGATE DALAM PEMBANGUNAN JARINGAN VPN-IP BERBASIS IPSEC. *Jurnal Elektro dan Informatika Swadharma (JEIS)* 1, 1 (December 2021), 1–7.

