JITET (Jurnal Informatika dan Teknik Elektro Terapan)
Vol. 13 No. 1, pISSN: 2303-0577 eISSN: 2830-7062 http://dx.doi.org/10.23960/jitet.v13i1.5588

IMPLEMENTASI JARINGAN VPN SITE-TO-SITE DAN PROTOCOL OSPF MENGGUNAKAN CISCO DI SEKOLAH BINA BANGSA

Hadi Prayitno[1], Irwan Agus Sobari[2*]

[1,2]Universitas Nusa Mandiri Jakarta; Jl. Kramat Raya, Senen, Jakarta Pusat DKI Jakarta
Telp. (021) 3190857

Received: 18 November 2024
Accepted: 14 Januari 2025
Published: 20 Januari 2025

Keywords:
VPN, OSPF, Switchport Security

Corespondent Email:
Irwan.igb@nusamandiri.ac.id

Abstrak. Perkembangan teknologi saat ini berlangsung sangat cepat. Kebutuhan akan informasi menjadi sangat penting terutama dalam pekerjaan, kebutuhan tersebut terus bertambah seiring dengan pengguna yang menginginkan informasi yang cepat, aman, dan efisien. Seperti di Sekolah Bina Bangsa yang belum terhubung secara langsung ke jaringan sehingga sangat rentan terhadap kebocoran data dan dapat dianggap kurang aman, sehingga perlu diterapkannya teknologi VPN (*Virtual Private Network*). Dengan adanya VPN (*Virtual Private Network*), pengiriman data dapat menjadi lebih aman karena adanya metode enkripsi yang disediakan oleh teknologi VPN ini. Protokol OSPF (*Open Shortest Path First*) dalam penggunaan nya merupakan teknologi yang diterapkan untuk membantu mengurangi bandwidth dalam penggunaan jaringan karena dalam protokol ini dapat menentukan jalur terbaik dalam memilih rute jaringan, sehingga diharapkan dapat mengurangi bandwidth yang ada. Untuk mencegah perangkat asing yang tidak terdaftar dalam sistem jaringan di sekolah, penulis mengusulkan penerapan *Switch-port Security* dengan konfigurasi violation shutdown. Dengan konfigurasi tersebut, jika perangkat asing mengakses jaringan sekolah, maka akan otomatis ter-shutdown. Sehingga, dengan diterapkannya sistem jaringan yang ada di Sekolah Bina Bangsa, diharapkan pengiriman data antara Kampus Kebon Jeruk dan PIK dapat dilakukan dengan aman, dapat mengurangi bandwidth dalam jaringan, dan juga jaringan internal tidak dapat diakses sembarangan oleh orang luar yang tidak terdaftar dalam sistem jaringan di Sekolah Bina Bangsa.

Abstract. *The development of technology is currently very rapid. The need for information is critical, especially in work, this need continues to grow along with users who want fast, safe, and efficient information. Sekolah Bina Bangsa is not directly connected to the network so it is very vulnerable to data leaks and can be considered less secure, so it is necessary to implement VPN (Virtual Private Network) technology. With VPN (Virtual Private Network), data delivery can be more secure because of the encryption method provided by this VPN technology. The OSPF (Open Shortest Path First) protocol is a technology that is applied to help reduce bandwidth in network usage because this protocol can determine the best path in choosing a network route, so it is expected to reduce the existing bandwidth. To prevent foreign devices that are not registered in the network system at school, the author proposes the implementation of Switch-port Security with a violation shutdown configuration. With this configuration, if a foreign device accesses the school network, it will automatically be shut down. Thus, by implementing the existing network system at Bina Bangsa School, it is hoped that data transmission between the Kebon Jeruk Campus and PIK can be carried out safely, can reduce bandwidth in the network, and also the internal network*

cannot be accessed carelessly by outsiders who are not registered in the network system at Bina Bangsa School.

1. PENDAHULUAN

Perkembangan teknis dalam bidang teknologi saat ini berkembang dengan sangat pesat. Kebutuhan akan informasi sangatlah penting terutama dunia kerja, kebutuhan tersebut terus berkembang seiring dengan semakin banyaknya pengguna yang menginginkan informasi secara cepat, aman, dan efisien. Hampir semua bidang teknologi memegang peranan penting dalam penyelesaian permasalahan yang diakibatkan oleh sistem, namun teknologi informasi yang ada saat ini menjadi "pedang bermata dua" karena memberikan kontribusi terhadap kesejahteraan manusia.

Satu hal yang perlu dipahami ketika melakukan aktivitas di internet adalah semakin banyak orang yang melakukan penyadapan terhadap data yang dikirim melalui internet dan kejahatan lainnya. Virtual Private Network (VPN) adalah teknologi yang memungkinkan terbentuknya sebuah jaringan data pribadi atau private pada jaringan publik dengan menerapkan otentikasi dan enkripsi sehingga hanya pihak tertentu yang dapat mengakses jaringan tersebut.

Dengan diterapkannya VPN pada sistem jaringan sekolah Bina Bangsa maka dapat memungkinkan antara kedua sekolah (Kebon Jeruk sebagai Pusat dan PIK sebagai cabang) dapat berkomunikasi secara aman di seluruh jaringan public dengan sedemikian rupa sehingga jaringan public beroperasi sebagai satu atau beberapa tautan komunikasi pribadi. [1].

Melihat masalah yang ada, ada beberapa yang didapat diantaranya, komunikasi antar pengguna masih belum optimal. Pengiriman data dari kantor cabang maupun ke kantor pusat atau sebaliknya masih belum terenkripsi yang mengakibatkan data dapat dilihat atau bahkan diambil oleh orang yang tidak berkepentingan sehingga butuh di terapkannya penerapan VPN di sistem jaringan Sekolah Bina Bangsa. [2]. Serta dengan menambahkan protokol routing OSPF *(Open Shortest Path First).*

Lalu dari sisi transfer data nya didukung dengan routing protocol OSPF yang dapat mencari rute tercepat dan terdistribusi yang meneruskan paket dengan pemberian label yang dapat membantu mempercepat pengiriman paket data pada jaringan.[3].

Dan dengan di terapkannya VPN site-to-site pada jaringan Sekolah Bina Bangsa untuk mencapai file sharing antara kantor pusat dan cabang sehingga lalu lintas informasi yang di kirim dapat aman dan rahasia

2. TINJAUAN PUSTAKA

Inovasi data dan juga jaringan terus berkembang dan banyaknya orang yang memanfaatkan inovasi ini tentunya mempunyai dampak yang berbeda-beda, mengingat semakin meningkatnya ketergantungan terhadap inovasi. Bagi sebagian besar orang saat ini, pekerjaan dapat dilakukan dengan menggunakan PC dan gadget pendukung lainnya, misalnya saja kebutuhan akan web yang kita perlukan secara konsisten untuk mengakses dokumen atau informasi yang kita simpan. Salah satu jenis penggunaan inovasi data adalah jaringan komputer [4]

OSPF *(Open Shortest Path First)* adalah suatu protokol routing yang dibuat oleh *Internet Engineering Task Force* (IETF) pada tahun 1987. Dalam penggunaan protokol routing ini bersifat terbuka, dimana produsen *switch* mana pun dapat memanfaatkan OSPF. Inklusivitas ini meluas hingga beralih produk dari perusahaan seperti Cisco dan Mikrotik. Munculnya OSPF sebagai protokol routing terkait erat dengan pertumbuhan organisasi web yang lebih besar [5].

VPN memberikan perlindungan terhadap data, menjaga kerahasiaan data selama proses transmisi, memastikan integritas data, otentikasi sumber data, melindungi dari replay attack, dan mengontrol akses selama proses transmisi melalui jaringan komputer publik[6]

Remote access yang umum juga dikenal virtual private dial-up network (VPDN), menyambungkan pengguna yang bergerak dengan local area network (LAN). Tipe VPN ini digunakan oleh karyawan perusahaan yang ingin terhubung ke jaringan khusus perusahaannya dari berbagai lokasi yang jauh (remote) dari perusahaannya. Seringnya, perusahaan yang ingin membuat jaringan VPN jenis ini akan bekerja sama dengan enterprise service provider (ESP) [7].

Site to Site adalah salah satu cara VPN IPSec Tunneling yang umum dipakai untuk menghubungkan lokasi yang berbeda menjadi satu jaringan. Penggunaan IPSec bisa melindungi pengiriman data antara host ke host, jaringan ke jaringan hingga jaringan ke host karena melakukan enkripsi terhadap paket data yang dikirim [8].

SSL VPN adalah tipe jaringan pribadi virtual (VPN) yang memanfaatkan protokol Secure Sockets Layer

(SSL). Koneksi SSL VPN memakai enkripsi ujung-ke-ujung (E2EE) untuk menjaga data yang dikirimkan antara perangkat lunak klien perangkat titik akhir dan server SSL VPN agar klien terhubung dengan aman ke internet[9].

IPsec VPN memakai protokol IPsec untuk melindungi komunikasi internet pada level IP dengan mengenkripsi dan memverifikasi paket IP sehingga lebih terjaga keamanannya[10].

Pendekatan keamanan Hybrid Endto-End VPN yang diperoleh dengan menggabungkan pendekatan keamanan IPSec/IPv6 dan OpenSSL yang bisa melindungi objek IoT pintar dalam lingkungan yang berbeda[11].

Switchport Security merupakan fitur yang ada pada perangkat jaringan Switch yang dirancang untuk meningkatkan keamanan pada suatu jaringan local atau LAN. Tujuan utama dari diterapkannya Switchport Security adalah untuk membatasi akses ke suatu Switch port dengan mengendalikan jumlah dan jenis perangkat yang diizinkan untuk terhubung dalam suatu lingkup jaringan kedalam port tersebut [12].

3. METODE PENELITIAN

Penulis melakukan pengamatan secara langsung pada Sekolah Bina Bangsa yang berada Pantai Indah Kapus jalan Walet Elok 8 R-8 No.1, RT.13/RW.6, Kapuk Muara, Kec. Penjaringan, Jkt Utara, Daerah Khusus Ibukota Jakarta 14460. Mengevaluasi hasil pengamatan yang kemudian dijadikan sebagai pertimbangan dalam mengambil keputusan. Berikut beberapa tindakan yang mencakup sebagai berikut:

A. Analisa Kebutuhan

Dalam melakukan perancangan jaringan penulis juga sadar akan membutuhkan pengumpulan data dan informasi seperti melakukan Wawancara terhadap salah satu Staff IT di Sekolah Bina Bangsa PIK untuk mengetahui apa saja yang digunakan dalam jaringan Sekolah Bina Bangsa PIK untuk membuat simulasi dan skema jaringan yang akan di implementasikan di Sekolah Bina Bangsa PIK

B. Desain

Penulis tidak merubah perangkat maupun kondisi jaringan yang sudah ada pada sistem jaringan di Sekolah Bina Bangsa PIK dikarenakan sudah terdapat jaringan yang sudah berjalan dan hanya menambahkan beberapa konfigurasi saja, dan melakukan desain menggunakan software Cisco Packet Tracer untuk membuat skema jaringan serta membuat jaringan usulan

C. Testing

Untuk mengetahui bagaimana jaringan yang sudah dibuat berhasil atau tidaknya, maka penulis melakukan uji testing dengan perintah Ping pada PC Client. Jika VPN belum terkoneksi maka pada saat melakukan uji testing Ping akan menunjukan hasil Destinantion Host Unreachable atau Request Time Out. Apabila VPN sudah terkoneksi maka akan menunjukan hasil Time-to-Live pada alamat IP yang di tuju.

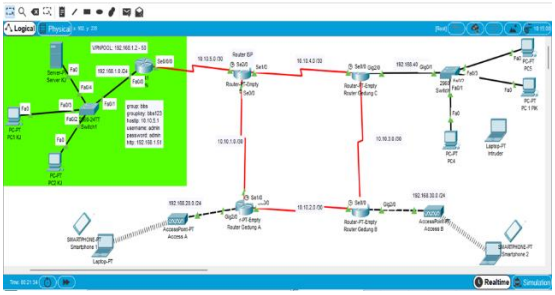
D. Implementasi

Penulis akan melakukan implementasi jaringan yang sudah dibuat guna sebagai solusi dan bisa menjadi penunjang kinerja dalam sistem jaringan di Sekolah Bina Bangsa PIK.

4. HASIL DAN PEMBAHASAN

4.1 Skema Jaringan

Pada sistem jaringan di Sekolah Bina Bangsa menggunakan Topologi Hybrid. Hal ini dikarenakan Topologi Hybrid yang digunakan dalam sistem jaringan Sekolah Bina Bangsa mempunyai beberapa Internet Service Provider (ISP). Sehingga penggunanya dapat menyesuaikan dengan kondisi gedung yang dimana topologi ini sangat fleksibel jika membandingkan dengan model topologi yang lainnya dan dapat menyesuaikan kondisi pengguna juga.



Gambar 1. Skema Jaringan

4.2 Implemntasi Jaringan

Dalam tahapan untuk implementasi jaringan ini dilakukan beberapa konfigurasi pada perangkat yang ada di sistem jaringan yang ada di Sekolah Bina Bangsa yaitu dengan menerapkan beberapa konfigurasi tambahan dan tidak mengubah skema ataupun arsitektur jaringan yang ada. Dalam implementasinya penerapan konfigurasi VPN dan OSPF di terapkan di Router lalu disarakna untuk melakukan penerapan Konfigurasi Switchport Security Violation Shutdiwn pada Switch yang ada di ruang guru guna mencegah perangkat lain dapat mngakses jaringan sekolah dengan bebas. Berikut di jabarkan untuk konfigurasi Router dan Switch.

A. Konfigurasi Router VPN

VPN#enable
VPN#configure terminal Configure each terminal, one at a time. Akhiri dengan CNTL/Z.
VPN(config)#aaa new-model
VPN(config)#aaa validation login vpn1 nearby

VPN(config)#aaa approval network vpn 2 neighborhood
VPN(config)#aaa approval network vpn2 neighborhood
VPN(config)#username administrator secret key administrator
VPN(config)#crypto isakmp strategy
VPN(config)#crypto isakmp strategy 10
VPN(config-isakmp)#encryption ?
3des Triple DES kunci tiga
AES - High level Encryption Standard
DES - Information Encryption Standard (56 digit keys).
VPN(config-isakmp)#encryption
VPN(config)#crypto isakmp client design bunch
VPN(config)#crypto isakmp client setup bunch bbs
VPN(config-isakmp-group)#key bbs123
VPN(config-isakmp-group)#pool VPNPOOL
VPN(config-isakmp-group)#exit
VPN(config)#crypto ipsec change set set1 esp-3des esp-md5-hmac
VPN(config)#crypto dynamic-map map1 10
VPN(config-crypto-map)#set change set set1
VPN(config-crypto-map)#reverse-course
VPN(config-crypto-map)#exit
VPN(config)#crypto map map1 client setup address answer
VPN(config)#crypto map map1 client validation list vpn1
VPN(config)#crypto map map1 isakmp approval list vpn2
VPN(config)#crypto map map1 10 ipsec-isakmp dynamic map1VPN(config)#crypto map map1 10 ipsec-isakmp dynamic map1

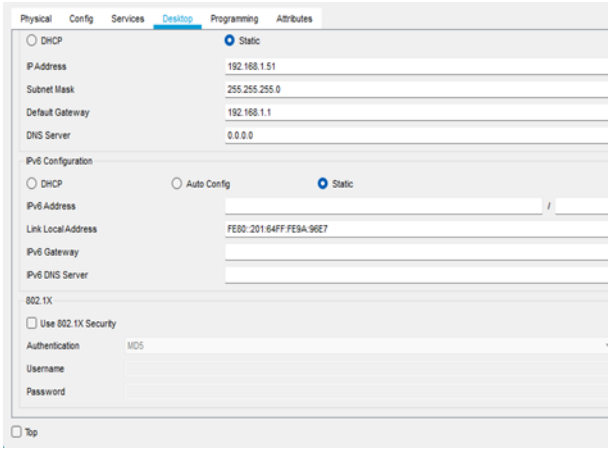
B. Konfigurasi Router ISP

ISP#enable
ISP#configure terminal
Enter design orders, one for every line. End with CNTL/Z.
ISP(config)#int se1/0
ISP(config-if)#no closure
ISP(config-if)#ip address 10.10.10.2 255.255.255.0
ISP(config-if)#
00:08:57: % OSPF-5-ADJCHG: Process 40, Nbr 192.168.40.1 on Serial1/0 from FULL to DOWN, Neighbor Down: Interface down or isolates
ISP(config-if)#exit
ISP(config)#int se0/0
ISP(config-if)#no closure
ISP(config-if)#ip address 11.11.11.2 255.255.255.0
ISP(config-if)#
00:09:41: % OSPF-5-ADJCHG: Process 40, Nbr 192.168.20.1 on Serial0/0 from FULL to DOWN, Neighbor Down: Interface down or segregated
ISP(config-if)#exit
ISP(config)#ip course 172.16.1.0 255.255.255.0 10.10.10.1
ISP(config)#ip course 192.168.10.0 255.255.255.0 11.11.11.1
ISP(config)#int se1/0
ISP(config-if)#encapsulation outline transfer ietf
ISP(config-if)#
ISP(config-if)#frame-transfer LMI-type ansi
ISP(config-if)#clock rate 56000
This order applies just to DCE interfaces
ISP(config-if)#no closure
ISP(config-if)#exit
ISP(config)#int se1/0.101 highlight point
ISP(config-subif)#
%Connect 5-CHANGED: Interface Serial1/0.101, changed state to up
ISP(config-subif)#ip address 10.10.5.0 255.255.255.0
Terrible cover/24 for address 10.10.5.0
ISP(config-subif)#frame-hand-off interface-dlci 101
ISP(config-subif)#ip ospf netbroadcast
ISP(config-subif)#ip ospf network broadcast
ISP(config-subif)#no closure
ISP(config-subif)#exit
ISP(config)#router ospf 1
ISP(config-router)#network 35.18.40.0 0.0.0.255 region 0
ISP(config-router)#exit
ISP(config)#

C. Konfigurasi Switch

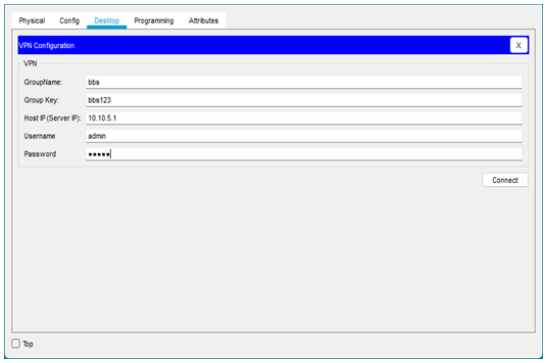
SR_Guru>enable
SR_Guru#configure terminal
Enter design orders, one for each line. End with CNTL/Z.
SR_Guru(config)#interface range fa0/1-24
SR_Guru(config-if-range)#switchport mode access
SR_Guru(config-if-range)#switchport port-security
SR_Guru(config-if-range)#switchport port-security macintosh address tacky
SR_Guru(config-if-range)#switchport port-security infringement closure
SR_Guru(config-if-range)#switchport port-security greatest 1
SR_Guru(config-if-range)#
SR_Guru(config-if-range)#!
SR_Guru#

D. Konfigurasi Server



Gambar 2 Konfigurasi Server

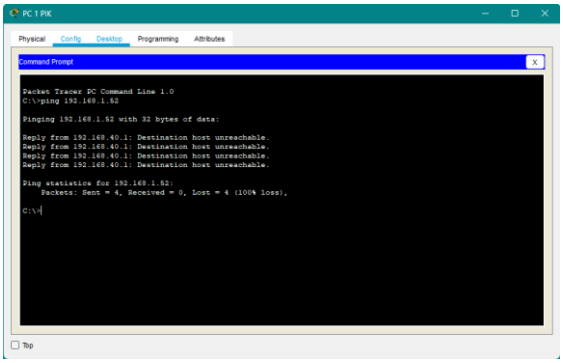
E. Konfigurasi VPN



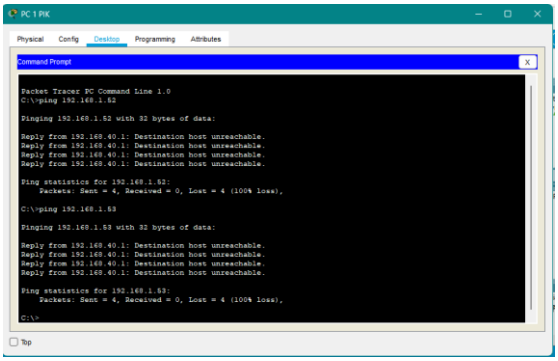
Gambar 3 Konfigurasi VPN

4.3 Pengujian Jaringan awal

Dalam penerapannya dan juga tahapan selanjutnya yang dilakukan adalah dengan melakukan konfigurasi dimana untuk menguji apakah apa yang telah di implementasikan akan berjalan secara lancar atau tidaknya maka di lakukan pengujian jaringan dengan melakukan test ping pada alamat IP yang di tuju. Apabila VPN belum terkoneksi dengan sempurna maka Test ping tidak bisa di lakukan dan akan menunjukan hasil Request Time Out atau Destination Host Unreachable. Akan tetapi apabila VPN sudah terkoneksi dengan sempurna maka hasilnya akan menunjukan Times to Live pada alamat IP yang di tuju.

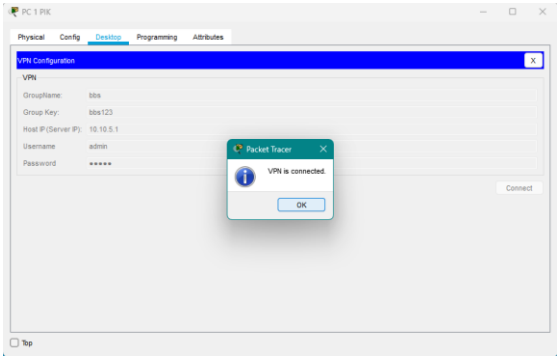


Gambar 4. Uji Test Ping Tanpa VPN Terkoneksi

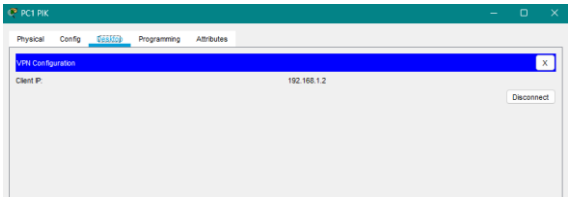


Gambar 5. Uji Test Ping Tanpa VPN Terkoneksi

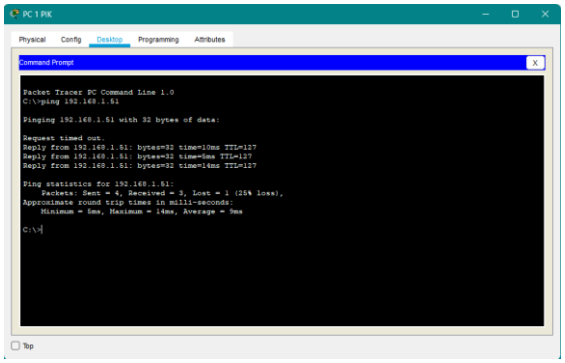
Pengujian jaringan berikutnya akan menerapkan konfigurasi VPN atau mengkoneksikan VPN untuk test ping dari PC yang ada di PIK menuju Server yang ada di Kebon Jeruk.



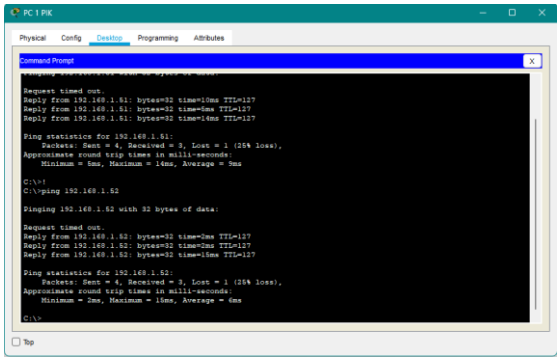
Gambar 6. VPN Terkoneksi



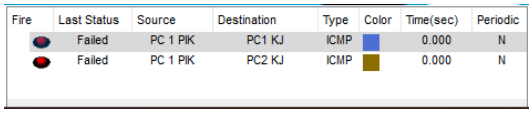
Gambar 7. Alamat Client IP VPN



Gambar 8. Uji Test Ping PC PIK ke Server KJ



Gambar 9. Test Ping PC PIK ke PC KJ



Gambar 10. Uji Kirim Pesan

Gambar 11. Uji Kirim Pesan

Pada Gambar 4 menunjukan hasil uji test ping yang dimana pada hasilnya menunjukan Destination Host Unreachable karena pada PC tersebut belum terkoneksi nya VPN maka tidak bisa mengakses alamat IP yang dituju apabila VPN belum di koneksikan

Pada Gambar 6 VPN dikoneksikan sehingga apabila jika ingin mengakses Server KJ ataupun berkomunikasi secara aman dalam jaringan diusulkan untuk mengkoneksikan VPN untuk bisa mengkakses Server ataupun PC yang ada di KJ.

Pada Gambar 8 di lakukan kembail Uji Test ping yang di lakukan di PC 1 PIK menuju alamat IP Server yang ada di KJ dengan alamat IP 192.168.1.51. apabila VPN sudah terkneksi dengan sempurna maka hasil yang di dapat dalam test ping akan menunjukan Hasil Times to Live atau lebih tepatnya seperti pada Gambar 8.

Pada Gambar 10 dilakukan test kirim pesan pada saat VPN belum terkoneksi maka hasil yang di dapat pada saat kirim pesan apabila VPN belum di koneksikan akan menunjukan Hasil Failed.

Pada Gambar 11 dilakukan kembali metode yang sama namun untuk ini VPN sudah di koneksikan sehingga pada saat VPN terkoneksi akan mendapatkan hasil Succesfull karena sudah terkoneksi dalam jaringan.

5. KESIMPULAN

Setelah membahas perihal peran jaringan komputer, penulis akan menarik kesimpulan dari semua yang telah di bahas dalam beberapa poin berikut:

1. Dengan diterapkannya sistem jaringan VPN Site-to-Site dalam sistem jaringan Bina Bangsa dapat membantu komunikasi antar kampus dapat terhubung dalam jaringan secara aman melalui metode enkripsi dan juga bisa menghemat anggaran.
2. Penerapan konfigurasi OSPF dalam sistem jaringan Sekolah Bina Bangsa PIK juga dapat membantu menjaga dan mengatur kualitas jaringan yang ada.
3. Dengan diterapkannya Switchport Security juga dapat membantu jaringan yang ada di Sekolah Bina Bangsa untuk menjaga keamanan serta memnimalisir terjadinya akses perangkat yang tidak dikenal yang di khawatirkan bisa mengakses jaringan di ruang guru secara terbuka oleh karena itu penulis menerapkan konfigurasi Switchport-security violation shutdown.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada kedua orang tua, bapak Irwan Agus Sobari yang telah membantu penelitian ini. Penulis juga mengucapkan banyak terima kasih pada Bapak pimpinan dan karyawan Sekolah Bina Bangsa PIK.

DAFTAR PUSTAKA

[1] F. Fathurrahmad and S. Yusuf, “Implementasi Jaringan VPN dengan Routing Protocol terhadap Jaringan Multiprotocol Label Switching (MPLS),” *J. JTIK (Jurnal Teknol. Inf. dan Komunikasi)*, vol. 3, no. 1, p. 29, 2019, doi: 10.35870/jtik.v3i1.83.

[2] T. B. Septiandoko, D. Desmulyati, and A. Taufik, “Implementasi Jaringan Internet Site To Site VPN Dengan Metode IPSec Pada PT Telkom Akses,” *Comput. Sci.*, vol. 1, no. 1, pp. 18–26, 2021, doi: 10.31294/coscience.v1i1.138.

[3] M. Alparisi, I. D. Irawati, and M. Iqbal, "Implementasi Jaringan Menggunakan Routing Protocol Ospf (open Shrotest Path First) Dan Mpls (multi Protocol Label Switch) Dengan Redudansi Hsrp," *eProceedings …*, vol. 6, no. 2, pp. 3786–3795, 2020.

[4] (2016) Andi & MADCOMS, *Manajemen Sistem Jaringan Komputer dengan Router Mikrotik*. Yogyakarta: ANDI, 2016.

[5] A. Indrajaya, *CISCO Kung Fu Jurus-Jurus Routing*. Jasakom., 12638BC.

[6] D. A. Pangestu, A. S. Budiman, and S. Sartini, "Rancangan Site-To-Site Vpn Dengan Pptp Pada Interkoneksi Antar Kantor Pt. Indosis Integrasi," *semanTIK*, vol. 8, no. 1, p. 1, 2022, doi: 10.55679/semantik.v8i1.9189.

[7] H. Pratama and N. F. Puspitasari, "Penerapan Protokol L2TP/IPSec dan Port Forwarding untuk Remote Mikrotik pada Jaringan Dynamic IP," *Creat. Inf. Technol. J.*, vol. 7, no. 1, p. 51, 2021, doi: 10.24076/citec.2020v7i1.253.

[8] F. Firmansyah, M. Wahyudi, and R. A. Purnama, "Analisis Performa Site to Site IP Security Virtual Private Network (VPN) Menggunakan Algoritma Enkripsi ISAKMP," *JUITA J. Inform.*, vol. 7, no. 2, p. 129, 2019, doi: 10.30595/juita.v7i2.4491.

[9] F. Setiawan, F. S. Chaniago, and A. Wibowo, "IMPLEMENTASI SSL VPN (SECURE SOCKET LAYER VIRTUAL PRIVATE NETWORK) PADA BADAN BANK TANAH," *J. Syntax IDEA*, vol. 6, no. 1, pp. 1–23, 2024.

[10] F. Triyansa and I. A. Sobari, "Implementasi Jaringan VPN Menggunakan L2TP Dengan IP Sec Pada PT Datindo Infonet Prima," *Comput. Sci.*, vol. 2, no. 2, pp. 82–89, 2022, doi: 10.31294/coscience.v2i2.1168.

[11] C. K. A. Riski, "Komparasi Protokol Virtual Private Network (Vpn) Pada Metode Pptp, L2tp, Sstp, Dan Openvpn," *Komparasi Protok. Virtual Priv. Netw. Pada Metod. Pptp, L2tp, Sstp, Dan Openvpn*, pp. 1–63, 2021.

[12] N. I. Febriyanto and I. A. Sobari, "Perancangan Jaringan Vpn Menggunakan Protokol L2Tp+Ipsec Sebagai Media Transmisi Data Pada Yayasan Sirajul Falah Indonesia," *J. Inform. dan Tek. Elektro Terap.*, vol. 12, no. 1, pp. 275–281, 2024, doi: 10.23960/jitet.v12i1.3703.