Jurnal ICT : Information Communication & Technology
Vol. 23, N0.1, Juli 2023, pp. 310-316
p-ISSN: 2302-0261, e-ISSN: 2303-3363

Perancangan dan Implementasi Jaringan Virtual Private Network (VPN) Pada PT. XYZ

Kikim Mukiman[1*], Zaenal Mutaqin Subekti[2], Satria[3], Muhamad Dedi Suryadi[4], Irmanto Budiman[5]
[1]Program Studi Komputerisasi Akuntansi, Universitas Bani Saleh Bekasi, Indonesia
[2,3]Program Studi Teknik Informatika, Universitas Bani Saleh Bekasi, Indonesia
[3]Program Studi Manajemen Informatika, Universitas Bani Saleh Bekasi, Indonesia
Email: [1]kikimmukiman@gmail.ac.id, [2]zms.stmikbanisaleh@gmail.com, [3]satria1905@gmail.com, ,[4]kangdedi@gmail.com,[5]irmantobudiman@gmail.com

INFORMASI ARTIKEL

Histori artikel:

Naskah masuk, 19 Mei 2023
Direvisi, 20 Juli 2023
Diiterima, 14 Agustus 2023

Kata Kunci:

VPN,
Keamanan,
Jaringan

ABSTRAK

Abstract- **A** company that has many computer devices connected to the intranet network and has several servers that are used in operations, some of these servers consist of web servers, database servers and file servers, the company has a main building and branch buildings located outside the city, so that when there are employees who want to access the server in the main building they have to go through an unsecured internet network. a virtual private network (VPN) network offers security on the network by encrypting messages sent and decrypting messages received, so that information or data sent is safe through the network from a branch building to a branch building or vice versa. in this study using four stages of research starting from requirements, design, implementation, and testing. from the test results using tracert to get the detected network address, namely the virtual private network (VPN) network address, so that the original network address is not detected and there is an encryption process so that data sent through a virtual private network (VPN) network becomes safe.

Abstrak- **S**ebuah perusahaan yang memiliki banyak perangkat komputer yang terhubung kedalam jaringan intranet dan memiliki beberapa server yang digunakan dalam operasional, beberapa server tersebut terdiri dari, web server, database server dan server file, perusahaan tersebut mempunyai gedung utama dan gedung cabang yang terletak di luar kota, sehingga ketika ada karyawan yang akan mengakses ke server yang ada di gedung utama harus melalui jaringan internet yang tidak aman. Jaringan virtual private network (VPN) menawarkan keamanan pada jaringan dengan cara melakukan enkripsi pada pesan yang dikirim dan dekripsi pada pesan yang di terima, sehingga informasi atau data yang dikirim menjadi aman melalui jaringan dari gedung cabang ke gedung cabang atau sebalik nya. Pada penelitian ini menggunakan empat tahapan penelitian mulai dari requirement, desain, implementation, dan testing. Dari hasil pengujian dengan menggunakan tracert mendapatkan alamat jaringan yang terdeteksi yaitu alamat jaringan virtual private network (VPN), sehingga alamat jaringan yang asli tidak terdeteksi dan ada proses enkripsi sehingga data yang dikirim melalui jaringan virtual private network (VPN) menjadi aman.

Penulis Korespondensi:

Kikim Mukiman
Program Studi Teknik Informatika,
Universitas Bani Saleh
Jl. M Hasibuan No. 68 Bekasi, Indonesia
Email: kikimmukiman@gmail.com

1. Pendahuluan

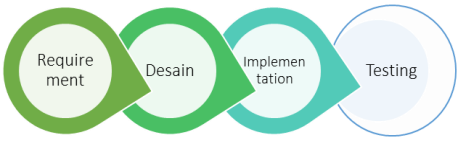
Keamanan jaringan (Network Security) dalam sebuah jaringan komputer sangat penting agar dikelola dengan baik dan benar sehingga tidak dapat memberikan celah untuk penyalah gunaan sumber daya jaringan. Tugas keamanan jaringan[1] dikontrol oleh admin jaringan, Tujuan keamanan jaringan ditujuan untuk mengantisipasi resiko berupa bentuk ancaman fisik maupun logika baik secara langsung ataupun tidak langsung yang dapat menggangu aktifias yang sedang berlangsung dalam sebuah jaringan komputer pada perusahaan.

Sebuah perusahaan yang memiliki banyak perangkat komputer yang terhubung kedalam jaringan intranet dan memiliki beberapa server yang digunakan dalam operasional, beberapa server tersebut terdiri dari, web server, database server dan server file. admin jaringan melakukan tugas monitoring trafik jaringan komputer intranet dan trafik yang masuk dan keluar pada server.

Pada perusahaan tersebut memiliki gedung utama yang berlokasi kota sebut saja pada daerah kota-a, kemudian gedung cabang berlokasi pada diluar kota, sebut saja kota-b yang membutuhkan akses ke server dari gedung cabang ke gedung utama, untuk mengamankan akses dari gedung utama ke gedung maka dapat dengan menggunakan virtual private network (VPN)[2][3][4] sebagai solusi dalam mengamankan akses jaringan komputer dari gedung utama ke gedung cabang.

2. Metode

Pada metode penelitian ini ada empat tahap, yaitu requirement yaitu melakukan tahap analisa kebutuhan dari kebutuhan hardware dan kebutuhan perangkat lunak, kemudian desain yaitu melakukan tugas merancang topology jaringan untuk menghubungkan dua gedung yaitu gedung utama dan gedung cabang dengan menggunakan virtual private network (VPN)[5], selanjutnya implementation yaitu melakukan penerapan pada perangkat infrastruktur seperti router pada gedung utama dan router pada gedung cabang supaya dapat terhubung dengan menggunakan jaringan virtual private network (VPN) dan supaya pertukaran data aman tidak disadap oleh pihak lain, terakhir adalah testing yaitu melakukan pekerjaan pengujian dengan mengakses data dari komputer atau desktop pada gedung cabang ke server yang ada pada gedung utama melalui koneksi jaringan virtual private network (VPN), dari hasil pengujian harapan nya didapatkan data-data yang dapat digunakan dalam pengambilan keputusan.



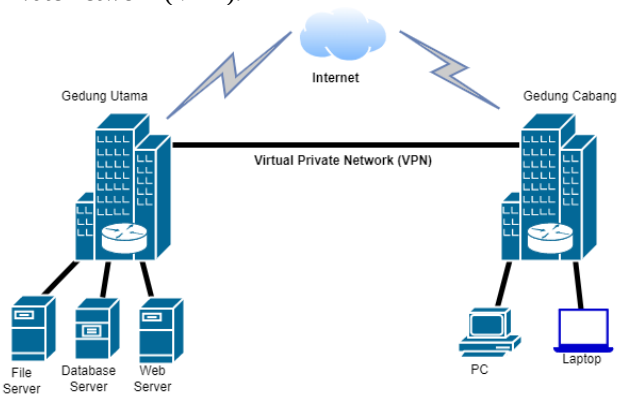
Gambar 1. Tahapan-tahapan metode [6]

2.1 Requirement

Pada tahap pertama requirement bertujuan untuk mengetahui Analisa kebutuhan[7] yaitu Analisa kebutuhan perangkat keras[8] dan Analisa kebutuhan perangkat lunak. Kebutuhan hardweare yang dibutuhkan yaitu router dengan menggunakan sistem operasi mikrotik, yang digunakan untuk core penghubung dari gedung utama dan gedung cabang, untuk kebutuhan perangkat lunak menggunakan aplikasi winbox yang digunakan untuk mengkonfigurasi router melalui remote, browser digunakan untuk melakukan pengetesan akses dan cmd digunakan untuk melakukan pengetesan akses koneksi.

2.2 Design

Kedua yaitu tahapan design, setelah analisa kebutuhan sudah selesai dilanjut dengan melakukan desin topologi jaringan[9][10] untuk menghubungkan jaringan dari gedung utama ke jaringann gedung cabang menggunakan virtual private network (VPN).



Gambar 2. Topologi jaringan VPN

2.3 Implementation

Ketiga yaitu tahap impelementasi, melakukan konfigurasi pada router gedung utama dan router cabang untuk menerapkan konfigurasi virtual private network.

Konfigurasi pada router gedung utama, berikut konfigurasi ip address, ether1 digunakan untuk lan pada gedung utama, dan ether2 digunakan untuk ke internet

```
/ip address
add address=192.168.10.1/24 interface=ether1
network=192.168.10.0
add address=8.8.8.1/24 interface=ether2
network=8.8.8.0

setting ip dhcp server pada ether1 pada router
gedung utama
/ip pool
add name=dhcp_pool1 ranges=192.168.10.2-
192.168.10.254
/ip dhcp-server
add address-pool=dhcp_pool1 disabled=no
interface=ether1 name=dhcp1
/ip dhcp-server network

add address=192.168.10.0/24
gateway=192.168.10.1
```

Konfigurasi pada router gedung cabang, berikut konfigurasi ip address, ether1 digunakan untuk internet, dan ether2 digunakan untuk lan gedung cabang.

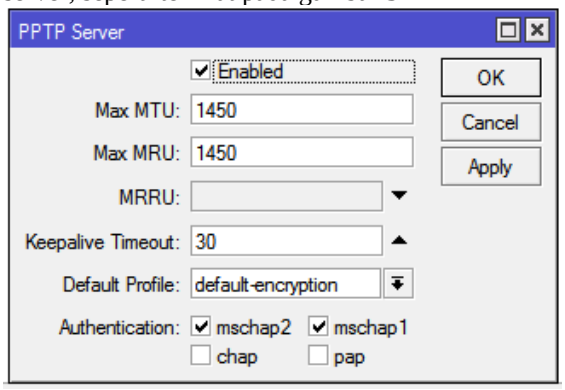
```
/ip address
add address=200.200.200.1/24 interface=ether2
network=200.200.200.0
add address=8.8.8.2/24 interface=ether1
network=8.8.8.0

setting ip dhcp server pada ether2 pada router
gedung cabang
/ip pool
add name=dhcp_pool1 ranges=200.200.200.2-
200.200.200.254
/ip dhcp-server
add address-pool=dhcp_pool1 disabled=no
interface=ether2 name=dhcp1
/ip dhcp-server network

Add address=200.200.200.0/24
gateway=200.200.200.1
```

2.4 Testing

Tahap terakhir dari tahapan penelitian yaitu testing[11], melakukan pengujian setelah melakukan implementasi atau penerapan konfigurasi pada router kemudian dilakukan pengujian.

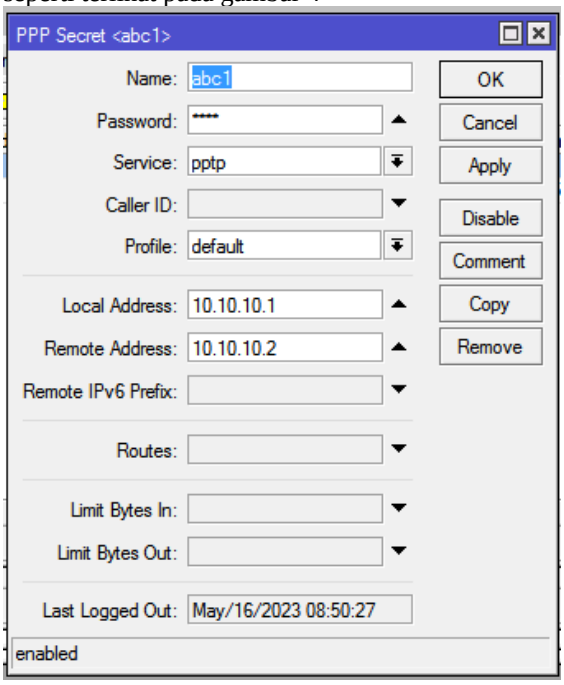
3. Hasil Pembahasan

Setelah setting ip address pada router gedung utama dan router gedung cabang selesai dan hasil koneksi dari terhubung dengan menggunakan ip publik, selanjutnya konfigurasi virtual private network pada router gedung utama, dengan menggunakan PPTP Server, lakukan enable service pptp server, klik pada menu ppp dan pilih pptp server, seperti terlihat pada gambar 3



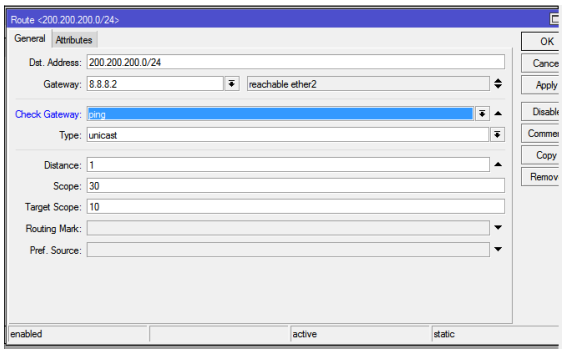
Gambar 3. Enable pptp server

Tambahkan secret profile, klik pada menu ppp, pilih secrets, dan klik tombol plus untuk menambah konfigurasi, isi pada name dan password, pada tab service pilih pptp, pada profile piilih default-encription, pada lokal address disi 50.50.50.1 dan remote address isi 50.50.50.100 klik apply dan OK, seperti terlihat pada gambar 4



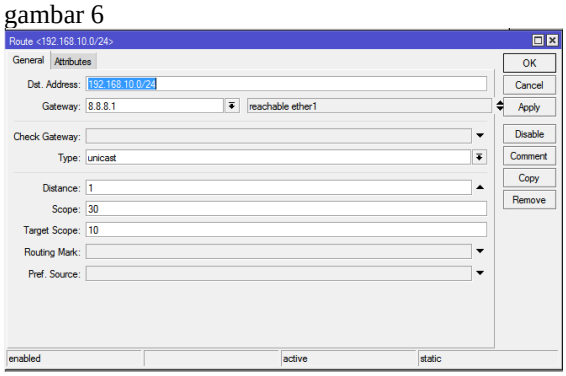
Gambar 4. menambah secrets

Tambahkan routing pada router gdung utama klik pada ip – routes kemudian klik tanda plus (+) isikan pada destination address 200.200.200.0/24 dan masukkan gateway 8.8.8.2, seperti terlihat pada gambar 5



Gambar 5. Routing pada gedung utama

Tambahkan routing pada router gedung cabang klik pada ip – routes kemudian klik tanda plus (+) isikan pada destination address 192.168.10.0/24 dan masukkan gateway 8.8.8.1, seperti terlihat pada gambar 6

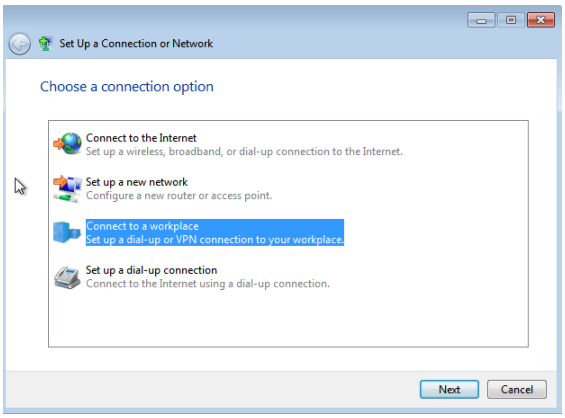


Gambar 6. Routing pada gedung cabang

Buat koneksi vpn dari client, pada sistem operasi windows 7, klik control panel – Network and Internet – Network and Sharing Center, seperti gambar dibawah ini, , seperti terlihat pada gambar 7

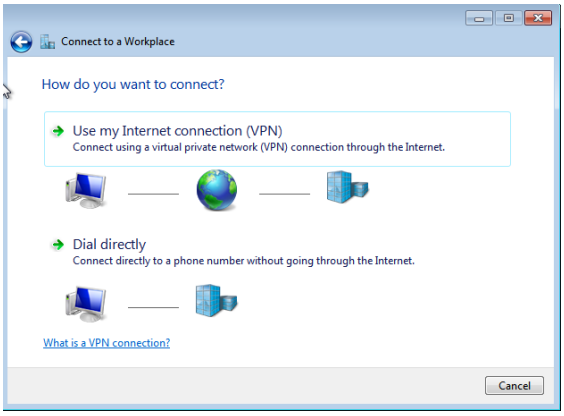
Gambar 7. Network and sharing center

Klik set up a new connection or network/connect to a workplace, seperti terlihat pada gambar 8



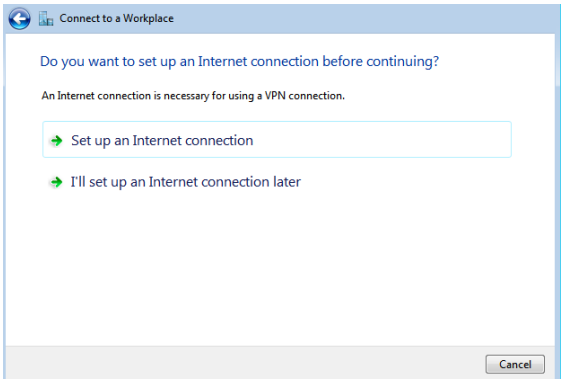
Gambar 8. Set up connection

Pilih use my internet connction (VPN), seperti terlihat pada gambar 9



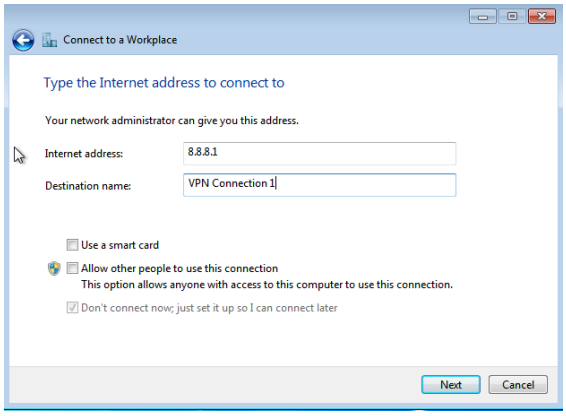
Gambar 9. Connect to workplace

Pilih I will set up an internet connection later, seperti terlihat pada gambar 10



Gambar 10. Setup internet connection

Kemudiaan isi internet address dan destination name, seperti terlihat pada gambar 11



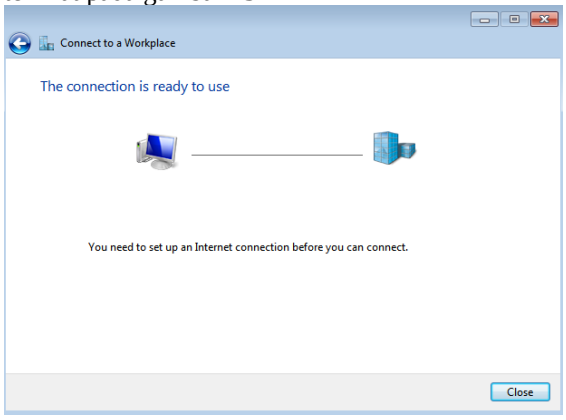
Gambar 11. Pengisian ip address

Pengisian username dan password akses vpn dari client, seperti terlihat pada gambar 12

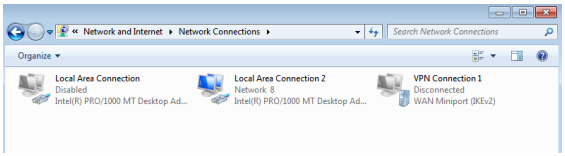
Gambar 12. username dan password vpn

Klik create, dan hasil nya seperti gambar dibawah ini.

Menunggu hasil koneksi, dan klik close, seperti terlihat pada gambar 13



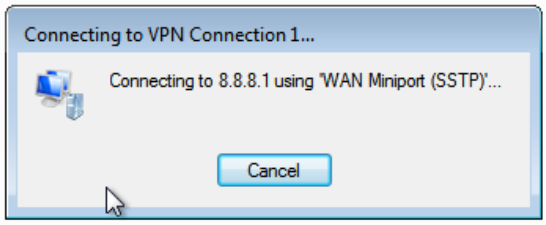
Gambar 13. membutuhkan koneksi internet



Gambar 14. network and internet

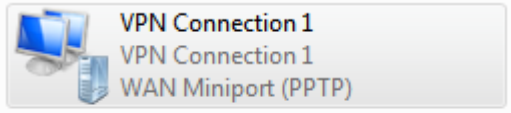
Klik kanan pada VPN Connection, kemudian isi username dan password, seperti terlihat pada gambar 15

Gambar 15. koneksi vpn



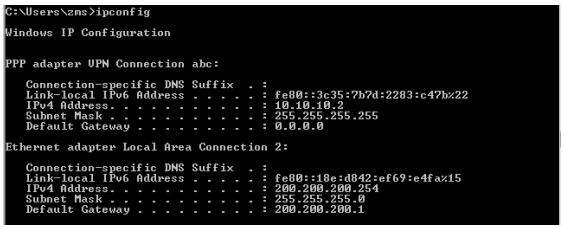
Gambar 16. proses koneksi vpn

Hasil nya terhubung, seperti terlihat pada gambar 17



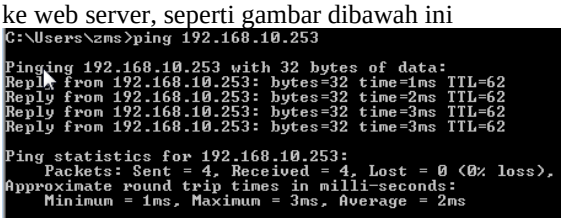
Gambar 17. hasil koneksi vpn

Lakukan cek ip address pada komputer client, seperti terlihat pada gambar 18



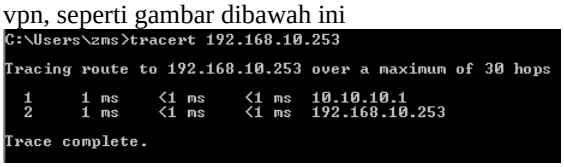
Gambar 18. ip address komputer client dan ip address vpn client

Lakukan pengujian dari cmd dengan perintah ping ke web server, seperti gambar dibawah ini



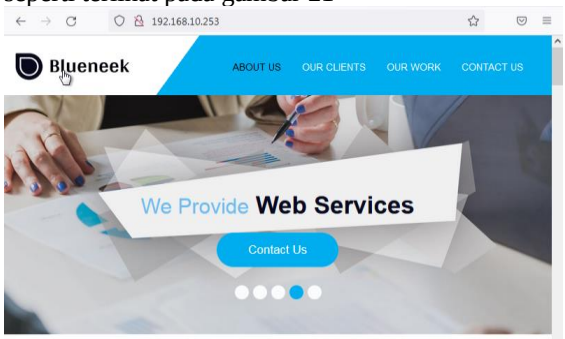
Gambar 19. Koneksi ke web server

Lakukan pengujian dari cmd dengan perintah traceroute ke ip web server menggunakan koneksi vpn, seperti gambar dibawah ini



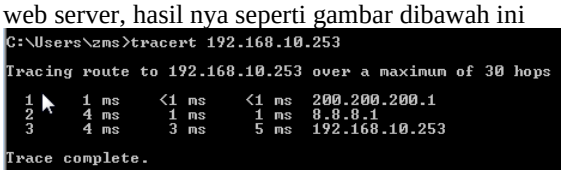
Gambar 20. hasil tracert ke web server

Lakukan pengujian melalui browser, dengan akses ke browser ke web server, melalui koneksi vpn, seperti terlihat pada gambar 21



Gambar 21. Hasil akses ke web server

Disconnect koneksi vpn, kemudian lakukan pengujian dari cmd dengan perintah traceroute ke ip web server, hasil nya seperti gambar dibawah ini



Gambar 22. hasil tracert ke web server tidak menggunakan koneksi vpn

4. Kesimpulan

Dari hasil pengujian pertama menghasilkan cek ip address pada komputer client dan ip address vpn, pengujian kedua menggunakan perintah ping dapat terhubung dari komputer cliant yang ada di gedung cabang ke server yang ada pada gedung utama, pengujian ketiga dengan menggunakan tracert menghasilkan jalur vpn dari jaringan komputer dari komputer client di gedung cabang ke server di gedung utama, pada pengujian keempat akses ke web server dengan menggunakan browser menghasilkan browser menampilkan landing page dari web server yang diakses dari jaringan virtual private network, dan pengujian kelima melakukan disconnect pada koneksi vpn kemudian melakukan tracert dari komputer client ke server

Ucapan Terima kasih

Ucapan terima kasih kepada fakultas teknologi informasi dan digital universitas bani saleh yang telah memberikan kesempatan untuk melakukan penelitian dosen internal.

Daftar Pustaka

[1] V. P. N. Ipsec, “Optimasi Keamanan Jaringan Point to Point Menggunakan VPN IPSec dan GRE,” pp. 297–305.

[2] T. Ariyadi and M. A. Prabowo, “Perbandingan Kinerja Virtual Private Network Antara Vpn Tunnel Dan Internet Protocols Security,” *INOVTEK Polbeng - Seri Inform.*, vol. 6, no. 1, p. 80, 2021, doi: 10.35314/isi.v6i1.1698.

[3] Normah, B. Rifai, S. Vambudi, and R. Maulana, “Analisa Sentimen Perkembangan Vtuber Dengan Metode Support Vector Machine Berbasis SMOTE,” *J. Tek. Komput. AMIK BSI*, vol. 8, no. 2, pp. 174–180, 2022, doi: 10.31294/jtk.v4i2.

[4] H. A. Musril, “Desain Virtual Private Network (VPN) Berbasis Open Shortest Path First (OSPF),” *InfoTekJar (Jurnal Nas. Inform. dan Teknol. Jaringan)*, vol. 3, no. 2, pp. 83–88, 2019, doi: 10.30743/infotekjar.v3i2.1055.

[5] T. Budimulya *et al.*, “PERANCANGAN VPN SEBAGAI PENDUKUNG SISTEM INFORMASI (Febrianti , Sidik , Susafa ’ ati , Nainggolan ,” pp. 197–202, 2022.

[6] K. Fahrezi, A. R. Mulana, S. Melinda, N. Nurhaliza, and S. Mulyati, “Penerapan Model Waterfall dalam Pengembangan Sistem Informasi Akademik Berbasis Web sebagai Sistem Pengolahan Nilai Siswa,” *J. Teknol. Sist. Inf. dan Apl.*, vol. 4, no. 2, p. 98, 2021, doi: 10.32493/jtsi.v4i2.10196.

[7] I. Husin, Z. M. Subekti, R. R. Rahayu, and D. N. Nurjannah, “Pengembangan Sistem Informasi Pelayanan Pelanggan Berbasis Web pada CV. Perum Jasa Tirta II,” *J. ICT Inf. Commun. Technol.*, vol. 20, no. 2, pp. 358–364, 2021, doi: 10.36054/jict-ikmi.v20i2.425.

[8] S. Hanadwiputra, Z. M. S, and I. N. Arifin, “MANAJEMEN INTERNET SERVICE PROVIDER POLICY BASED ROUTE STUDI KASUS : GEDUNG SERBA GUNA ISTANAKU,” vol. 11, no. 2, 2021.

[9] B. Arifwidodo, B. Setiyadi, and S. Ikhwan, "Implementasi Intrusion Prevention System (IPS) Pada Software Defined Network (SDN) Menggunakan RYU Controller," vol. 21, pp. 113–117, 2022.

[10] Z. Mutaqin Subekti, K. Mukiman, A. Fikri Adluwal Fadhil, and M. Asyrofi, "Penerapan Limit Akses Browsing Internet pada saat Jam Kerja di PT XYZ," *J. Teknol. Terpadu*, vol. 7, no. 1, pp. 31–38, 2021, doi: 10.54914/jtt.v7i1.342.

[11] F. Rusdi *et al.*, "Point Operation," vol. 2016, pp. 54–59, 2016.