



SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

**ANALISA KINERJA VPN DENGAN
LAYER 2 TUNNELING PROTOCOL DAN IPSEC
MENGUNAKAN ROUTER MIKROTIK
(STUDI KASUS RSU BUNDA MARGONDA)**

TUGAS AKHIR

FAISAL FITRI

0110217064

PROGRAM STUDI TEKNIK INFORMATIKA

DEPOK

FEBRUARI 2022



STT-NF

SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

**ANALISA KINERJA VPN DENGAN
LAYER 2 TUNNELING PROTOCOL DAN IPSEC
MENGUNAKAN ROUTER MIKROTIK
(STUDI KASUS RSU BUNDA MARGONDA)**

TUGAS AKHIR

**Diajukan sebagai salah satu syarat untuk memperoleh gelar
strata satu**

STT NF
FAISAL FITRI
0110217064

PROGRAM STUDI TEKNIK INFORMATIKA

DEPOK

FEBRUARI 2022

HALAMAN PENYATAAN ORISINALITAS

Skripsi/tugas akhir ini adalah hasil karya sendiri,
dan semua sumber baik yang dikutip maupun dirujuk
telah saya nyatakan dengan benar.

Nama : Faisal Fitri

NIM : 0110217064



STT - NF

Depok, Februari 2022

Penulis,

Faisal Fitri

HALAMAN PENGESAHAN

Skripsi/tugas akhir ini diajukan oleh :

Nama : Faisal Fitri

NIM : 0110217064

Program Studi : Teknik Informatika

Judul Skripsi : Analisa Kinerja VPN dengan Layer 2 Tunneling Protocol dan IPSec Menggunakan Router Mikrotik (Studi Kasus RSUD Bunda Margonda).

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer pada Program Studi Teknik Informatika, Sekolah Tinggi Teknologi Terpadu Nurul Fikri.

DEWAN PENGUJI

Pembimbing

Henry Saptono, S.Si., M.Kom

Penguji I

Penguji II

STT - NF

April Rustianto, S.Komp., M.T

Reza Maulana, S.Kom., M.Kom

Ditetapkan di : Depok

Tanggal : Februari 2022

KATA PENGANTAR

Alhamdulillah, puji dan syukur penulis sampaikan kepada Allah SWT karena atas berkat dan rahmat-Nya penulis dapat menyelesaikan skripsi/tugas akhir yang berjudul ” *Analisa Kinerja VPN Dengan Layer 2 Tunneling Protocol dan IPSec Menggunakan Router Mikrotik (Studi Kasus RSUD Bunda Margonda).*” Penulisan skripsi/tugas akhir ini dilakukan dalam rangka memenuhi persyaratan untuk mencapai gelar Sarjana Komputer Program Studi Teknik Informatika pada Sekolah Tinggi Teknologi Terpadu Nurul Fikri.

Dalam penyelesaian studi dan penulisan skripsi/tugas akhir ini, penulis banyak memperoleh bantuan baik pengajaran, bimbingan dan arahan dari berbagai pihak baik secara langsung maupun tidak langsung. Untuk itu penulis menyampaikan penghargaan dan terima kasih tak terhingga kepada:

1. Bapak Dr. Lukman Rosyidi, S.T., M.M., M.T selaku Ketua Sekolah Tinggi Teknologi Terpadu Nurul Fikri.
2. Bapak Rio Adriansyah, S.Si., M.Si selaku Ketua Program Studi Teknik Informatika Sekolah Tinggi Teknologi Terpadu Nurul Fikri.
3. Bapak Hendry Saptono, S.Si, M.Kom, selaku dosen pembimbing yang telah menyediakan waktu, tenaga, dan pikiran untuk mengarahkan penulis dalam penyusunan skripsi/tugas akhir ini.
4. Bapak April Rustianto, S.Komp., M.T dan Bapak Reza Maulana, S.Kom., M.Kom selaku dosen penguji yang telah bersedia menyediakan waktunya untuk menguji serta memberikan saran dalam penyusunan skripsi/tugas akhir ini.
5. Para Dosen di lingkungan Sekolah Tinggi Teknologi Terpadu Nurul Fikri yang telah membimbing penulis dalam menuntut ilmu yang telah diberikan.
6. Kedua orang tua dan keluarga penulis yang telah memberikan dukungan materil dan moril sehingga penulis dapat terus berjuang dalam meraih mimpi dan cita-cita.
7. dr. Imelda Rachmawati, MARS selaku Direktur RSUD Bunda Margonda yang telah memberikan kesempatan kepada penulis untuk melakukan penelitian dalam penyusunan skripsi/tugas akhir ini.
8. Staff IT RSUD Bunda Margonda dan Staff IT PT. BMHS yang telah memberikan dukungan dalam menyelesaikan penyusunan Skripsi/tugas akhir ini.

Penulis menyadari bahwa dalam penulisan skripsi/tugas akhir ini tentu saja masih banyak terdapat kekurangan-kekurangan yang mungkin disebabkan oleh keterbatasan kemampuan dan pengetahuan yang penulis miliki. Oleh karena itu, penulis mohon maaf apabila terdapat kekurangan di dalam penulisan skripsi/tugas akhir ini dan dengan rendah hati penulis menerima kritik dan saran yang membangun dari pembaca..

Akhir kata, penulis berharap Allah SWT berkenan membalas segala kebaikan semua pihak yang telah membantu dan harapan penulis semoga skripsi/tugas akhir ini dapat memberikan manfaat bagi pembaca.

Depok, Februari 2022

Penulis,

Faisal Fitri



STT - NF

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPERLUAN AKADEMIS

Sebagai civitas akademik Sekolah Tinggi Teknologi Terpadu Nurul Fikri, saya yang bertanda tangan dibawah ini :

Nama : Faisal Fitri
NIM : 0110217064
Program Studi : Teknik Informatika
Jenis Karya : Skripsi / Tugas Akhir

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada STT Nurul Fikri **Hak Bebas Royalti Noneksklusif (*Non-Exclusive Royalti – Free Right*)** atas karya ilmiah saya yang berjudul :

Analisa Kinerja VPN dengan Layer 2 Tunneling Protocol dan IPSec Menggunakan Router Mikrotik (Studi Kasus RSU Bunda Margonda).

Dengan Hak Bebas Royalti Noneksklusif ini STT-NF berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

STT - NF

Dibuat di : Depok

Pada Tanggal : Februari 2022

Yang menyatakan

Faisal Fitri

ABSTRAK

Nama : Faisal Fitri
NIM : 0110217064
Program Studi : Teknik Informatika
Judul : Analisa Kinerja VPN dengan Layer 2 Tunneling Protocol dan IPSec Menggunakan Router Mikrotik (Studi Kasus RSUD Bunda Margonda).

Perkembangan teknologi informasi dan jaringan komputer telah memberikan dampak yang sangat signifikan bagi efektifitas pekerjaan manusia di zaman modern. Salah satunya adalah RSUD Bunda Margonda yang merupakan salah satu instansi yang memberikan layanan kesehatan sesuai dengan kemajuan teknologi informasi dan jaringan komputer. Dalam jaringan komputer, keamanan merupakan faktor penting yang harus diperhatikan. Salah satu cara untuk mengatasi permasalahan pada keamanan jaringan *internet* adalah dengan menggunakan teknologi *Virtual Private Network* (VPN). Apalagi pada saat pandemi *covid-19* yang terjadi sekarang ini, karyawan *back office* RSUD Bunda Margonda diberlakukan kerja *Work From Home* (WFH) yang mengharuskan karyawan untuk dapat terhubung ke jaringan dan data perusahaan menggunakan *internet* atau jaringan publik. Salah satu solusi dari permasalahan di atas adalah dengan menerapkan sebuah teknologi VPN. Penelitian ini merupakan penelitian kualitatif deskriptif dengan pendekatan studi kasus yang bertujuan untuk menerapkan VPN berbasis L2TP+IPSec menggunakan *mikrotik router* pada jaringan RSUD Bunda Margonda dan melakukan pengujian serta analisa kinerja dari hasil pengujian yang dilakukan dengan mengacu pada standar TIPHON (*Telecommunications and Internet Protocol Harmonization Over Network*) dengan kategori “sangat bagus”, “bagus”, dan “buruk”. Hasil Penelitian menunjukkan bahwa rancangan VPN dengan L2TP+IPSec menggunakan *mikrotik router* di RSUD Bunda Margonda telah berfungsi sesuai dengan konfigurasi. Performa dan konektivitas *throughput*, *jitter*, dan *packet loss* antara *site to site* dari RSUD Bunda Margonda ke *head office* masuk kategori “sangat bagus”, “bagus”, dan “bagus”. Performa dan konektivitas *throughput*, *jitter*, dan *packet loss remote acces* dari *client* ke RSUD Bunda Margonda masuk kategori “sangat bagus”, “bagus”, dan “buruk”. Oleh karena itu, penggunaan teknologi VPN berbasis protokol L2TP dan IPsec dapat diterapkan dengan menggunakan perangkat lain selain *mikrotik*, misalnya *Cisco*, *Juniper*, dan *Ubiquiti*.

Kata kunci: Kinerja Virtual Private Network (VPN), Mikrotik Router, L2TP+IPSec

ABSTRACT

Name : Faisal Fitri

NIM : 0110217064

Studi Program : Teknik Informatika

Title : *Performance Analysis of VPN with Layer 2 Tunneling Protocol and IPSec Using MikroTik Router (Case Study: RSU Bunda Margonda)*

The development of information technology and computer networks has a very significant impact on the effectiveness of modern human work in modern era. One example is RSU Bunda Margonda which is one of the health service providers that provides healthcare services in line with the advancements in information technology and computer networks. In computer networks, security is an important factor that need to be considered. One way to address security issues in internet networks is by using Virtual Private Network (VPN) technology. Especially during the current Covid-19 pandemic, back office employees at RSU Bunda Margonda are forced to work from Home (WFH) which requires employees to be able to connect to company networks and data using the internet or public networks. One solution to the above problems is to apply a Virtual Private Network (VPN) technology. This research is a descriptive qualitative research with a case study approach that aims to apply a L2TP+IPSec-based VPN using a mikrotik router on the RSU Bunda Margonda network and conduct testing and performance analysis from the results of tests carried out with reference to the TIPHON standard (Telecommunications and Internet Protocol Harmonization Over Network) with categories of “very good”, “good”, and “not good.” The research results show that the design of a VPN with L2TP+IPSec using a mikrotik router at RSU Bunda Margonda has worked according to the configuration. Throughput, jitter and packet loss performance and connectivity between site to site from RSU Bunda Margonda to the head office are categorized as the “very good”, “good” and “good” categories. Performance and connectivity throughput, jitter and packet loss remote access from the client to RSU Bunda Margonda are categorized as the "very good", "good" and "poor" categories. Therefore, the use of Virtual Private Network (VPN) technology based on L2TP and IPsec protocols can be applied using other devices besides mikrotik, for example Cisco, Juniper, and Ubiquiti.

Keywords: *Virtual Private Network (VPN) Performance, Mikrotik Router, L2TP+IPSec*

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PERNYATAAN ORISINALITAS	ii
HALAMAN PENGESAHAN	iii
KATA PENGANTAR	iv
HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPERLUAN AKADEMIS.....	vi
ABSTRAK	viii
ABSTRACT	viii
DAFTAR ISI	ix
DAFTAR GAMBAR	xii
DAFTAR TABEL	xiv
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	3
1.3 Tujuan dan Manfaat	3
1.3.1 Tujuan	3
1.3.2 Manfaat	3
1.4 Batasan Masalah	4
1.5 Sistematika Penulisan	4
BAB II LANDASAN TEORI	6
2.1 Jaringan Komputer	6
2.2 Protokol Jaringan	8
2.3 Osi Layer	8
2.4 Virtual Private Network	10
2.4.1 Pengertian VPN	10
2.4.2 Perkembangan VPN	11
2.4.3 Tipe VPN	12
2.4.4 Protokol VPN	12
2.5 Mikrotik	15
2.5.1 Jenis Mikrotik	15
2.5.2 Fungsi Mikrotik	16
2.5.3 Lisensi Mikrotik	17

2.6 Penelitian Tekait	18
BAB III METODOLOGI PENELITIAN	22
3.1 Jenis Metode Penelitian	22
3.2 Teknik Pengumpulan Data	22
3.2.1 Observasi	22
3.2.1 Studi Pustaka	22
3.2.1 Diskusi dan Wawancara	22
3.3 Prosedur Penelitian	22
3.3.1 Studi Linteratur	23
3.3.2 Ananlisis Kebutuhan Sistem	23
3.3.3 Pengujian dan Analisis Hasil	24
3.3.4 Penarikan Kesimpulan dan Saran	24
3.4 Lingkungan Pengujian	24
3.5 Alat dan Bahan	24
3.6 Jadwal Penelitian	25
BAB IV ANALISA DAN PERANCANGAN	26
4.1 Analisa Sistem Berjalan Saat ini	27
4.2 Analisa Kebutuhan Sistem	27
4.2.1 Analisa Kebutuhan Internet	27
4.2.2 Analisa Pengalamatan IP Address	28
4.2.3 Analisa Kebutuhan Hardware	28
4.2.4 Analisa Kebutuhan Software	30
4.3 Perancangan Sistem	30
4.3.1 Perancangan Topologi VPN L2TP+IPSec Site to site	30
4.3.1 Perancangan Topologi VPN L2TP+IPSec Remote Acces.....	31
4.4 Perancangan pengujian VPN L2TP+IPSec	32
4.4.1 Perancangan Fungsionalitas VPN	32
4.4.2 Perancangan Pengujian Peforma Throughput	32
4.4.3 Perancangan Pengujian Peforma Jitter	33
4.4.4 Perancangan Pengujian Peforma Packet Loss	35
BAB V IMPLEMENTASI DAN PENGUJIAN	37
5.1 Implementasi	37
5.1.1 Konfigurasi L2TP+IPSec VPN Server	37
5.1.2 Konfigurasi L2TP+IPSec VPN Client	42

5.1.3 Konfigurasi L2TP+IPSec VPN Client Remote Access	44
5.2 Pengujian Peforma VPN L2TP+IPSec	47
5.2.1 Pengujian Fungsionalitas VPN	47
5.2.2 Skenario Pengujian VPN	47
5.2.3 Pengujian Peforma Throughput	52
5.2.4 Pengujian Peforma Jitter	54
5.2.5 Pengujian Peforma Packet Loss	62
BAB VI KESIMPULAN DAN SARAN	66
6.1 Kesimpulan	66
6.2 Saran	67
DAFTAR PUSTAKA	68



STT - NF

DAFTAR GAMBAR

Gambar 2.1 Local Area Networkk	7
Gambar 2.2 Metropolitan Area Network	7
Gambar 2.3 Wide Area Networkk	8
Gambar 2.4 OSI Layer	9
Gambar 2.5 Virtual Private Network	11
Gambar 2.6 Remote Access	12
Gambar 2.7 Site-to-Site	13
Gambar 2.8 Mikrotik RouterOS	16
Gambar 2.9 Mikrotik RouterBoard	16
Gambar 3.1 Prosedur Penelitian	23
Gambar 4.1 Topologi Jaringan Produksi	27
Gambar 4.2 Topologi VPN L2TP+IPSec Site to Site	31
Gambar 4.3 Topologi VPN L2TP+IPSec Remote Access	31
Gambar 5.1 Konfigurasi L2TP Server HOF	37
Gambar 5.2 Konfigurasi L2TP Server RSUD Bunda Margonda	38
Gambar 5.3 Konfigurasi Secret HOF	38
Gambar 5.4 Konfigurasi IP Pool RSUD	39
Gambar 5.5 Konfigurasi Profile RSUD	40
Gambar 5.6 Konfigurasi Secret RSUD	40
Gambar 5.7 Ipsec Proposal HOF	41
Gambar 5.8 Ipsec Proposal RSUD	41
Gambar 5.9 Connect VPN RSUD-HOF	42
Gambar 5.10 Active Connecton VPN RSUD	43
Gambar 5.11 Konfigurasi Route Mikrotik HOF	43
Gambar 5.12 Konfigurasi Route Mikrotik RSUD	44
Gambar 5.13 Konfigurasi VPN Win 11	45
Gambar 5.14 VPN Connected	46
Gambar 5.15 Terhubung dengan VPN Server	46
Gambar 5.16 Ping ke host VPN Client	47
Gambar 5.17 Ping ke host VPN Server	48
Gambar 5.18 Traceroute ke host VPN Client	48

Gambar 5.19 Traceroute ke host VPN Server	49
Gambar 5.20 Ping ke host VPN Server RSUBM	50
Gambar 5.21 Ping ke host VPN Remote Acces	50
Gambar 5.22 Traceroute ke host VPN Server RSUBM	51
Gambar 5.23 Traceroute ke host VPN Remote Acces	51
Gambar 5.24 Skenario Pengujian Site to Site	53
Gambar 5.25 Skenario Pengujian Remote Acces	54
Gambar 5.26 Pengujian 1 Troughput Site to Site	55
Gambar 5.27 Pengujian 2 Troughput Site to Site	55
Gambar 5.28 Pengujian 1 Troughput Remote Access	56
Gambar 5.29 Pengujian 2 Troughput Remote Access	57
Gambar 5.30 Pengujian 1 Jitter Site to Site	58
Gambar 5.31 Pengujian 2 Jitter Site to Site	59
Gambar 5.32 Pengujian 1 Jitter Remote Access	60
Gambar 5.33 Pengujian 2 Jitter Remote Access	61
Gambar 5.34 Pengujian 1 Packet Loss Site to Site	62
Gambar 5.35 Pengujian 2 Packet Loss Site to Site	63
Gambar 5.36 Pengujian 1 apcket Loss Remote Access	64
Gambar 5.37 Pengujian 2 Packet Loss Remote Access	65

STT - NF

DAFTAR TABEL

Tabel 2.1 Penelitian Terkait	18
Tabel 3.1 Jadwal Penelitian	25
Tabel 4.1 Pengalamatan IP Address	26
Tabel 4.2 Spesifikasi Routerboard 1100 AHx2 VPN Server	28
Tabel 4.3 Spesifikasi Routerboard 1100 AHx2 VPN Client	29
Tabel 4.4 Spesifikasi Kebutuhan Software	30
Tabel 4.5 Index Peforma Throughput	32
Tabel 4.6 Pengujian Throughput	33
Tabel 4.7 Index Peforma Jitter	34
Tabel 4.8 Pengujian Jitter	34
Tabel 4.9 Index Peforma Paket Loss	35
Tabel 4.10 Pengujian Paket Loss	35
Tabel 5.1 Comment Line Iperf	52
Tabel 5.2 Hasil Troughput Site to Site.....	56
Tabel 5.3 Hasil Troughput Remote Access.....	57
Tabel 5.4 Hasil Jitter Site to Site.....	59
Tabel 5.5 Hasil Jitter Remote Access.....	61
Tabel 5.6 Hasil Packet Loss Site to Site.....	63
Tabel 5.7 Hasil Packet Loss Remote Access.....	65

STT - NF

BAB I PENDAHULUAN

1.1 Latar Belakang Masalah

Dewasa ini teknologi telah berkembang sangat cepat, khususnya dibidang teknologi informasi dan komunikasi. Perkembangan tersebut telah memberikan dampak yang sangat signifikan bagi efektifitas pekerjaan manusia di zaman modern ini. Suatu jaringan wireless memungkinkan orang-orang untuk berkomunikasi, mengakses aplikasi dan informasi tanpa menggunakan kabel. Jaringan wireless menyediakan kebebasan pergerakan dan kemampuan untuk meluaskan aplikasi pada bagian-bagian yang berbeda dari suatu bangunan, kota besar, atau hal lainnya hampir diseluruh dunia. Sebagai contoh, karyawan di dalam sebuah perusahaan, instansi, atau bentuk usaha lainnya dapat berinteraksi, bertukar informasi dan data dengan karyawan di kantor cabang lainnya, karyawan di lapangan, ataupun konsumen dengan cepat tanpa harus bertatap muka. Jaringan wireless mengijinkan orang-orang untuk saling berhubungan dengan jaringan publik (internet).[1]

Perkembangan teknologi informasi dan jaringan komputer telah memberikan dampak yang sangat signifikan bagi efektifitas pekerjaan manusia moderen. Hal ini juga diperkuat oleh Rahmat Hidayat (2019) yang mengungkapkan bahwa pada aktifitas dalam sebuah perusahaan atau instansi dan bentuk usaha lainnya dalam berinteraksi dengan kantor cabang, karyawan di lapangan maupun konsumen dapat mengakses melalui jaringan publik (Internet).[2] Hal ini menjadikan mekanisme keamanan jaringan harus diimplementasi dengan baik dan efisien untuk memastikan tidak ada data yang dapat diambil oleh pihak yang tidak berkepentingan. Salah satu cara untuk mengatasi permasalahan pada keamanan jaringan di internet adalah dengan menggunakan teknologi Virtual Private Network (VPN). Secara umum, VPN adalah suatu proses yang berupa sebuah jaringan umum (public network atau internet) yang diamankan untuk difungsikan sebagai sebuah jaringan pribadi (private network).

RSU Bunda Margonda merupakan instansi penyedia layanan kesehatan yang telah beroperasi sejak tahun 2005 yang merupakan unit usaha dari PT. Bundamedik Healthcare System (BMHS). RSU Bunda Margonda memiliki visi menjadi rumah sakit swasta terdepan dalam pelayanan kedokteran dan keperawatan di kota Depok dan sekitarnya. Adapun misi dari RSU Bunda Margonda adalah memberikan pelayanan jasa rumah sakit yang berkualitas tinggi kepada masyarakat yang dilayani dengan

menciptakan produk-produk unggulan serta memberikan pelayanan jasa rumah sakit sesuai dengan kemajuan teknologi. Selama ini pertukaran data antar Head Office, Unit Usaha dan Anak Usaha lainnya yaitu dengan menggunakan flashdrive dan e-mail dimana dengan menggunakan cara tersebut dinilai tidak efektif dan efisien terutama dalam menjaga kerahasiaan data perusahaan.

Pada jaringan yang berjalan saat ini, terdapat beberapa aplikasi webbase, yang nantinya dapat diakses oleh seluruh karyawan, Head Office, Unit Usaha, Anak Usaha serta karyawan yang berada di luar kantor (*remote access*) untuk mengakses jaringan perusahaan sehingga dapat meningkatkan kinerja dan efektifitas dari penggunaan sektor jaringan komputer dan internet apalagi pada saat pandemi covid19 yang terjadi sekarang ini dimana karyawan *back office* diberlakukan kerja dari rumah atau sering disebut juga dengan *Work From Home* (WFH). Salah satu solusi dari permasalahan diatas adalah dengan menerapkan sebuah teknologi *Virtual Private Network* (VPN) yang sejalan dengan kebijakan rumah sakit yang telah memutuskan untuk melindungi kerahasiaan data perusahaan terutama data medis pasien sehingga tidak dapat di akses secara public. Jenis *Virtual Private Network* (VPN) yang akan diterapkan pada jaringan produksi yang berjalan saat ini yaitu, *Virtual Private Network* (VPN) Berbasis Protokol Layer 2 Tunneling Protokol (L2TP) dan IPsec, agar dapat menghubungkan beberapa gedung divisi menjadi satu jaringan private karena VPN L2TP+IPsec dapat langsung dipasang dalam berbagai sistem operasi yang banyak digunakan pada saat ini. Disamping itu VPN L2TP+IPsec sangat mudah untuk proses kofigurasinya dan dapat melampaui batas kebanyakan firewall, retriksi jaringan dan ISP.

Dalam implementasi *Virtual Private Network* (VPN) ini, penulis menggunakan perangkat router MikroTik yang dimiliki masing-masing Unit Usaha dan Anak Usaha PT.BMHS. Selain memiliki fitur yang cukup lengkap, penggunaan router MikroTik ini dapat mendukung kebutuhan networking pada jaringan RSU Bunda Margonda, serta dapat menekan biaya dalam pengadaan perangkat infrastruktur. Penggunaan IPsec pada lapisan transport dalam OSI Reference Model untuk melindungi protokol IP (Internet Protocol) dengan menggunakan teknik Tunneling (Terowongan) untuk mengirimkan informasi melalui jaringan internet atau dalam jaringan intranet secara aman.

1.2 Rumusan Masalah

Dalam Jaringan Komputer, faktor keamanan menjadi penting terutama bila menggunakan jaringan public. VPN merupakan solusi tepat untuk koneksi antar Unit Usaha, dan Anak Usaha serta Head Office Suatu perusahaan termasuk di RSUD Bunda Margonda sekalipun. Berdasarkan hal tersebut, dapat dirumuskan permasalahan penelitian sebagai berikut :

1. Bagaimanakah rancangan VPN dengan L2TP+IPSec menggunakan router mikrotik yang akan diimplementasikan di RSUD Bunda Margonda ?
2. Bagaimana kinerja dari VPN dengan L2TP+IPSec menggunakan router mikrotik di RSUD Bunda Margonda?

1.3 Tujuan dan Manfaat Penelitian

1.3.1 Tujuan Penelitian

Penelitian ini bertujuan untuk :

1. Menerapkan VPN berbasis L2TP+IPSec menggunakan Mikrotik Router pada jaringan RSUD Bunda Margonda.
2. Melakukan pengujian dan analisa kinerja terhadap VPN berbasis L2TP+IPSec pada Mikrotik Router.

1.3.2 Manfaat Penelitian

Penelitian ini dilakukan untuk memperoleh manfaat sebagai berikut:

1. Menghasilkan sebuah konektivitas *Road Warrior* (Ksatria Jalanan) yaitu koneksi VPN yang menghubungkan perangkat personal (PC/Laptop/Smartphone) dengan jaringan lokal melalui jaringan internet provider telekomunikasi sehingga dapat mengakses *resource* jaringan kantor dari mana saja bagi karyawan back office.
2. Mengetahui bagaimana kinerja jaringan VPN sesungguhnya dari penerapan VPN L2TP+IPSec berbasis mikrotik router di RSUD Bunda Margonda.
3. Memberikan pengetahuan dan wawasan dibidang jaringan internet serta meningkatkan kemampuan dan dapat menerapkan teori yang didapat secara langsung di dalam masyarakat dan dunia kerja.
4. Menghasilkan suatu karya tulis yang bisa menjadi salah satu rujukan bagi siapapun yang ingin mengetahui dan menerapkan VPN L2TP+IPSec berbasis Mikrotik Router.

5. Bagi penulis sebagai Mahasiswa Teknik Informatika dengan konsentrasi studi Network Engineer, untuk memenuhi salah satu syarat kelulusan Strata Satu (S1) Program Studi Teknik Informatika di Sekolah Tinggi Teknologi Terpadu Nurul Fikri Jakarta.

1.4 Batasan Masalah

Agar dapat menjawab rumusan masalah dan tidak membahas diluar tujuan penelitian, maka diperlukan batasan masalah yang akan diteliti, yaitu sebagai berikut :

1. Pengujian peforma *Troughput*, *Jitter*, dan *Packet Loss* dengan menggunakan tool *Iperf* dilakukan hanya melibatkan topologi antar site (anak usaha/cabang), antar site dengan *head office*, dan *remote acces* dari client ke VPN server L2TP+IPSec Mikrotik Router RSU Bunda Margonda dengan hasil penilaian merujuk kepada standar TIPHON.
2. Tidak melakukan pengujian keamanan.

1.5 Sistematika Penulisan

Untuk memberikan gambaran yang lebih jelas dan sistematis, skripsi/tugas akhir ini dibagi menjadi lima bab dan tiap bab memiliki beberapa sub bab dengan urutan sebagai berikut:

BAB I PENDAHULUAN, merupakan bab pembuka yang memberikan gambaran umum mengenai pelaksanaan tugas akhir. Bab ini terdiri dari latar belakang, perumusan masalah, batasan masalah, tujuan dan manfaat penelitian, dan sistematika penulisan.

BAB II LANDASAN TEORI, bab ini akan menjelaskan tentang landasan teori yang digunakan sebagai dasar acuan dalam pembahasan penelitian ini.

BAB III METODOLOGI PENELITIAN, bab ini akan menjelaskan tentang tahapan penelitian mengenai analisis kebutuhan desain VPN, metode pengumpulan data dan metode pengembangan sistem yang dilakukan dalam analisis dan perancangan VPN menggunakan Aplikasi VPN Mikrotik dan VPN Berbasis Protokol Layer 2 Tunneling Protokol (L2TP) dan IPSec.

BAB IV ANALISA DAN PERANCANGAN, bab ini berisi tentang analisa dan rancangan Virtual Private Network (VPN) Berbasis Protokol Layer 2 Tunneling Protokol (L2TP) dan IPSec.

BAB V IMPLEMENTASI DAN PENGUJIAN, bab ini berisi tentang implementasi serta pengujian Virtual Private Network (VPN) Berbasis Protokol Layer 2 Tunneling Protokol (L2TP) dan IPSec

BAB VI KESIMPULAN DAN SARAN, bab ini berisi kesimpulan dari Tugas Akhir yaitu inti dari jawaban pada rumusan masalah, dan saran untuk peneliti selanjutnya yang meneliti Virtual Private Network (VPN) Berbasis Protokol Layer 2 Tunneling Protokol (L2TP) dan IPSec.



STT - NF

BAB II

LANDASAN TEORI

Pada BAB ini peneliti membaca dan mempelajari teori-teori terkait dan hasil penelitian sebelumnya yang dapat mendukung pemecahan masalah penelitian. Selain itu penulis juga mengumpulkan data dari situs- situs internet yang berhubungan dengan tugas akhir penulis. Dengan berbagai teori, teknik, metode, dan temuan-temuan lainnya yang pernah digunakan oleh orang lain untuk mengatasi atau menjawab permasalahan di atas. Dengan bertujuannya untuk mendapatkan landasan teori mengenai masalah yang akan diteliti.

2.1 Jaringan Komputer

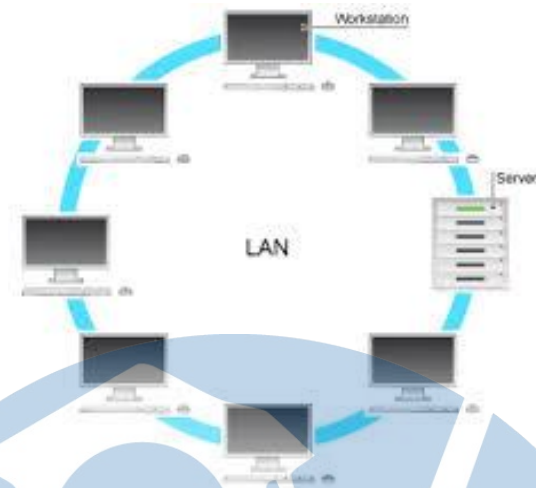
Rahmat Hidayat (2019) menyatakan bahwa jaringan komputer adalah sekelompok komputer otonom yang saling berhubungan satu dengan lainnya menggunakan protokol komunikasi melalui media komunikasi sehingga dapat saling berbagi informasi, aplikasi dan perangkat keras secara bersama-sama.[2] Jaringan komputer dapat diartikan juga sebagai kumpulan sejumlah terminal komunikasi yang berada di berbagai lokasi yang terdiri lebih dari satu komputer yang saling berhubungan. Adapun Manfaat jaringan komputer antara lain: [3]

1. Berbagi sumber daya / pertukaran data.
2. Mempermudah berkomunikasi / bertransaksi.
3. Membantu akses informasi
4. Mampu memberikan akses informasi dengan cepat dan up-to-date.

Berikut ini adalah jaringa-jaringan komputer berdasarkan dari jangkauannya[4]:

a. LAN (*Local Area Network*)

Local Area Network sering kita jumpai di perkantoran, kampus, maupun warnet. Jaringan ini dapat menghubungkan lebih dari 2 komputer di ruangan jarak dekat (terbatas) hingga beberapa KM saja. Jaringan ini biasanya terdiri dari komputer, printer, dan perangkat lainnya.



Gambar 2.1 Local Area Network

b. **MAN (*Metropolitan Area Network*)**

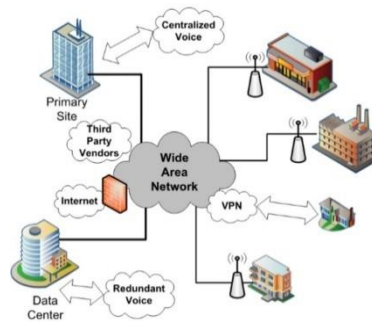
Sesuai dengan namanya maka jenis jaringan ini memberikan layanan hingga wilayah yang luas dan kemampuan tranfer datapun bekecepatan sangat tinggi. Wilayah yang dapat menadi cakupan berkisar hingga 50 Km. MAN ini merupakan rangkaian LAN yang berukuran dan berjarak lebih besar.



Gambar 2.2 Metropolitan Area Network

c. **WAN (*Wide Area Network*)**

Jenis jaringan ini memberikan layanan lebih luas lagi dibandingkan MAN yaitu dapat menghubungkan suatu wilayah bahkan dengan negara lain. WAN pada dasarnya merupakan kumpulan beberapa MAN yang ada di beberapa lokasi sehingga dibutuhkan sebuah device yaitu router untuk menghubungkannya.



Gambar 2.3 Wide Area Network

2.2 Protokol Jaringan

Jaringan Protokol ini merupakan himpunan aturan-aturan yang memungkinkan komputer satu dapat berhubungan dengan komputer yang lain. Aturan-aturan ini meliputi tata cara bagaimana agar komputer bisa saling berkomunikasi, biasanya berupa bentuk (model) komunikasi, waktu saat berkomunikasi, barisan traffic saat berkomunikasi, pemeriksaan error saat transmisi data, dan lain-lain. [5] Berbagai protokol yang terdapat dari lapisan teratas sampai terbawah yang ada dalam sederetan protokol dipandang dari sudut komunikasi data, ada beberapa protokol yang banyak digunakan pada jaringan komputer, diantaranya :

1. TCP/IP (*Transmission Control Protocol / Internet Protocol*)

TCP/IP merupakan protocol standar pada jaringan internet yang tidak tergantung pada jenis komputer yang digunakan. Dengan menggunakan TCP/IP akan memungkinkan berbagai komputer (seperti PC IBM, Machintos, Sun, HP, dll) berinteraksi satu sama lain tanpa mengalami masalah yang signifikan.

2. UDP (*User Datagram Protocol*)

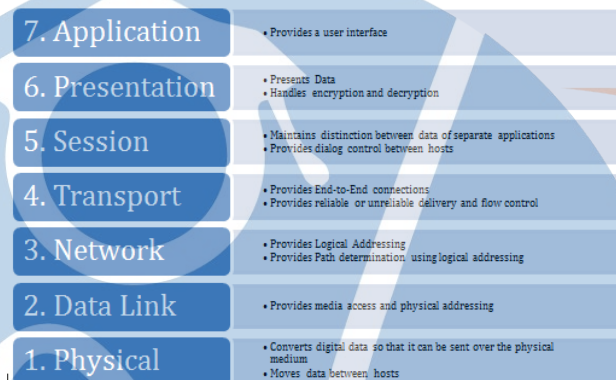
User Datagram Protokol (UDP) adalah sebuah protokol yang bekerja pada Transport Layer, mulai digunakan dan dikembangkan oleh US Department Of Defence (DoD) untuk digunakan bersama Protokol IP di Network Layer. Protokol UDP memberikan alternatif transport untuk proses yang tidak membutuhkan pengiriman yang handal.

2.3 Osi Layer

Model referensi jaringan terbuka OSI atau OSI Reference Model for Open Networking adalah sebuah model arsitektur jaringan yang dikembangkan oleh badan Internasional Organization for Standardzation (ISO) di Eropa pada tahun 1977. [6] OSI

sendiri merupakan singkatan dari Open System Interconnection. Model ini disebut juga dengan “Model tujuh lapis OSI” (OSI Seven Layer Model).

OSI Reference Model pun digunakan sebagai titik awal untuk mempelajari bagaimana beberapa protokol jaringan di dalam sebuah kumpulan protokol dapat berfungsi dan berinteraksi. OSI Reference Model memiliki tujuh lapis, yakni sebagai berikut :



Gambar 2.4 OSI Layer

Berikut penjelasan mengenai fungsi dari OSI Layer [7]:

1. Lapisan Ke-7 Application Layer

Application Layer ini memiliki fungsi sebagai antarmuka aplikasi dengan fungsional jaringan, jadi fungsinya lebih kepada mengatur bagaimana aplikasi dapat mengakses jaringan serta membuat message problemnya. Protokol yang berada pada lapisan ini adalah HTTP, FTP, SMTP, dan NFS.

2. Lapisan Ke-6 Presentation Layer

Presentation Layer berguna untuk mentranslasi data yang akan di transmisikan aplikasi ke dalam format yang sesuai dengan transmisi data jaringan. Protokol yang ada pada lapisan ini yakni Software Redirektor, Workstation, Network Shell, serta Remote Desktop Protocol.

3. Lapisan Ke-5 Session Layer

Session Layer ini memiliki fungsi mendefinisikan sebuah koneksi terbuat, dijaga atau dihapuskan, Pada layer ini terjadi resolusi nama.

4. Lapisan Ke-4 Transport Layer

Transport Layer memiliki fungsi memecah data menjadi sebuah paket data dan memeberikan penomoran secara urut sehingga dapat dengan mudah tersusun di

tempat tujuan pada waktu diterima. Pada lapisan layer ini terjadi notifikasi bahwa paket telah sukses diterima, dan jika ada paket data yang hilang ditengah jalan, maka secara otomatis akan di transmisikan ulang.

5. Lapisan Ke-3 Network Layer

Network Layer memiliki fungsi untuk mendefinisikan alamat IP, kemudian membuat header tiap paket data, dan melakukan routing dengan internetworking menggunakan router dan switch layer 3.

6. Lapisan Ke-2 Data Link Layer

Data Link Layer ini memiliki fungsi mengelompokkan bit-bit data menjadi sebuah frame, di dalam lapisan ini juga terjadi aktifitas mengkoreksi kesalahan, flow control, pengalamatan hardware, dan menentukan jalannya perangkat jaringan seperti hub, bridge, repeater, dan switch layer 2 berjalan.

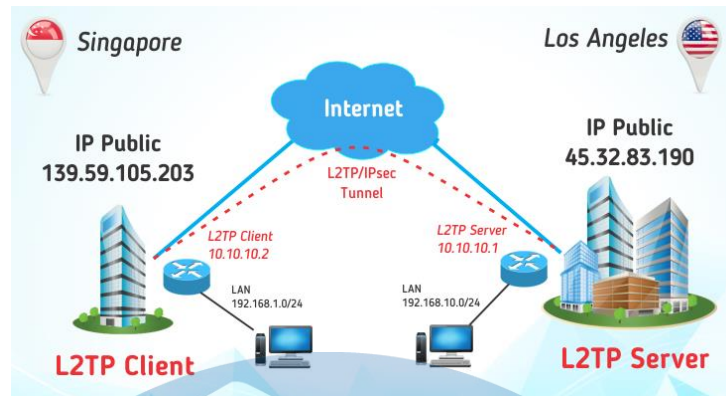
7. Lapisan Ke-1 Physical Layer

Physical Layer ini memiliki fungsi untuk mendefinisikan media transmisi jaringan, metode pensinyalan, sinkronisasi bit, arsitektur jaringan, topologi jaringan dan pengabelan. Hal lain yang terjadi pada layer 1 ini adalah mendefinisikan *network interface card* (NIC) agar bisa berinteraksi dengan media kabel atau radio.

2.4 Virtual Private Network (VPN)

2.4.1 Pengertian Virtual Private Network (VPN)

Virtual Private Network (VPN) adalah fasilitas yang memungkinkan koneksi jarak jauh (*remote access*) menggunakan jaringan publik untuk akses *Local Area Network* (LAN) pada suatu institusi atau perusahaan. [8] VPN merupakan suatu cara untuk membuat sebuah jaringan bersifat privat dan aman dengan menggunakan jaringan publik seperti contohnya internet. VPN dapat mengirimkan data antara dua komputer yang melewati jaringan publik sehingga seolah-olah terhubung secara *point-to-point*. Data dienkapsulasi dengan *header* yang berisi informasi *routing* untuk mendapatkan koneksi *point-to-point* sehingga dapat melewati jaringan publik dan dapat mencapai tujuan akhir.



Gambar 2.5 Virtual Private Network

Sedangkan untuk mendapatkan koneksi bersifat privasi, data yang dikirim harus dienkripsi terlebih dahulu untuk menjaga kerahasiannya sehingga paket yang tertangkap ketika melewati jaringan publik tidak terbaca karena harus melewati proses dekripsi. Proses enkapsulasi data sering disebut dengan istilah *Tunneling*.

2.4.2 Perkembangan Virtual Private Network (VPN)

VPN dikembangkan untuk membangun sebuah intranet dengan jangkauan luas melalui jaringan internet. Internet sudah menjadi suatu komponen penting dalam suatu perusahaan saat ini. Intranet dalam perusahaan dapat berkembang sesuai dengan perkembangan perusahaan tersebut. Dengan kata lain, semakin besar perusahaan semakin besar pula intranet pada perusahaan tersebut. Sehingga permasalahan semakin kompleks apabila suatu perusahaan mempunyai kantor cabang atau unit usaha dengan jarak yang jauh. Sedangkan pada pihak lain selalu berhubungan, misalnya mengirim suatu data dan sinkronisasi data.

Perkembangan intranet yang cepat menawarkan solusi untuk membangun sebuah intranet menggunakan jaringan publik atau internet. Dalam perkembangan intranet ini menuntut lima kebutuhan yang mendasar diantaranya [9]:

1. Kerahasiaan, yaitu kemampuan *encrypt* pesan sepanjang jaringan yang tidak aman.
2. Kendali Akses, yaitu menentukan siapa yang diberikan akses ke jaringan dan informasi apa dan banyak orang dapat menerima.
3. *Authentication*, yaitu menguji identitas dari dua perusahaan yang mengadakan transaksi atau pertukaran data.
4. *Integritas*, yaitu menjamin bahwa file tidak berubah dalam perjalanan.

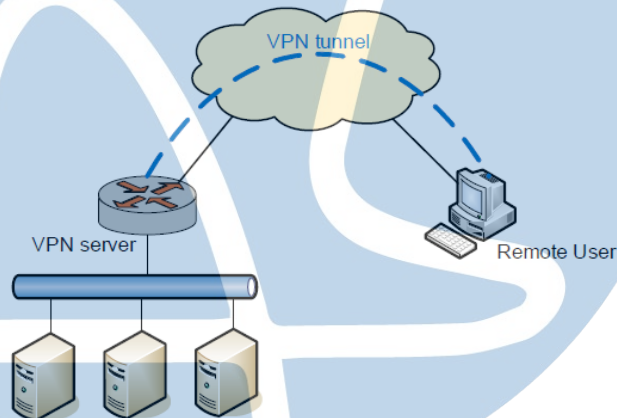
5. *Non-repudiation*, yaitu mencegah dari penyangkalan bahwa mereka telah mengirim dan menerima sebuah file.

2.4.3 Tipe Virtual Private Network (VPN)

Secara garis besar tipe dalam VPN yang biasa digunakan adalah Site-to-site dan Remote Access.[10] Oleh karena itu penulis akan menjelaskan tipe-tipe tersebut.

1. Remote Access

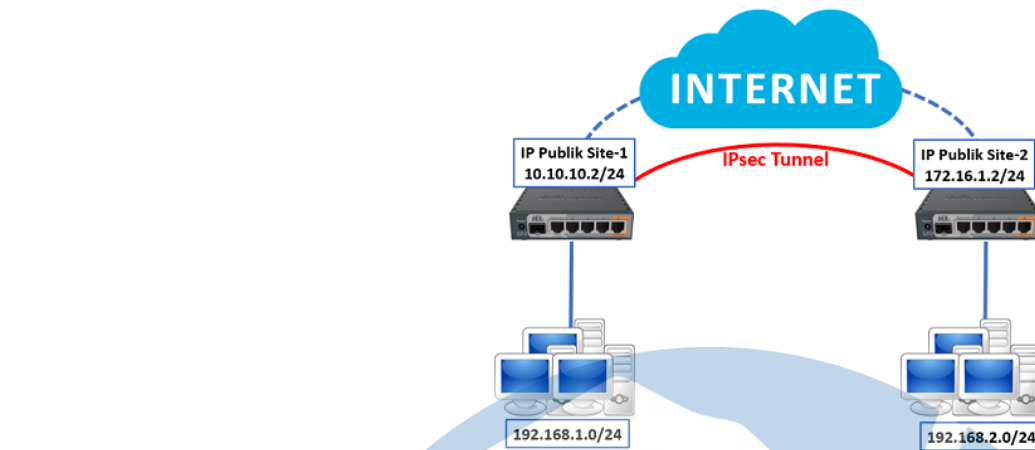
Koneksi remote Access pada VPN dibuat untuk dapat mengakses jarak jauh bagi sebuah klien. Klien *Remote Access* adalah pengguna komputer tunggal yang mana melakukan koneksi ke jaringan pribadi dari lokasi jarak jauh. Sebuah VPN server menyediakan akses untuk dapat mengakses sumber pada jaringan yang terkoneksi pada VPN server. Protokol yang dapat digunakan pada *Remote Access* adalah *Point-to-Point Tunneling Protocol (PPTP)*, *Layer Two Tunneling Protocol version 2 (L2TP v2)*, *Secure Socket Layer (SSL)*, *Layer Two Forwarding (L2F) Protokol* dan *IPSec*.



Gambar 2.6 Remote Access

2. Site-to-Site

Site-to-site dapat juga disebut juga *LAN-to-LAN* adalah berkomunikasi antar dua atau lebih jaringan lokal (LAN) berbeda. Suatu perusahaan pusat dengan cabangnya yang berkomunikasi dengan jarak yang berjauhan secara langsung oleh sebab itu dibangunlah VPN *Site-to-Site* sebagai solusi yang mutakhir, hal ini dilakukan untuk menghemat biaya panarikan kabel fiber optik yang akan memakan biaya yang sangat besar. Pada Site-to-Site, protokol yang dapat digunakan adalah IP Security (IPSec), Geberic Routing Encapsulation (GRE), Layer Two Tunneling Protocol Version3 (L2TPv3).



Gambar 2.7 Site-to-Site

2.4.4 Protokol Virtual Private Network (VPN)

Terdapat beberapa protokol yang biasa digunakan untuk pengembangan *Virtual Private Network* (VPN) adalah sebagai berikut :

1. PPTP (*Point to Point Tunneling Protocol*).

PPTP merupakan salah satu type VPN yang paling sederhana dalam konfigurasi.[11] Selain itu juga fleksibel. Mayoritas operating system sudah support sebagai PPTP Client, baik operating system pada PC ataupun gadget seperti android. Komunikasi PPTP menggunakan protokol TCP port 1723, dan menggunakan IP Protocol 47/GRE untuk enkapsulasi paket datanya. Pada setting PPTP, kita bisa menentukan network security protocol yang digunakan untuk proses autentikasi PPTP pada Mikrotik, seperti pap, chap, mschap dan mschap2. Kemudian setelah tunnel terbentuk, data yang ditransmisikan akan dienkripsi menggunakan Microsoft Point-to-Point Encryption (MPPE). Proses enkripsi biasanya akan membuat ukuran header paket yang ditransmisikan akan bertambah. Jika kita monitoring, traffick yang melewati tunnel PPTP akan mengalami overhead

2. L2TP (*Layer Two Tunneling Protocol*).

L2TP merupakan pengembangan dari PPTP ditambah L2F. Network security Protocol dan enkripsi yang digunakan untuk autentikasi sama dengan PPTP. Akan tetapi untuk melakukan komunikasi, L2TP menggunakan UDP port 1701. Biasanya untuk keamanan yang lebih baik, L2TP dikombinasikan dengan IPsec, menjadi L2TP/IPsec.[12] Contohnya untuk Operating system Windows, secara default OS Windows menggunakan L2TP/IPsec. Akan tetapi, konsekuensinya tentu saja konfigurasi yang harus dilakukan tidak se-simple PPTP. Sisi client pun harus sudah support IPsec ketika menerapkan L2TP/IPsec. Dari segi enkripsi, tentu enkripsi pada

L2TP/IPSec memiliki tingkat sekuritas lebih tinggi daripada PPTP yg menggunakan MPPE. Traffick yang melewati tunnel L2TP akan mengalami overhead

3. SSTP (*Secure Socket Tunneling Protocol*).

Untuk membangun vpn dengan metode SSTP diperlukan sertifikat SSL di masing-masing perangkat, kecuali keduanya menggunakan RouterOS. Komunikasi SSTP menggunakan TCP port 443 (SSL), sama hal nya seperti website yang secure (https). Anda harus memastikan clock sudah sesuai dengan waktu real jika menggunakan certificate. Manyamakan waktu router dengan real time bisa dengan fitur NTP Client. Sayangnya belum semua OS Support VPN dengan metode SSTP. Traffick yang melewati tunnel SSTP akan mengalami overhead.

4. OpenVPN

VPN ini biasa digunakan ketika dibutuhkan keamanan data yang tinggi. Secara default, OpenVPN menggunakan UDP port 1194 dan dibutuhkan certificate pada masing-masing perangkat untuk bisa terkoneksi. Untuk client compatibility, OpenVPN bisa dibangun hampir pada semua Operating System dengan bantuan aplikasi pihak ketiga. OpenVPN menggunakan algoritma sha1 dan md5 untuk proses autentikasi, dan menggunakan beberapa chiper yaitu blowfish128, aes128, aes192 dan aes256. Trafik yang melewati tunnel OpenVPN akan mengalami overhead.

5. L2TP+IPsec

Salah satu service VPN yang terdapat di Mikrotik adalah **L2TP (Layer 2 Tunneling Protocol)**. [13] L2TP merupakan pengembangan dari PPTP ditambah L2F. Network security Protocol dan enkripsi yang digunakan untuk autentikasi sama dengan PPTP. Akan tetapi untuk melakukan komunikasi, L2TP menggunakan UDP port 1701. Biasanya untuk keamanan yang lebih baik, L2TP dikombinasikan dengan IPSec, menjadi L2TP/IPSec. Contohnya untuk Operating system Windows, secara default OS Windows menggunakan L2TP/IPSec. Akan tetapi, konsekuensinya tentu saja konfigurasi yang harus dilakukan tidak se-simple PPTP. Sisi client pun harus sudah support IPSec ketika menerapkan L2TP/IPSec. Dari segi enkripsi, tentu enkripsi pada L2TP/IPSec memiliki tingkat sekuritas lebih tinggi daripada PPTP yg menggunakan MPPE. L2TP lebih (*firewall friendly*) dibandingkan jenis VPN yang lainnya seperti PPTP. Hal ini sebuah Keuntungan besar jika menggunakan protocol ini, karena kebanyakan Firewall tidak mensupport GRE. Namun untuk L2TP tidak memiliki encripsi sehingga kita memerlukan service tambahan guna menunjang

keamanan yang lebih tinggi. Oleh karena itu kita akan memadukan L2TP dengan IPSec.

2.5 Mikrotik

Rahmat Hidayat (2019) menyatakan bahwa mikrotik merupakan sistem operasi berupa perangkat lunak yang digunakan untuk menjadikan komputer menjadi router jaringan.[2] Sistem operasi ini sangat cocok untuk keperluan administrasi jaringan komputer, misalnya untuk membangun sistem jaringan komputer skala kecil maupun besar. Perbedaan mikrotik dengan sistem operasi lama adalah kelebihan fitur wirelessnya. Maka tak heran jika mikrotik disebut sebagai salah satu sistem operasi yang paling ringan dan sederhana. Dengan demikian, banyak warnet yang menggunakan mikrotik.

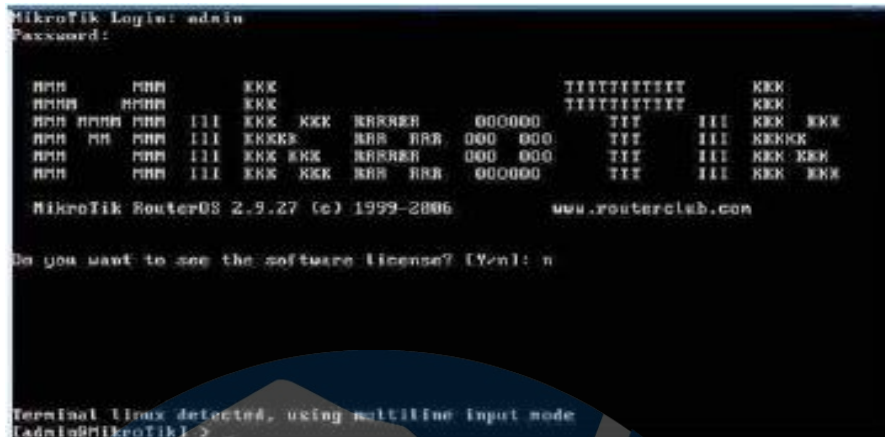
Namun banyak orang masih bingung dengan perbedaan antara mikrotik dan router. Router adalah perangkat keras yang berfungsi untuk menjembatani antara 2 jaringan. Sementara itu, mikrotik adalah sistem operasi yang termasuk dalam open source system namun bukan berarti termasuk software gratis. Mikrotik banyak digunakan oleh ISP, provider hotspot, ataupun perusahaan untuk kebutuhan intranet dan internet. Fasilitas yang ditawarkan mikrotik seperti management bandwidth, statefull firewall, hotspot for plug-and-play access, remote winbox GUI admin, dan routing

2.5.1 Jenis Mikrotik

Mikrotik tersedia tidak hanya dalam satu macam saja. Perusahaan mikrotik mengembangkan dua jenis produknya yang diberi nama Mikrotik RouterOS dan RouterBoard.[13] Berikut adalah penjelasannya:

1. Mikrotik RouterOS

Mikrotik RouterOS merupakan sistem operasi berbasis UNIX yang mampu menjadikan komputer biasa yang mampu menyediakan fitur seperti router, firewall, bridge, hotspot, proxy server dan lainnya. Karena sangat mudah digunakan, banyak orang menggunakan sistem operasi ini untuk membangun router mereka.



Gambar 2.8 Mikrotik RouterOS

2. RouterBoard

Jika Mikrotik RouterOS berupa sistem operasi perangkat lunak, RouterBoard justru sebuah perangkat keras jaringan yang dikembangkan oleh Perusahaan Mikrotik. RouterBoard diinstal sistem operasi mikrotik RouterOS. Meski berbentuk perangkat keras, namun RouterBoard berukuran sangat kecil dan praktis. RouterBoard terdiri atas processor, RAM, ROM dan memory flash.



Gambar 2.9 Mikrotik RouterBoard

2.5.2 Fungsi Mikrotik

Belakangan ini banyak perusahaan yang menggunakan mikrotik sebagai router dan hasilnya mereka sangat puas apa yang diberikan mikrotik. Terlebih kemajuan dunia wireless yang menyajikan berbagai macam pelayanan mulai melirik produk ini, berbagai fitur yang ditawarkan mikrotik diantaranya:

1. Firewall dan NAT.

Pada fitur ini mendukung koneksi peer to peer, source NAT dan destination NAT. Mampu memfilter berdasarkan MAC, IP address, Range Port, Protocol IP, pemilihan opsi protocol ICMP, TCP Flags dan MSS.

2. Hotspot Web Gateway.

Hotspot gateway dengan autentifikasi RADIUS mendukung limit data rate, SSL, dan HTTPS.

3. IPSec.

Protokol AH dan ESP untuk IPSec, MODP Diffie-Hellmann groups 1, 2, 5, MD5 dan algoritma SHA1 hashing. Algoritma enkripsi menggunakan DES, 3DES, AES-128, AES-192, AES-256, *Perfect Forward Secrecy* (PFS).

4. Point to Point Tunneling Protocol.

PPTP, PPOE, dan L2TP *Access Concentrator*, protokol autentikasi menggunakan PAP, CHAP, MSCHAPv1, MSCHAPv2, autentikasi dan laporan Radius, Enkripsi MPPE, kompresi untuk PPOE, Limit data rate.

5. Proxy.

Cache untuk FTP dan HTTP proxy server, HTTPS proxy, Transparent proxy untuk DNS dan HTTP, mendukung protokol SOCKS, mendukung parent proxy, static DNS.

6. Routing.

Routing statik dan dinamik seperti contoh : RIP v1/v2, OSPFv2, BGPv4.

7. WinBox.

Aplikasi mode GUI untuk mengakses dan konfigurasi mikrotik

2.5.3 Lisensi Mikrotik

Mikrotik RouterOS merupakan Operating System yang diperuntukan untuk RouterBoard Mikrotik. RouterOS dapat didownload secara gratis disini. Walaupun gratis namun pada RouterOS terdapat sebuah lisensi. Lisensi ini mengikat pada media penyimpanan, sehingga ketika terjadi kerusakan pada peripheral RouterBoard selain pada harddisk, lisensi ini tidak akan hilang.

Hampir semua lisensi pada Mikrotik berbayar namun beberapa juga gratis. Lisensi RouterOS dapat dibeli pada website resmi Mikrotik maupun reseller Mikrotik. Pada RouterOS Lisensi dibedakan menjadi enam :

➤ Lisensi level 0 (Free)

Lisensi pada Mikrotik dimulai dari level 0 yang merupakan lisensi tidak berbayar alias free, fitur-fiturnya dibuka semua tanpa dibatasi. Hanya saja lisensi ini dibatasi waktu yaitu 24 jam. Maksud dari 24jam adalah durasi penggunaan, waktu

24jam tersebut akan berkurang jika kita menggunakan/membuka RouterOS dengan lisensi tersebut.

➤ **Lisensi level 1 (Demo)**

Lisensi level 1 ini juga Free alias gratis. Perbedaan pertama dengan level 0 adalah anda harus mendaftarkan akun di www.mikrotik.com. Perbedaan kedua adalah masa berlaku lisensinya. Dimana level 0 dibatasi 24jam waktu penggunaan. Sedangkan Level 1 Unlimited

➤ **Lisensi level 3 (CPE)**

Lisensi ini biasanya sudah melekat pada perangkat CPE (Customer Premise Equipment) atau perangkat station. Dimana perangkat dengan level 3 ini tidak dapat menjadi Access Point (tidak dapat memancarkan sinyal) hanya bisa menerima sinyal (station).

➤ **Lisensi level 4 (WISP)**

Level 4 ini adalah lisensi yang umum digunakan untuk router entry-level. Diperuntukan untuk pengguna rumahan yang tidak banyak penggunanya.

➤ **Lisensi level 5 (WISP)**

Lisensi level 5 ini biasanya sudah melekat pada router mid-range. Dengan user 500 sampai unlimited, lisensi ini cocok untuk router yang akan digunakan pada jaringan skala menengah hingga atas.

➤ **Lisensi level 6 (Controller)**

Merupakan Lisensi tertinggi dari MikroTik. Lisensi ini biasanya ditanamkan pada router high-end mikrotik seperti seri CCR (Cloud Core Router). Dengan maksimal user unlimited, level 6 dapat anda gunakan untuk router yang handle jaringan skala besar seperti ISP misalnya.

2.6 Penelitian Terkait

Adapun penelitian terdahulu terkait dengan penelitian yang telah dilakukan oleh peneliti diantaranya tergambar dalam tabel dibawah ini:

Tabel 2.1 Penelitian Terkait

No	Judul Penelitian	Tahun	Kesimpulan
1	Perancangan dan Implementasi	2019	1. Rancangan Virtual Private Network (VPN) berbasis layer 2 tunneling protokol dan IPsec

<p>Virtual Private Network (VPN) Berbasis Protokol Layer 2 Tunneling Protokol (L2TP) dan IPSec dengan menggunakan router mikrotik (Studi Kasus PT.Haruka Evolusi Digital Utama) [2]</p>	<p>telah berfungsi sesuai dengan konfigurasi yang telah terancang. Rancangan yang implementasikan oleh peneliti adalah dengan menambahkan fitur Layer 2 Tunneling Protokol (L2TP) yang dipadukan dengan IP Security (IPSec) dengan mengkonfigurasi perangkat router MikroTik RB1100AHx2 sebagai Virtual Private Network (VPN) Server dan router MikroTik RB450G sebagai Virtual Private Network (VPN) Client. Hal ini dibuktikan dengan adanya autentikasi Virtual Private Network (VPN) Client berupa username dan password yang sesuai dengan konfigurasi yang telah dirancang sebelumnya.</p> <p>2.Virtual Private Network (VPN) berbasis L2TP dan IPsec dapat terhubung dengan baik, dapat dilihat dari hasil pengujian koneksi jaringan yang dilakukan dengan melakukan percobaan koneksi dengan mengirimkan paket ICMP (ping) secara terus menerus sebanyak 30 kali dari Virtual Private Network (VPN) Server menuju Virtual Private Network (VPN) Client, begitupun sebaliknya serta melakukan pengujian traceroute untuk trace route untuk melihat apakah paket yang dikirim sudah melewati jaringan L2TP yang dibuat. sehingga dapat disimpulkan dalam rancangan dan implementasi Virtual Private Network (VPN) berbasis layer 2 tunneling protokol dan IPsec pertukaran data dan informasi antar gedung divisi menjadi lebih ekonomis, efisien dan aman melalui jaringan (public network atau internet).</p> <p>3.Performasi dari Virtual Private Network (VPN) berbasis layer 2 tunneling protokol dan IPsec cukup baik, hal ini didapat dari hasil pengujian pada jenis tunnel berbeda secara bergantian. Dapat dilihat pada tabel pengujian performa terhadap kedua protokol tersebut bahwa protokol L2TP lebih cepat dibandingkan dengan menggunakan L2TP dan IPSec. karena pada protokol L2TP memiliki kemampuan untuk memungkinkan eksekusi beberapa perintah</p>
---	---

			<p>dalam waktu yang sama (Multithreading) sedangkan pada protokol L2TP over IPsec membutuhkan waktu yang lama dalam melakukan proses pertukaran kunci dalam hal ini proses pembentukan SA dan dukungan penggunaan algoritma enkripsi serta otentifikasi. Penurunan performa mungkin terjadi tergantung dari kondisi perangkat yang terhubung secara bersamaan. Perpaduan protokol L2TP dan IPsec dapat memberikan keamanan ganda</p> <p>dalam keamanan suatu jaringan atau yang dikenal Confidential, Integrity, Availability (CIA).</p>
2	Analisa Perbandingan Quality Of Service Antara Protokol PPTP dan L2TP Pada Virtual Private Network Berbasis Router Mikrotik [8]	2019	<ol style="list-style-type: none"> 1. Masing – masing parameter pada setiap percobaan menunjukkan kualitas yang sama. Tetapi perbedaan terdapat pada nilai masing – masing parameter QoS. 2. Parameter delay menunjukkan hasil bahwa PPTP memiliki waktu delay yang lebih singkat dibandingkan dengan L2TP. 3. Pada parameter throughput, PPTP memiliki nilai yang lebih besar dibandingkan L2TP di setiap percobaan. 4. Pada packet loss, baik PPTP maupun tidak terdapat paket yang hilang. 5. Kinerja protokol PPTP pada jaringan VPN lebih baik dari protokol L2TP dari pengujian sisi Quality of Service (QoS) yang dilakukan
3	Analisis Jaringan VPN Menggunakan PPTP dan L2TP [10]	2017	<p>Secara umum PPTP memiliki QoS yang lebih baik dibandingkan L2TP. Perbandingan rata-rata delay antara PPTP dan L2TP memperlihatkan terjadi kenaikan delay 15% hingga 44% pada saat menggunakan L2TP. Performansi L2TP dilihat dari parameter QoS memiliki nilai yang lebih kecil dibandingkan PPTP, tetapi masih termasuk kategori sangat bagus sesuai dengan standarisasi TIPHON. Penambahan IPsec pada L2TP untuk memberikan pengamanan yang lebih baik menyebabkan proses pengiriman data menjadi lebih lama dibandingkan PPTP. Paket</p>

			data L2TP didapatkan memiliki enkripsi yang lebih berlapis dibandingkan PPTP.
4	Analisa Virtual Private Network Menggunakan OpenVPN dan Point to Point Tunneling Protocol [11]	2016	VPN menggunakan PPTP dan OpenVPN dapat diimplementasikan pada jaringan server sehingga user atau client dapat mengakses dimana saja dan kapan saja melalui jaringan internet. Pengujian yang dilakukan pada performa menghasilkan perbedaan yang tidak begitu signifikan, tetapi apabila diamati OpenVPN lebih unggul dari PPTP, hal ini ditunjukkan saat pengujian transfer file OpenVPN memiliki waktu lebih cepat. Sedangkan pada pengujian keamanan OpenVPN lebih unggul dari PPTP, hal ini dapat dilihat dari lebih banyaknya jumlah paket yang diterima oleh OpenVPN saat dilakukan serangan sebelum akhirnya mengalami gangguan pada service VPN.

STT - NF

BAB III

METODOLOGI PENELITIAN

3.1 Metode Penelitian

Di dalam melakukan penelitian, terdapat metode atau metodologi penelitian bervariasi, seorang peneliti harus mengetahui dan menetapkan metode seperti apa yang akan diterapkan di dalam penelitiannya. Berdasarkan rumusan masalah dan tujuan penelitian, bahwa metode yang dipilih oleh peneliti adalah metode kualitatif deskriptif, dengan pendekatan studi kasus yang bertujuan untuk mengetahui sejauh mana kinerja dari hasil pengujian yang dilakukan.

3.2 Teknik Pengumpulan Data

Berikut pengumpulan data yang dilakukan peneliti memperoleh sebuah informasi yang dibutuhkan untuk mencapai tujuan dari penelitian ini, diantara sebagai berikut :

3.2.1 Observasi

Teknik observasi yang dilakukan adalah observasi langsung (Participant Observation). Peneliti melakukan pengamatan langsung terhadap aktivitas jaringan produksi yang berjalan, yang mencakup proses design topologi, analisa, konfigurasi, pengujian.

3.2.2 Studi Pustaka

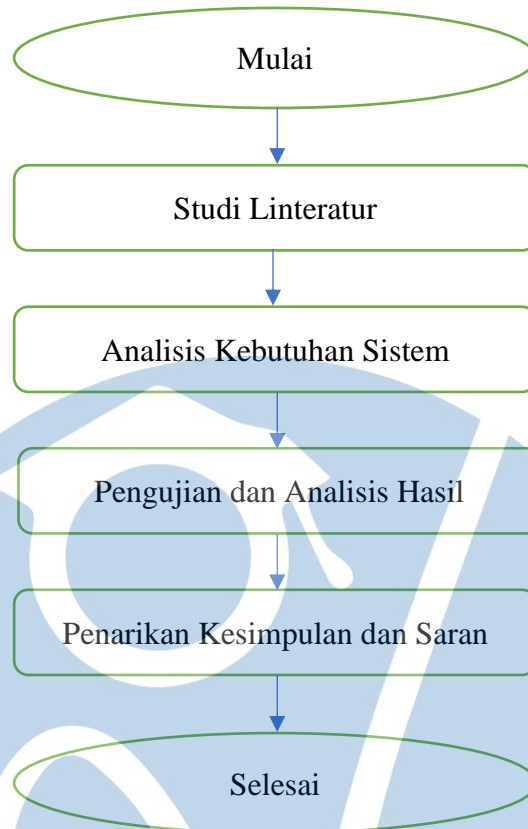
Selain observasi, pengumpulan data dilakukan juga dengan menggunakan teknik dan studi pustaka. Studi pustaka adalah metode yang digunakan untuk menelusuri riwayat data atau mengkaji literatur dan laporan-laporan yang berkaitan dengan judul penelitian.

3.2.3 Wawancara dan Diskusi

Diskusi dan Wawancara dilakukan secara langsung kepada beberapa team dari divisi IT RSUD Bunda Margonda dan IT Head Office.

3.3 Prosedur Penelitian

Dalam tahapan penelitian melakukan serangkaian prosedur tau tahapan -tahapan penelitian sebagai berikut :



Gambar 3.1 Prosedur Penelitian

3.3.1 Studi Literatur

Pada tahapan ini dilakukan dengan mencari, mengumpulkan, serta membaca artikel, buku elektronik (e-book), jurnal ilmiah, website maupun beberapa skripsi penelitian lainnya untuk mengkaji mengenai perancangan dan implementasi Virtual Private Network (VPN) berbasis protokol L2TP dan IPSec. Hasil dari studi literatur adalah pembuatan acuan rancangan penelitian dan acuan bagaimana penelitian harus dilakukan dan data apa saja yang diperlukan untuk tujuan penelitian ini agar dapat tercapai. Analisis yang dilakukan juga berpacu kepada studi literatur yang relevan dengan tema penelitian ini.

3.3.2 Analisis Kebutuhan Sistem

Pada tahap ini penulis melakukan analisis kebutuhan perangkat apa saja yang dapat mendukung konektivitas jaringan unit usaha dengan head office dan dari Client ke jaringan internal unit usaha serta kemudian mengevaluasi hasil temuan dari permasalahan yang ada.

3.3.3 Pengujian dan Analisi Hasil

Pada tahapan ini dilakukan pengujian performa Troughput, Jitter, dan Packet Loss dengan menggunakan tool Iperf dari RSU Bunda Margonda ke Head Office dan Dari Client Ke Jaringan Internal RSU Bunda Margonda

3.3.4 Penarikan Kesimpulan

Dari hasil pengujian dapat ditarik kesimpulan apakah kinerja VPN L2TP+IPSec mempunyai performa yang stabil dibandingkan dengan dibandingkan protokol VPN lainya dan saran – saran untuk perbaikan atau kelanjutan penelitian berikutnya.

3.4 Lingkungan Pengujian

Dalam penelitian ini, penulis melakukan pengujian langsung terhadap jaringan produksi RSU Bunda Margonda, Jl. Margonda Raya No.28, Pondok Cina, Beji Kota Depok, Jawa Barat 16424.

3.5 Alat dan Bahan

Di dalam kegiatan ini dibuthkan beberapa peralatan berupa perangkat keras maupun perangkat lunak. Berikut adalah perangkat lunak yang akan digunakan antara lain :

- Winbox
- IPERF

Adapun perangkat keras yang digunakan untuk melakukan pengujian antara lain :

- Procecor : Intel(R)Core(TM) i5-10210U CPU@ 1.60GHz
- RAM : 8 GB DDR4
- OS : Windows 11 Home SL

3.6 Jadwal Penelitian

Berikut jadwal pelaksanaan penelitian yang dilakukan dalam rentang 7 Bulan, mulai dari bulan Desember 2020 sampai dengan bulan Juni 2021.

Tabel 3.1 Jadwal Penelitian

No	Tahapan Kerja	2020	2021					
		Des	Jan	Feb	Mar	April	Mei	Jun
1	Analisis Sistem							
2	Studi Literatur							
3	Pembuatan Proposal							
4	Presentasi Proposal							
5	Analisis dan Perancangan							
6	Implementasi dan Pengujian							
7	Penarikan Kesimpulan dan Saran							
8	Pra Sidang							
9	Sidang							

STT - NF

BAB IV

ANALISA PERANCANGAN

Pada bab ini peneliti akan menguraikan analisa dan perancangan yang akan diterapkan dalam penelitian.

4.1 Analisa Sistim Berjalan

Pada jaringan produksi RSU Bunda Margonda yang berjalan saat ini terdiri dari beberapa unit pelayanan, dari poliklinik utama sudah terkoneksi menggunakan kabel fiber optic ke poliklinik BPJS dan Poliklinik Eksekutif, dimana setiap user akan melakukan pertukaran data baik secara internal maupun secara external (Head Office) untuk kepentingan unit masing-masing sehingga pelayanan menjadi optimal. Kondisi saat sekarang ini pertukaran data secara external (head office) masih menggunakan email dan google drive sehingga untuk mengakses data tersebut masih menggunakan public server di internet sehingga pertukaran data tidak bisa diakses langsung dari user RSU Bunda Margonda ke File Sharing yang ada di server local head office. Untuk mendukung kebutuhan ini salah satu cara menghubungkan jaringan RSU Bunda Margonda (internal) dengan Head Office (external) agar menjadi satu jaringan private adalah dengan menggunakan Virtual Private Network (VPN) berbasis protokol L2TP+IPSec pada jaringan produksi yang berjalan.

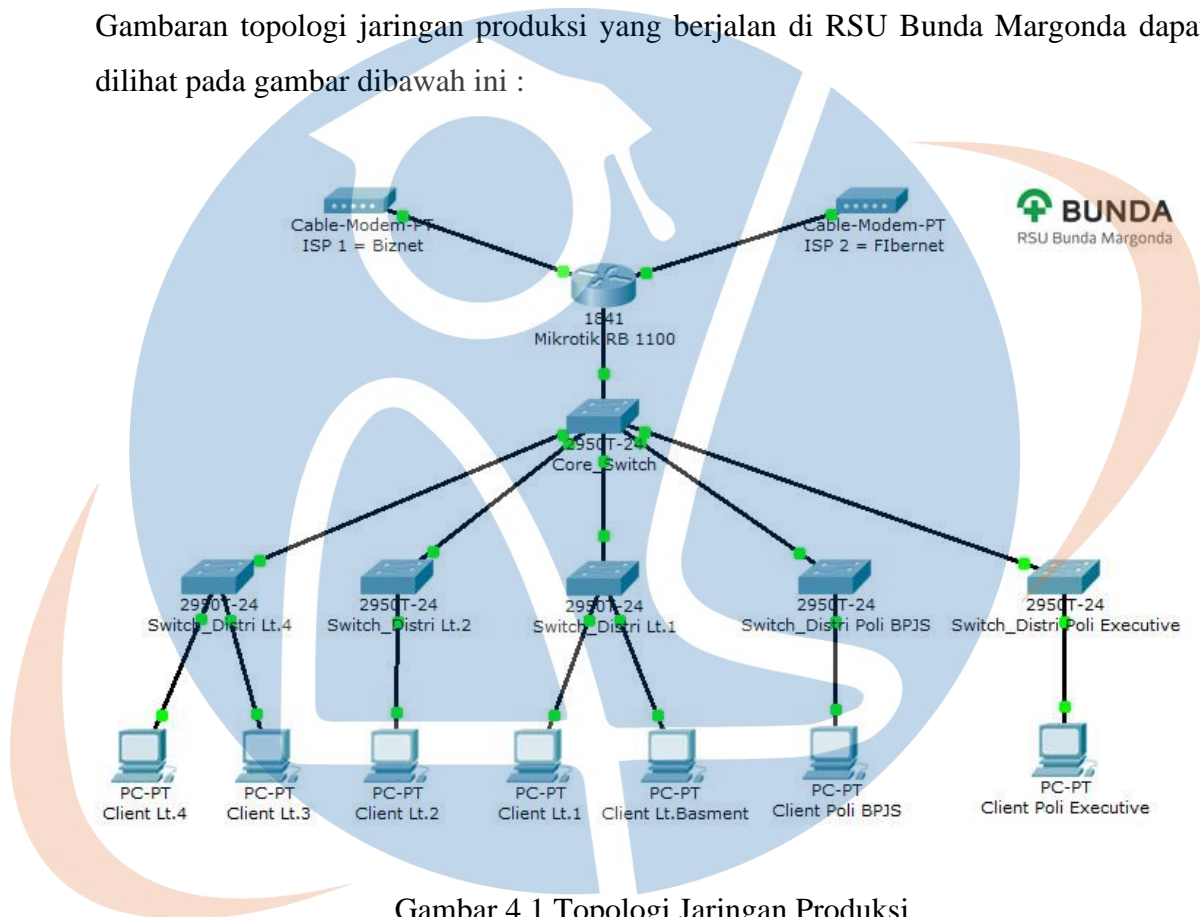
Segmen IP address yang digunakan di RSU Bunda Margonda dapat dilihat pada tabel dibawah ini:

Tabel 4.1 Pengalamatan IP Address

IP Address	Keterangan
202.169.57.194/29	IP Public Main Line RSU Bunda Margonda
103.157.81.114/29	IP Public Backup Line RSU Bunda Margonda
10.50.20.254/24	IP Local VoIP RSU Bunda Margonda
10.50.30.254/24	IP Local Server RSU Bunda Margonda
10.50.40.254/24	IP Local Lantai Besment RSU Bunda Margonda
10.50.50.254/24	IP Local Lantai 1 RSU Bunda Margonda
10.50.60.254/24	IP Local Lantai 2 RSU Bunda Margonda

10.50.70.254/24	IP Local Lantai 3 RSU Bunda Margonda
10.50.80.254/24	IP Local Lantai 4 RSU Bunda Margonda
10.50.90.254/24	IP Local Poliklinik BPJS RSU Bunda Margonda
10.50.91.254/24	IP Local Poli Eksekutif RSU Bunda Margonda

Gambaran topologi jaringan produksi yang berjalan di RSU Bunda Margonda dapat dilihat pada gambar dibawah ini :



Gambar 4.1 Topologi Jaringan Produksi

4.2 Analisa Kebutuhan Sistim

4.2.1 Analisa Kebutuhan Internet

PT. Bundamedik Healthcare System (BMHS) memiliki sumber bandwidth dengan menggunakan jasa layanan *Internet Service Provider* (ISP) di masing-masing unit usaha maupun di Head Office sendiri. Pada Head Office menggunakan mainline internet dengan bandwitdh dedicated sebesar 50 Mbps dan backup line dengan bandwitdh dedicated sebesar 30 Mbps, sedangkan di RSU Bunda Margonda memiliki bandwitdh dedicated sebesar 60 Mbps serta penambahan link untuk backup dengan bandwitdh dedicated sebesar 10 Mbps.

Untuk unit usaha lainnya harus memiliki minimal bandwidth dedicated sebesar 30 Mbps atau Upto 75 Mbps untuk kestabilan koneksi tunneling vpn ke head office.

4.2.2 Analisa Pengalamatan IP Address

Pada analisa pengalamatan IP Address yang akan digunakan pada saat implementasi menggunakan IPV4. Terdapat IP Publik yang didapat dari *Internet Service Provider* (ISP) adalah IP Statik sehingga IP Address bersifat tetap, sedangkan untuk IP lokal menggunakan DHCP agar mempermudah dalam mendistribusikan IP kepada Komputer Client. Untuk VPN server site to site menggunakan IP Public mainline ISP head office dengan IP Address **103.123.65.123**, sedangkan untuk IP Tunneling VPN sendiri menggunakan IP Address **10.20.30.1/24** dengan segmen terpisah, sehingga antara IP Address local dan IP Address VPN tidak mengalami deadlock, hal ini memudahkan juga untuk pengalamatan IP Address seandainya ada keperluan dari unit usaha lainnya untuk melakukan koneksi ke VPN server head office.

Sedangkan untuk VPN server di RSUD Bunda Margonda sendiri menggunakan IP Public dari mainline ISP **202.169.57.194** dan IP Tunneling VPN untuk untuk kebutuhan remote acces menggunakan IP Address **192.168.17.1/24**.

4.2.3 Analisa Kebutuhan Hardware

Perangkat router yang digunakan di Head Office maupun di RSUD Bunda Margonda adalah perangkat Mikrotik, untuk spesifikasi lengkapnya dapat dilihat pada tabel dibawah ini:

- Router Mikrotik Head Office RB1100Ahx2 digunakan sebagai VPN server.

Tabel 4.2 Spesifikasi Routerboard 1100 AHx2 VPN Server

Details RB1100AHx2 Router 1310/100/1000 Lev.6 Multi Processor	
Product code	RB1100AHx2
Architecture	PPC
CPU	P202ASSE2KFB
CPU core count	2
CPU nominal frequency	1066 MHz

Dimensions	1U case: 44 x 176 x 442 mm, 1200g. Board only: 365g
License level	6 (Wireless Client and Bridge, Wireless AP, Synchronous interface, EoIP tunnels, PPPoE tunnels, PPTP tunnels, L2TP tunnels, VLAN interfaces, P2P firewall rules, NAT rules1, HotSpot active users, RADIUS client, Queues1, Web proxy, RIP, OSPF, BGP protocols, Upgrade) Unlimited
Operating System	RouterOS
Size of RAM	2 GB
Storage size	128 MB
Storage type	NAND
Tested ambient	-35°C to 70°C

- Router Mikrotik RSU Bunda Margonda RB1100Ahx2 digunakan sebagai VPN Client.

Tabel 4.3 Spesifikasi Routerboard 1100 AHx2 VPN Client

Details RB1100AHx2 Router 1310/100/1000 Lev.6 Multi Processor	
Product code	RB1100AHx2
Architecture	PPC
CPU	P202ASSE2KFB
CPU core count	2
CPU nominal frequency	1066 MHz
Dimensions	1U case: 44 x 176 x 442 mm, 1200g. Board only: 365g
License level	6 (Wireless Client and Bridge, Wireless AP, Synchronous interface, EoIP tunnels, PPPoE tunnels, PPTP tunnels, L2TP tunnels, VLAN interfaces, P2P firewall rules, NAT rules1, HotSpot active users, RADIUS client, Queues1, Web proxy, RIP, OSPF, BGP protocols, Upgrade) Unlimited
Operating System	RouterOS
Size of RAM	2 GB
Storage size	128 MB
Storage type	NAND
Tested ambient	-35°C to 70°C

4.2.4 Analisa Kebutuhan Software

Software (perangkat lunak) yang dibutuhkan dalam melakukan proses intruksi atau menjalankan perangkat keras untuk mendukung pengujian kinerja VPN L2TP+IPSec ini, serta berdasarkan hasil rekomendasi yang didapatkan penulis dari penelitian terkait antara lain dapat dilihat pada tabel dibawah ini:

Tabel 4.4 Spesifikasi Kebutuhan Software

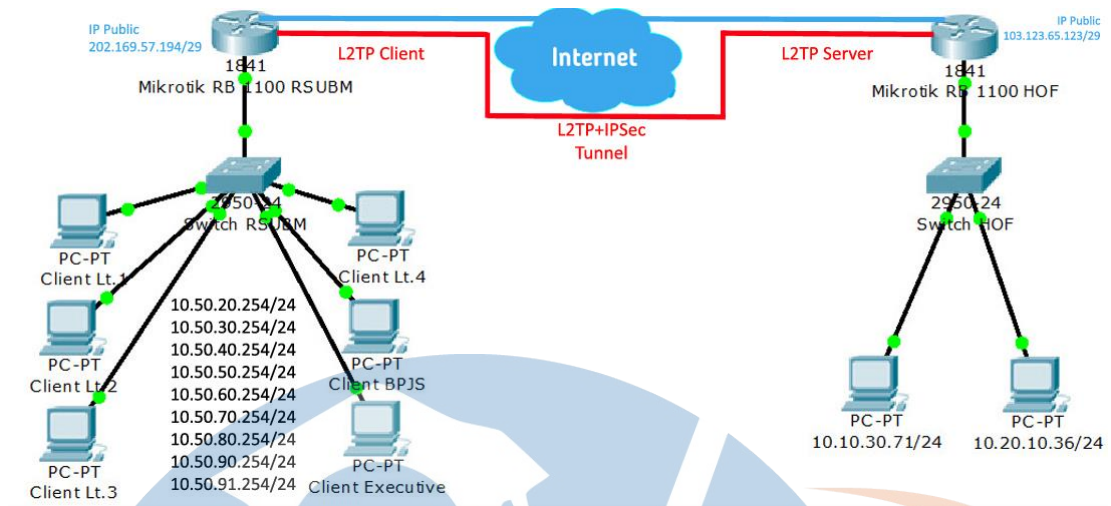
Nama	Versi	Keterangan
Winbox	3.18	Digunakan sebagai utility untuk meremote perangkat mikrotik kedalam mode GUI (Graphical User Interface).
Iperf	3.13	Digunakan sebagai tool Network Analyzer yang banyak digunakan oleh Network Administrator untuk menganalisa kinerja jaringannya dan mengontrol lalu lintas data.

4.3 Perancangan Sistim

4.3.1 Perancangan Topologi VPN L2TP+IPSec Site to Site

Setelah menganalisa kebutuhan pada jaringan yang berjalan saat ini, supaya pertukaran data menjadi optimal dan efisien, penulis menerapkan Virtual Private Network (VPN) berbasis L2TP+IPSec menggunakan tipe site to site antara RSUD Bunda Margonda dengan Head Office supaya menjadi satu jaringan private.

Berikut ini rancangan topologi jaringan menggunakan VPN L2Tp+IPSec dengan tipe site to site :

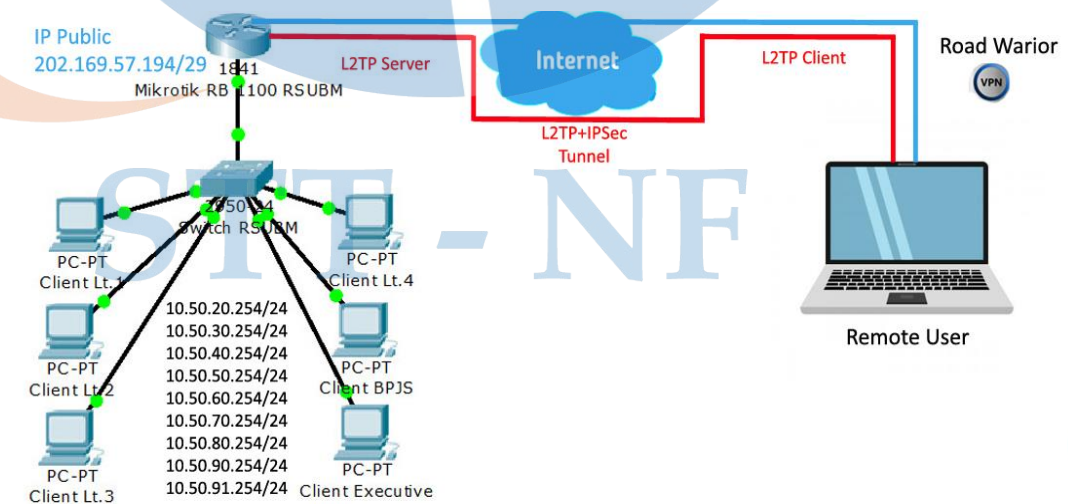


Gambar 4.2 Topologi VPN L2TP+IPSec Site to Site

4.3.2 Perancangan Topologi VPN L2TP+IPSec Remote Access

Setelah perancangan topologi VPN L2TP+IPSec Site to Site antara RSU Bunda Margonda dengan Head Office, penulis juga merancang tipe VPN L2TP+IPSec Remote Access hal ini bertujuan mengoptimalkan unit tertentu seperti direktur, manager, dan staff bagian lainnya yang berada di luar rumah sakit maupun yang bekerja di rumah (wfh) dapat melakukan akses ke jaringan produksi RSU Bunda Margonda sesuai dengan kebutuhannya masing-masing.

Berikut ini rancangan topologi jaringan menggunakan VPN L2TP+IPSec dengan tipe remote access :



Gambar 4.3 Topologi VPN L2TP+IPSec Remote Access

4.4 Perancangan Pengujian VPN L2TP+IPSec

4.4.1 Perancangan Fungsionalitas VPN

Perancangan fungsionalitas VPN ini bertujuan untuk menguji dan memastikan bahwa komunikasi antar site berlangsung melalui tunneling VPN L2TP+IPSec dengan menggunakan tool iperf yang sudah terpasang di VPN server dan di VPN Client, dengan cara melakukan ping dan memastikan dari header packet network nya, apakah IP Address source dan IP Address destination berasal dari IP Tunneling VPN yang sudah di konfigurasi.

4.4.2 Perancangan Pengujian Performa Throughput

Throughput yaitu kecepatan (rate) transfer data efektif diukur dalam bps.[14] Throughput merupakan jumlah total kedatangan paket yang sukses yang diamati pada tujuan selama interval waktu tertentu dibagi oleh durasi interval waktu tersebut.[7]

Nilai throughput berdasarkan standar TIPHON dapat dilihat pada tabel dibawah ini [15]:

Tabel 4.5 Index Performa Throughput

Kategori	Troughput	Indeks
Sangat Buruk	0-338 kbps	0
Buruk	338-700 kbps	1
Sedang	700-1200 kbps	2
Bagus	1200 kbps – 2,1 Mbps	3
Sangat Bagus	> 2,1 Mbps	4

Untuk pengujian performa througput antar site dan remote acces dilakukan dengan cara file transfer / test disk menggunakan tool Iperf dan melakukan perhitungannya dengan data sebagai berikut :

Tabel 4.6 Pengujian Throughput

Ukuran File	Troughput / Bandwidth iperf (mbps)
50 Mb	
100 Mb	
150 Mb	
200 Mb	
300 Mb	
400 Mb	
500 Mb	
600 Mb	
700 Mb	
800 Mb	

Setelah rata-rata hasil throughput / bandwidth dari masing – masing pengujiannya di dapat, dengan merujuk ke tabel 4.5 index performa throughput, dapat disimpulkan kategori performa throuput dengan menggunakan tunneling L2TP+IPSec di RSUD Bunda Margonda.

4.4.3 Perancangan Pengujian Performa Jitter

Jitter adalah variasi kedatangan paket, hal ini diakibatkan oleh variasi-variasi dalam panjang antrian, dalam waktu pengolahan data, dan juga dalam waktu penghimpunan ulang paket-paket di akhir perjalanan.[16]

Nilai jitter berdasarkan standar TIPHON dapat dilihat pada tabel dibawah ini[15]:

Tabel 4.7 Index Performa Jitter

Kategori	Jitter	Indeks
Buruk	> 125 ms	1
Sedang	75 – 125 ms	2
Bagus	0 – 75 ms	3
Sangat Bagus	0 ms	4

Untuk pengujian performa jitter antar site dan remote acces dilakukan dengan cara file transfer / test disk menggunakan tool Iperf dan melakukan perhitungannya dengan data sebagai berikut :

Tabel 4.8 Pengujian Jitter

Ukuran File	Jitter (ms)
50 Mb	
100 Mb	
150 Mb	
200 Mb	
300 Mb	
400 Mb	
500 Mb	
600 Mb	
700 Mb	
800 Mb	

Setelah rata-rata hasil jitter dari masing – masing pengujiannya di dapat, dengan merujuk ke tabel 4.7 index peforma jitter, dapat disimpulkan kategori

peforma jitter dengan menggunakan tunneling L2TP+IPSec di RSUD Bunda Margonda.

4.4.4 Perancangan Pengujian Peforma Packet Loss

Merupakan suatu parameter yang menggambarkan suatu kondisi yang menunjukan jumlah total paket yang hilang, dapat terjadi karena collision dan congestion pada jaringan [17]. Untuk pengujian performa packet loss dilakukan perhitungan.

Berikut merupakan perhitungan nilai packet loss berdasarkan standar TIPHON[15]:

Tabel 4.9 Index Peforma Paket Loss

Kategori	Paket Loss	Indeks
Buruk	> 25 %	1
Sedang	15 – 24 %	2
Bagus	3 – 14 %	3
Sangat Bagus	0 – 2 %	4

Untuk pengujian performa paket loss antar site dan remote acces dilakukan dengan menggunakan tool Iperf dan melakukan perhitungannya dengan data sebagai berikut[18] :

Tabel 4.10 Pengujian Paket Loss

Ukuran File	Pcaket Loss (%)
50 Mb	
100 Mb	
150 Mb	
200 Mb	

300 Mb	
400 Mb	
500 Mb	
600 Mb	
700 Mb	
800 Mb	

Setelah rata-rata hasil packet loss dari masing – masing pengujiannya didapat, dengan merujuk ke tabel 4.9 index peforma paket loss, dapat disimpulkan kategori peforma paket loss dengan menggunakan tunneling L2TP+IPSec di RSU Bunda Margonda.

STT - NF

BAB V

IMPLEMENTASI DAN PENGUJIAN

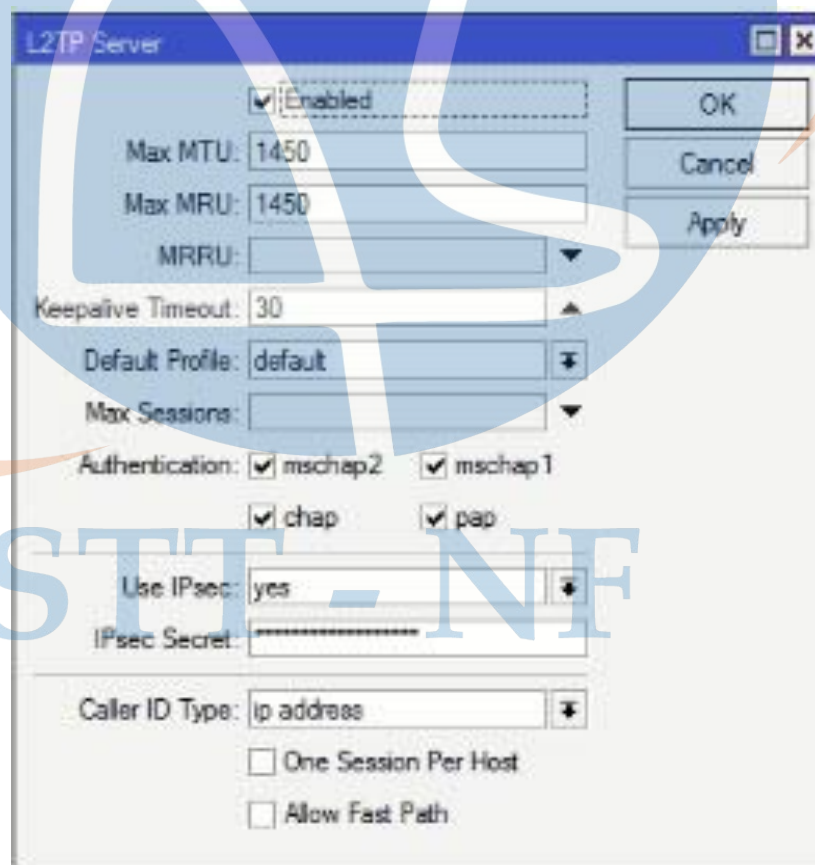
Pada bab ini peneliti akan membahas implementasi dan hasil pengujian kinerja VPN dengan Layer 2 Tunneling Protocol dan IPsec Menggunakan Router Mikrotik di RSUD Bunda Margonda.

5.1 Implementasi

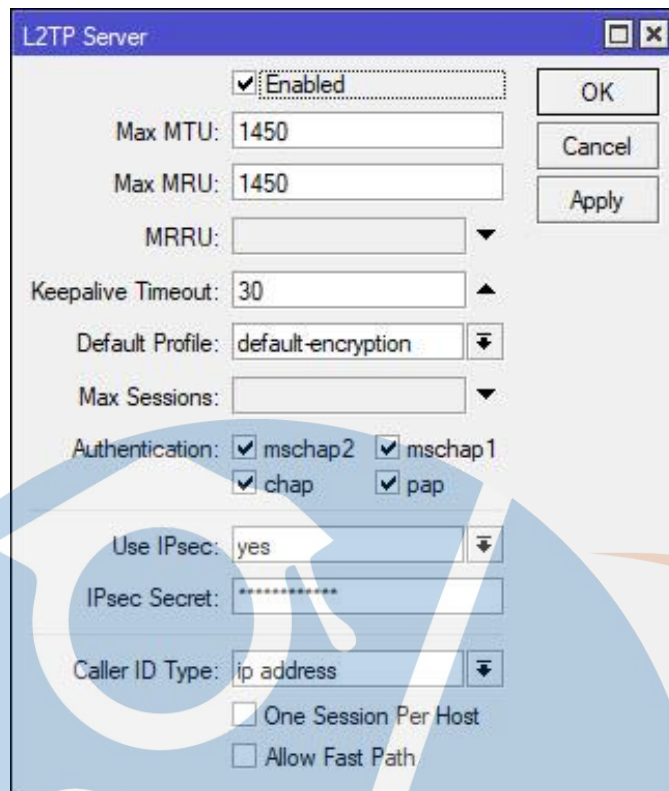
Tahapan implementasi sistem merupakan tahapan konfigurasi Virtual Private Network (VPN) Berbasis Protokol Layer 2 Tunneling Protokol (L2TP) dan IPsec dari sisi server, client dan remote access.

5.1.1 Konfigurasi L2TP+IPsec VPN Server

Pertama, peneliti melakukan konfigurasi untuk *L2TP Server*. Untuk mengaktifkan router sebagai *L2TP server* pada menu **PPP** -> Pilih **L2TP Server**.

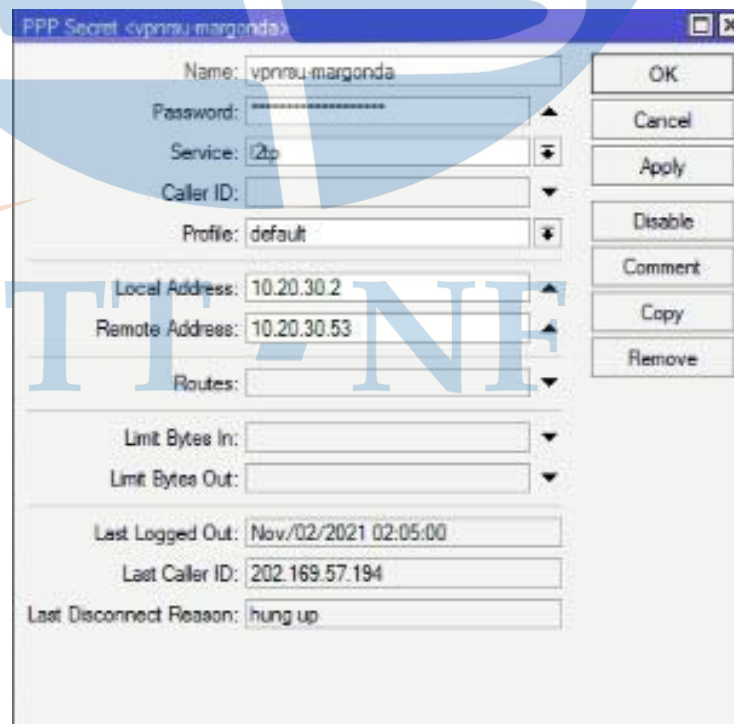


Gambar 5.1 Konfigurasi L2TP Server HOF



Gambar 5.2 Configurasi L2TP Server RSUBM

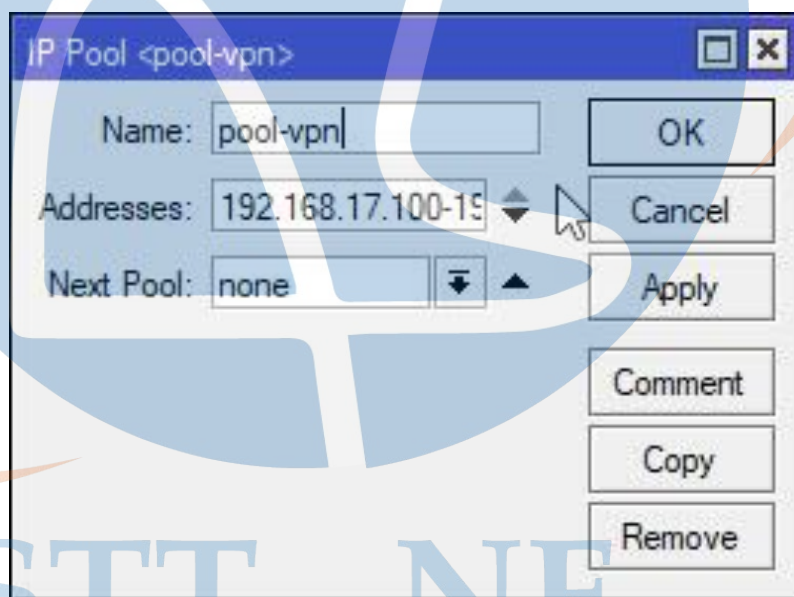
Langkah selanjutnya peneliti mengaktifkan opsi **'Enabled'**, secara otomatis L2TP Server telah aktif. Kemudian peneliti melakukan setting pada Tab **Secret**. Pilih Tab **Secret** -> Klik **Add [+]**.



Gambar 5.3 Configurasi Secret HOF

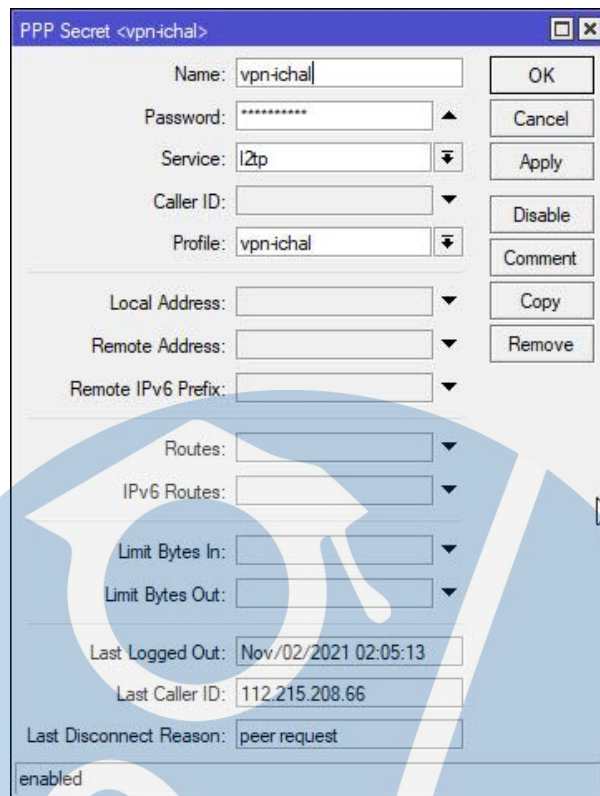
Disini peneliti akan mengisi beberapa parameter standar yang utama untuk melakukan koneksi. Seperti '*Name & Password*' diisikan untuk dial koneksi L2TP dari client. Kemudian '*Service*' bisa diisikan dengan '*l2tp*' dan bisa juga dengan '*any*' untuk semua jenis service PPP. Dan parameter selanjutnya yang juga penting adalah setting Ip Address pada "*Local Address*" dan "*Remote Address*". IP Address inilah yang nantinya kan ditambahkan secara otomatis ketika koneksi L2TP terbentuk dan sebagai gateway untuk komunikasi data. Peneliti juga menambahkan pada parameter "*Route*" dengan mengisi network dari 'Kantor Cabang', sehingga akan ditambahkan rule routing baru secara otomatis.

Untuk mikrotik RSU Bunda Margonda karena akan dijadikan server remote access, sebelum peneliti melakukan setting PPP secret dan PPP Profile, peneliti melakukan settingan terlebih dahulu pada IP Pool. IP -> Pool -> add[+]

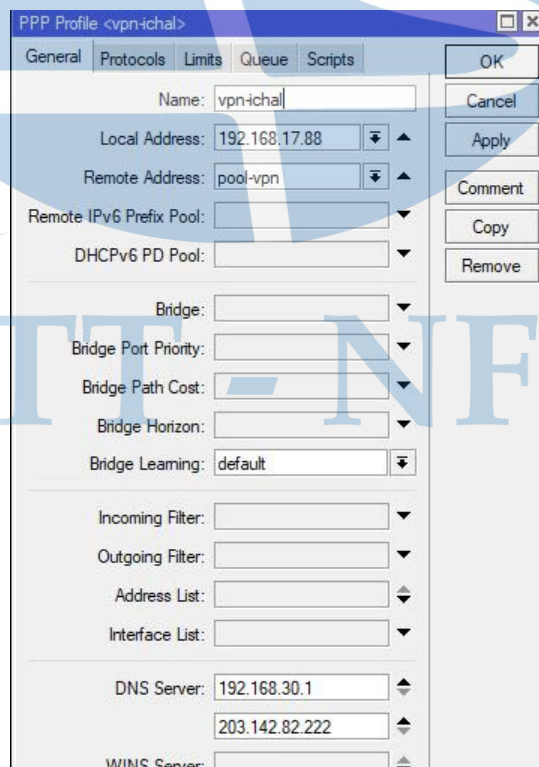


Gambar 5.4 Configurasi IP Pool RSUBM

Setelah itu peneliti melakukan create PPP Profile dan PPP Secret. Pilih Tab Profile -> Klik Add[+], Pilih Tab S=cret -> Klik Add[+].

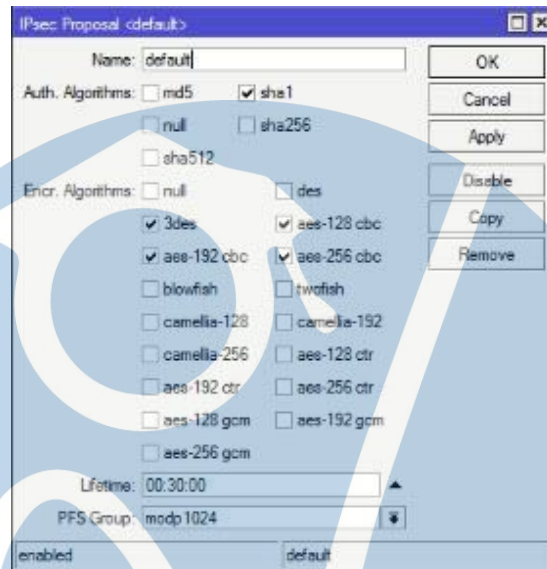


Gambar 5.5 Configurasi Profile RSUBM

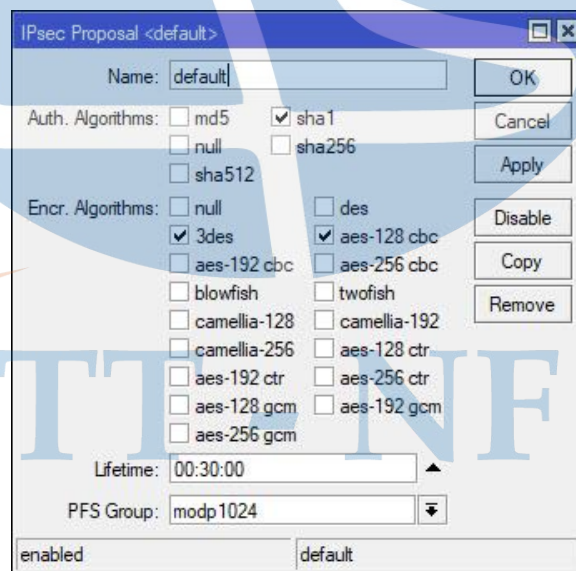


Gambar 5.6 Configurasi Secret RSUBM

Untuk menambah tingkat keamanan peneliti akan memadukan L2TP dengan IPSec. Pilih pada menu IP -> IPSec. Kemudian peneliti akan melakukan setting terlebih dahulu pada tab 'IPsec Proposal'. Pada parameter yang tersedia peneliti isikan seperti tampilan gambar berikut.



Gambar 5.7 Ipsec Proposal HOF

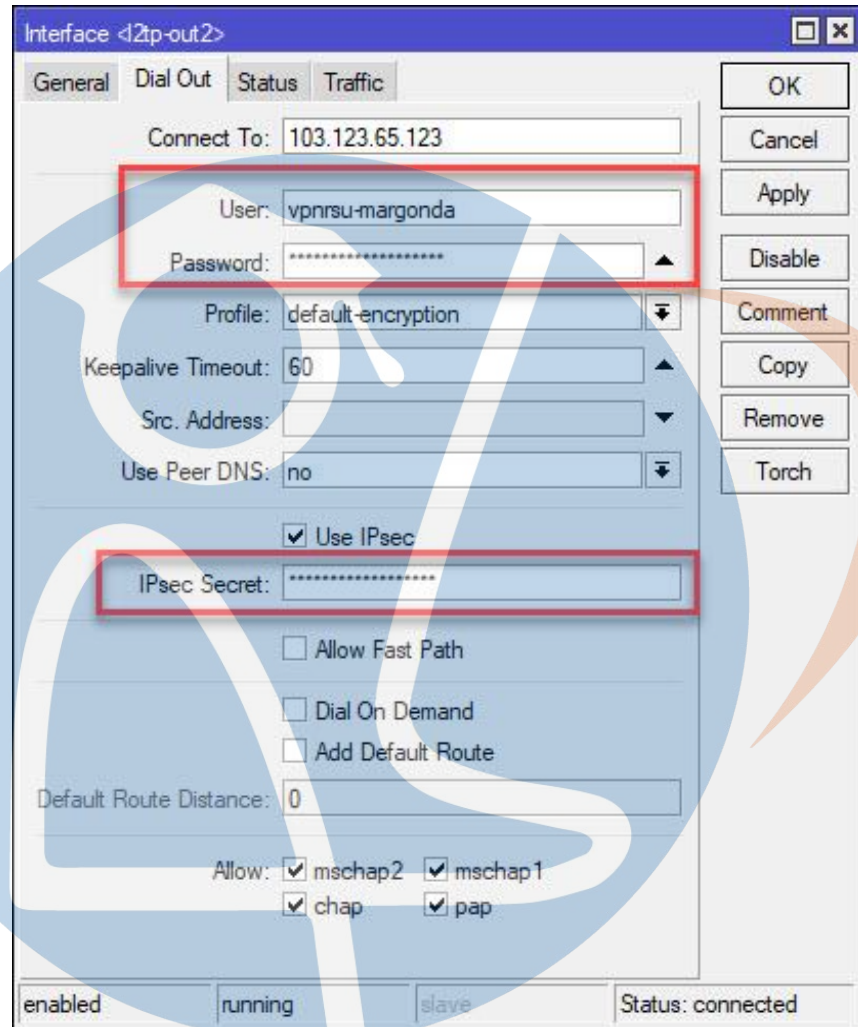


Gambar 5.8 Ipsec Proposal RSUBM

Konfigurasi IPSec untuk L2TP Server sudah selesai dari sisi HOF dan RSU bunda Margonda.

5.1.2 Konfigurasi L2TP+IPSec VPN Client

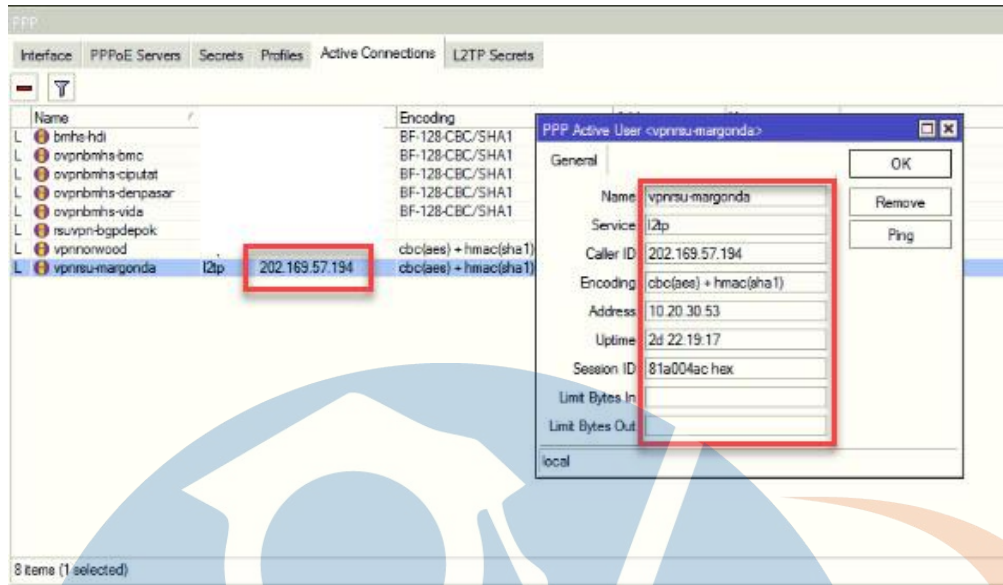
Untuk L2TP Client peneliti melakukan dial ke L2TP server. Pilih Menu PPP | klik Add [+] | pilih L2TP Client. Kemudian akan muncul tampilan seperti berikut.



Gambar 5.9 Connect VPN RSUBM-HOF

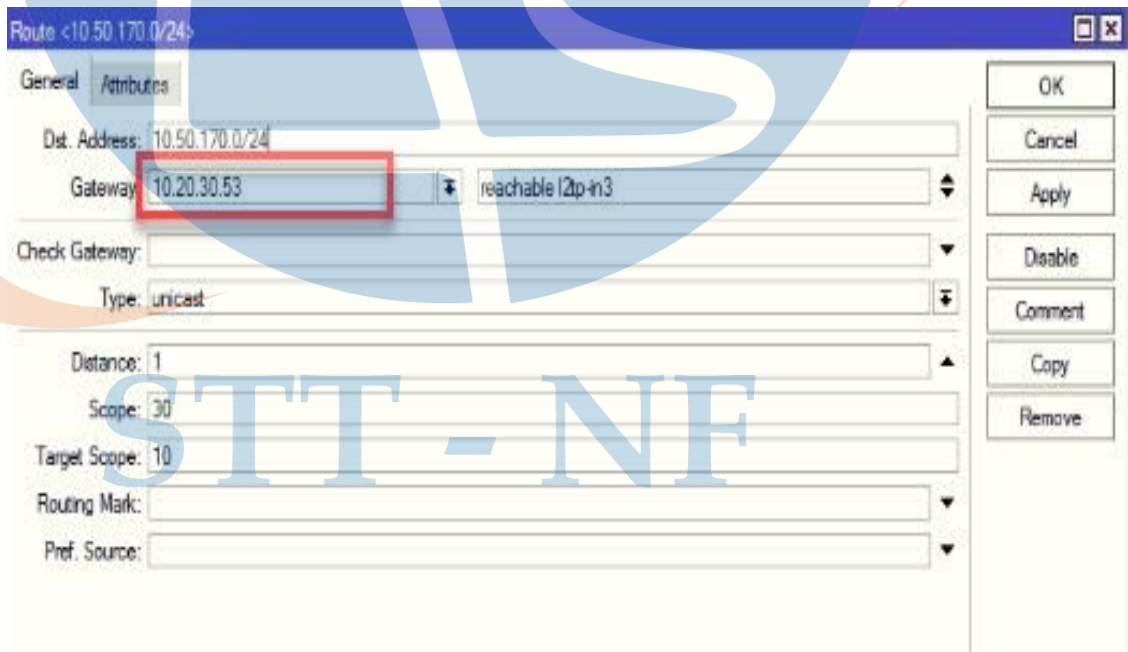
Langkah selanjutnya peneliti melakukan pengisian pada parameter 'Connect to' dengan IP public HOF yang menjadi L2TP server. Kemudian parameter 'User, Password, & IPSecret' peneliti isikan seperti konfigurasi Secret di L2TP server HOF.

Untuk memastikan konfigurasi sudah terkoneksi, peneliti melakukan pengecekan pada PPP | Active Connection di mikrotik HOF kemudian muncul tampilan seperti berikut.

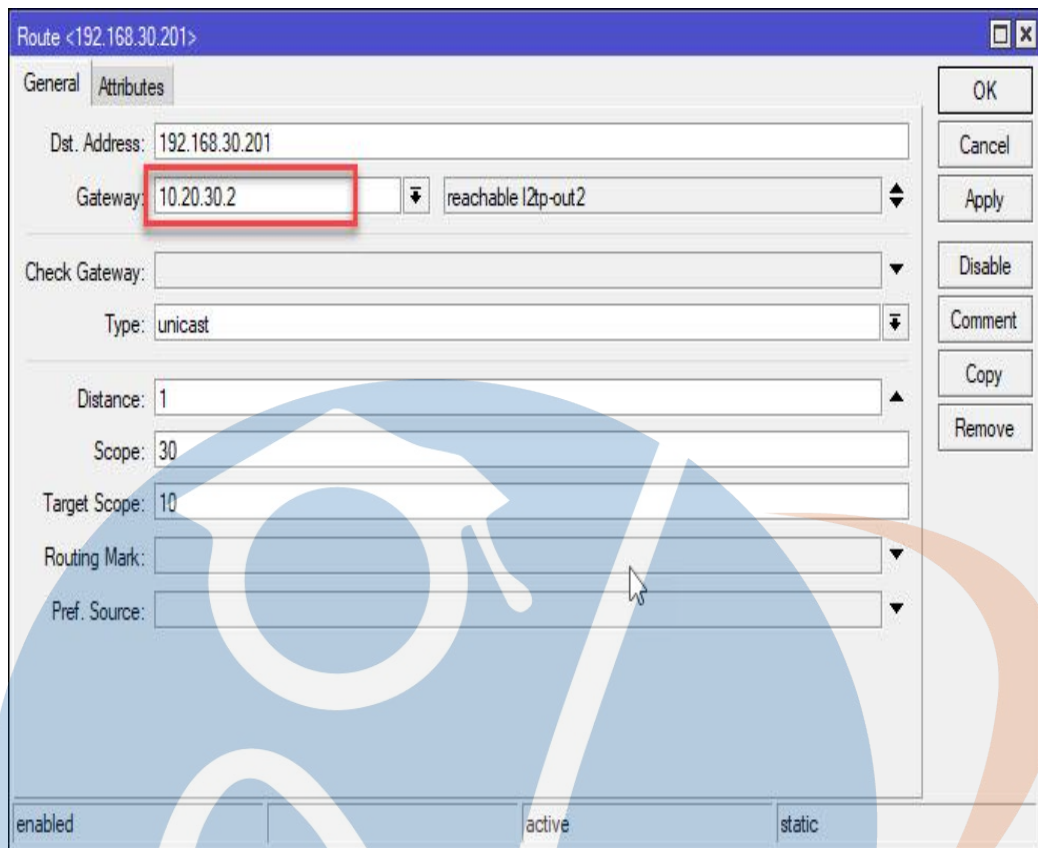


Gambar 5.10 Active Connecton VPN RSUBM

Setelah itu peneliti melakukan proses route di sisi client dan di sisi server dengan pengaturan gateway sesuai dengan IP VPN yang sudah di konfigurasi sebelumnya.



Gambar 5.11 Configurasi Route Mikrotik HOF



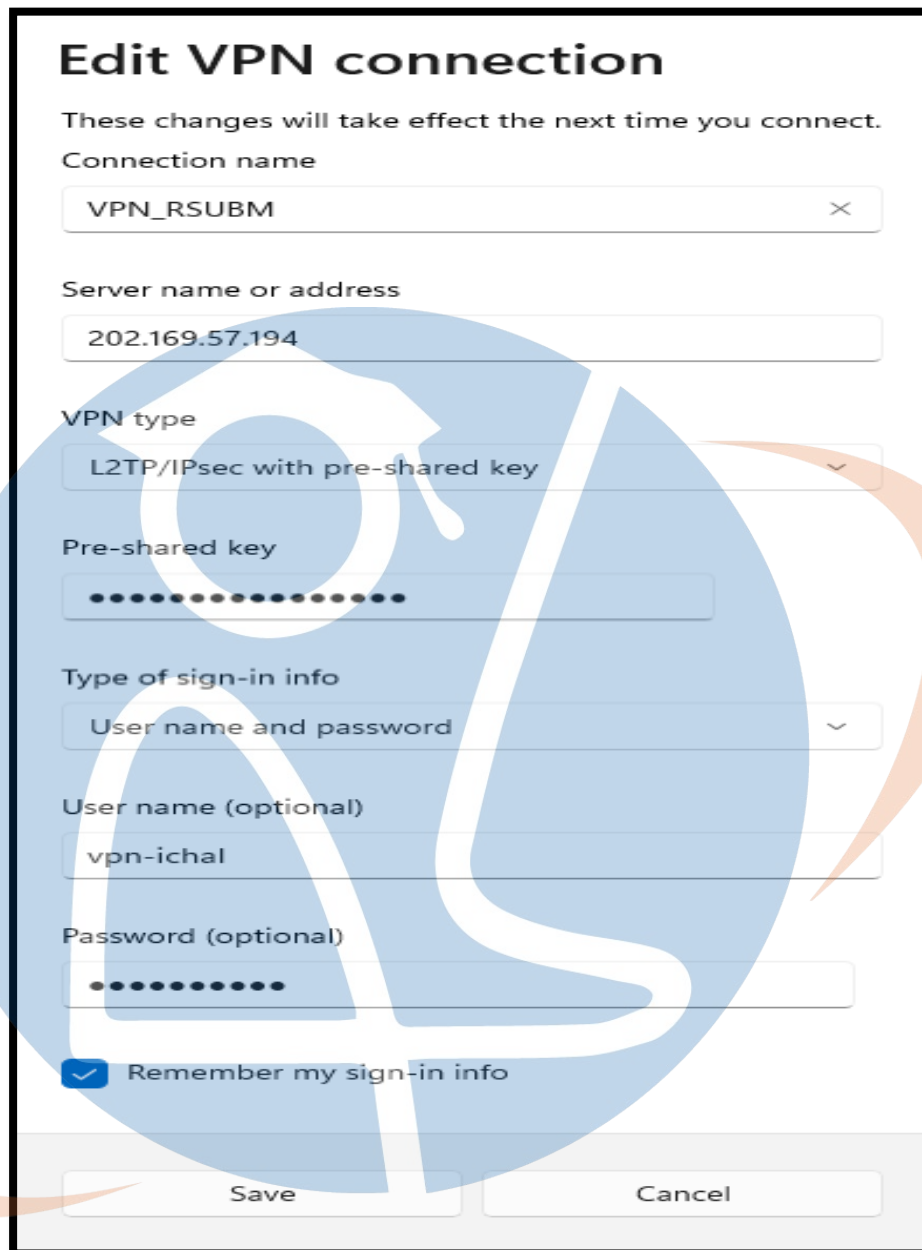
Gambar 5.12 Konfigurasi Route Mikrotik RSUBM

5.1.3 Konfigurasi L2TP+IPSec VPN Client Remote Access

Konfigurasi user remote access bertujuan untuk menghubungkan suatu client dengan network Virtual Private Network (VPN) Server melalui jalur internet dan pengguna seolah-olah berada dalam satu jaringan lokal. Dalam mengkoneksikan client dengan Virtual Private Network (VPN) server dibutuhkan beberapa tahapan settingan pada komputer client.

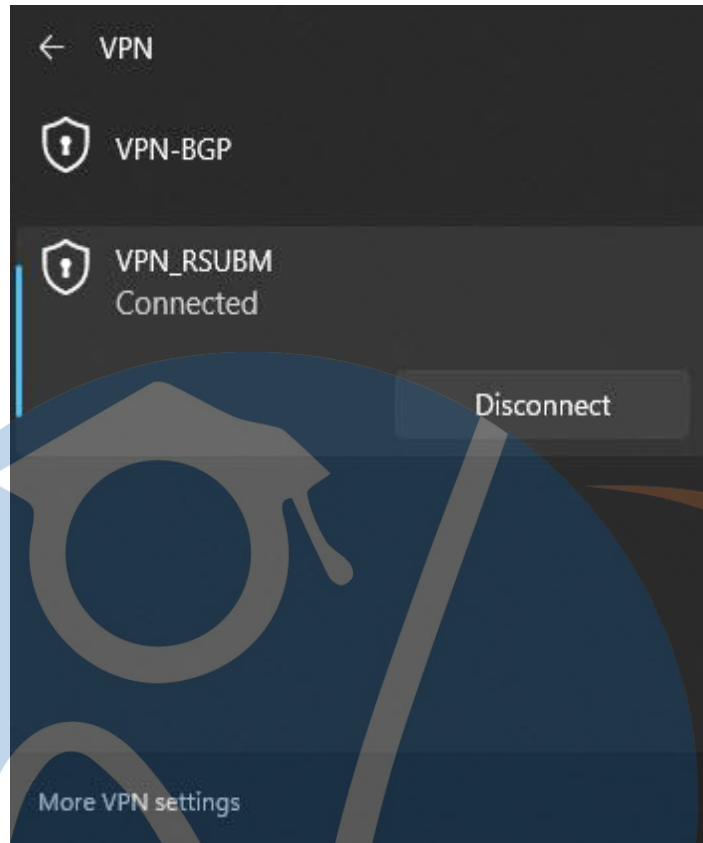
Berikut adalah tahapan konfigurasi Virtual Private Network (VPN) remote access dengan menggunakan sistem operasi Windows 11 SL:

1. Peneliti memastikan PC atau Laptop telah terhubung ke internet lalu masuk menu Setting - Network and Internet.- VPN – Add VPN – Save.
2. Edit VPN Connection seperti gambar dibawah ini.



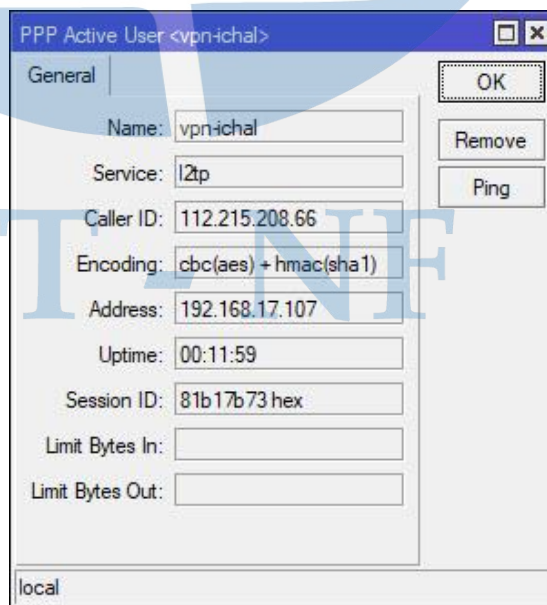
Gambar 5.13 Konfigurasi VPN Win 11

3. Setelah peneliti memastikan semua sudah dikonfigurasi dengan benar, kemudian peneliti melakukan login sesuai dengan username dan password kemudian klik connect dan akan terhubung dengan jaringan private “VPN SERVER” yang dituju seperti gambar dibawah ini:



Gambar 5.14 VPN Connected

4. Peneliti melakukan pengecekan di Mikrotik PPP-Active Connections profile yang sudah di setting di windows 11 dalam keadaan active user.



Gambar 5.15 Terhubung dengan VPN Server

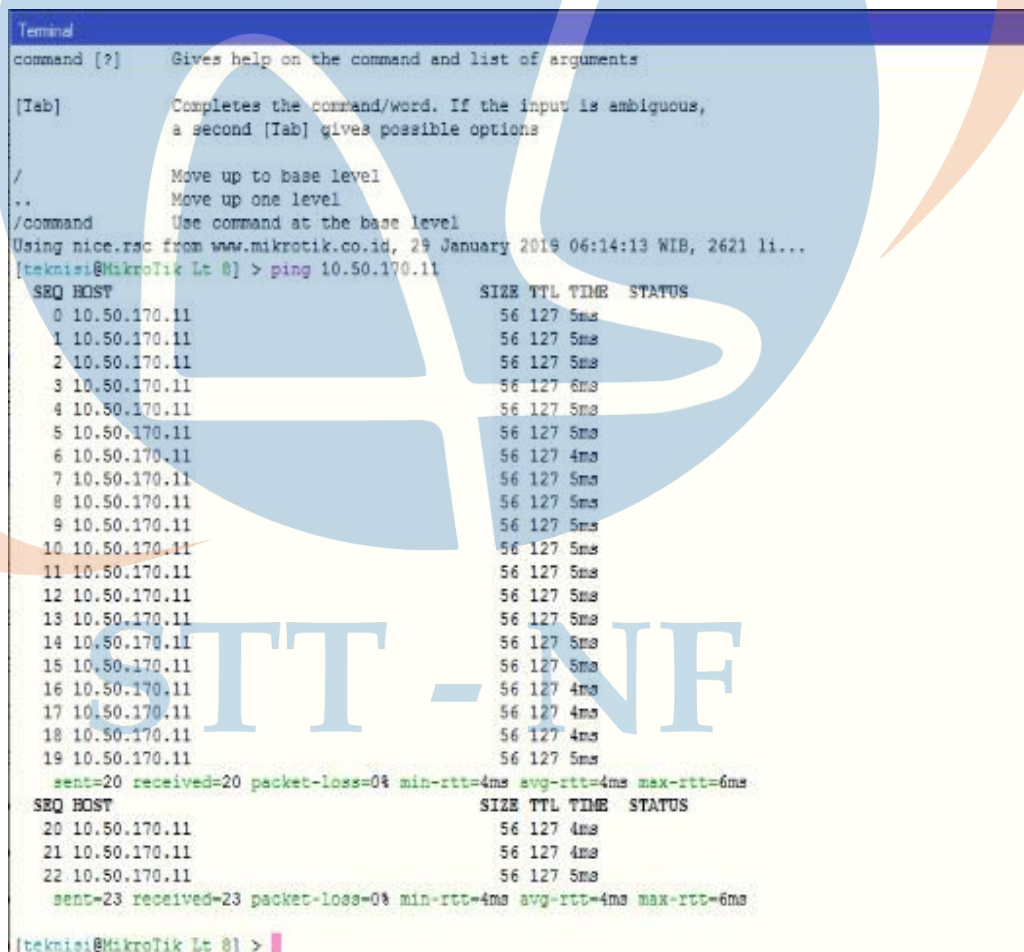
5.2 Pengujian Performa VPN L2TP+IPSec

Tahapan pengujian performa Virtual Private Network (VPN) Berbasis Protokol Layer 2 Tunneling Protokol (L2TP) dan IPSec meliputi pengujian fungsionalitas, throughput, Jitter, dan packet loss.

5.2.1 Pengujian Fungsionalitas VPN

Pada pengujian konektivitas jaringan ini peneliti melakukan test koneksi dari mengirimkan paket ICMP (ping) secara real time dan tracert dari VPN Server menuju VPN client begitupun sebaliknya, Pengujian ini bertujuan untuk melihat kemampuan dari server Virtual Private Network (VPN) dalam mengirimkan dan menerima packet data. Berikut ini adalah cara pengujian yang di lakukan:

1. Pengujian Site to Site



```
Terminal
command [?] Gives help on the command and list of arguments
[Tab] Completes the command/word. If the input is ambiguous,
a second [Tab] gives possible options
/ Move up to base level
.. Move up one level
/command Use command at the base level
Using nice.rsc from www.mikrotik.co.id, 29 January 2019 06:14:13 WIB, 2621 li...
[teknisi@MikroTik Lt 0] > ping 10.50.170.11
SEQ HOST SIZE TTL TIME STATUS
0 10.50.170.11 56 127 5ms
1 10.50.170.11 56 127 5ms
2 10.50.170.11 56 127 5ms
3 10.50.170.11 56 127 6ms
4 10.50.170.11 56 127 5ms
5 10.50.170.11 56 127 5ms
6 10.50.170.11 56 127 4ms
7 10.50.170.11 56 127 5ms
8 10.50.170.11 56 127 5ms
9 10.50.170.11 56 127 5ms
10 10.50.170.11 56 127 5ms
11 10.50.170.11 56 127 5ms
12 10.50.170.11 56 127 5ms
13 10.50.170.11 56 127 5ms
14 10.50.170.11 56 127 5ms
15 10.50.170.11 56 127 5ms
16 10.50.170.11 56 127 4ms
17 10.50.170.11 56 127 4ms
18 10.50.170.11 56 127 4ms
19 10.50.170.11 56 127 5ms
sent=20 received=20 packet-loss=0% min-rtt=4ms avg-rtt=4ms max-rtt=6ms
SEQ HOST SIZE TTL TIME STATUS
20 10.50.170.11 56 127 4ms
21 10.50.170.11 56 127 4ms
22 10.50.170.11 56 127 5ms
sent=23 received=23 packet-loss=0% min-rtt=4ms avg-rtt=4ms max-rtt=6ms
[teknisi@MikroTik Lt 0] >
```

Gambar 5.16 Ping ke host VPN Client

```

Terminal
a second [Tab] gives possible options

/      Move up to base level
..     Move up one level
/command Use command at the base level
[admin@MikroTikRSUBM] > ping 192.168.30.201
  SEQ HOST                                SIZE TTL TIME  STATUS
  0 192.168.30.201                          56 126 6ms
  1 192.168.30.201                          56 126 5ms
  2 192.168.30.201                          56 126 5ms
  3 192.168.30.201                          56 126 5ms
  4 192.168.30.201                          56 126 44ms
  5 192.168.30.201                          56 126 6ms
  6 192.168.30.201                          56 126 5ms
  7 192.168.30.201                          56 126 5ms
  8 192.168.30.201                          56 126 5ms
  9 192.168.30.201                          56 126 5ms
 10 192.168.30.201                          56 126 5ms
 11 192.168.30.201                          56 126 5ms
 12 192.168.30.201                          56 126 5ms
 13 192.168.30.201                          56 126 6ms
 14 192.168.30.201                          56 126 5ms
 15 192.168.30.201                          56 126 5ms
 16 192.168.30.201                          56 126 5ms
 17 192.168.30.201                          56 126 5ms
 18 192.168.30.201                          56 126 5ms
 19 192.168.30.201                          56 126 5ms
    sent=20 received=20 packet-loss=0% min-rtt=5ms avg-rtt=7ms max-rtt=44ms
  SEQ HOST                                SIZE TTL TIME  STATUS
 20 192.168.30.201                          56 126 5ms
    sent=21 received=21 packet-loss=0% min-rtt=5ms avg-rtt=7ms max-rtt=44ms
[admin@MikroTikRSUBM] >

```

Gambar 5.17 Ping ke host VPN Server

```

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\IT-INFRA>tracert 10.50.170.11

Tracing route to 10.50.170.11 over a maximum of 30 hops
  0  *          *          *          Request timed out.
  1  <1 ms      <1 ms      <1 ms      192.168.30.1
  2  <5 ms      <5 ms      <5 ms      10.20.30.53
  3  <5 ms      <5 ms      <5 ms      10.50.170.11
  4  <5 ms      <5 ms      <5 ms
Trace complete.

C:\Users\IT-INFRA>tracert 10.50.170.11

Tracing route to 10.50.170.11 over a maximum of 30 hops
  0  2 ms       1 ms       1 ms       192.168.30.2
  1  <1 ms      <1 ms      <1 ms      192.168.30.1
  2  <5 ms      <5 ms      <5 ms      10.20.30.53
  3  <5 ms      <5 ms      <5 ms      10.50.170.11
  4  <5 ms      <5 ms      <5 ms
Trace complete.

C:\Users\IT-INFRA>tracert 10.50.170.11

Tracing route to 10.50.170.11 over a maximum of 30 hops
  0  1 ms       1 ms       1 ms       192.168.30.2
  1  <1 ms      <1 ms      <1 ms      192.168.30.1
  2  <6 ms      <6 ms      <6 ms      10.20.30.53
  3  <6 ms      <5 ms      <5 ms      10.50.170.11
  4  <6 ms      <5 ms      <5 ms
Trace complete.

C:\Users\IT-INFRA>

```

Gambar 5.18 Traceroute ke host VPN Client

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.16299.15]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\PC_EDP2>tracert 192.168.30.201

Tracing route to 192.168.30.201 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms    10.50.170.254
  2     4 ms     4 ms     4 ms     10.20.30.2
  3     5 ms     5 ms     5 ms     192.168.30.201

Trace complete.

C:\Users\PC_EDP2>tracert 192.168.30.201

Tracing route to 192.168.30.201 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms    10.50.170.254
  2     5 ms     4 ms     4 ms     10.20.30.2
  3     5 ms     5 ms     5 ms     192.168.30.201

Trace complete.

C:\Users\PC_EDP2>tracert 192.168.30.201

Tracing route to 192.168.30.201 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms    10.50.170.254
  2     5 ms     4 ms     4 ms     10.20.30.2
  3     5 ms     5 ms     5 ms     192.168.30.201

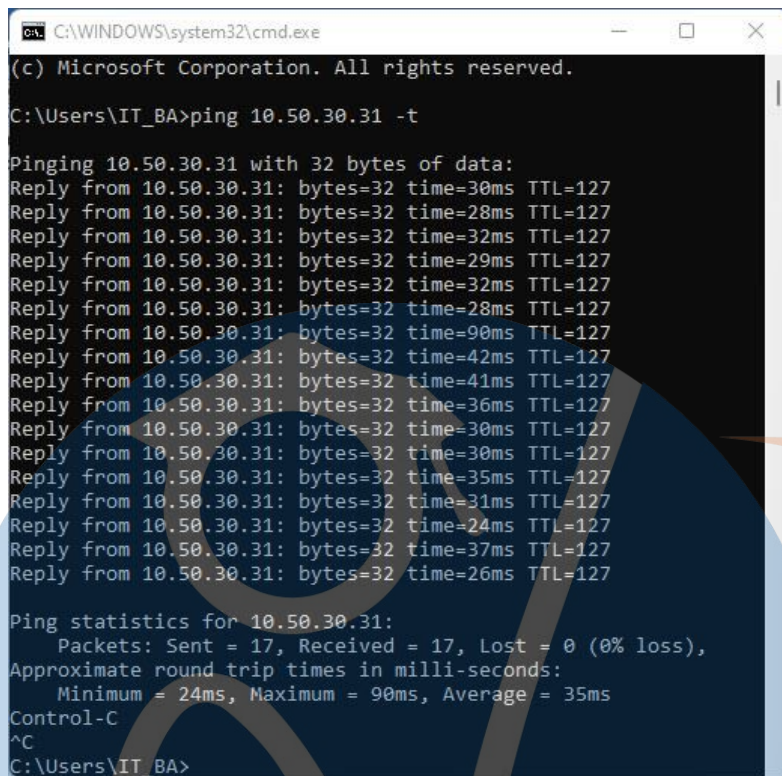
Trace complete.

C:\Users\PC_EDP2>
```

Gambar 5.19 Traceroute ke host VPN Server

STT - NF

2. Remote Access

A screenshot of a Windows command prompt window titled "C:\WINDOWS\system32\cmd.exe". The prompt shows the user running the command "ping 10.50.30.31 -t". The output displays 17 successful replies from 10.50.30.31 with varying response times and a TTL of 127. The ping statistics show 17 packets sent and received with 0% loss, and an average round trip time of 35ms.

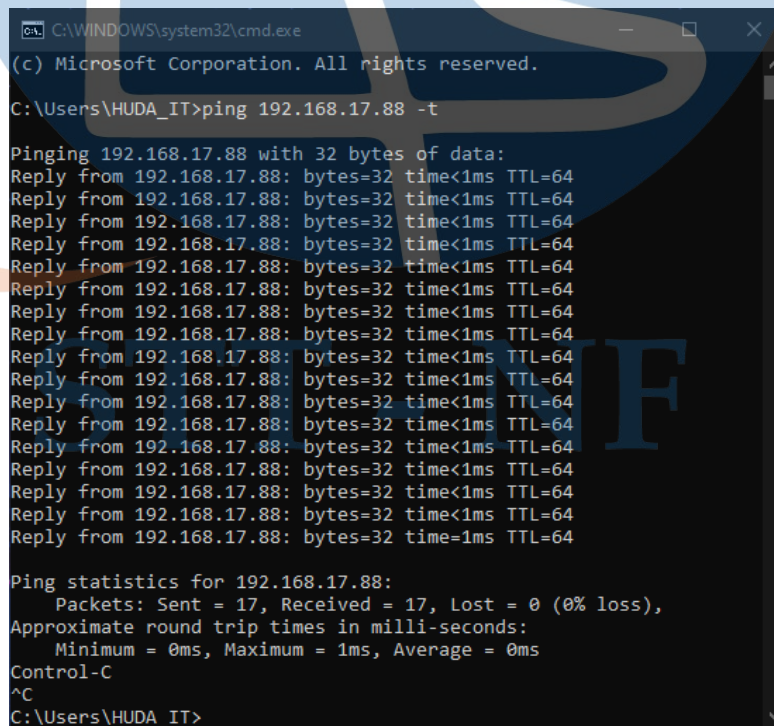
```
C:\WINDOWS\system32\cmd.exe
(c) Microsoft Corporation. All rights reserved.

C:\Users\IT_BA>ping 10.50.30.31 -t

Pinging 10.50.30.31 with 32 bytes of data:
Reply from 10.50.30.31: bytes=32 time=30ms TTL=127
Reply from 10.50.30.31: bytes=32 time=28ms TTL=127
Reply from 10.50.30.31: bytes=32 time=32ms TTL=127
Reply from 10.50.30.31: bytes=32 time=29ms TTL=127
Reply from 10.50.30.31: bytes=32 time=32ms TTL=127
Reply from 10.50.30.31: bytes=32 time=28ms TTL=127
Reply from 10.50.30.31: bytes=32 time=90ms TTL=127
Reply from 10.50.30.31: bytes=32 time=42ms TTL=127
Reply from 10.50.30.31: bytes=32 time=41ms TTL=127
Reply from 10.50.30.31: bytes=32 time=36ms TTL=127
Reply from 10.50.30.31: bytes=32 time=30ms TTL=127
Reply from 10.50.30.31: bytes=32 time=30ms TTL=127
Reply from 10.50.30.31: bytes=32 time=35ms TTL=127
Reply from 10.50.30.31: bytes=32 time=31ms TTL=127
Reply from 10.50.30.31: bytes=32 time=24ms TTL=127
Reply from 10.50.30.31: bytes=32 time=37ms TTL=127
Reply from 10.50.30.31: bytes=32 time=26ms TTL=127

Ping statistics for 10.50.30.31:
    Packets: Sent = 17, Received = 17, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 24ms, Maximum = 90ms, Average = 35ms
Control-C
^C
C:\Users\IT_BA>
```

Gambar 5.20 Ping ke host VPN Server RSUBM

A screenshot of a Windows command prompt window titled "C:\WINDOWS\system32\cmd.exe". The prompt shows the user running the command "ping 192.168.17.88 -t". The output displays 17 successful replies from 192.168.17.88 with a response time of less than 1ms and a TTL of 64. The ping statistics show 17 packets sent and received with 0% loss, and an average round trip time of 0ms.

```
C:\WINDOWS\system32\cmd.exe
(c) Microsoft Corporation. All rights reserved.

C:\Users\HUDA_IT>ping 192.168.17.88 -t

Pinging 192.168.17.88 with 32 bytes of data:
Reply from 192.168.17.88: bytes=32 time<1ms TTL=64
Reply from 192.168.17.88: bytes=32 time<1ms TTL=64
Reply from 192.168.17.88: bytes=32 time<1ms TTL=64
Reply from 192.168.17.88: bytes=32 time<1ms TTL=64
Reply from 192.168.17.88: bytes=32 time<1ms TTL=64
Reply from 192.168.17.88: bytes=32 time<1ms TTL=64
Reply from 192.168.17.88: bytes=32 time<1ms TTL=64
Reply from 192.168.17.88: bytes=32 time<1ms TTL=64
Reply from 192.168.17.88: bytes=32 time<1ms TTL=64
Reply from 192.168.17.88: bytes=32 time<1ms TTL=64
Reply from 192.168.17.88: bytes=32 time<1ms TTL=64
Reply from 192.168.17.88: bytes=32 time<1ms TTL=64
Reply from 192.168.17.88: bytes=32 time<1ms TTL=64
Reply from 192.168.17.88: bytes=32 time<1ms TTL=64
Reply from 192.168.17.88: bytes=32 time<1ms TTL=64
Reply from 192.168.17.88: bytes=32 time<1ms TTL=64
Reply from 192.168.17.88: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.17.88:
    Packets: Sent = 17, Received = 17, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
Control-C
^C
C:\Users\HUDA_IT>
```

Gambar 5.21 Ping ke host VPN Remote Acces

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.22000.258]
(c) Microsoft Corporation. All rights reserved.

C:\Users\IT_BA>tracert 10.50.30.31

Tracing route to HUDA_IT [10.50.30.31]
over a maximum of 30 hops:

  1    29 ms    53 ms    37 ms    192.168.17.88
  2    31 ms    29 ms    33 ms    HUDA_IT [10.50.30.31]

Trace complete.

C:\Users\IT_BA>tracert 10.50.30.31

Tracing route to HUDA_IT [10.50.30.31]
over a maximum of 30 hops:

  1    26 ms    26 ms    42 ms    192.168.17.88
  2    36 ms    36 ms    29 ms    HUDA_IT [10.50.30.31]

Trace complete.

C:\Users\IT_BA>
```

Gambar 5.22 Traceroute ke host VPN Server RSUBM

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.19042.928]
(c) Microsoft Corporation. All rights reserved.

C:\Users\HUDA_IT>tracert 192.168.17.88

Tracing route to 192.168.17.88 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms    192.168.17.88

Trace complete.

C:\Users\HUDA_IT>tracert 192.168.17.88

Tracing route to 192.168.17.88 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms    192.168.17.88

Trace complete.

C:\Users\HUDA_IT>
```

Gambar 5.23 Traceroute ke host VPN Remote Acces

5.2.2 Skenario Pengujian VPN

Untuk pengujian Peforma Throughput, Jitter, dan Packet Loss peneliti akan melakukan pengujian dengan melakukan file transfer / test disk menggunakan Iperf dengan ukuran file yang berbeda baik secara site to site maupun secara remote access, di sini penulis melakukan file transfer / test disk dengan ukuran file 50 Mb, 100Mb, dan 150 Mb, 200 Mb, 300 Mb, 400 Mb, 500 Mb, 600 Mb, 700 Mb, 800 Mb dengan rentang waktu 60 detik Pengujian ini dilakukan dengan cara menjalankan perintah dari sisi server :: <iperf -s > dan dari sisi client : <iperf -c <ipserver> -F <lokasi file> -i2 -u -b -t60 >. , dapat dilihat pada tabel dibawah ini:

Tabel 5.1 Comment Line Iperf

Comment Line Iperf	Description
-s	Perintah dari sisi server (identifikasi sebagai server)
-c	Perintah dari sisi client (identifikasi sebagai client)
-F	Perintah membaca file local dan menulis ke jaringan
-i	Perintah untuk menentukan interval waktu
-u	Perintah untuk penggunaan udp melalui tcp
-b	Perintah untuk pengaturan penggunaan bandwidht
-t	Perintah untuk setelan waktu dalam hitungan detik untuk ditransmisikan (default 10 detik)

Skenario Pengujian VPN menggunakan iperf dilakukan seperti dibawah ini :

1. Site to Site

Untuk pengujian konektivitas site to site peneliti menjalankan perintah dari sisi client RSUD Bunda Margonda ke server HOF dengan melakukan file transfer / test disk dengan cara mengirimkan file sesuai dengan ukuran yang telah di tentukan, dengan pengaturan interval 2 detik, selama 60 Detik menggunakan bandwidth default main line ISP 50 Mbps.

```

: < iperf3.exe -c 192.168.30.201 -F
C:\Users\PC_EDP2\Desktop\FILE_TESTING\100.rar -i2 -u -
b50m -t60 >

```

```

C:\Users\PC_EDP2\Desktop\iperf-3.1.3-win64>iperf3.exe -c 192.168.30.201 -F C:\Users\PC_EDP2\Desktop\FILE_TESTING\50.rar -i2 -u -b 50m -t60
Connecting to host 192.168.30.201, port 5201
[ 4] local 10.50.170.11 port 62624 connected to 192.168.30.201 port 5201
[ ID] Interval           Transfer     Bandwidth   Total Datagrams
[ 4] 0.00-2.00 sec    11.4 MBytes  47.9 Mbits/sec  1461
[ 4] 2.00-4.00 sec    11.9 MBytes  50.1 Mbits/sec  1528
[ 4] 4.00-6.00 sec    11.9 MBytes  50.0 Mbits/sec  1527
[ 4] 6.00-8.00 sec    11.9 MBytes  49.8 Mbits/sec  1519
[ 4] 8.00-8.70 sec     4.38 MBytes  52.4 Mbits/sec   561
-----
[ ID] Interval           Transfer     Bandwidth   Jitter    Lost/Totl  Datagrams
[ 4] 0.00-8.70 sec    51.5 MBytes  49.7 Mbits/sec  1.775 ms  6295/6570 (96%)
[ 4] Sent 6570 datagrams
      Sent 51.5 MByte / 51.5 MByte (100%) of C:\Users\PC_EDP2\Desktop\FILE_TESTING\50.rar
iperf Done.
C:\Users\PC_EDP2\Desktop\iperf-3.1.3-win64>

```

Gambar 5.24 Skenario Pengujian Site To Site

2. Remote Access

Untuk pengujian konektivitas remote access, peneliti menjalankan perintah dari sisi client ke server dengan melakukan file transfer / test disk dengan cara mengirimkan file sesuai dengan ukuran yang telah di tentukan, dengan pengaturan interval 2 detik, selama 60 Detik menggunakan bandwidth provider seluler sebear 20 Mbps

```

: < iperf3.exe -c 10.50.30.31 -F
D:\STIKOM_NF2017\SKRIPSI\SKRIPSI_FINAL\SS_IPERF\FILE_TESTING\100.rar -i2 -u -b 20m -t60 >

```

```

Select Command Prompt
Report bugs to: https://github.com/esnet/iperf

C:\Users\IT_BA\Downloads\iperf>iperf3.exe -c 10.50.30.31 -F D:\STIKOM_NF2017\SKRIPSI\SKRIPSI_FINAL\SS_IPERF\FILE_TESTING\50.rar -i2 -u -b 20m -t60
Connecting to host 10.50.30.31, port 5201
[ 4] local 192.168.17.110 port 50301 connected to 10.50.30.31 port 5201
[ ID] Interval      Transfer    Bandwidth  Total Datagrams
[ 4] 0.00-2.01    sec 4.60 MBytes 19.2 Mbits/sec 589
[ 4] 2.01-4.00    sec 4.74 MBytes 19.9 Mbits/sec 607
[ 4] 4.00-6.00    sec 4.78 MBytes 20.0 Mbits/sec 612
[ 4] 6.00-8.00    sec 4.77 MBytes 20.0 Mbits/sec 610
[ 4] 8.00-10.00   sec 4.76 MBytes 20.0 Mbits/sec 609
[ 4] 10.00-12.01  sec 4.76 MBytes 19.9 Mbits/sec 609
[ 4] 12.01-14.00  sec 4.78 MBytes 20.1 Mbits/sec 612
[ 4] 14.00-16.00  sec 4.77 MBytes 20.0 Mbits/sec 611
[ 4] 16.00-18.01  sec 4.74 MBytes 19.8 Mbits/sec 607
[ 4] 18.01-20.01  sec 4.78 MBytes 20.1 Mbits/sec 612
[ 4] 20.01-21.71  sec 4.05 MBytes 20.0 Mbits/sec 518

[ ID] Interval      Transfer    Bandwidth  Jitter    Lost/Total Datagrams
[ 4] 0.00-21.71   sec 51.5 MBytes 19.9 Mbits/sec 10.146 ms 673/6595 (10%)
[ 4] Sent 6595 datagrams
Sent 51.5 MByte / 51.5 MByte (100%) of D:\STIKOM_NF2017\SKRIPSI\SKRIPSI_FINAL\SS_IPERF\FILE_TESTING\50.rar
iperf Done.
C:\Users\IT_BA\Downloads\iperf>

```

Gambar 5.25 Skenario Pengujian Remote Acces

5.2.3 Pengujian Peforma Throughput

Throughput merupakan jumlah total kedatangan paket yang sukses yang diamati pada destination selama interval waktu tertentu dibagi oleh durasi interval waktu tersebut. Throughput merupakan kemampuan sebenarnya suatu jaringan dalam melakukan pengiriman data. Biasanya throughput selalu dikaitkan dengan bandwidth karena throughput memang bisa disebut juga dengan bandwidth dalam kondisi yang sebenarnya. Bandwidth lebih bersifat fix sementara throughput sifatnya adalah dinamis tergantung *traffic* yang sedang terjadi. Dengan menggunakan tool iperf peneliti mendapatkan rata – rata bandwidth secara otomatis dalam satuan mbps. Untuk menentukan nilai troughput dan kategori, disesuaikan dengan Tabel 4.5 Index Performa Throughput yang didasarkan pada standar TIPHON. Dalam melakukan pangujian data peneliti memvariasikan nama dan ukuran file.

Berikut adalah cara pengujian dan tabel hasil pengujian peforma trougphut site to site dan remote access :

1. Site to Site

➤ Pengujian 1 ukuran file 50 Mb :

Iperf Client RSUD Bunda Margonda

```

: < iperf3.exe -c 192.168.30.201 -F
C:\Users\PC_EDP2\Desktop\FILE_TESTING\50.rar -i2 -u -
b50m -t60 >

```

```

C:\Users\PC_EDP2\Desktop\iperf-3.1.3-win64>iperf3.exe -c 192.168.30.201 -F C:\Users\PC_EDP2\Desktop\FILE_TESTING\50.rar -i2 -u -b 50m -t60
Connecting to host 192.168.30.201, port 5201
[ 4] local 10.50.170.11 port 62624 connected to 192.168.30.201 port 5201
[ ID] Interval      Transfer      Bandwidth     Total Datagrams
[ 4] 0.00-2.00 sec  11.4 MBytes  47.9 Mbits/sec  1461
[ 4] 2.00-4.00 sec  11.9 MBytes  50.1 Mbits/sec  1528
[ 4] 4.00-6.00 sec  11.9 MBytes  50.0 Mbits/sec  1527
[ 4] 6.00-8.00 sec  11.9 MBytes  49.8 Mbits/sec  1519
[ 4] 8.00-8.70 sec  4.38 MBytes  52.4 Mbits/sec  561
-----
[ ID] Interval      Transfer      Bandwidth     Jitter        Lost/Tot. Datagrams
[ 4] 0.00-8.70 sec  51.5 MBytes  49.7 Mbits/sec  1.775 ms      6295/6570 (96%)
[ 4] Sent 6570 datagrams
      Sent 51.5 MByte / 51.5 MByte (100%) of C:\Users\PC_EDP2\Desktop\FILE_TESTING\50.rar
iperf Done.

```

Gambar 5.26 Pengujian 1 Troughput Site to Site

➤ Pengujian 2 ukuran file 100 Mb :

Iperf Client RSU Bunda Margonda

```

: < iperf3.exe -c 192.168.30.201 -F
C:\Users\PC_EDP2\Desktop\FILE_TESTING\100.rar -i2 -u
-b50m -t60 >

```

```

C:\Users\PC_EDP2\Desktop\iperf-3.1.3-win64>iperf3.exe -c 192.168.30.201 -F C:\Users\PC_EDP2\Desktop\FILE_TESTING\100.rar -i2 -u -b 50m -t60
Connecting to host 192.168.30.201, port 5201
[ 4] local 10.50.170.11 port 62625 connected to 192.168.30.201 port 5201
[ ID] Interval      Transfer      Bandwidth     Total Datagrams
[ 4] 0.00-2.00 sec  11.4 MBytes  47.8 Mbits/sec  1459
[ 4] 2.00-4.00 sec  12.0 MBytes  50.3 Mbits/sec  1536
[ 4] 4.00-6.00 sec  11.9 MBytes  49.7 Mbits/sec  1517
[ 4] 6.00-8.00 sec  11.9 MBytes  50.0 Mbits/sec  1525
[ 4] 8.00-10.00 sec 12.0 MBytes  50.1 Mbits/sec  1530
[ 4] 10.00-12.00 sec 11.9 MBytes  50.0 Mbits/sec  1527
[ 4] 12.00-14.00 sec 11.9 MBytes  49.9 Mbits/sec  1523
[ 4] 14.00-16.00 sec 11.9 MBytes  49.8 Mbits/sec  1521
[ 4] 16.00-18.00 sec 12.1 MBytes  50.6 Mbits/sec  1543
[ 4] 18.00-18.30 sec 1.90 MBytes  52.7 Mbits/sec  243
-----
[ ID] Interval      Transfer      Bandwidth     Jitter        Lost/Tot. Datagrams
[ 4] 0.00-18.30 sec 109 MBytes  49.9 Mbits/sec  1.896 ms      13218/13894 (95%)
[ 4] Sent 13894 datagrams
      Sent 109 MByte / 109 MByte (100%) of C:\Users\PC_EDP2\Desktop\FILE_TESTING\100.rar
iperf Done.

```

Gambar 5.27 Pengujian 2 Troughput Site to Site

Untuk pengujian troughput site to site ke 3 sampai dengan terakhir peneliti menggunakan perintah yang sama sehingga didapat data sebagai berikut

:

Tabel 5.2 Hasil Troughput Site to Site

Ukuran File	Troughput / Bandwidth iperf (mbps)	Kategori
50 Mb	49,7	Sangat Bagus
100 Mb	49,9	Sangat Bagus
150 Mb	50	Sangat Bagus
200 Mb	49,9	Sangat Bagus
300 Mb	49,9	Sangat Bagus
400 Mb	49,9	Sangat Bagus
500 Mb	49,9	Sangat Bagus
600 Mb	49,9	Sangat Bagus
700 Mb	49,9	Sangat Bagus
800 Mb	49,9	Sangat Bagus

2. Remote Access

- Pengujian 1 ukuran file 50 Mb :

Iperf Client Remote Access

```

: < iperf3.exe -c 10.50.30.31 -F
D:\STIKOM_NF2017\SKRIPSI\SKRIPSI_FINAL\SS_IPERF\FILE_TE
STING\50.rar -i2 -u -b 20m -t60 >
  
```

```

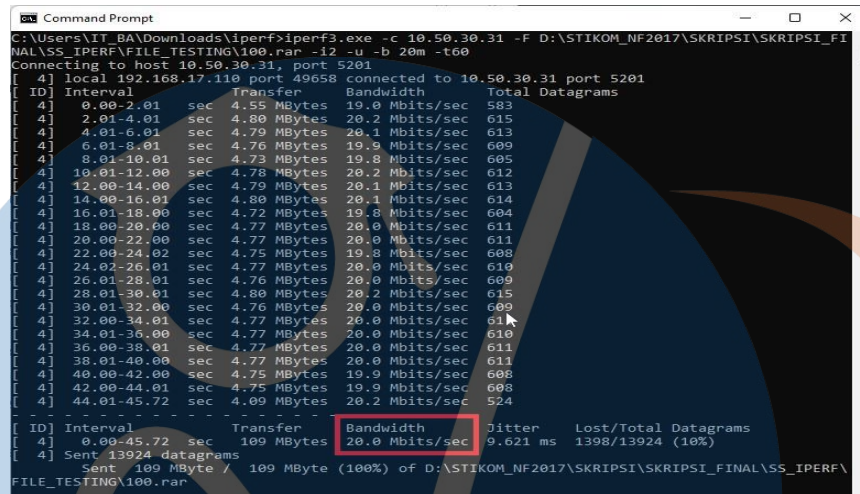
Report bugs to: https://github.com/esnet/iperf
C:\Users\IT_BA\Downloads\iperf>iperf3.exe -c 10.50.30.31 -F D:\STIKOM_NF2017\SKRIPSI\SKRIPSI_FINAL\SS_IPERF\FILE_TESTING\50.rar -i2 -u -b 20m -t60
Connecting to host 10.50.30.31, port 5201
[ 4] local 192.168.17.110 port 50301 connected to 10.50.30.31 port 5201
[ ID] Interval           Transfer     Bandwidth   Total Datagrams
[ 4] 0.00-2.01 sec     4.60 MBytes  19.2 Mbits/sec  589
[ 4] 2.01-4.00 sec     4.74 MBytes  19.9 Mbits/sec  607
[ 4] 4.00-6.00 sec     4.78 MBytes  20.0 Mbits/sec  612
[ 4] 6.00-8.00 sec     4.77 MBytes  20.0 Mbits/sec  610
[ 4] 8.00-10.00 sec    4.76 MBytes  20.0 Mbits/sec  609
[ 4] 10.00-12.01 sec   4.76 MBytes  19.9 Mbits/sec  609
[ 4] 12.01-14.00 sec   4.78 MBytes  20.1 Mbits/sec  612
[ 4] 14.00-16.00 sec   4.77 MBytes  20.0 Mbits/sec  611
[ 4] 16.00-18.01 sec   4.74 MBytes  19.8 Mbits/sec  607
[ 4] 18.01-20.01 sec   4.78 MBytes  20.1 Mbits/sec  612
[ 4] 20.01-21.71 sec   4.05 MBytes  20.0 Mbits/sec  518
-----
[ ID] Interval           Transfer     Bandwidth   Jitter    Lost/Total Datagrams
[ 4] 0.00-21.71 sec    51.5 MBytes  19.9 Mbits/sec  10.146 ms  673/6595 (10%)
[ 4] Sent 6595 datagrams
Sent 51.5 MByte / 51.5 MByte (100%) of D:\STIKOM_NF2017\SKRIPSI\SKRIPSI_FINAL\SS_IPERF\
  
```

Gambar 5.28 Pengujian 1 Troughput Remote Access

➤ Pengujian 2 ukuran file 100 Mb :

Iperf Client Remote Access

```
: < iperf3.exe -c 10.50.30.31 -F
D:\STIKOM_NF2017\SKRIPSI\SKRIPSI_FINAL\SS_IPERF\FILE_TESTING\100.rar -i2 -u -b 20m -t60 >
```



Gambar 5.29 Pengujian 2 Troughput Remote Access

Untuk pengujian troughput remote access yang ke 3 sampai dengan terakhir peneliti menggunakan perintah yang sama sehingga didapat data sebagai berikut :

Tabel 5.3 Hasil Troughput Remote Access

Ukuran File	Troughput / Bandwidth iperf (mbps)	Kategori
50 Mb	19,9	Sangat Bagus
100 Mb	20	Sangat Bagus
150 Mb	20	Sangat Bagus
200 Mb	20	Sangat Bagus
300 Mb	20	Sangat Bagus
400 Mb	20	Sangat Bagus
500 Mb	20	Sangat Bagus

600 Mb	20	Sangat Bagus
700 Mb	20	Sangat Bagus
800 Mb	20	Sangat Bagus

5.2.4 Pengujian Peforma Jitter

Masih menggunakan tool iperf dan data sebelumnya baik secara site to site dan remote akses, peneliti selanjutnya melakukan pengujian jitter. Jitter ini mengacu kepada variasi keterlambatan waktu dari pengiriman paket, sebagai contoh paket 1 memiliki keterlambatan waktu pengiriman 10ms, paket 2 memiliki keterlambatan waktu pengiriman 13ms dan paket 3 memiliki keterlambatan waktu 15ms, jadi untuk menentukan nilai jitter ini dengan menjumlah keterlambatan waktu pengiriman paket 1, paket 2, paket 3, dan membagi dengan jumlah pengiriman paket tersebut, untuk pengujian jitter ini dengan menggunakan tool iperf, peneliti secara otomatis mendapatkan nilai jitter dalam satuan ms dari setiap pengujian yang dilakukan, dan selanjutnya peneliti menentukan kategori jitter sesuai dengan Tabel 4.7 Index Performa Jitter yang didasarkan pada standar TIPHON. Dalam melakukan pangujian data peneliti memvariasikan nama dan ukuran file.. Berikut adalah cara pengujian dan tabel hasil pengujian peforma jitter site to site dan remote access :

1. Site to Site

➤ Pengujian 1 ukuran file 50 Mb :

Iperf Client RSU Bunda Margonda

```

: < iperf3.exe -c 192.168.30.201 -F
C:\Users\PC_EDP2\Desktop\FILE_TESTING\50.rar -i2 -u -
b50m -t60 >

```

```

[ 4] 0.00-2.00 sec 11.4 MBytes 47.9 Mbits/sec 1461
[ 4] 2.00-4.00 sec 11.9 MBytes 50.1 Mbits/sec 1528
[ 4] 4.00-6.00 sec 11.9 MBytes 50.0 Mbits/sec 1527
[ 4] 6.00-8.00 sec 11.9 MBytes 49.8 Mbits/sec 1519
[ 4] 8.00-8.70 sec 4.38 MBytes 52.4 Mbits/sec 561
-----
[ ID] Interval      Transfer      Bandwidth      Jitter      Lost/Total Datagrams
[ 4] 0.00-8.70 sec 51.5 MBytes 49.7 Mbits/sec 1.775 ms    6295/6570 (96%)
[ 4] Sent 6570 datagrams
      Sent 51.5 MByte / 51.5 MByte (100%) of C:\Users\PC_EDP2\Desktop\FILE_TESTING\50.rar
iperf Done.
C:\Users\PC_EDP2\Desktop\iperf-3.1.3-win64>

```

Gambar 5.30 Pengujian 1 Jitter Site to Site

➤ Pengujian 2 ukuran file 100 Mb :

Iperf Client RSU Bunda Margonda

```
: < iperf3.exe -c 192.168.30.201 -F
C:\Users\PC_EDP2\Desktop\FILE_TESTING\100.rar -i2 -u -
b50m -t60 >
```

```
[ 4] local 10.50.170.11 port 62625 connected to 192.168.30.201 port 5201
[ ID] Interval      Transfer      Bandwidth      Total Datagrams
[ 4] 0.00-2.00    sec 11.4 MBytes  47.8 Mbits/sec  1459
[ 4] 2.00-4.00    sec 12.0 MBytes  50.3 Mbits/sec  1536
[ 4] 4.00-6.00    sec 11.9 MBytes  49.7 Mbits/sec  1517
[ 4] 6.00-8.00    sec 11.9 MBytes  50.0 Mbits/sec  1525
[ 4] 8.00-10.00   sec 12.0 MBytes  50.1 Mbits/sec  1530
[ 4] 10.00-12.00  sec 11.9 MBytes  50.0 Mbits/sec  1527
[ 4] 12.00-14.00  sec 11.9 MBytes  49.9 Mbits/sec  1523
[ 4] 14.00-16.00  sec 11.9 MBytes  49.8 Mbits/sec  1521
[ 4] 16.00-18.00  sec 12.1 MBytes  50.6 Mbits/sec  1543
[ 4] 18.00-18.30  sec 1.90 MBytes  52.7 Mbits/sec   243
-----
[ ID] Interval      Transfer      Bandwidth      Jitter      Lost/Total Datagrams
[ 4] 0.00-18.30   sec 109 MBytes  49.9 Mbits/sec  1.896 ms    13218/13894 (95%)
[ 4] Sent 13894 datagrams
      Sent 109 MByte / 109 MByte (100%) of C:\Users\PC_EDP2\Desktop\FILE_TESTING\100.rar
iperf Done.
C:\Users\PC_EDP2\Desktop\iperf-3.1.3-win64>
```

Gambar 5.31 Pengujian 2 Jitter Site to Site

Untuk pengujian jitter site to site ke 3 sampai dengan terakhir peneliti menggunakan perintah yang sama sehingga didapat data sebagai berikut :

Tabel 5.4 Hasil Jitter Site to Site

Ukuran File	Jitter (ms)	Kategori
50 Mb	1,775	Bagus
100 Mb	1,896	Bagus
150 Mb	1,636	Bagus
200 Mb	2,268	Bagus
300 Mb	1,986	Bagus
400 Mb	2,178	Bagus

500 Mb	2,143	Bagus
600 Mb	2,159	Bagus
700 Mb	1,960	Bagus
800 Mb	2,024	Bagus

2. Remote Access

- Pengujian 1 ukuran file 50 Mb :

Iperf Client Remote Access

```
: < iperf3.exe -c 10.50.30.31 -F D:\STIKOM_NF2017\SKRIPSI\SKRIPSI_FINAL\SS_IPERF\FILE_TESTING\50.rar -i2 -u -b 20m -t60 >
```

```
C:\Users\IT_BA\Downloads\iperf>iperf3.exe -c 10.50.30.31 -F D:\STIKOM_NF2017\SKRIPSI\SKRIPSI_FINAL\SS_IPERF\FILE_TESTING\50.rar -i2 -u -b 20m -t60
Connecting to host 10.50.30.31, port 5201
[ 4] local 192.168.17.110 port 50301 connected to 10.50.30.31 port 5201
[ ID] Interval      Transfer      Bandwidth    Total Datagrams
[ 4] 0.00-2.01    sec  4.60 MBytes  19.2 Mbits/sec  589
[ 4] 2.01-4.00    sec  4.74 MBytes  19.9 Mbits/sec  607
[ 4] 4.00-6.00    sec  4.78 MBytes  20.0 Mbits/sec  612
[ 4] 6.00-8.00    sec  4.77 MBytes  20.0 Mbits/sec  610
[ 4] 8.00-10.00   sec  4.76 MBytes  20.0 Mbits/sec  609
[ 4] 10.00-12.01  sec  4.76 MBytes  19.9 Mbits/sec  609
[ 4] 12.01-14.00  sec  4.78 MBytes  20.1 Mbits/sec  612
[ 4] 14.00-16.00  sec  4.77 MBytes  20.0 Mbits/sec  611
[ 4] 16.00-18.01  sec  4.74 MBytes  19.8 Mbits/sec  607
[ 4] 18.01-20.01  sec  4.78 MBytes  20.1 Mbits/sec  612
[ 4] 20.01-21.71  sec  4.05 MBytes  20.0 Mbits/sec  518
- - - - -
[ ID] Interval      Transfer      Bandwidth    Jitter      Lost/Total Datagrams
[ 4] 0.00-21.71   sec  51.5 MBytes  19.9 Mbits/sec  10.146 ms  673/6595 (10%)
[ 4] Sent 6595 datagrams
      Sent 51.5 MByte / 51.5 MByte (100%) of D:\STIKOM_NF2017\SKRIPSI\SKRIPSI_FINAL\SS_IPERF\FILE_TESTING\50.rar
iperf Done.
```

Gambar 5.32 Pengujian 1 Jitter Remote Access

- Pengujian 2 ukuran file 100 Mb :

Iperf Client Remote Access

```
: < iperf3.exe -c 10.50.30.31 -F D:\STIKOM_NF2017\SKRIPSI\SKRIPSI_FINAL\SS_IPERF\FILE_TESTING\100.rar -i2 -u -b 20m -t60 >
```

```

4] local 192.168.17.110 port 49658 connected to 10.50.30.31 port 5201
ID] Interval Transfer Bandwidth Total Datagrams
4] 0.00-2.01 sec 4.55 MBytes 19.0 Mbits/sec 583
4] 2.01-4.01 sec 4.80 MBytes 20.2 Mbits/sec 615
4] 4.01-6.01 sec 4.79 MBytes 20.1 Mbits/sec 613
4] 6.01-8.01 sec 4.76 MBytes 19.9 Mbits/sec 609
4] 8.01-10.01 sec 4.73 MBytes 19.8 Mbits/sec 605
4] 10.01-12.00 sec 4.78 MBytes 20.2 Mbits/sec 612
4] 12.00-14.00 sec 4.79 MBytes 20.1 Mbits/sec 613
4] 14.00-16.01 sec 4.80 MBytes 20.1 Mbits/sec 614
4] 16.01-18.00 sec 4.72 MBytes 19.8 Mbits/sec 604
4] 18.00-20.00 sec 4.77 MBytes 20.0 Mbits/sec 611
4] 20.00-22.00 sec 4.77 MBytes 20.0 Mbits/sec 611
4] 22.00-24.02 sec 4.75 MBytes 19.8 Mbits/sec 608
4] 24.02-26.01 sec 4.77 MBytes 20.0 Mbits/sec 610
4] 26.01-28.01 sec 4.76 MBytes 20.0 Mbits/sec 609
4] 28.01-30.01 sec 4.80 MBytes 20.2 Mbits/sec 615
4] 30.01-32.00 sec 4.76 MBytes 20.0 Mbits/sec 609
4] 32.00-34.01 sec 4.77 MBytes 20.0 Mbits/sec 611
4] 34.01-36.00 sec 4.77 MBytes 20.0 Mbits/sec 610
4] 36.00-38.01 sec 4.77 MBytes 20.0 Mbits/sec 611
4] 38.01-40.00 sec 4.77 MBytes 20.0 Mbits/sec 611
4] 40.00-42.00 sec 4.75 MBytes 19.9 Mbits/sec 608
4] 42.00-44.01 sec 4.75 MBytes 19.9 Mbits/sec 608
4] 44.01-45.72 sec 4.09 MBytes 20.2 Mbits/sec 524
ID] Interval Transfer Bandwidth Jitter Lost/Total Datagrams
4] 0.00-45.72 sec 109 MBytes 20.0 Mbits/sec 9.621 ms 1398/13924 (10%)
4] Sent 13924 datagrams
Sent 109 MByte / 109 MByte (100%) of D:\STIKOM_NF2017\SKRIPSI\SKRIPSI_FINAL\SS_IPERF\
FILE_TESTING\100.pap

```

Gambar 5.33 Pengujian 2 Jitter Remote Access

Untuk pengujian jitter remote access yang ke 3 sampai dengan terakhir peneliti menggunakan perintah yang sama sehingga didapat data sebagai berikut :

Tabel 5.5 Hasil Jitter Remote Access

Ukuran File	Jitter (ms)	Kategori
50 Mb	10,146	Bagus
100 Mb	9,621	Bagus
150 Mb	10,589	Bagus
200 Mb	10,552	Bagus
300 Mb	5,135	Bagus
400 Mb	10,542	Bagus
500 Mb	10,094	Bagus
600 Mb	5,036	Bagus
700 Mb	4,002	Bagus
800 Mb	4,241	Bagus

5.2.5 Pengujian Peforma Packet Loss

Peneliti selanjutnya melakukan perhitungan Packet Loss. Paccket Loss merupakan suatu parameter yang menggambarkan suatu kondisi yang menunjukkan jumlah total paket yang hilang, selisih antara paket yang di kirim dengan paket yang diterima (Yanto, 2013), untuk menentukan nilai Packet Loss dan kategori sesuai dengan Tabel 4.9 Index Performa Packet Loss dari pengujian sebelumnya, baik secara site to site maupun remote access dengan menggunakan tool iperf, secara otomatis hasil persentase paket terkirim sudah ditampilkan, jadi untuk mencari persentase packet loss peneliti tinggal menguragi 100% - persentase data terkirim yang pengujiannya juga mengacu kepada standar TIPHON. Dalam melakukan pangujian data peneliti memvariasikan nama dan ukuran file.

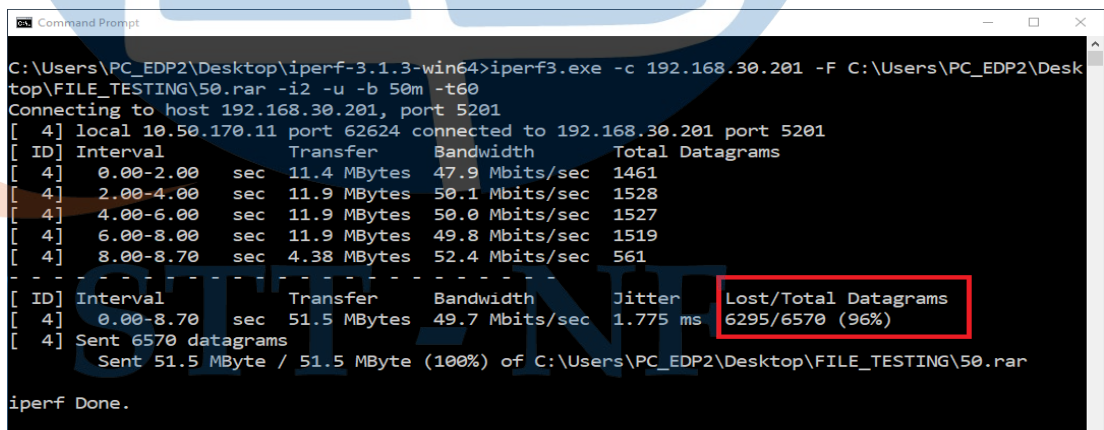
Berikut adalah cara pengujian dan tabel hasil pengujian peforma packet loss site to site dan remote access :

1. Site to Site

- Pengujian 1 ukuran file 50 Mb :

Iperf Client RSU Bunda Margonda

```
> iperf3.exe -c 192.168.30.201 -F C:\Users\PC_EDP2\Desktop\FILE_TESTING\50.rar -i2 -u -b50m -t60 >
```



```
Command Prompt
C:\Users\PC_EDP2\Desktop>iperf-3.1.3-win64>iperf3.exe -c 192.168.30.201 -F C:\Users\PC_EDP2\Desktop\FILE_TESTING\50.rar -i2 -u -b 50m -t60
Connecting to host 192.168.30.201, port 5201
[ 4] local 10.50.170.11 port 62624 connected to 192.168.30.201 port 5201
[ ID] Interval      Transfer      Bandwidth      Total Datagrams
[ 4]  0.00-2.00  sec   11.4 MBytes   47.9 Mbits/sec   1461
[ 4]  2.00-4.00  sec   11.9 MBytes   50.1 Mbits/sec   1528
[ 4]  4.00-6.00  sec   11.9 MBytes   50.0 Mbits/sec   1527
[ 4]  6.00-8.00  sec   11.9 MBytes   49.8 Mbits/sec   1519
[ 4]  8.00-8.70  sec    4.38 MBytes   52.4 Mbits/sec    561
-----
[ ID] Interval      Transfer      Bandwidth      Jitter      Lost/Total Datagrams
[ 4]  0.00-8.70   sec   51.5 MBytes   49.7 Mbits/sec  1.775 ms    6295/6570 (96%)
[ 4] Sent 6570 datagrams
Sent 51.5 MByte / 51.5 MByte (100%) of C:\Users\PC_EDP2\Desktop\FILE_TESTING\50.rar
iperf Done.
```

Gambar 5.34 Pengujian 1 Packet Loss Site to Site

➤ Pengujian 2 ukuran file 100 Mb :

Iperf Client RSU Bunda Margonda

```

: < iperf3.exe -c 192.168.30.201 -F
C:\Users\PC_EDP2\Desktop\FILE_TESTING\100.rar -i2 -u -
b50m -t60 >

```

```

C:\Users\PC_EDP2\Desktop\iperf-3.1.3-win64>iperf3.exe -c 192.168.30.201 -F C:\Users\PC_EDP2\Desktop\FILE_TESTING\100.rar -i2 -u -b50m -t60
Connecting to host 192.168.30.201, port 5201
[ 4] local 10.50.170.11 port 62625 connected to 192.168.30.201 port 5201
[ ID] Interval      Transfer      Bandwidth      Total Datagrams
[ 4] 0.00-2.00 sec  11.4 MBytes  47.8 Mbits/sec  1459
[ 4] 2.00-4.00 sec  12.0 MBytes  50.3 Mbits/sec  1536
[ 4] 4.00-6.00 sec  11.9 MBytes  49.7 Mbits/sec  1517
[ 4] 6.00-8.00 sec  11.9 MBytes  50.0 Mbits/sec  1525
[ 4] 8.00-10.00 sec 12.0 MBytes  50.1 Mbits/sec  1530
[ 4] 10.00-12.00 sec 11.9 MBytes  50.0 Mbits/sec  1527
[ 4] 12.00-14.00 sec 11.9 MBytes  49.9 Mbits/sec  1523
[ 4] 14.00-16.00 sec 11.9 MBytes  49.8 Mbits/sec  1521
[ 4] 16.00-18.00 sec 12.1 MBytes  50.6 Mbits/sec  1543
[ 4] 18.00-18.30 sec  1.90 MBytes  52.7 Mbits/sec   243
-----
[ ID] Interval      Transfer      Bandwidth      Jitter      Lost/Total Datagrams
[ 4] 0.00-18.30 sec 109 MBytes  49.9 Mbits/sec  1.896 ms    13218/13894 (95%)
[ 4] Sent 13894 datagrams
      Sent 109 MByte / 109 MByte (100%) of C:\Users\PC_EDP2\Desktop\FILE_TESTING\100.rar
iperf Done.

```

Gambar 5.35 Pengujian 2 Packet Loss Site to Site

Untuk pengujian packet loss site to site ke 3 sampai dengan terakhir peneliti menggunakan perintah yang sama sehingga didapat data sebagai berikut :

Tabel 5.6 Hasil Packet Loss Site to Site

Ukuran File	Persentase data terkirim %	Paket Loss %	Kategori
50 Mb	96 %	4 %	Bagus
100 Mb	95 %	5 %	Bagus
150 Mb	95 %	5 %	Bagus
200 Mb	95 %	5 %	Bagus
300 Mb	94 %	5 %	Bagus
400 Mb	95 %	5 %	Bagus
500 Mb	95 %	5 %	Bagus

600 Mb	95 %	5 %	Bagus
700 Mb	95 %	5 %	Bagus
800 Mb	95 %	5 %	Bagus

2. Remote Access

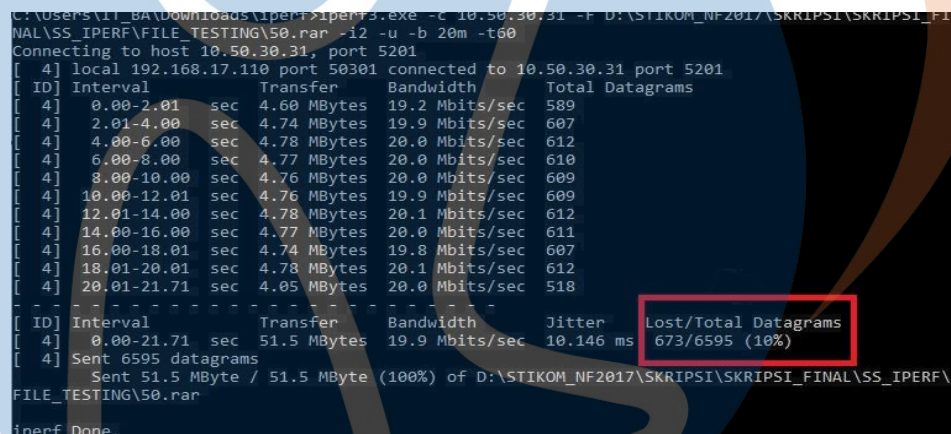
➤ Pengujian 1 ukuran file 50 Mb :

Iperf Client Remote Access

```

: < iperf3.exe -c 10.50.30.31 -F
D:\STIKOM_NF2017\SKRIPSI\SKRIPSI_FINAL\SS_IPERF\FILE
_TESTING\50.rar -i2 -u -b 20m -t60 >

```



```

C:\Users\IT_BA\Downloads\iperf>iperf3.exe -c 10.50.30.31 -F D:\STIKOM_NF2017\SKRIPSI\SKRIPSI_FINAL\SS_IPERF\FILE_TESTING\50.rar -i2 -u -b 20m -t60
Connecting to host 10.50.30.31, port 5201
[ 4] local 192.168.17.110 port 50301 connected to 10.50.30.31 port 5201
[ ID] Interval      Transfer      Bandwidth      Total Datagrams
[ 4] 0.00-2.01    sec 4.60 MBytes  19.2 Mbits/sec  589
[ 4] 2.01-4.00    sec 4.74 MBytes  19.9 Mbits/sec  607
[ 4] 4.00-6.00    sec 4.78 MBytes  20.0 Mbits/sec  612
[ 4] 6.00-8.00    sec 4.77 MBytes  20.0 Mbits/sec  610
[ 4] 8.00-10.00   sec 4.76 MBytes  20.0 Mbits/sec  609
[ 4] 10.00-12.01  sec 4.76 MBytes  19.9 Mbits/sec  609
[ 4] 12.01-14.00  sec 4.78 MBytes  20.1 Mbits/sec  612
[ 4] 14.00-16.00  sec 4.77 MBytes  20.0 Mbits/sec  611
[ 4] 16.00-18.01  sec 4.74 MBytes  19.8 Mbits/sec  607
[ 4] 18.01-20.01  sec 4.78 MBytes  20.1 Mbits/sec  612
[ 4] 20.01-21.71  sec 4.05 MBytes  20.0 Mbits/sec  518
[ ID] Interval      Transfer      Bandwidth      Jitter          Lost/Total Datagrams
[ 4] 0.00-21.71   sec 51.5 MBytes  19.9 Mbits/sec  10.146 ms      673/6595 (10%)
[ 4] Sent 6595 datagrams
      Sent 51.5 MByte / 51.5 MByte (100%) of D:\STIKOM_NF2017\SKRIPSI\SKRIPSI_FINAL\SS_IPERF\FILE_TESTING\50.rar
iperf Done.

```

Gambar 5.36 Pengujian 1 packet Loss Remote Access

➤ Pengujian 2 ukuran file 100 Mb :

Iperf Client Remote Access

```

: < iperf3.exe -c 10.50.30.31 -F
D:\STIKOM_NF2017\SKRIPSI\SKRIPSI_FINAL\SS_IPERF\FILE
_TESTING\100.rar -i2 -u -b 20m -t60 >

```

```

4] local 192.168.17.110 port 49658 connected to 10.50.30.31 port 5201
ID] Interval Transfer Bandwidth Total Datagrams
4] 0.00-2.01 sec 4.55 MBytes 19.0 Mbits/sec 583
4] 2.01-4.01 sec 4.80 MBytes 20.2 Mbits/sec 615
4] 4.01-6.01 sec 4.79 MBytes 20.1 Mbits/sec 613
4] 6.01-8.01 sec 4.76 MBytes 19.9 Mbits/sec 609
4] 8.01-10.01 sec 4.73 MBytes 19.8 Mbits/sec 605
4] 10.01-12.00 sec 4.78 MBytes 20.2 Mbits/sec 612
4] 12.00-14.00 sec 4.79 MBytes 20.1 Mbits/sec 613
4] 14.00-16.01 sec 4.80 MBytes 20.1 Mbits/sec 614
4] 16.01-18.00 sec 4.72 MBytes 19.8 Mbits/sec 604
4] 18.00-20.00 sec 4.77 MBytes 20.0 Mbits/sec 611
4] 20.00-22.00 sec 4.77 MBytes 20.0 Mbits/sec 611
4] 22.00-24.02 sec 4.75 MBytes 19.8 Mbits/sec 608
4] 24.02-26.01 sec 4.77 MBytes 20.0 Mbits/sec 610
4] 26.01-28.01 sec 4.76 MBytes 20.0 Mbits/sec 609
4] 28.01-30.01 sec 4.80 MBytes 20.2 Mbits/sec 615
4] 30.01-32.00 sec 4.76 MBytes 20.0 Mbits/sec 609
4] 32.00-34.01 sec 4.77 MBytes 20.0 Mbits/sec 611
4] 34.01-36.00 sec 4.77 MBytes 20.0 Mbits/sec 610
4] 36.00-38.01 sec 4.77 MBytes 20.0 Mbits/sec 611
4] 38.01-40.00 sec 4.77 MBytes 20.0 Mbits/sec 611
4] 40.00-42.00 sec 4.75 MBytes 19.9 Mbits/sec 608
4] 42.00-44.01 sec 4.75 MBytes 19.9 Mbits/sec 608
4] 44.01-45.72 sec 4.09 MBytes 20.2 Mbits/sec 524
ID] Interval Transfer Bandwidth Jitter Lost/Total Datagrams
4] 0.00-45.72 sec 109 MBytes 20.0 Mbits/sec 9.621 ms 1398/13924 (10%)
4] Sent 13924 datagrams
Sent 109 MByte / 109 MByte (100%) of D:\STIKOM_NF2017\SKRIPSI\SKRIPSI_FINAL\SS_IPERF\
ETHE_TESTING\100.pap

```

Gambar 5.37 Pengujian 2 Packet Loss Remote Access

Untuk pengujian packet loss remote access yang ke 3 sampai dengan terakhir peneliti menggunakan perintah yang sama sehingga didapat data sebagai berikut :

Tabel 5.7 Hasil Packet Loss Remote Access

Ukuran File	Persentase data terkirim %	Paket Loss %	Kategori
50 Mb	10 %	90 %	Buruk
100 Mb	10 %	90 %	Buruk
150 Mb	20 %	80 %	Buruk
200 Mb	14 %	76 %	Buruk
300 Mb	14 %	76 %	Buruk
400 Mb	8,5 %	91.5 %	Buruk
500 Mb	11 %	89 %	Buruk
600 Mb	10 %	90 %	Buruk
700 Mb	9.4 %	90.6 %	Buruk
800 Mb	10 %	90 %	Buruk

BAB VI

KESIMPULAN DAN SARAN

Berdasarkan hasil penelitian dari beberapa pengujian di atas, maka dapat diambil beberapa kesimpulan dari penggunaan teknologi Virtual Private Network (VPN) berbasis Protokol L2TP dan IPsec yang diterapkan pada RSUD Bunda Margonda adalah sebagai berikut :

6.1 Kesimpulan

Dari penelitian yang dilakukan, dapat disimpulkan bahwa Rancangan VPN dengan L2TP+IPSec menggunakan router mikrotik di RSUD Bunda Margonda telah berfungsi sesuai dengan konfigurasi yang telah di implementasikan oleh peneliti, Router Mikrotik Head Office (HOF) sebagai VPN server Site To Side, dan Router Mikrotik RSUD Bunda Margonda sebagai VPN Server Remote Access (Road Warrior), Hal ini telah dibuktikan dengan adanya autentifikasi Virtual Private Network (VPN) client berupa username, password, serta ipsec yang sesuai dengan konfigurasi yang telah peneliti lakukan. Virtual Private Network (VPN) berbasis layer 2 tunneling protokol dan IPSec dapat terhubung dengan baik, dapat dilihat dari hasil pengujian fungsionalitas VPN, dengan melakukan ping (paket ICMP) secara simultan baik dari VPN server maupun dari VPN Client, serta melakukan traceroute dari VPN Server maupun VPN Client untuk mengetahui jalur lalulintas koneksi VPN apakah gateway nya melalui IP VPN yang sudah di setting sebelumnya sehingga tidak mengganggu lalulintas network di jaringan lokal masing-masing VPN Server.

Untuk pengujian performa dari konektivitas VPN L2TP+IPSec dapat dilihat dari tabel hasil pengujian Troughput, Jitter, dan Paket Loss, yang dilakukan antara site to site dan remote acces. Performa dan konektivitas trougput, jitter, dan paket loss antara site to site dari RSUD Bunda Margonda ke Head Office masuk kategori sangat bagus, bagus, dan bagus (TIPHON), ini dikarenakan antar site menggunakan bandwidth Decicated Line sehingga koneksi antar kedua site berjalan dengan stabil, sedangkan untuk pengujian peforma dan konektivitas trougput, jitter, dan packet loss remote acces dari client ke RSUD Bunda Margonda masuk kategori sangat bagus, bagus, dan buruk (TIPHON), ini dikarenakan menggunakan badwith dari smartphone sehingga pemakaian bandwidth tidak full mengakibatkan koneksi tidak stabil.

6.2 Saran

Berdasarkan penelitian yang telah dilakukan, terdapat saran yang dapat dilakukan untuk penelitian selanjutnya, yaitu :

1. Penggunaan teknologi Virtual Private Network (VPN) berbasis protokol L2TP dan IPsec dapat diterapkan dengan menggunakan perangkat lain selain mikrotik, misalnya Cisco, Juniper, dan Ubiquiti.
2. Untuk parameter pengujian Packet Loss Remote Access mendapatkan hasil pengujian buruk dikarenakan penguji menggunakan Hotspot Thatering dari ponsel sehingga bandwidth tidak full di gunakan pada laptop, untuk mendapatkan hasil yang lebih bagus bisa menggunakan Internet Rumahan yang telah menggunakan fasilitas kabel FO, sehingga koneksi tetap stabil.
3. Perlu dibuat Standar Operating Procedure (SOP) yang berguna untuk penggunaan serta pemanfaatan jaringan secara optimal, selain itu dapat bermanfaat jika ada penelitian selanjutnya.
4. Penggunaan Virtual Private Network (VPN) berbasis protokol L2TP dan IPsec ini dapat dikembangkan pada vendor perangkat lain selain mikrotik dan dapat dikembangkan pula dengan metode enkripsi L2TP/IKEv2 atau yang sekarang banyak di gunakan tunneling OVPN.



STT - NF

DAFTAR PUSTAKA

- [1] Madcoms, *Membangun sistem jaringan komputer untuk pemula*, Ed 1. Yogyakarta: Andi Offset, 2015.
- [2] R. Hidayat, “Perancangan dan implementasi virtual private network (VPN) berbasis layer 2 Tunneling protocol (L2TP) dan IPSEC dengan menggunakan router mikrotik,” *J. Inform. Terpadu*, 2019.
- [3] Daryanto, *Teknik Komputer*. Malang: Alfabeta, 2010.
- [4] Kustatnto and Saputro, *Membangun Server Internet dengan Mikrotik OS*, J. Gaya Media, 2010.
- [5] Pratama, *Handbook Jaringan Komputer*. Bandung: Informatika Bandung, 2015.
- [6] I. Sofana, *Membangun Jaringan Komputer*. Bandung: Bandung Informatika, 2013.
- [7] D. T. P. Yanto, “Praktikalitas media pembelajaran interaktif pada proses pembelajaran rangkaian listrik,” *INVOTEK J. Inov. Vokasional dan ...*, vol. 19, no. 01, pp. 75–82, 2019.
- [8] D. Dahnil, “Analisa Perbandingan Quality Of Service Antara Protokol PPTP dan L2TP Pada Virtual Private Network Berbasis Router Mikrotik,” *J. Ilm. Inform. Glob.*, vol. 10, no. 2, pp. 107–113, 2019.
- [9] A. Husnul, *Jaringan Komputer dan Internet*. Jakarta: Mediakita, 2011.
- [10] S. Ikhwan and A. Amalina, “Analisis Jaringan VPN Menggunakan PPTP dan L2TP (Studi Kasus : Dinhubkominfo Kabupaten Banyumas),” *J. Infotel*, vol. 9, no. 3, pp. 265–270, 2017.
- [11] A. B. U. Prihatin Oktivasari, “Analisa Virtual Private Network Menggunakan Open VPN Dan Point To Point Tunneling Protocol,” *J. Penelit. Komun. dan Opini Publik*, vol. 2, pp. 185–202, 2016.
- [12] Sridevi, “L2TP/IPsec Interworkin,” *JSR-International J. Sci. Res.*, vol. 3, no. 8, pp. 89–91, 2013.
- [13] Athailah, *Mikrotik untuk Pemula*. Jakarta: Mediakita, 2013.
- [14] H. Fahmi, “Analisa Pengukuran Delay, Jitter, Packet Lost dan Throughput Untuk Mendapatkan Kualitas Peforma Radio Streaming Yang Baik Pada Radio Simfoni FM Malang,” *J. Teknol. Inf. dan Komun.*, vol. 7, no. 2, 2018.
- [15] ETSI, *Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); End to End Quality of Service in TIPHON Systems; Part 1: General aspects of Quality of Service(QoS)*. France: Sophia Antipolis Cedex, 2002.

- [16] Y. A. Pranata, I. Fibriani, and S. B. Utomo, “Analisis Optimasi Kinerja Quality Of Service Pada Layanan Komunikasi Data Menggunakan Ns-2 Di Pt. PIn (Persero),” Universitas Jember, 2016.
- [17] yanto, “Analisis Qos (Quality of Service) Pada Jaringan Internet (Studi Kasus : Fakultas Teknik Universitas Tanjungpura),” *Anal. Qos (Qual. Serv.)*, pp. 1–6, 2013.
- [18] M. Riadi, “Pengertian, Layanan dan Parameter Quality of Service (QoS),” Universitas Jendral Soedirman, 2019.



STT - NF