Implementasi Customer User Group Menggunakan Metode EOIP Tunnel dan IP Tunnel Untuk Sharing Data Dari Kantor Pusat Ke Kantor Cabang PT Xyz

TUGAS AKHIR

SYIFA AFIFAH NURDIEN
41517110119

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2022

http://digilib.mercubuana.ac.id/

Implementasi Customer User Group Menggunakan Metode EOIP Tunnel dan IP Tunnel Untuk Sharing Data Dari Kantor Pusat Ke Kantor Cabang PT Xyz

Tugas Akhir

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh:

SYIFA AFIFAH NURDIEN
41517110119

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2022

http://digilib.mercubuana.ac.id/

LEMBAR PERNYATAAN ORISINALITAS

LEMBAR PERNYATAAN ORISINALITAS

Yang bertanda tangan dibawah ini:

NIM	:	41517110119
Nama	:	Syifa Afifah Nurdien
Judul Tugas Akhir	:	Implementasi Customer User Group Menggunakan Metode EOIP Tunnel dan IP Tunnel Untuk Sharing Data Dari Kantor Pusat Ke Kantor Cabang PT Xyz

Menyatakan bahwa Laporan Tugas Akhir saya adalah hasil karya sendiri dan bukan plagiat. Apabila ternyata ditemukan didalam laporan Tugas Akhir saya terdapat unsur plagiat, maka saya siap untuk mendapatkan sanksi akademik yang terkait dengan hal tersebut.

Jakarta, 3 April 2022

(Syifa Afifah Nurdien)

UNIVERSITAS
MERCU BUANA

ii

http://digilib.mercubuana.ac.id/

SURAT PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR

Sebagai mahasiswa Universitas Mercu Buana, saya yang bertanda tangan di bawah ini :

Nama Mahasiswa	:	Syifa Afifah Nurdien
NIM	:	41517110119
Judul Tugas Akhir	:	Implementasi Customer User Group Menggunakan Metode EOIP Tunnel dan IP Tunnel Untuk Sharing Data Dari Kantor Pusat Ke Kantor Cabang PT Xyz

Dengan ini memberikan izin dan menyetujui untuk memberikan kepada Universitas Mercu Buana **Hak Bebas Royalti Noneksklusif** (*None-exclusive Royalty Free Right*) atas karya ilmiah saya yang berjudul diatas beserta perangkat yang ada (jika diperlukan).

Dengan Hak Bebas Royalti/Noneksklusif ini Universitas Mercu Buana berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat dan mempublikasikan tugas akhir saya.

Selain itu, demi pengembangan ilmu pengetahuan di lingkungan Universitas Mercu Buana, saya memberikan izin kepada Peneliti di Lab Riset Fakultas Ilmu Komputer, Universitas Mercu Buana untuk menggunakan dan mengembangkan hasil riset yang ada dalam tugas akhir untuk kepentingan riset dan publikasi selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Jakarta, 1 Agustus 2022

(Syifa Afifah Nurdien)

http://digilib.mercubuana.ac.id/

SURAT PERNYATAAN LUARAN TUGAS AKHIR

SURAT PERNYATAAN LUARAN TUGAS AKHIR

Sebagai mahasiswa Universitas Mercu Buana, saya yang bertanda tangan di bawah ini :

Nama Mahasiswa	:	Syifa Afifah Nurdien
NIM	:	41517110119
Judul Tugas Akhir	:	Implementasi Customer User Group Menggunakan Metode EOIP Tunnel dan IP Tunnel Untuk Sharing Data Dari Kantor Pusat Ke Kantor Cabang PT Xyz

Menyatakan bahwa :

1. Luaran Tugas Akhir saya adalah sebagai berikut :

No	Luaran	Jenis		Status	
1	Publikasi Ilmiah	Jurnal Nasional Tidak Terakreditasi		Diajukan	✓
		Jurnal Nasional Terakreditasi	✓		
		Jurnal International Tidak Bereputasi		Diterima	
		Jurnal International Bereputasi			
	Disubmit/dipublikasikan di :	Nama Jurnal	: Jurnal Teknologi dan Sistem Komputer		
		ISSN	: 2338-0403		
		Link Jurnal	:https://jtsiskom.undip.ac.id/author/submission/14540		
		Link File Jurnal Jika Sudah di Publish	:		

2. Bersedia untuk menyelesaikan seluruh proses publikasi artikel mulai dari submit, revisi artikel sampai dengan dinyatakan dapat diterbitkan pada jurnal yang dituju.
3. Diminta untuk melampirkan scan KTP dan Surat Pernyataan (Lihat Lampiran Dokumen HKI), untuk kepentingan pendaftaran HKI apabila diperlukan

Demikian pernyataan ini saya buat dengan sebenarnya.

Jakarta, 1 Agustus 2022

(Syifa Afifah Nurdien)

http://digilib.mercubuana.ac.id/

LEMBAR PERSETUJUAN PENGUJI

NIM	:	41517110119
Nama	:	Syifa Afifah Nurdien
Judul Tugas Akhir	:	Implementasi Customer User Group Menggunakan Metode EOIP Tunnel dan IP Tunnel Untuk Sharing Data Dari Kantor Pusat Ke Kantor Cabang PT Xyz

Tugas Akhir ini telah diperiksa dan disidangkan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana.

Jakarta, 28 Juli 2022

(Sabar Rudiarto, M.Kom)

UNIVERSITAS MERCU BUANA

http://digilib.mercubuana.ac.id/

LEMBAR PERSETUJUAN PENGUJI

NIM	:	41517110119
Nama	:	Syifa Afifah Nurdien
Judul Tugas Akhir	:	Implementasi Customer User Group Menggunakan Metode EOIP Tunnel dan IP Tunnel Untuk Sharing Data Dari Kantor Pusat Ke Kantor Cabang PT Xyz

Tugas Akhir ini telah diperiksa dan disidangkan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana.

Jakarta, 28 Juli 2022

(Afiyati, S.Si, MT)

UNIVERSITAS MERCU BUANA

http://digilib.mercubuana.ac.id/

LEMBAR PERSETUJUAN PENGUJI

NIM	:	41517110119
Nama	:	Syifa Afifah Nurdien
Judul Tugas Akhir	:	Implementasi Customer User Group Menggunakan Metode EOIP Tunnel dan IP Tunnel Untuk Sharing Data Dari Kantor Pusat Ke Kantor Cabang PT Xyz

Tugas Akhir ini telah diperiksa dan disidangkan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana.

Jakarta, 28 Juli 2022

(Wawan Gunawan, S.Kom, MT)

UNIVERSITAS
MERCU BUANA

http://digilib.mercubuana.ac.id/

LEMBAR PENGESAHAN

LEMBAR PENGESAHAN

NIM : 41517110119

Nama : Syifa Afifah Murden

Judul Tugas Akhir : Implementasi Customer User Group Menggunakan Metode EOIP Tunnel dan IP Tunnel Untuk Sharing Data Dari Kantor Pusat ke Kantor Cabang PT. xyz

Tugas Akhir ini telah diperiksa dan disidangkan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana.

Jakarta,

Menyetujui,

(Dr. Harwikarya, MT)
Dosen Pembimbing

UNIVERSITAS
MERCU BUANA

Mengetahui,

(Wawan Gunawan, S.Kom, MT)
Koord. Tugas Akhir Teknik Informatika

(Ir. Emil R. Kaburuan, Ph.D., IPM.)
Ka. Prodi Teknik Informatika

http://digilib.mercubuana.ac.id/

KATA PENGANTAR

Puji syukur kita panjatkan Puji Syukur penulis panjatkan kepada Allah swt., karena atas karunia yang telah diberikan kepada penulis sehingga penulis dapat menyelesaikan Laporan Tugas Akhir tepat waktu, dimana Laporan Tugas Akhir ini merupakan salah satu persyaratan untuk dapat menyelesaikan Program Studi Strata Satu (S1) pada Jurusan Teknik Informatika Universitas Mercu Buana.

Penulis menyadari bahwa Laporan Tugas Akhir ini masih belum dapat dikatakan sempurna. Karena itu, kritikan dan saran yang membangun sangat penulis harapkan demi sem purnanya laporan ini kedepan. Penulis juga menyadari bahwa Laporan Tugas Akhir ini tidak dapat selesai tepat pada waktunya tanpa bantuan, bimbingan, dan motivasi dari berbagai pihak. Ucapan terima kasih ini penulis tujukan kepada:

1. Bapak Dr. Harwikarya, MT selaku Dosen Pembimbing Tugas Akhir yang telah membimbing penulis dengan semua nasihat, semangat dan ilmunya dalam menyusun laporan tugas akhir ini.
2. Bapak Ir. Emil R. Kaburuan, Ph.D., IPM selaku Kepala Program Studi Informatika Universitas Mercu Buana.
3. Bapak Wawan Gunawan, S.Kom., MT selaku Koordinator Tugas Akhir Teknik Informatika Universitas Mercu Buana.
4. Kedua orang tua yang selama ini telah membesarkan penulis.
5. Keluarga, teman-teman serta semua pihak yang telah memotivasi dan ikut memberikan bantuannya kepada penulis yang namanya tidak dapat penulis sebutkan satu per satu

Akhir kata, penulis berharap semoga Allah swt. membalas kebaikan yang telah diberikan kepada penulis dan penulis berharap semoga laporan tugas akhir ini bermanfaat bagi kita semua. Amin

Jakarta, 03 April 2022
Penulis

http://digilib.mercubuana.ac.id/

DAFTAR ISI

UNIVERSITAS MERCU BUANA

http://digilib.mercubuana.ac.id/

NASKAH JURNAL

Implementasi Customer User Group Menggunakan Metode EOIP Tunnel dan IP Tunnel Untuk Sharing Data Dari Kantor Pusat Ke Kantor Cabang PT Xyz

Implementation of Customer User Group Using EOIP Tunnel and IP Tunnel Methods for Sharing Data from Head Office to Branch Offices at PT Xyz

Syifa Afifah Nurdien [*1)], Harwikarya [2)]

[1,2)] *Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana, Jl. Meruya Selatan No. 1, Kembangan, Jakarta Barat, Indonesia 11650*

How to cite: S. A. Nurdien and Harwikarya, " Implementasi Customer User Group Menggunakan Metode EOIP Tunnel dan IP Tunnel Untuk Sharing Data Dari Kantor Pusat Ke Kantor Cabang PT Xyz" *Jurnal Teknologi dan Sistem Komputer*, vol. 9, no. x, pp. xx-xx, 2021. doi: 10.14710/jtsiskom.2022.xxxxx [Online].

Abstract *– The development of technology that is growing every day makes the internet as one of the important things. Likewise, companies that really need a stable and secure internet in exchanging data between the head office and branch offices. However, in practice sometimes some problems are found, some of which are latency stability and security in data exchange. Seeing the problems mentioned earlier, the authors propose to design a Custoner User Group using the EOIP Tunnel and IP Tunnel Methods for Sharing Data. With the IP Tunnel and EoIP Tunnel methods, it becomes easy to connect the branch office network to the head office network and protect data security. From the results of implementation testing by ping experiments with the default size, size 1000, size 1400 and by adding the IPsec security component it runs smoothly. However, the ping experiment with size 1500 experienced RTO (request time out) due to MTU (Maximum Transmission Unit) which was not supported on the switch device.*

Keywords *– Customer User Group, EOIP Tunnel, IP Tunnel*

Abstrak *– Perkembangan teknologi yang semakin berkembang setiap harinya menjadikan internet sebagai salah satu hal yang penting. Begitu pula dengan perusahaan yang sangat membutuhkan internet yang stabil dan aman dalam melakukan pertukaran data antar kantor pusat ke kantor cabang. Namun dalam prakteknya terkadang ditemukan beberapa masalah beberapa diantaranya adalah stabilitas latency dan keamanan dalam pertukaran data. Melihat masalah yang disebutkan tadi, maka penulis mengusulkan untuk merancang Custoner User Group menggunakan Metode EOIP Tunnel dan IP Tunnel Untuk Sharing Data. Dengan metode IP Tunnel dan EoIP Tunnel menjadi mudah dalam menghubungkan jaringan kantor cabang ke jaringan kantor pusat dan keamanan data terlidungi. Dari hasil pengujian implementasi dengan percobaan ping dengan default size, size 1000, size 1400 dengan dan atau tanpa menambahkan komponen keamanan IPsec berjalan dengan lancer. Namun pada percobaan ping dengan size 1500 mengalami RTO (request time out) dikarenakan MTU (Maximum Transmission Unit) yang tidak didukung pada perangkat switch.*

Kata kunci *– Customer User Group, EOIP Tunnel, IP Tunnel.*

[*)] Corresponding author (Syifa Afifah Nurdien)
Email: 41517110119@student.mercubuana.ac.id

I. PENDAHULUAN

Semakin berkembangnya teknologi internet saat ini menjadikan kebutuhan akan koneksi internet yang cepat dan stabil sebagai hal yang sangat penting [1]. Sharing data antar kantor pusat dengan kantor cabang dapat menjadi masalah yang sangat penting dalam suatu komunikasi data. Hal ini harus diperhatikan oleh setiap perusahaan dalam melakukan kegiatan komunikasi di dunia internet, sehingga kerahasiaan informasi suatu perusahaan dapat terjaga dengan baik [2].

PT Xyz merupakan perusahaan yang bergerak di bidang telekomunikasi dengan kantor pusat berada di Jakarta Pusat serta kantor cabang yang tersebar di Jakarta Barat dan Jakarta Selatan. Sebelumnya PT Xyz masih mengandalkan layanan Google (Gmail & Google Drive) untuk kebutuhan sharing data. PT Xyz menginginkan jaringan interkoneksi sendiri yang akan menggantikan layanan Google dalam sharing data.

Pada umumnya terdapat beberapa pilihan media dalam pembuatan jaringan interkoneksi mulai dari kabel fiber optic, radio, ataupun VSAT. Namun dalam pembuatan jalur tersebut membutuhkan banyak biaya

Copyright ©2021, The authors. Published by Department of Computer Engineering, Universitas Diponegoro
Submitted: 27 January 2021; Revised: 7 July 2021; Accepted: 10 August 2021; Published: 31 October 2021
http://digilib.mercubuana.ac.id/

terlebih apabila jarak antar cabang sangat jauh seperti antar kota, provinsi atau bahkan negara. Solusi lainnya adalah dapat menyewa saluran point to point dengan menggunakan media transmisi, namun hal tersebut juga dapat menghabiskan biaya [1]

Penelitian ini akan menerapkan *Server Private* dengan beberapa metode *tunneling*. Dengan *Server Private* karyawan atau staff di kantor pusat dan kantor cabang dapat saling berkomunikasi dan dapat sharing data melalui *Server Private* dengan jaringan lokal kantor pusat dan kantor cabang melalui internet yang bersifat private yang lebih dikenal dengan *Virtual Private Network* (VPN) [2]–[4].

Penelitian kali ini akan berfokus pada percobaan implementasi *customer user group* menggunakan metode tunneling yaitu dengan membangun jaringan privat diatas jaringan publik.

Metode *tunneling* memiliki beragam jenis yang masing-masing memiliki kelebihan dan kekurangannya sehingga dapat digunakan sesuai kebutuhan [5].

EOIP (*Ethernet Over IP*). EOIP adalah Mikrotik RouterOS *protocol* yang memanfaatkan jalur koneksi internet untuk membangun koneksi bridging ethernet antar router yang membuat kedua jaringan yang berbeda seolah-olah berada pada satu lingkup yang privat [1].

Salah satu jenis *protocol* yang digunakan dalam IPV4 adalah IPIP (IP in IP). Cara kerja IPIP tunnel adalah dengan mengenkapsulasi paket IP didalam paket IP lainnya dengan cara header terluar ditambahkan alamat sumber, IP masuk tunnel dan IP tujuan, IP keluar tunnel [6].

IP Sec (Internet Protocol Security) adalah sekumpulan standar dan protokol yang bertujuan untuk menyediakan keamanan dan kerahasiaan dalam pertukaran data di layer network [7]. IPSec menawarkan 3 layanan utama, yaitu otentikasi dan integritas data, kerahasiaan, dan manajemen kunci [8].

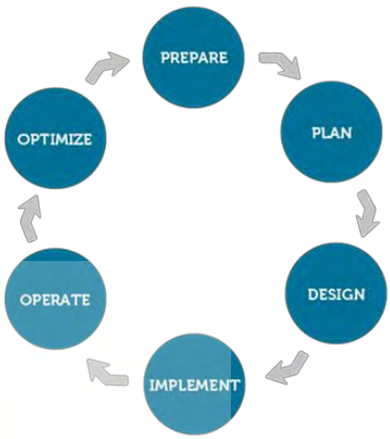
Berdasarkan penelitian yang dilakukan Kavita Rani, Avinash Jethi yang membahas implementasi dan Analisa IP Tunnel pada VPN (*Virtual Private Network*) menyatakan VPN menghasilkan enkripsi dan dekripsi data yang aman dengan bantuan IP tunneling di *end point*. Pada dasarnya VPN merutekan melalui internet dari jaringan pribadi untuk mentransfer data dari sumber ke tujuan [9].

Pada penelitian lainnya membahas penggunaan jaringan VPN untuk transmisi sinyal pada jaringan perusahaan menyatakan untuk membangun jaringan perusahaan disarankan untuk menggunakan teknologi VPN yang memungkinkan terpenuhinya dasar persyaratan untuk keamanan dan kualitas layanan dan aplikasi [2].

Perbedaan penelitian ini dengan penelitian sebelumnya adalah melakukan implementasi customer user group dengan menggabungkan dua metode yaitu EOIP (*Ethernet Over Ip*) tunnel dan juga IP tunnel dan akan dilakukan pengujian menggunakan tools ping *Windows Server* dengan default size, size 1000, size 1400 dengan dan atau tanpa menambahkan komponen keamanan IP Sec (*Internet Protocol Security*) yang diharapkan dapat melindungi data yang akan dikirimkan sehingga mengurangi resiko data tersebar [5].

III. METODE PENELITIAN

Pada penelitian ini merupakan jenis penelitian kualitatif dan metode penelitian yang digunakan yaitu studi kasus. Dalam penelitian ini, penulis menggunakan metode perancangan jaringan PPDIOO (Prepare, Plan, Design, Implement, Operate and Optimize). Metode ini merupakan metode yang diterapkan oleh Cisco untuk mendukung jaringan berkembang [9], [11].



Gambar 1. Metode PPDIOO

A. Prepare

Prepare merupakan tahapan awal dalam penelitian untuk melakukan rencana kerja yang berhubungan dengan analisa pokok pembahasan, seperti masalah yang dihadapi, topologi jaringan yang akan dibangun, dan kebutuhan dari sisi hardware maupun software [11], [12]. Data perangkat serta spesifikasinya dirangkum pada Tabel 2 dan Tabel 3.

Tabel 1 Kebutuhan Perangkat Keras/Hardware.

No	Deskripsi	Spesifikasi
1	Laptop	Lenovo, Intel Core i5, RAM 8GB
2	PC	Lenovo ThinkStation P320, Intel Core i7, RAM 8GB
3	Router	RB1100AHx2
4	Switch	

Tabel 2 Kebutuhan Perangkat Lunak/Software

No	Deskripsi	Spesifikasi
1	Sistem operasi Laptop	Windows 10, 64-bit
2	Sistem operasi PC	Windows 10, 64-bit
3	Sistem operasi Router	Winbox v3.1.9
4	Aplikasi GNS3	v.2.2.0

http://digilib.mercubuana.ac.id/

Copyright ©2021, The authors. Published by Department of Computer Engineering, Universitas Diponegoro
Submitted: 27 January 2021; Revised: 7 July 2021; Accepted: 10 August 2021; Published: 31 October 2021

5	Aplikasi Oracle VM Virtual Box	v6.0.10

B. Plan

Plan adalah tahapan perencanaan jaringan untuk mengidentifikasi persyaratan jaringan yang sesuai dengan kebutuhan, tujuan dan fasilitas dalam proses penelitian [11].

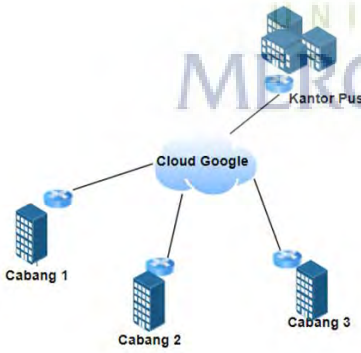
Alur perancangan penelitian yang dimulai dengan membuat design topologi untuk kantor pusat dan kantor cabang. Kemudian dilanjutkan dengan instalasi perangkat pada kantor pusat dan kantor cabang. Kebutuhan untuk proses instalasi telah dirangkun pada tabel 1 dan tabel 2. Selanjutnya melakukan konfigurasi arsitektur jaringan di kantor pusat dan juga pada kantor cabang.

Selanjutnya dilakukan tahap pengujian menggunakan metode test tools bandwith test dengan ping sebanyak 1000 kali dengan beban 1500 dari Server Private ke PC Cabang dan pengujian dilakukan dengan menambahkan komponen keamanan IPSec. Setelah selesai maka dilakukan analisa hasil dan membuat kesimpulan.

C. Design

Topologi Kantor yang sedang berjalan

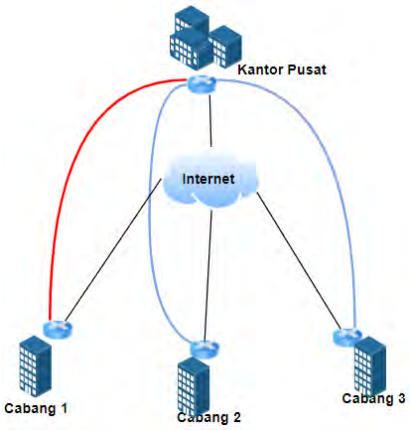
Pada topologi yang sedang berjalan pada kantor pusat dan kantor cabang PT Xyz untuk sharing data menggunakan layanan google dengan koneksi internet Seperti pada gambar 3 berikut.



Gambar 2 Topologi kantor yang sedang berjalan

Topologi yang diusulkan

Pada topologi yang di usulkan ini sudah menerapkan VPN menggunakan metrode EoIP Tunnel dan IP Tunnel untuk sharing data ke server private dengan jaringan lokal pada setiap kantor. Terlihat pada gambar 4 di bawah terbentuk terowongan tunnel dengan warna merah menggunakan metode IP Tunnel dan warna biru menggunakan EoIP Tunnel.



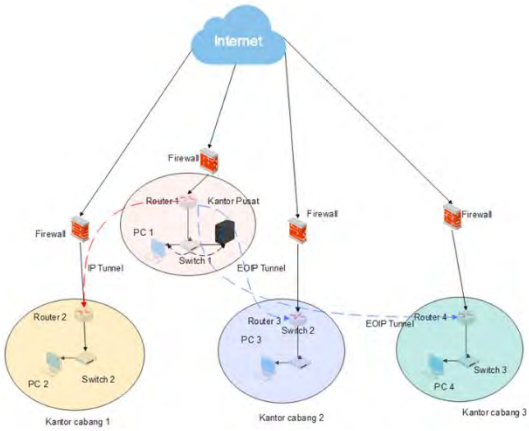
Gambar 3 Topologi kantor yang diusulkan

D. Implement

Pada tahap ini melakukan implementasi sesuai dengan perencanaan dan design topologi yang sudah dibuat. Tahapan tersebut dimulai dari instalasi perangkat pada tools GNS3 yang di dalamnya akan di gunakanan perangkat Router, Switch unmanage, PC dan Server, melakukan konfigurasi Customer User Group Menggunakan Metode EOIP Tunnel dan IP Tunnel serta melakukan pengujian menggunakan metode test tools bandwith test dengan ping sebanyak 1000 kali dengan beban 1500 dari Server Private ke PC Cabang. Dan menambahkan komponen keamanan IPSec.

E. Operate

Tahapan ini melakukan percobaan skenario yang telah disiapkan. Dalam implementasi ini penulis akan mengunakan 3 buah Router, 3 buah swicth, 3 buah PC dan 1 Server yang akan di alokasikan di kantor pusat dan kantor cabang. Metode Eoip Tunnel dan IP Tunnel akan terbentuk di atas jaringan Internet Service Provide (ISP), berikut desain topologi Eoip Tunnel dan IP Tunnel (IPIP).

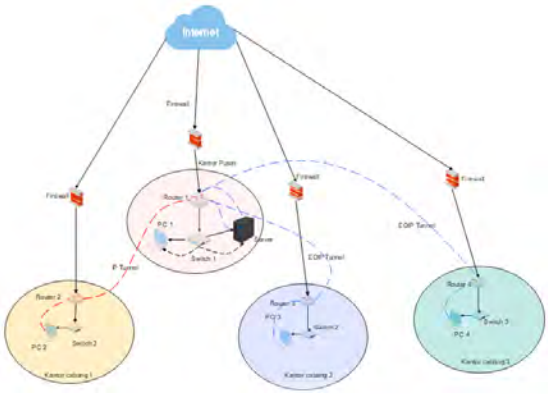


Gambar 4 Topologi EOIP Tunnel & IP Tunnel

Pada gambar 4 terdapat sebuah garis warna merah dari router 2 ke router 1 dimana garis tersebut melewati jaringan internet dan membentuk sebuah terowongan (Tunneling) dengan metode IP Tunnel (IPIP), sedangkan pada garis berwarna biru dari router 3 ke router 1 dan dari router 4 ke router 1 dimana akan membentuk

Copyright ©2021, The authors. Published by Department of Computer Engineering, Universitas Diponegoro
Submitted: 27 January 2021; Revised: 7 July 2021; Accepted: 10 August 2021; Published: 31 October 2021
http://digilib.mercubuana.ac.id/

teroworngan (Tunneling) dengan metode EoIP Tunnel. Pada kedua metode tersebut untuk dapat berkomunikasi ke kantor pusat menggunakan IP point to point tunneling, selanjutnya IP point to point tersebut akan di routing ke segment LAN private setiap kantor agar bisa saling berkomunikasi dan terlebih berkomunikasi ke server private. Berikut desain topologi komunikasi kantor cabang ke server private.



Gambar 5 Topologi Tunnel Akses ke Server Private di Kantor Pusat.

Pada gambar 9 menjelaskan bagaimana tahapan PC di setiap kantor bisa

saling berkomunikasi dengan server private kantor pusat. Berikut uraiannya :

1. Pada PC 1 di kantor pusat untuk berkomunikasi dengan server private hanya melalui segment kantor pusat atau hanya melalui switch 1.
2. Pada PC 2 yang berada di kantor cabang 1 untuk berkomunikasi ke server private melalui service Internet dengan jalur IP Tunnel (IPIP), terlihat pada gambar diatas ada sebuah garis merah putus – putus yang mengarah ke server private. Berikut uraian rute yang di lalui :
   a. PC 2 ke Router 2 melalui LAN segmentasi kantor cabang 1.
   b. Router 2 ke Router 1 memalui service internet dengan jalur IP Tunnel (IPIP)
   c. Router 1 ke Server Private melalui LAN segmentasi kantor pusat.
3. Pada PC 3 yang berada di kantor cabang 2 untuk berkomunikasi ke server private melalui service Internet dengan jalur EoIP Tunnel, terlihat pada gambar diatas ada sebuah garis biru putus – putus yang mengarah ke server private. Berikut uraian rute yang di lalui :
   a. PC 3 ke Router 3 melalui LAN segmentasi kantor cabang 2.
   b. Router 3 ke Router 1 memalui service internet dengan jalur EoIP Tunnel.
   c. Router 1 ke Server Private melalui LAN segmentasi kantor pusat.
4. Pada PC 4 yang berada di kantor cabang 3 untuk berkomunikasi ke server private melalui service Internet dengan jalur EoIP Tunnel, terlihat pada gambar diatas ada sebuah garis biru putus – putus yang mengarah ke server private. Berikut uraian rute yang di lalui :
   a. PC 4 ke Router 4 melalui LAN segmentasi kantor cabang 3.
   b. Router 4 ke Router 1 memalui service internet dengan jalur EoIP Tunnel.
   c. Router 1 ke Server Private melalui LAN segmentasi kantor pusat.

Pengalamatan IP Address

Tabel 3 Pengalamatan IP Address

Perangkat	*Interface*	IP *Address*	Deskripsi
Router 1	Ethernet 1	192.168.137.10/24	Ke WAN ISP
	Ethernet 2	172.16.10.1/24	Ke Switch 1 (Lan)
	IP Tunnel To cabang 1	172.10.20.1/30	Tunnel Cabang 1
	Eoip to Cabang 2	172.10.10.1/30	Tunnel ke Cabang 2
	Eoip to Cabang 3	172.10.30.1/30	Tunnel ke Cabang 3
Router 2	Ethernet 1	192.168.137.20/24	Ke WAN ISP
	Ethernet 2	172.16.20.1/24	Ke Switch 2 (Lan)
	IP Tunnel to Kantor Pusat	172.10.20.2/30	Tunnel Kantor Pusat
Router 3	Ethernet 1	192.168.137.30/24	Ke WAN ISP
	Ethernet 2	172.16.30.1/24	Ke Switch 3 (Lan)
	EoIP to Kantor Pusat	172.10.10.2/30	Tunnel Kantor Pusat
Router 4	Ethernet 1	192.168.137.40/24	Ke WAN ISP
	Ethernet 2	172.16.40.1/24	Ke Switch 4 (Lan)
	EoIP to Kantor Pusat	172.10.30.2/30	Tunnel Kantor Pusat
PC 1	DHCP IP	-	User
PC 2	DHCP IP	-	User
PC 3	DHCP IP	-	User

Copyright ©2021, The authors. Published by Department of Computer Engineering, Universitas Diponegoro
http://digilib.mercubuana.ac.id/
Submitted: 27 January 2021; Revised: 7 July 2021; Accepted: 10 August 2021; Published: 31 October 2021

PC 4	DHCP IP	-	User
Server	Static IP	10.10.10.10/24	Server Private

Konfigurasi

Berkut adalah uraian Langkah-langkah dalam mengkonfigurasi mulai dari kantor pusat, kantor cabang 1, kantor cabang 2, dan kantor cabang 3.

Tabel 4 Konfigurasi

No	Aktivitas	Keterangan
1	Konfigurasi Internet Router 1	Membuat koneksi internet di kantor pusat
2	Konfigurasi Internet Router 2	Membuat koneksi internet di kantor cabang 1
3	Konfigurasi Internet Router 3	Membuat koneksi internet di kantor cabang 2
4	Konfigurasi Internet Router 4	Membuat koneksi internet di kantor cabang 3
5	Konfigurasi IP Tunnel Router 2	Membuat Tunneling ip to ip pada kantor cabang 1
6	Konfigurasi IP Tunnel Router 1	Membuat Tunneling ip to ip pada kantor pusat
7	Konfigurasi EoIP Tunnel Router 1	Membuat Tunneling dengan EoIP pada kantor pusat
8	Konfigurasi EoIP Tunnel Router 3	Membuat Tunneling dengan EoIP pada kantor cabang 2
9	Konfigurasi EoIP Tunnel Router 4	Membuat Tunneling dengan EoIP pada kantor cabang 3

Tahapan Eksperimen

Langkah pertama adalah dengan Membuat koneksi internet di kantor pusat dengan melakukan konfigurasi internet pada router 1. Kemudian Membuat koneksi internet di kantor cabang 1 dengan melakukan konfigurasi internet pada router 2. Lalu Membuat koneksi internet di kantor cabang 2 dengan melakukan konfigurasi internet pada router 3. Lalu Membuat koneksi internet di kantor cabang 3 dengan melakukan konfugurasi internet pada router 4.

Selanjutnya adalah Membuat Tunneling ip to ip pada kantor cabang 1 dengan Konfigurasi IP Tunnel Router 2. Kemudian Membuat Tunneling ip to ip pada kantor pusat dengan Konfigurasi IP Tunnel Router 1. Lalu Membuat Tunneling dengan EoIP pada kantor pusat dengan Konfigurasi EoIP Tunnel Router 1. Kemudian Membuat Tunneling dengan EoIP pada kantor cabang 2 dengan Konfigurasi EoIP Tunnel Router 3. Dan yang terakhir Membuat Tunneling dengan EoIP pada kantor cabang 3 dengan Konfigurasi EoIP Tunnel Router 4.

Setelah implementasi pada kantor pusat dan kantor-kantor cabang berhasil berjalan maka akan lanjut pada tahap pengujian untuk mendapatkan perbandingan stabilitas latency tanpa ip sec dan dengan ip sec pada IP Tunnel dan EoIP Tunnel. Pengujian akan dilakukan melalui tools ping Windows Server. Pengujian dengan tools ping dilakukan dengan 8 tahap pengujian :

1. Ping tanpa beban dan tidak menggunakan ip sec.
2. Ping tanpa beban dan menggunakan ip sec.
3. Ping dengan beban 1000 dan tidak menggunakan ip sec.
4. Ping dengan beban 1000 dan menggunakan ip sec.
5. Ping dengan beban 1400 dan tidak menggunakan ip sec.
6. Ping dengan beban 1400 dan menggunakan ip sec.
7. Ping dengan beban 1500 dan tidak menggunakan ip sec.
8. Ping dengan beban 1500 dan menggunakan ip sec.

III. HASIL DAN PEMBAHASAN

Setelah implementasi pada kantor pusat dan kantor cabang berhasil berjalan maka akan lanjut pada tahap pengujian untuk mendapatkan perbandingan stabilitas latency tanpa ip sec dan dengan ip sec pada IP Tunnel dan EoIP Tunnel. Pengujian akan dilakukan melalui tools ping Windows Server.

A. Pengujian melalui PING

Pengujian ini dilakukan dari *Server Private* berbasis OS Windows Server ke PC Cabang 1. Cabang 2 dan Cabang 3 dengan ping tanpa beban dan menggunakan beban dari 1000, 1400 dan 1500 untuk mengetahui gambaran stabilitas *latency* menggunakan IP Sec dan tanpa IP Sec pada metode IP *Tunnel* dan juga EOIP *Tunnel*.

1. Ping tanpa beban dan tidak menggunakan ip sec.
   A. Ping tanpa beban dan tidak menggunakan ip sec server ke PC kantor cabang 1. Hasil pengujian tanpa beban dan tidak menggunakan ip sec dari server ke PC kantor cabang 1 lancar dan stabil dengan 0 *packet loss* dan *average* 3ms
   B. Ping tanpa beban dan tidak menggunakan ip sec server ke PC kantor cabang 2. Hasil pengujian tanpa beban dan tidak menggunakan ip sec dari server ke PC kantor cabang 2 lancar dan stabil dengan 0 packet loss dan average 3ms
   C. Ping tanpa beban dan tidak menggunakan ip sec server ke PC kantor cabang 3. Hasil pengujian tanpa beban dan tidak menggunakan ip sec dari server ke PC kantor cabang 3 lancar dan stabil dengan 0 packet loss dan average 3ms
2. Ping tanpa beban dan menggunakan ip sec.
   A. Ping tanpa beban dan menggunakan ip sec server ke PC kantor cabang 1. Hasil pengujian tanpa beban dan menggunakan ip sec dari server ke PC kantor cabang 1 lancar dan stabil dengan 0 packet loss dan average 3ms.
   B. Ping tanpa beban dan menggunakan ip sec server ke PC kantor cabang 2. Hasil

UNIVERSITAS MERCU BUANA

http://digilib.mercubuana.ac.id/

Copyright ©2021, The authors. Published by Department of Computer Engineering, Universitas Diponegoro
Submitted: 27 January 2021; Revised: 7 July 2021; Accepted: 10 August 2021; Published: 31 October 2021

pengujian tanpa beban dan menggunakan ip sec dari server ke PC kantor cabang 2 lancar dan stabil dengan 0 packet loss dan average 3ms.

C. Ping tanpa beban dan menggunakan ip sec server ke PC kantor cabang 3. Hasil pengujian tanpa beban dan menggunakan ip sec dari server ke PC kantor cabang 3 lancar dan stabil dengan 0 packet loss dan average 3ms.

3. Ping dengan beban 1000 dan tidak menggunakan ip sec.
   A. Ping dengan beban 1000 dan tidak menggunakan ip sec server ke PC kantor cabang 1. Hasil pengujian ping dengan beban 1000 dan tidak menggunakan ip sec dari server ke PC kantor cabang 1 lancar dan stabil dengan 0 packet loss dan average 3ms.
   B. Ping dengan beban 1000 dan tidak menggunakan ip sec server ke PC kantor cabang 2. Hasil pengujian ping dengan beban 1000 dan tidak menggunakan ip sec dari server ke PC kantor cabang 2 lancar dan stabil dengan 0 packet loss dan average 3ms.
   C. Ping dengan beban 1000 dan tidak menggunakan ip sec server ke PC kantor cabang 3.Hasil pengujian ping dengan beban 1000 dan tidak menggunakan ip sec dari server ke PC kantor cabang 3 lancar dan stabil dengan 0 packet loss dan average 3ms.
4. Ping dengan beban 1000 dan menggunakan ip sec.

A. Ping dengan beban 1000 dan menggunakan ip sec server ke PC kantor cabang 1. Hasil pengujian ping dengan beban 1000 dan menggunakan ip sec dari server ke PC kantor cabang 1 lancar dan stabil dengan 0 packet loss dan average 4ms.

B. Ping dengan beban 1000 dan menggunakan ip sec server ke PC kantor cabang 2. Hasil pengujian ping dengan beban 1000 dan menggunakan ip sec dari server ke PC kantor cabang 2 lancar dan stabil dengan 0 packet loss dan average 4ms.

C. Ping dengan beban 1000 dan menggunakan ip sec server ke PC kantor cabang 3. Hasil pengujian ping dengan beban 1000 dan menggunakan ip sec dari server ke PC kantor cabang 3 lancar dan stabil dengan 0 packet loss dan average 4ms.

5. Ping dengan beban 1400 dan tidak menggunakan ip sec.
   A. Ping dengan beban 1400 dan tidak menggunakan ip sec server ke PC kantor cabang 1. Hasil pengujian ping dengan beban 1400 dan tidak menggunakan ip sec dari server ke PC kantor cabang 1 lancar dan stabil dengan 0 packet loss dan average 3ms.
   B. Ping dengan beban 1400 dan tidak menggunakan ip sec server ke PC kantor cabang 2. Hasil pengujian ping dengan beban 1400 dan tidak menggunakan ip sec dari server ke PC kantor cabang 2 lancar dan stabil dengan 0 packet loss dan average 3ms.
   C. Ping dengan beban 1400 dan tidak menggunakan ip sec server ke PC kantor cabang 3. Hasil pengujian ping dengan beban 1400 dan tidak menggunakan ip sec dari server ke PC kantor cabang 3 lancar dan stabil dengan 0 packet loss dan average 3ms.
6. Ping dengan beban 1400 dan menggunakan ip sec.
   A. Ping dengan beban 1400 dan menggunakan ip sec server ke PC kantor cabang 1. Hasil pengujian ping dengan beban 1400 dan menggunakan ip sec dari server ke PC kantor cabang 1 lancar dan stabil dengan 0 packet loss dan average 3ms.
   B. Ping dengan beban 1400 dan menggunakan ip sec server ke PC kantor cabang 2.Hasil pengujian ping dengan beban 1400 dan menggunakan ip sec dari server ke PC kantor cabang 2 lancar dan stabil dengan 0 packet loss dan average 4ms.
   C. Ping dengan beban 1400 dan menggunakan ip sec server ke PC kantor cabang 3. Hasil pengujian ping dengan beban 1400 dan menggunakan ip sec dari server ke PC kantor cabang 3 lancar dan stabil dengan 0 packet loss dan average 4ms.
7. Ping dengan beban 1500 dan tidak menggunakan ip sec.
   A. Ping dengan beban 1500 dan tidak menggunakan ip sec server ke PC kantor cabang 1. Hasil pengujian ping dengan beban 1500 dan tidak menggunakan ip sec dari server ke PC kantor cabang 1 gagal dengan keterangan destination host unreachable.
   B. Ping dengan beban 1500 dan tidak menggunakan ip sec server ke PC kantor cabang 2. Hasil pengujian ping dengan beban 1500 dan tidak menggunakan ip sec dari server ke PC kantor cabang 2 gagal dengan keterangan destination host unreachable.
   C. Ping dengan beban 1500 dan tidak menggunakan ip sec server ke PC kantor cabang 3. Hasil pengujian ping dengan beban 1500 dan tidak menggunakan ip sec dari server ke PC kantor cabang 3 gagal dengan keterangan destination host unreachable.
8. Ping dengan beban 1500 dan menggunakan ip sec.
   A. Ping dengan beban 1500 dan menggunakan ip sec server ke PC kantor cabang 1. Hasil pengujian ping dengan beban 1500 dan tidak menggunakan ip sec dari server ke PC kantor cabang 1 gagal dengan keterangan request

http://digilib.mercubuana.ac.id/

Copyright ©2021, The authors. Published by Department of Computer Engineering, Universitas Diponegoro
Submitted: 27 January 2021; Revised: 7 July 2021; Accepted: 10 August 2021; Published: 31 October 2021

time out dan destination host unreachable. Dengan 5 packet lost dan average 7 ms

B. Ping dengan beban 1500 dan menggunakan ip sec server ke PC kantor cabang 2. Hasil pengujian ping dengan beban 1500 dan menggunakan ip sec dari server ke PC kantor cabang 2 gagal dengan keterangan destination host unreachable.
C. Ping dengan beban 1500 dan menggunakan ip sec server ke PC kantor cabang 3. Hasil pengujian ping dengan beban 1500 dan menggunakan ip sec dari server ke PC kantor cabang 3 gagal dengan keterangan destination host unreachable.

Berdasarkan hasil penelitian yang telah dilakukan dengan menggunakan tools ping Windows Server dengan berbagai beban dengan dan atau tanpa menggunakan ip sec dari server ke PC cabang 1, PC cabang 2, dan PC cabang 3 maka didapatkan hasil seperti tabel berikut.

Tabel 5 Hasil pengujian

Pengujian	**IP Tunnel Cabang 1**	**EOIP Cabang 2**	**EOIP Cabang 3**
Ping tanpa beban dan tidak menggunakan ip sec	✓	✓	✓
Ping tanpa beban dan menggunakan ip sec	✓	✓	✓
Ping dengan beban 1000 dan tidak menggunakan ip sec	✓	✓	✓
Ping dengan beban 1000 dan menggunakan ip sec	✓	✓	✓
Ping dengan beban 1400 dan tidak menggunakan ip sec	✓	✓	✓
Ping dengan beban 1400 dan menggunakan ip sec	✓	✓	✓
Ping dengan beban 1500 dan tidak menggunakan ip sec	request time out	request time out	request time out
Ping dengan beban 1500 dan menggunakan ip sec	request time out	request time out	request time out

Pada skenario pengujian ping dengan dengan default size, size 1000, size 1400 dengan dan atau tanpa menambahkan komponen keamanan IPsec dari server ke PC cabang 1, cabang 2, dan cabang 3 berjalan dengan lancer dan stabil dengan 0 packet loss dan average 3ms.

Pada skenario pengujian ping dengan beban 1500 dari server ke PC cabang 1, cabang 2, dan cabang 3 selalu mengalami request time out dengan atau tanpa tambahan komponen keamanan IPSec. Hal tersebut disebabkan oleh tidak adanya support dari MTU (*Maximum Transmission Unit*) pada perangkat switch yang digunakan.

Salah satu fitur yang paling menarik dari protokol TCP adalah ukuran MTU (*Maximum Transmission Unit*). MTU memiliki peran besar dalam memecah data menjadi paket, dan ukuran paket maksimum dari MTU adalah ukuran maksimum yang dapat dicapai. Ukuran MTU dapat dimodifikasi ke nilai yang berbeda untuk mesin yang sama. Dan ukuran MTU maksimum untuk perangat berkabel adalah 1500 *byte* [13].

IV. KESIMPULAN

Berdasarkan hasil penelitian dan pengujian implementasi *Customer User Group* Menggunakan Metode EOIP *Tunnel* dan IP *Tunnel* Untuk Sharing Data Dari Kantor Pusat Ke Kantor Cabang dapat disimpulkan bahwa metorde IP Tunnel dan EoIP Tunnel mampu menghubungkan kantor pusat dan kantor cabang dengan

http://digilib.mercubuana.ac.id/

Copyright ©2021, The authors. Published by Department of Computer Engineering, Universitas Diponegoro
Submitted: 27 January 2021; Revised: 7 July 2021; Accepted: 10 August 2021; Published: 31 October 2021

baik. Tersedianya filtur keamanan IP Sec yang dapat di aktifkan dalam IP *Tunnel* dan EoIP *Tunnel* dalam pertukaran dan komunikasi data membuat data yang akan dikirimkan menjadi lebih aman. Namun pada hasil pengujian Ping dengan size 1500 tidak dapat berjalan dikarenakan ketidak supportan MTU (*Maximum Transmission Unit*) pada perangkat switch.

UCAPAN TERIMA KASIH

Penulis mengucapkan terimakasih kepada PT Xyz yang sudah mengizinkan dan memfasilitasi penulis dalam melakukan penelitian dan berbagai pihak yang sudah membantu dalam segala prosesnya.

DAFTAR PUSTAKA

[1] S. Hidayatulloh and R. A. F. Adam, "IMPLEMENTASI INTERCITY BERBASIS TUNNELING MIKROTIK MENGGUNAKAN METODE EOIP TUNNEL," *J. Teknoinfo*, vol. 14, no. 1, pp. 66–70, Jan. 2020, doi: 10.33365/jti.v14i1.327.

[2] M. A. Khizirova, K. S. Chezhimbayeva, A. D. Mukhamejanova, Z. D. Manbetova, and B. Ongar, "Using of virtual private network technology for signal transmission in corporate networks," *News Natl. Acad. Sci. Repub. Kazakhstan, Ser. Geol. Tech. Sci.*, vol. 3, no. 447, 2021, doi: 10.32014/2021.2518-170X.69.

[3] A. Rachmawan and A. Prihanto, "Perbandingan Protokol L2TP dan PPTP Untuk Membangun Jaringan Intranet di Atas VPN," *J. Manaj. Inform.*, vol. 8, no. 2, pp. 53–57, 2018.

[4] M. Mardianto, "Analisis Quality Of Service (QoS) pada Jaringan VPN dan MPLS VPN Menggunakan GNS3," *J. Sains dan Inform.*, vol. 5, no. 2, pp. 98–107, 2019, doi: 10.34128/jsi.v5i2.191.

[5] Sidik, A. Sudaryana, and R. Santoso, "Implementasi Virtual Interface Menggunakan Metode EOIP Tunnel Pada Jaringan WAN PT. Indo Matra Lestari," *J. Tek. Komput. AMIK BSI*, vol. VI, no. 1, pp. 103–110, Jan. 2020, doi: 10.31294/jtk.v4i2.

[6] F. Wuryo Handono and H. Nurdin, "Virtual Private Network Tunneling Dengan ProtokolIP in IP Melalui Jaringan Internet," *INFORMATICS Educ. Prof.*, vol. 2, no. 1, pp. 61–70, 2017, Accessed: Sep. 22, 2021. [Online]. Available: http://ejournal-binainsani.ac.id/index.php/ITBI/article/view/657/536.

[7] F. Hauser, M. Haberle, M. Schmidt, and M. Menth, "P4-IPsec: Site-to-Site and Host-to-Site VPN with IPsec in P4-Based SDN," *IEEE Access*, vol. 8, 2020, doi: 10.1109/ACCESS.2020.3012738.

[8] Prayogi Wicaksana, F. Hadi, and H. Aulia Fitrul, "Perancangan Implementasi VPN Server Menggunakan Protokol L2TP dan IPSec Sebagai Keamanan Jaringan," *J. KomtekInfo*, vol. 8, no. 3, pp. 169–175, Aug. 2021, doi: 10.35134/komtekinfo.v8i3.128.

[9] A. J. Kavita Rani, "Implementation and Analysis of IP Tunnel in Virtual Private Networks," *Int. J. Innov. Technol. Explor. Eng.*, vol. 9, no. 5, 2020, doi: 10.35940/ijitee.d1956.039520.

[10] A. P. Sari, Sulistiyono, and N. Kemala, "Perancangan Jaringan Virtual Private Network Berbasis IP Security Menggunakan Router Mikrotik," *J. PROSISKO*, vol. 7, no. 2, pp. 150–164, 2020.

[11] M. R. R. Fernando, L. M. N. Magaly, and C. S. M. Jose, "Analysis of Methodologies of Data Networks LAN," *Int. J. Adv. Eng. Res. Sci.*, vol. 3, no. 9, pp. 52–61, 2016, doi: 10.22161/ijaers/3.9.9.

[12] T. R. Rachmadi, "Analisis Kinerja Jaringan Wireless LAN Menggunakan Metode QOS (Quality of Service) Di Perpustakaan SMK Negeri 5 Bandar Lampung," *J. Eng. Comput. Sci. ...*, vol. 1, no. 1, pp. 110–117, 2021.

[13] A. Masri and M. Al-Jabi, "Toward IoT fog computing-enabled system energy consumption modeling and optimization by adaptive TCP/IP protocol," *PeerJ Comput. Sci.*, vol. 7, pp. 1–23, 2021, doi: 10.7717/peerj-cs.653.

UNIVERSITAS MERCU BUANA

http://digilib.mercubuana.ac.id/

Copyright ©2021, The authors. Published by Department of Computer Engineering, Universitas Diponegoro
Submitted: 27 January 2021; Revised: 7 July 2021; Accepted: 10 August 2021; Published: 31 October 2021

©2021. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution-ShareAlike 4.0 International License.

UNIVERSITAS
MERCU BUANA

http://digilib.mercubuana.ac.id/

KERTAS KERJA

Ringkasan

Kertas kerja ini merupakan material kelengkapan artikel jurnal dengan judul Implementasi Customer User Group Menggunakan Metode EOIP Tunnel dan IP Tunnel Untuk Sharing Data Dari Kantor Pusat Ke Kantor Cabang PT Xyz yang berisi semua material hasil penelitan Tugas Akhir yang tidak dimuat/atau disertakan di artikel jurnal. Seluruh langkah-langkah perancangan, tahapan implementasi serta hasil pengujian akan dijelaskan dalam laporan ini.

Pendahuluan

Semakin berkembangnya teknologi internet saat ini menjadikan kebutuhan akan koneksi internet yang cepat dan stabil sebagai hal yang sangat penting [1]. Begitu pula dengan munculnya banyak perusahaan yang semakin membutuhkan kemudahan, keamanan dan stabilitas dalam internet dan juga berbagi data antar cabang perusahaan. Sharing data antar kantor pusat dengan kantor cabang dapat menjadi masalah yang sangat penting dalam suatu komunikasi data. Hal ini harus diperhatikan oleh setiap perusahaan dalam melakukan kegiatan komunikasi di dunia internet, sehingga kerahasiaan informasi suatu perusahaan dapat terjaga dengan baik [2]. Sebagai gambaran perusahaan memiliki satu kantor pusat dan beberapa kantor cabang yang sistemnya masih menggunakan layanan Google (Gmail & Google Drive) untuk kebutuhan sharing data [3].

PT Xyz merupakan perusahaan yang bergerak di bidang telekomunikasi dengan kantor pusat berada di Jakarta Pusat serta kantor cabang yang tersebar di beberapa wilayah seperti Jakarta Barat dan Jakarta Selatan. Jika PT Xyz menginginkan untuk menghubungkan tiap-tiap cabang kantornya agar dapat bertukar data dan membangun jaringan interkoneksi sendiri dengan mudah, pada umumnya terdapat beberapa pilihan yaitu dengan dengan membuat interkoneksi dengan berbagai pilihan media yang tersedia, mulai dari kabel fiber optic, radio, ataupun VSAT. Namun dalam pembuatan jalur khusus seperti itu akan membutuhkan banyak biaya terlebih apabila jarak antar cabang sangat jauh seperti

http://digilib.mercubuana.ac.id/

antar kota, provinsi atau bahkan negara. Solusi lainnya adalah dapat menyewa saluran point to point dengan menggunakan media transmisi, namun hal tersebut juga dapat menghabiskan biaya mahal [1].

Pada penelitian kali ini akan menerapkan Server Private dengan beberapa metode tunneling yang akan menggantikan layanan Google dalam sharing data dari kantor pusat ke kantor cabang lainnya. Dengan Server Private karyawan atau staff di kantor pusat dan kantor cabang dapat saling berkomunikasi dan dapat sharing data melalui Server Private dengan jaringan lokal kantor pusat dan kantor cabang melalui internet yang bersifat private yang lebih dikenal dengan virtual private network (VPN) [2]–[4]. Penelitian kali ini akan berfokus pada percobaan implementasi customer user group menggunakan metode tunneling yaitu dengan membangun jaringan privat di atas jaringan publik.

Metode *tunneling* memiliki beragam jenis yang masing-masing memiliki kelebihan dan kekurangannya sehingga dapat digunakan sesuai kebutuhan [5]. Pada penelitian kali ini metode yang digunakan adalah menggunakan metode EOIP (*Ethernet Over Ip*) *tunnel* dan juga metode IP *tunnel* [5]–[7]. Yang mana diharapkan dapat menjadi solusi yang dapat menghubungkan banyak cabang perusahaan dengan baik dan dengan biaya yang murah. Dan dari segi keamanan lebih terproteksi jika menggunakan tunnel karena dapat melakukan pembuatan rule untuk siapa saja yang dapat mengakses *file* tersebut dengan menggunakan *permission* dari windows *sharing* dengan cara mencantumkan *user* mana saja yang dapat mengakses dari setiap *workgroup* di sisi windowsnya.

UNIVERSITAS MERCU BUANA

http://digilib.mercubuana.ac.id/