LOGIC : Jurnal Ilmu Komputer dan Pendidikan
Volume 2, No. 1, Tahun 2023
ISSN 2985-4172 (media online)
Hal 153-159

Penerapan Teknologi Fortigate Dalam Pembangunan Jaringan VPN Berbasis SSL-VPN (Studi Kasus: Kementerian PANRB)

Nur Bayu[1], Atang Susila[2*]

[1,2]Fakultas Ilmu Komputer, Teknik Informtaika,Universitas Pamulang, Kota Tangerang Selatan, Indonesia
Email: [1]nurbayu15@gmail.com, [2*]atang.g66@gmail.com

Abstrak − Kebutuhan akses jarak jauh dalam komuniasi data pada jaringan publik ke sumber daya jaringan menjadi hal yang penting dalam kegiatan operasional. Dengan meningkatnya kebutuhan untuk menyediakan akses jarak jauh ke sumber daya jaringan kantor maka VPN dikembangkan. *Virtual Private Network* (VPN) adalah sebuah teknologi komunikasi yang memungkinkan untuk dapat terkoneksi ke jaringan publik dan menggunakannya untuk bergabung dengan jaringan lokal. Perangkat *FortiGate* sebagai *firewall* dan *gateway* yang saling terhubung dan membentuk tunnel sebagai jalur khusus yang menghubungkan jaringan private lokal yang ada di KEMENPANRB walaupun dalam mengaksesnya menggunakan jaringan yang bersifat publik. Dari hasil penelitian didapatkan hasil, waktu yang lebih cepat dengan menggunakan teknologi VPN. Dengan menghilangkan selisih waktu tersebut user dapat lebih cepat untuk mendapatkan dokumen yang dibutuhkan dan dapat dengan segera melakukan pekerjaan yang lainnya. Dengan demikian, waktu kerja pegawai menjadi lebih efisien dan produktivitas pekerjaan menjadi meningkat serta dapat menunjang kinerja.

Kata Kunci: VPN; Fortigate; SSL VPN; Efisiensi

Abstract *− The need for remote access in communicating data on public networks to network resources is important in operational activities. With the increasing need to provide remote access to office network resources, VPNs were developed. Virtual Private Network(VPN) is a communication technology that allows you to connect to a public network and use it to join a local network. FortiGate devices as firewalls and gateways are connected to each other and form tunnels as special lines that connect local private networks in KEMENPANRB even though accessing them uses a public network. From the research results, the results show that the time is faster by using VPN technology. By eliminating the time difference, the user can get the documents needed faster and can immediately do other work. Thus, employee work time becomes more efficient and work productivity increases and can support performance. Thus, employee work time becomes more efficient and work productivity increases and can support performance.*

Keywords*: VPN; Fortigate; SSL VPN; Efficiency*

1. PENDAHULUAN

Banyak manfaat dan pengaruh besar yang dapat kita implementasikan dengan berkembangnya teknologi bagi segala aspek kehidupan. Teknologi saat ini telah memberikan kemudahan dalam penyampaian suatu informasi. Berkembang pesatnya teknologi saat ini membuat infrastruktur yang dimiliki harus sesuai dengan kebutuhan, termasuk infrastruktur jaringan. Kementerian PANRB membutuhkan sebuah solusi untuk mempermudah dalam hal memperoleh kecepatan waktu kemudahan berkomunikasi tanpa memikirkan lokasi kerja yang jauh.

Kebutuhan akses jarak jauh yang aman dalam komuniasi data pada jaringan umum (*public network / internet*) ke sumber daya jaringan menjadi hal yang penting dalam kegiatan operasional sehari-hari. Pegawai yang bekerja di luar kota kantor memerlukan akses ke sumber daya jaringan dengan tepat waktu dan komprehensif. Dengan meningkatnya kebutuhan untuk menyediakan akses jarak jauh ke sumber daya jaringan kantor maka konsep *Virtual Private Network* (VPN) dikembangkan.

Sistem *Virtual Private Network* (VPN) merupakan sebuah jaringan publik yang mempunyai mekanisme keamanan menggunakan internet untuk menghubungkan antar remote site secara aman dimana di didalamnya dapat dibuat jaringan dalam jaringan. Tujuan dari sistem VPN Server ini dalam Kementerian PANRB ini adalah untuk memudahkan pegawai agar tetap dapat bekerja terhubung kedalam jaringan lokal Kementerian PANRB.

LOGIC : Jurnal Ilmu Komputer dan Pendidikan
Volume 2, No. 1, Tahun 2023
ISSN 2985-4172 (media online)
Hal 153-159

FortiGate sebuah pilihan terbaik untuk sistem keamanan yang menyediakan perlindungan tinggi terhadap ancaman keamanan yang dinamis dan menyederhanakan infrastruktur keamanan IT organisasi. Penelitian ini bertujuan untuk membangun VPN *(Virtual Private Network)* berbasis SSL-VPN. Penelitian dilakukan pada jaringan Wide Area Network menggunakan perangkat FortiGate sebagai firewall dan gateway yang saling terhubung dan membentuk tunnel sebagai jalur khusus yang menghubungkan jaringan private secara aman. Hasil penelitian menunjukan bahwa perangkat pengguna dapat mengakses server yang berada pada kantor secara real time, dan kinerja transfer data sukses diterima, dan semakin besar paket yang dikirim maka waktu proses transfer file juga akan semakin lama.

Fortigate merupakan perangkat keamanan jaringan yang menjamin secara keseluruhan sekaligus berfungsi sebagai gateway dan router bagi jaringan LAN (Local Area Network) sehingga tidak dibutuhkan lagi router ataupun perangkat tambahan load balancing bila ada lebih dari satu koneksi WAN (Wide Area Network) (Faizan, Hegde, & Yaligar, 2019). Satu perbedaan yang utama, konten FortiASIC yang di custom sendiri serta prosesor jaringan fortinet memungkinkan sistem fortigate mendeteksi dan mengeliminir secara real time ancaman yang terintegrasi, bahkan dalam skala kompleks, tanpa menurunkan kinerja jaringan, sementara serangkaian proses manajemen, analisa, database dan solusi perlindungan end point bekerja meningkatkan penyebaran fleksibilitas dan memberikan dampak yang nyata dalam mengurangi biaya operasional manajemen keamanan jaringan (Sistem, Agustina, & Rifqi, 2021).

Berdasarkan uraian diatas, maka penulis akan menyusun skripsi dengan judul "PENERAPAN TEKNOLOGI FORTIGATE DALAM PEMBANGUNAN JARINGAN VPN BERBASIS SSL-VPN (STUDI KASUS: KEMENTERIAN PANRB" Penelitian ini mempunyai tujuan untuk memudahkan para pegawai dapat melakukan pekerjaan menjadi lebih efisien dan produktivitas pekerjaan menjadi meningkat serta dapat menunjang kinerja.

2. METODE

2.1 Metode Pengumpulan Data

Metode yang akan digunakan dalam proses pengumpulan data sebagai bahan pengembangan sistem adalah studi pustaka atau literatur yang merupakan metode yang dilakukan dengan cara observasi dan studi pustaka mencari sumber dari jurnal, e-book, buku-buku yang membahas tentang VPN Server.

2.2 Metode Pengembangan Sistem

Dalam Pengembangan sistem yang digunakan dalam penelitian ini adalah PPDIOO (*Prepare, Plan, Design, Implement, Operate, and Optimize)*.

Gambar 1. Metode PPDIO

LOGIC : Jurnal Ilmu Komputer dan Pendidikan
Volume 2, No. 1, Tahun 2023
ISSN 2985-4172 (media online)
Hal 153-159

Pemilihan metode ini kareka metode ini dinilai tepat untuk pengembangan jaringan keamanan komputer. Tahapan yang digunakan diantaranya:

a) *Prepare*

Peneliti mengamati topologi yang diterapkan pada Kementerian PANRB dan penambahan alat atau perangkat apa saja yang akan digunakan.

b) *Plan*

Pada tahap ini peneliti melakukan analisa permasalahan, perencanaan kebutuhan dalam membangun sebuah VPN Server perlu memahami topologi yang digunakan dan yang akan dipakai. Karena untuk mencegah terjadinya kesalahan konfigurasi nantinya.

c) *Design*

Setelah mendapatkan data dan permasalahan, peneliti mulai merancang topologi.

d) *Implement*

Pada tahap ini sistem akan dikonfigurasi sedemikian rupa yang bertujuan untuk keberhasilan penelitian. Peneliti akan menguji coba atau mengimplementasikan.

e) *Operate*

Tahap operate merupakan proses pengoperasian dengan melakukan konfigurasi yang sudah dirancang.

f) *Optimize*

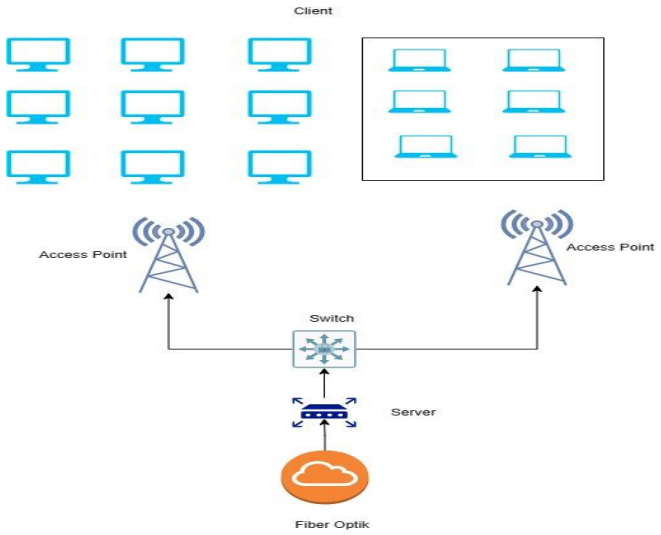
Peneliti melakukan optimasi terhadap sistem yang sudah dibangun dengan mengatur dan membuat sistem agar dapat berjalan dengan baik.

3. ANALISA DAN PEMBAHASAN

Analisis network adalah analisis yang dilakukan terhadap rencana pelaksanaan suatu proyek dengan menggunakan suatu bagan network yang menggambarkan serangkaian kegiatan dari pelaksanaan proyek tersebut

3.1 Analisa Skema Jaringan Awal

Berikut adalah skema pada jaringan yang sudah diterapkan pada instansi, peneliti menganalisa jaringan ini agar bisa dapat mendapatkan pola dan titik pemasangan.



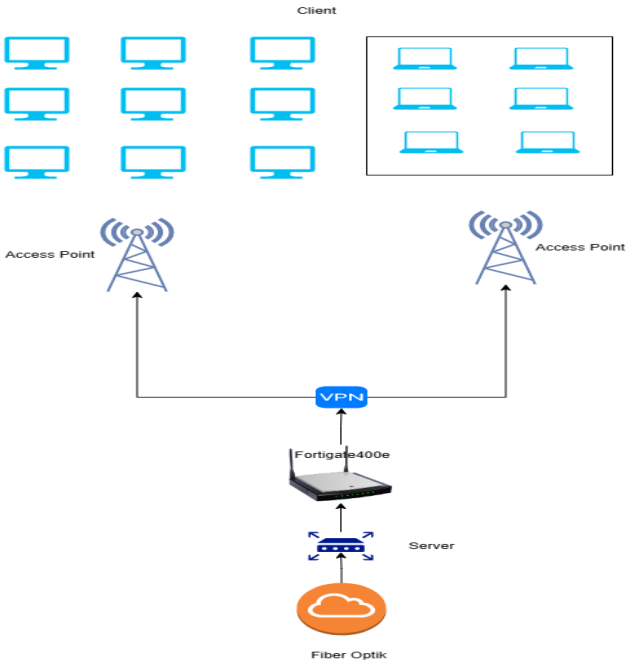
Gambar 2. Skema Jaringan Awal

LOGIC : Jurnal Ilmu Komputer dan Pendidikan
Volume 2, No. 1, Tahun 2023
ISSN 2985-4172 (media online)
Hal 153-159

Kebutuhan teknologi yang dibutukan adalah teknologi yang memungkinkan pegawai dapat tehubung ke jaringan meskipun sedang tidak berada di area jaringan kantor.

3.2 Analisa Skema Jaringan Usulan

Berikut adalah skema jaringan usulan yang dibuat oleh peneliti dimana point dasar tidak dirubah nanum kebutuhan perangkat ditambahkan.



Gambar 3. Skema Jaringan Usulan

3.3 Rancangan Jaringan Usulan

Rancangan yang diusulkan menggunakan teknologi VPN berbasis SSL-VPN yang menghubungkan jaringan pegawai yang berada diluar kantor dengan jaringan yang berada dikantor menggunakan infrastruktur jaringan yang sudah ada di KEMENTERIAN PANRB, karena jaringan.

Topologi jaringan menggunakan teknologi VPN berbasis SSL-VPN dengan rincian sebagai berikut:

a. FortiGate-400 yang berfungsi sebagai router, yang bertugas meneruskan dan mengatur paket data kepada client melalui switch.

b. Selanjutnya paket data tersebut melewati switch, dan switch mendistribusikan paket paket tersebut ke access point, server – server, dan printer agar dapat terhubung dengan baik

c. Konfigurasi VPN berbasis SSL-VPN dan menggunakan mode tunnel mode.

3.4 Implementasi Jaringan Usulan

Implementasi topologi jaringan yang diusulkan dilakukan dengan tahapan berikut:

Konfigurasi VPN berbasis SSL-VPN dengan melakukan konfigurasi interfaces dan IP address. Langkah selanjutnya dengan membuat firewall policy yang dipergunakan untuk membuka jalur traffic dan melakukan scanning terhadap antivirus, antispam, web filtering dan IPS. Setelah membuat interfaces dan pengaturan IP address beserta firewall policy, langkah selanjutnya adalah membuat routing. Routing digunakan untuk meneruskan paket-paket jaringan dari satu jaringan ke jaringan lainnya melalui sebuah internetwork. Routing yang dipakai adalah static route. Tahapan selanjutnya yaitu konfigurasi SSL-VPN. Dalam tahap konfigurasi SSL-VPN, FortiGatemenggunakan mode NAT, dan mempunyai IP Publik Statis yang sebelumnya sudah

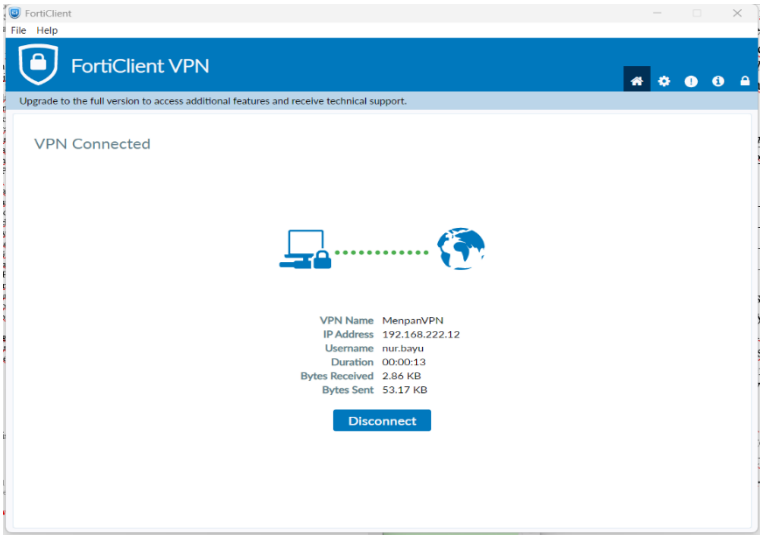
LOGIC : Jurnal Ilmu Komputer dan Pendidikan
Volume 2, No. 1, Tahun 2023
ISSN 2985-4172 (media online)
Hal 153-159

dikonfigurasi. Konfigurasi lanjutan yang diperlukan dalam membuat SSL-VPN pada yaitu membuat tunneling. Selanjutnya membuat Firewall address untuk mendefinisikan IP address yang diperbolehkan melewati Firewall policy dilanjutkan dengan membuat Firewall policy untuk outbound dan inbound traffic VPN IPSec. Setelah konfigurasi, Firewall address, dan Firewall policy, langkah terakhir yaitu membuat konfigurasi routing static untuk SSL-VPNSetelah membuat interfaces dan pengaturan IP address beserta firewall policy, langkah selanjutnya adalah membuat routing. Routing digunakan untuk meneruskan paket-paket jaringan dari satu jaringan ke jaringan lainnya melalui sebuah internetwork. Routing yang dipakai adalah static route. Tahapan selanjutnya yaitu konfigurasi SSL-VPN. Dalam tahap konfigurasi SSL-VPN, FortiGatemenggunakan mode NAT, dan mempunyai IP Publik Statis yang sebelumnya sudah dikonfigurasi. Konfigurasi lanjutan yang diperlukan dalam membuat SSL-VPN pada yaitu membuat tunneling. Selanjutnya membuat Firewall address untuk mendefinisikan IP address yang diperbolehkan melewati Firewall policy dilanjutkan dengan membuat Firewall policy untuk outbound dan inbound traffic VPN IPSec. Setelah konfigurasi, Firewall address, dan Firewall policy, langkah terakhir yaitu membuat konfigurasi routing static untuk SSL-VPN.

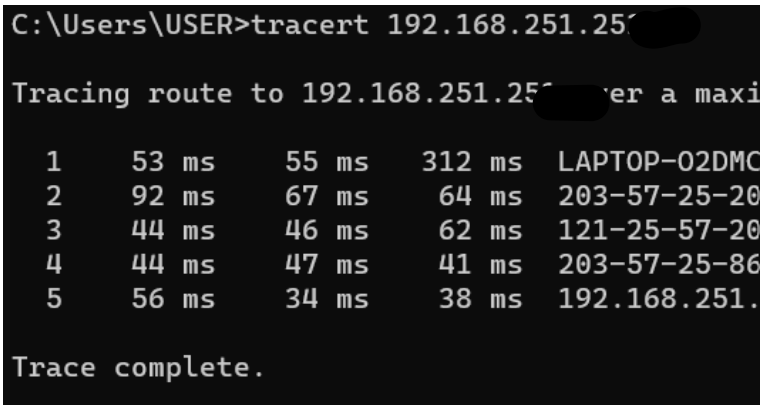
3.5 Pengujian Jaringan Usulan

Untuk memastikan jaringan yang baru dapat bekerja sesuai dengan yang direncanakan maka dilakukan serangkaian pengujian sebagai berikut :

a. Pengujian menggunakan aplikasi Forticlient



Gambar 4. Pengujian Koneksi dengan Forticlient

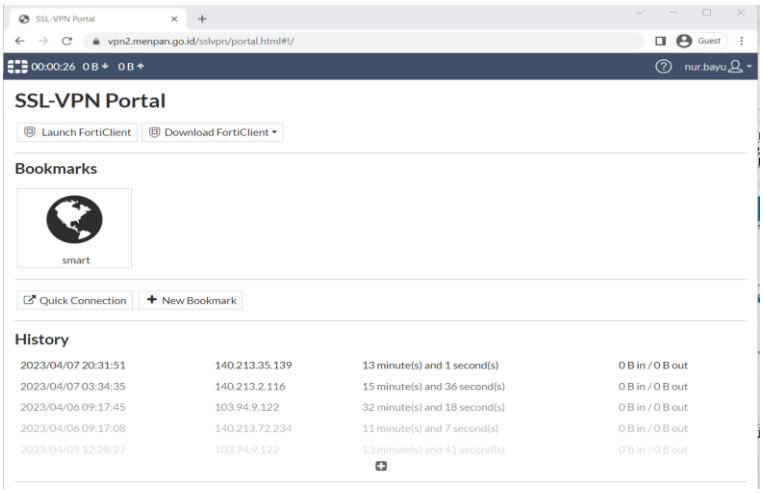


Gambar 5. Uji Trace Server

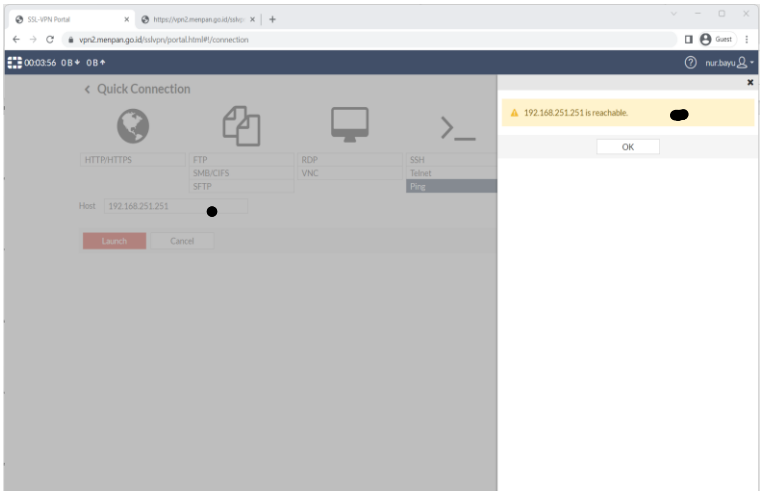
LOGIC : Jurnal Ilmu Komputer dan Pendidikan
Volume 2, No. 1, Tahun 2023
ISSN 2985-4172 (media online)
Hal 153-159

Pengujian koneksi berhasil ditandai dengan berjalannya traffic dan trace server aplikasi.

b. Pengujian menggunakan Bowser



Gambar 6. Pengujian Koneksi dengan Browser



Gambar 7. Uji ping Server

4. KESIMPULAN

Berdasarkan dari hasil perancangan dan pengujian dapat ditarik kesimpulan bahwa telah dihasilkan sebuah jalur lintas komunikasi proses pertukaran data yang aman dan terpercaya (*secure and reliable*) antara jaringan yang digunakan pegawai dengan jaringan kantor. Dengan adanya jalur SSL-VPN, Pegawai KEMENTERIAN PANRB yang berada diluar area Gedung kantor dapat terkoneksi dengan jaringan lokal kantor sehingga dapat melakukan pekerjaan tanpa terbatas jarak dan targer tercapai tepat waktu.

REFERENCES

AFRIANTO, I. (2019). KAJIAN *VIRTUAL PRIVATE NETWORK* (VPN) SEBAGAI SISTEM PENGAMANAN DATA PADA JARINGAN KOMPUTER (Studi Kasus Jaringan Komputer Unikom). *Majalah Ilmiah UNIKOM*, *12*(1).

Alcatel. (2021). *3 PERBEDAAN UNMANAGED SWITCH DAN MANAGED SWITCH*. Https://Alcatelkomunikasi.Com/3-Perbedaan-Unmanaged-Switch-Dan-Managed-Switch/.

Amera. (2021). *Winbox Mikrotik: Fitur-fitur, Cara Menggunakan & Link Download*. GFN.

LOGIC : Jurnal Ilmu Komputer dan Pendidikan
Volume 2, No. 1, Tahun 2023
ISSN 2985-4172 (media online)
Hal 153-159

Bayu, A. (2020). *PENGEMBANGAN JARINGAN KOMPUTER DENGAN METODE PPDIOO PADA PT. SAKTI INTI MAKMUR CABANG PALEMBANG*.

Desmira. (2016). ANALISISJARINGAN LAN DAN WLAN PLTU PADA PT. PEMBANGKITAN JAWA BALI UNIT MUARA KARANG JAKARTA. *Jurnal PROSISKO*, *3*(2).

Hafid, M. (2020). *FortiClient Untuk Memudahkan Anda Terkoneksi Jaringan Kantor Anda dari Rumah Selama WFH*. Https://Dapenbri.Co.Id/2020/10/05/Gunakan-Saja-Forticlient-Untuk-Memudahkan-Anda-Terkoneksi-Jaringan-Vpn-Kantor-Anda-Dari-Rumah-Anda/.

Hidayatulloh, S. (2014). ANALISIS DAN OPTIMALISASI KEAMANAN JARINGAN MENGGUNAKAN PROTOKOL IPSEC. *JI*, *1*(2).

Jho. (2023). *PuTTY: Aplikasi Remote Server & SSH Client Andalan*. JogjaHosting.

Kusuma, G. H. A. (2021). Perancangan Skema Sistem Keamanan Jaringan Web Server menggunakan Web Application Firewall dan Fortigate untuk Mencegah Kebocoran Data di Masa Pandemi Covid-19. *Journal of Informatics and Advanced Computing*, *2*(2).

Maryanto. (2018). *Metode Internet Protocol Security (IPSec) Dengan Virtual Private Network (VPN) Untuk Komunikasi Data*.

Putra, O. D., Destiarini, & Rahman, A. (2022). PENGGUNAAN *VIRTUAL PRIVATE NETWORK* (VPN) PADA PT SEMEN BATURAJA (PERSERO) TBK. *INTECH*, *3*(1).

Putra, P. R. (2011). *VPN (VIRTUAL PRIVATE NETWORK)*. Https://Eripahle.Wordpress.Com/2011/09/24/Vpn-Virtual-Private-Network/.

Rosmana. (2015). IMPLEMENTASI *VIRTUAL PRIVATE NETWORK* (VPN) DENGAN OTENTIKASI RADIUS SERVER PADA PT. ANUGERAH TUNGGAL MANDIRI JAKARTA. *Jurnal Techno Nusa Mandiri*, *7*(1).

Subekti, R. (2020). IMPLEMENTASI *VIRTUAL PRIVATE NETWORK* (VPN) SEBAGAI SOLUSI SECURITY SELAMA WORK FROM HOME. *JUNIF*, *1*(1).