ANALISIS IMPLEMENTASI PPPOE DENGAN ROUTER MIKROTIK SEBAGAI SECURITIY JARINGAN KOMPUTER

(Studi Kasus: Perpustakaan Fikom)

Oleh :

MUHAMMAD NUR ILHAM
T3120022

SKRIPSI

PROGRAM SARJANA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS ICHSAN GORONTALO
GORONTALO
2024

PERSETUJUAN SKRIPSI

ANALISIS IMPLEMENTASI PPPOE DENGAN ROUTER MIKROTIK SEBAGAI SECURITIY JARINGAN KOMPUTER

(Studi Kasus: Perpustakaan Fikom)

Oleh

MUHAMMAD NUR ILHAM
T3120022

SKRIPSI

Telah disetujui dan siap diseminarkan

Gorontalo, Juni 2024

Pembimbing Utama	Pembimbing Pendamping
Rofiq Harun, M.Kom	**Andi Bode, M.Kom**
NIDN. 0919048404	**NIDN. 0922099101**

PENGESAHAN SKRIPSI

ANALISIS IMPLEMENTASI PPPOE DENGAN ROUTER MIKROTIK SEBAGAI SECURITIY JARINGAN KOMPUTER

Oleh

MUHAMMAD NUR ILHAM

T3120022

Diperiksa oleh Panitia Ujian Strata Satu (S1)

Universitas Ichsan Gorontalo

1. Ketua Penguji
   Irvan Abraham Salihi, M.Kom .....
2. Anggota
   Warid Yunus, M.Kom .....
3. Anggota
   Mohamad Efendi Lasulika, M.Kom .....
4. Anggota
   Rofiq Harun, M.Kom .....
5. Anggota
   Andi Bode, M.Kom .....

Mengetahui

Dekan Fakultas Ilmu Komputer	Ketua Program Studi
Irvan Abraham Salihi. S.Kom., M.Kom	**Sudirman S. Panna M.Kom**
NIDN.0912117702	**NIDN. 0928028101**

PERNYATAAN SKRIPSI

Dengan ini saya menyatakan bahwa :

1. Karya tulis (Skripsi) saya ini adalah asli dan belum pernah diajukan untuk mendapatkan gelar akademik (sarjana) baik di Universitas Ichsan Gorontalo maupun di perguruan tinggi lainnya.
2. Karya tulis (Skripsi) saya ini adalah murni gagasan, rumusan, dan penelitian saya sendiri, tanpa bantuan pihak lain, kecuali arahan Tim Pembimbing.
3. Dalam karya tulis (Skripsi) saya ini tidak terdapat karya atau pendapat yang telah dipublikasikan orang lain, kecuali secara tertulis dicantumkan sebagai acuan/sitasi dalam naskah dan dicantumkan pula dalam daftar pustaka.
4. Pernyataan ini saya buat dengan sesungguhnya dan apabila dikemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka saya bersedia menerima sanksi akademik berupa pencabutan gelar yang telah diperoleh karena karya tulis ini, serta sanksi lainnya sesuai dengan norma-norma yang berlaku di Universitas Ichsan Gorontalo.

Gorontalo, Juni 2024
Yang membuat pernyataan,

Materai
10.000

Muhammad Nur Ilham

ABSTRACT

MUHAMMAD NUR ILHAM. T3120022. ANALYSIS OF PPPoE IMPLEMENTATION WITH MIKROTIK ROUTER AS COMPUTER NETWORK SECURITY (CASE STUDY: LIBRARY OF COMPUTER SCIENCE FACULTY)

This study aims to analyze the implementation of the Point-to-Point Over Ethernet (PPPoE) Protocol using a Mikrotik router as a security solution on a computer network. The PPPoE is a protocol used to connect end users to a network via Ethernet media. Mikrotik is known as a reliable router device for network management and settings. In this study, PPPoE configuration is carried out on the Mikrotik router to secure network access, and as an evaluation of the effectiveness of its implementation in terms of authentication, data encryption, and user access control. This study indicates that PPPoE with a Mikrotik router can improve network security through better user authentication management and also provide an additional protection layer against potential external threats. In addition, the implementation of PPPoE also allows for more efficient bandwidth settings and restrictions on access to the network following the policies applied. This study contributes to the development of Mikrotik-based network security solutions using PPPoE as an effective user access management mechanism.

Keywords: PPPoE, Mikrotik, network security, authentication, data encryption

ABSTRAK

MUHAMMAD NUR ILHAM. T3120022. ANALISIS IMPLEMENTASI PPPOE DENGAN ROUTER MIKROTIK SEBAGAI SECURITIY JARINGAN KOMPUTER (STUDI KASUS: PERPUSTAKAAN FIKOM)

Penelitian ini bertujuan untuk menganalisis implementasi Protokol Point-to-Point Over Ethernet (PPPoE) dengan menggunakan router Mikrotik sebagai solusi keamanan pada jaringan komputer. PPPoE adalah protokol yang digunakan untuk menghubungkan pengguna akhir ke jaringan melalui media Ethernet, sementara Mikrotik dikenal sebagai perangkat router yang dapat diandalkan untuk manajemen dan pengaturan jaringan. Dalam penelitian ini, dilakukan konfigurasi PPPoE pada router Mikrotik untuk mengamankan akses jaringan, serta evaluasi terhadap efektivitas implementasinya dalam hal autentikasi, enkripsi data, dan pengendalian akses pengguna. Hasil penelitian menunjukkan bahwa PPPoE dengan router Mikrotik mampu meningkatkan keamanan jaringan melalui pengelolaan otentikasi pengguna yang lebih baik, serta memberikan lapisan perlindungan tambahan terhadap potensi ancaman eksternal. Selain itu, penerapan PPPoE ini juga memungkinkan pengaturan bandwidth yang lebih efisien dan pembatasan akses ke jaringan sesuai dengan kebijakan yang diterapkan. Penelitian ini memberikan kontribusi dalam pengembangan solusi keamanan jaringan berbasis Mikrotik dengan menggunakan PPPoE sebagai mekanisme pengelolaan akses pengguna yang efektif.

Kata kunci: PPPoE, Mikrotik, keamanan jaringan, autentikasi, enkripsi data

KATA PENGANTAR

Alhamdulillah, penulis dapat menyelesaikan Skripsi ini dengan judul **"ANALISIS IMPLEMENTASI *PPPOE* DENGAN ROUTER MIKROTIK SEBAGAI *SECURITIY* JARINGAN KOMPUTER PADA PERPUSTAKAAN FIKOM"** untuk memenuhi salah satu syarat penyusunan Skripsi Program studi Teknik Informatika Fakultas Ilmu Komputer Universitas Ichsan Gorontalo.

Penulis menyadari sepenuhnya bahwa skripsi ini tidak mungkin terwujud tanpa bantuan dan dorongan dari berbagai pihak, baik bantuan moril maupun materil. Untuk itu, dengan segala keikhlasan dan kerendahan hati, penulis mengucapkan banyak terima kasih dan penghargaan yang setinggi – tingginya kepada:

1. Ibu Dr. Dra. Juriko Abdussamad, M.Si, selaku Ketua Yayasan Pengembangan Ilmu Pengatahuan dan Teknologi (YPIPT) Ichsan Gorontalo,
2. Bapak Dr. Abd. Gaffar Latjokke, M.Si, selaku Rektor Universitas Ichsan Gorontalo,
3. Bapak Irvan A. Salihi M.Kom, selaku Dekan Fakultas Ilmu Komputer Universitas Ichsan Gorontalo,
4. Bapak Sudriman Melangi M.Kom, selaku Wakil Dekan 1 Bidang Akademik Fakultas Ilmu Komputer Universitas Ichsan Gorontalo,
5. Ibu Irma Surya Kumala Idris, M.Kom, selaku Wakil Dekan II Bidang Administrasi Umum dan Keuangan Fakultas Ilmu Komputer Universitas Ichsan Gorontalo,
6. Bapak Sudirman S Panna, M.Kom, selaku Ketua Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Ichsan Gorontalo,
7. Bapak Rofiq Harun, M.Kom, Selaku Pembimbing utama Yang telah Membimbing Penulis Selama Penyusunan Penelitian Ini,
8. Bapak Andi Bode, M.Kom, selaku Pembimbing Pendamping Yang telah Membimbing Penulis selama Penyusunan Penelitian Ini,
9. Bapak dan Ibu Dosen Universitas Ichsan Gorontalo yang telah mendidik dan mengajarkan berbagai disiplin ilmu kepada penulis,

10. Kedua Orang Tua saya yang tercinta, atas segala kasih saying, jerih payah dan doa restunya dalam membesarkan dan mendidik penulis,
11. Rekan-rekan seperjuangan yang telah banyak memberikan bantuan dan dukungan moril yang sangat besar kepada penulis,

Semoga Allah, SWT melimpahkan balasan atas jasa-jasa mereka kepada kamu. Penulis menyadari sepenuhnya bahwa apa yang telah dicapai ini masih jauh dari kesempurnaan dan masih banyak terdapat kekurangan. Oleh karena itu, penulis sangat mengharapkan adanya kritik dan saran yang konstruktif. Akhirnya penulis berharap semoga hasil yang telah dicapai ini dapat bermanfaat bagi kita semua, Aamiin.

Gorontalo, Juni 2023

Penulis

DAFTAR ISI

PERSETUJUAN SKRIPSI ii
PENGESAHAN SKRIPSI iii
KATA PENGANTAR iv
DAFTAR ISI vi
DAFTAR GAMBAR i
Daftar table ii
BAB I PENDAHULUAN 1
1.1. LATAR BELAKANG 1
1.2. Identifikasi Masalah 4
1.3. Rumusan Masalah 4
1.4. Tujuan Penelitian 4
1.5. MANFAAT PENELITIAN 4
BAB II LANDASAN TEORI 5
2.1. Tinjauan Pustaka 5
2.2. Tinjauan Teori 8
2.2.1. Konsep Dasar Jaringan Komputer 8
2.2.2. Konsep Dasar Keamanan Jaringan Komputer 10
2.2.3. Jenis Serangan Keamanan Jaringan 10
2.3. Router Mikrotik 11
2.4. PPPOE 12
2.5. Firwall 13
2.6. Kerangka Pemikiran 15
BAB III METODOLOGI PENELITIAN 16
3.1. Jenis, Metode, Subjek, Objek, Waktu, dan Lokasi Penelitian 16
3.2. Pengumpulan Data 16
3.2.1. Data primer 16
3.2.2. Data Sekunder 16
3.3. Pengembangan Sistem 16
3.4. Desain Sistem 16
3.5. Rancangan Sistem 17

3.6. Konstruksi Sistem 17
3.7. Pengujian Sistem 18
BAB IV HASIL PENLITIAN 19
4.1. Analisa dan implementasi sistem 19
4.1.1. Analisis kebutuhan sistem 19
4.1.2 perancangan topologi jaringan 22
4.2. Implementasi PPPOE 22
4.2.1. Perancangan seting-an PPPOE 22
4.2.2. Perancangan seting-an access point 24
BAB V PEMBAHASAN DAN HASIL 27
5.1. Perancangan seting-an mikrotik untuk keamamanan pembatasan akses situs – situs tertentu dalam perpustakaan 27
5.1.1. Perancagan sistem filters rules 27
5.1.2. Pencarian IP addres pada CMD 29
5.1.3. Perancangan sistem keamanan address list 30
5.2. Hasil tampilan perancangan sistem keamanan yang sudah di block atau di batasi pada browser atau chrome 31
5.2.1. Hasil tampilan chrome situs yang sebelum dan sudah di block 31
5.3. hasil tampilan kemanan situs yang telah di bock pada CMD 34
BAB VI PENUTUP 35
6.1. Kesimpulan 35
6.2. Saran 35
DAFTAR PUSTAKA 40
JADWAL PENELITIAN ..... Error! Bookmark not defined.

DAFTAR GAMBAR

Gambar 2.1 Kerangka Pikir 15

Gambar 3. 1 perancangan sistem 17

Gambar 4. 1 Topologi Jaringan 22
Gambar 4. 2 Konfigurasi PPPOE 23
Gambar 4. 3 Profil PPPOE 23
Gambar 4. 4 Secret PPPOE 24
Gambar 4. 5 Konfigurasi Access Point 25
Gambar 4. 6 Konfigurasi Access Point 25
Gambar 4. 7 Spedtest 26

Gambar 5. 1 Tampilan Firewall 27
Gambar 5. 2 Menu General 27
Gambar 5. 3 Menu Advanced 28
Gambar 5. 4 Menu Action 29
Gambar 5. 5 CMD Nslookup 30
Gambar 5. 6 Menu Address List 30
Gambar 5. 7 Address List 31
Gambar 5. 8 Tampilan Situs yang Belum di Block 32
Gambar 5. 9 tampilan situs yang telah di Block 33
Gambar 5. 10 Tampilan Block Pada CMD 34

Daftar table

Tabel 2. 1 Penelitian Terkait 5

Tabel 4. 1 Kebutuhan Perangkat Keras 19

Tabel 4. 2 Kebutuhan Perangkat Lunak 20

BAB I
PENDAHULUAN

1.1. LATAR BELAKANG

Semakin bertambah jumlah pengguna dan semakin meluasnya jangkauan komunikasi, maka peluang serangan juga semakin meningkat. Serangan atau intrusi dapat didefinisikan sebagai tindakan untuk masuk ke dalam wilayah atau mengakses secara ilegal yang berpotensi membahayakan perangkat jaringan lainnya.[1].dan mengakibatkan peningkatan kebutuhan akan jaringan komunikasi. Pada awalnya, pertukaran data hanya menggunakan hardcopy tulisan tangan, dokumen, laporan bulanan, dll. Karena keterbatasan waktu, beralih ke komunikasi melalui jaringan internet dan efektifitas.[2].

Fakultas Ilmu Komputer Universitas Ichsan Gorontalo menggunakan Laboratorium Komputer dan kelas untuk pembelajaran sehari-hari. Dosen juga sering meminta mahasiswa untuk mencari materi di media pencari informasi manapun untuk mendapatkan informasi dari internet, yang membutuhkan koneksi jaringan. Selain itu, siswa memiliki kebebasan untuk melakukan aktivitas yang mereka inginkan. Mereka dapat mengunjungi situs web yang berfokus pada pembelajaran, mengakses pemutar musik dan video, dan mengakses situs-situs sosial dan sumber pendidikan lainnya.

Yang saya lihat masih ada kendala dalam jaringan seperti mahasiswa hanya bisa menggunakan satu perangtat pada satu akun mereka dan juga kalau ada kendala pada satu jaringan. Jaringan lain terpengaruh. Soalnya jaringan di fakultas ilmu komuter ini menggunakan jaringan yang hanya bisa di akses dalam 1 perangkat

Menurut Ongkowinoto (2021), *PPPoE* (*Point to Point Protocol over Ethernet*) adalah salah satu protokol jaringan yang sering digunakan untuk membuat koneksi antara komputer dan *server*. Salah satu keunggulan teknologi atau metode *PPPoE* adalah meningkatkan keamanan akses internet dengan penggunaan username dan password yang unik untuk mengatur batasan kecepatan dan melakukan filter

terhadap lalu lintas internet. Selain itu, *PPPoE* juga menyediakan fitur-fitur dasar seperti autentikasi, enkripsi, dan kompresi data. Oleh karena itu, *PPPoE* menjadi salah satu pilihan utama dalam mengelola koneksi internet, memungkinkan penyedia layanan internet untuk menawarkan berbagai jenis layanan yang berbeda.

Selain itu, PPPoE juga berguna untuk mencegah serangan dari komputer lain yang berada dalam satu router. Tanpa menggunakan *PPPoE*, perangkat lain dapat dengan mudah mengidentifikasi alamat MAC dan IP dari perangkat tersebut. Namun, dengan menggunakan *PPPoE*, baik alamat MAC maupun IP tidak terlihat karena otentikasi dilakukan melalui penggunaan username dan password.[3]

Protokol Point-to-Point over Ethernet (*PPPoE*) digunakan untuk mengenkapsulasi frame PPP ke dalam frame Ethernet. Pada masa pergantian abad, saat DSL menjadi populer sebagai solusi untuk mengirimkan paket melalui koneksi DSL ke jaringan IP ISP dan ke seluruh internet, PPPoE menjadi protokol yang umum digunakan. Dalam bukunya berjudul "*Cisco IOS in a Nutshell*", James Boney mencatat bahwa kebanyakan penyedia DSL menggunakan PPPoE untuk menyediakan otentikasi, enkripsi, dan kompresi. Penggunaan PPPoE secara umum memanfaatkan fasilitas PPP untuk mengotentikasi pengguna melalui username dan password, terutama melalui protokol Password Authentication Protocol (PAP).[4]

sistem PPPoE Server. Instansi ini menggunakan router mikrotik sebagai servernya. Memang kebanyakan instansi menggukan router mikrotik, karena dengan konfigurasi yang mudah yang disertai basic GUI (Graphical User Interface). Pihak instansi mencari alat untuk dijadikan server selain router mikrotik. Sebenarnya ada banyak router seperti Juniper, Vyatta, dan Cisco. tapi yang lebih bagus dan efektif yakni router Cisco.[5]

Dalam pengembangan jaringan komputer, keamanan jaringan menjadi prioritas utama. Keamanan jaringan mengacu pada kemampuan suatu jaringan untuk melindungi dirinya sendiri. Segala jenis ancaman, baik langsung maupun tidak langsung, dapat mengganggu aktivitas dalam jaringan komputer. Untuk melindungi jaringan dari serangan-serangan tersebut, diperlukan penerapan konsep *firewall*.

Firewall dirancang untuk mencegah akses yang tidak diinginkan, baik dari internal maupun eksternal jaringan. Prinsip kerja *firewall* cukup sederhana, yaitu melakukan pemeriksaan dan pengendalian terhadap lalu lintas data yang masuk dan keluar dari jaringan sebelum diteruskan ke tujuan yang dituju.[6]

Seperti dalam peneitian sebelumnya yang dilakukan oleh (Eri Prasetyo, Amir Hamzah dan Edhy Sutanta,2016). Demgan judul ANALISA QUALITY OF SERVICE (QOS) KINERJA POINT TO POINT PROTOCOL OVER ETHERNET (PPPoE) DAN POINT TO POINT TUNNELING PROTOCOL (PPTP) tentang kualitas jaringan dan upaya untuk mengidentifikasi fitur dan karakteristik layanan di Laboratorium Komputer IST AKPRIND Yogyakarta berdasarkan Hasil pengujian *packet loss* pada PPPoE dan PPTP dalam kondisi sepi maupun padat dengan beban paket 1.000 byte, 10.000 *byte*, 40.000 *byte*, 65.500 byte semuanya menunjukkan tidak ada paket yang hilang atau persentase *packet loss* adalah 0%.[7] Atau dalam peneltian oleh (Vicky Bin Djusmin) dengan judul HOTSPOT BERBASIS KONEKSI PPPoE (POINT TO POINT PROTCOL OVER ETHERNET) DENGAN OTENTIKASI USER MANAGER MIKROTIK PADA WARNET STARCOM berdasarkan hasil pengujian Dengan fitur PPPoE pada mikrotik dapat mengamankan komunikasi data karena data yang dikirimkan telah melalui enkripsi sehingga walaupun ada pengguna lain yang melakukan penyadapan data pada jaringan wireless maka isi data yang sesungguhnya tidak dapat diketahui.[8]

Dengan mempertimbangkan latar belakang tersebut, peneliti ingin melakukan penelitian yang diberi judul " **ANALISIS IMPLEMENTASI PPPOE DENGAN ROUTER MIKROTIK SEBAGAI SECURITIY JARINGAN KOMPUTER"**

1.2. Identifikasi Masalah

Berdasarkan uraian latar belakang masalah di atas, maka identifikasi masalahnya adalah :

1. Banyaknya pengguna layanan akses internet pada kampus perpustakaan fikom yang mengakibatkan kurang maksimal keamanan jaringan komputer
2. Pelayanan jaringan internet di perpustakaan fikom belum menerapkan Layanan PPPOE dengan router Mikrotik sebagai keamanan jaringan komputer

1.3. Rumusan Masalah

Berdasarakan rumusan masalah diatas maka rumusan masalah dari penelitian ini yaitu:

1. Bagaimana cara analisis implementasi PPPoE dengan router MikroTik dapat menjadi solusi efektif dalam meningkatkan keamanan jaringan computer ?
2. Apakah penggunaan PPPoE dengan router mikrotik sebagai keamanan jaringan computer efektif menghindari adanya serangan ?

1.4. Tujuan Penelitian

Adapun tujuan penelitian dari tugas akhir ini adalah sebagai berikut:

1. Menganalisis implementasi PPPoE dengan router MikroTik sebagai solusi efektif untuk meningkatkan keamanan jaringan komputer.
2. Mengidentifikasi efektifitas penggunaan PPPoE dengan router mikrotik sebagai keamanan jaringan komputer dalam menghindari serangan.

1.5. MANFAAT PENELITIAN

Dampak dari tujuan penelitian ini adalah:

1. **Manfaat Teoritis:** memberikan kontribusi pengetahuan yang baru dan mendalam dalam domain keamanan jaringan komputer. Hasil penelitian ini dapat menjadi referensi dan sumber informasi bagi akademisi, mahasiswa, atau pihak-pihak yang tertarik dalam bidang keamanan jaringan komputer.
2. **Manfaat Praktis:** memberikan rekomendasi dan solusi konkret dalam mengimplementasikan PPPoE dengan router MikroTik untuk meningkatkan keamanan jaringan komputer. Dengan demikian, penelitian ini dapat membantu

institusi tersebut dalam melindungi data dan sistem jaringan mereka dari serangan dan intrusi yang berpotensi merugikan.

BAB II
LANDASAN TEORI

2.1. Tinjauan Pustaka

Berdasarkan kajian pustaka sebelumnya yang telah banyak dilakukan penelitian mengenai analisis implementasi PPPoE dengan router mikrotik sebagai securitiy jaringan koputer. Hasil dari penelitian tersebut diantaranya:

Tabel 2. 1 Penelitian Terkait

NO	PENELITI	JUDUL	TAHUN	HASIL
1.	Nursobah 1) , Pitrasacha Aditya 2) , Supriady 3)	IMPLEMENTASI JARINGAN PPPOE DAN *HOTSPOT SERVER* RT/RW NET BERBASIS MIKROTIK DENGAN FITUR MIKHMON DI ADINET SAMARINDA SEBERANG	2023	hasil analisis dan perancangan jaringan di Adinet Samarinda Seberang dapat ditarik kesimpulan yaitu: Adinet merupakan organisasi yang bertujuan untuk membangun jaringan yang aman dan stabil serta memberikan harga yang terjangkau sehingga semua masyarakat atau yang berekonomi rendah dapat menikmati internet tanpa mengeluarkan biaya yang besar. Belum adanya dokumentasi yang jelas untuk jaringan PPPoE dan *hotspot server* di Adinet Samarinda Seberang menyebabkan keadaan jaringan menjadi kurang dalam pengelolaan dan

				mempersulit dalam pemeliharaan jaringan. Untuk mengatasi itu penelitian ini akan menghasilkan sebuah dokumentasi jaringan yang ada di Adinet Samarinda Seberang Seiring berjalannya waktu dan bertambah banyaknya pelanggan, terjadi permasalahan pada jaringan yaitu terjadinya bentrok alamat IP dan juga terjadinya looping. Oleh karena itu diperlukan pengalamatan ulang setiap perangkat dalam jaringan baik kabel LAN maupun WLAN agar tidak terjadi bentrok[9]
2.	Sopian Sumardi1, Mohammad Taufan Asri Zaen2	PERANCANGAN JARINGAN KOMPUTER BERBASIS MIKROTIK ROUTER OS PADA SMAN 4 PRAYA	2018	hasil pemaparan uraian pembahasan pada bab-bab sebelumnya dan hasil uji coba yang dilakukan pada penelitian ini, dapat disimpulkan beberapa hal sebagai berikut: Menghasilkan rancangan jaringan komputer Local area Network (LAN) dan Wireless Fidelity (WiFi) area berbasis mikrotik

				router yang dapat di implementasikan pada SMAN 4 Praya. 2) Dari sisi administrator, sistem login pada mikrotik *hotspot* dapat lebih mempermudah dalam hal pemeliharaan dan monitoring. Karena seluruh aktivitas penggunakan dapat dilihat dari mikrotik.[10]
3.	BIMA FASEHAN	RANCANG BANGUN SISTEM KEAMANAN JARINGAN KOMPUTER MENGGUNAKAN FIREWALL FILTER PADA LABORATORIUM JURUSAN TEKNIK KOMPUTER	2021	n hasil percobaan dan analisis data pada sistem wireless backbone MPLS didapatkan bahwa Dari scenario pengukuran kualitas komunikasi dengan Packet Generator didapatkan *delay* dan jitter terbesar terjadi pada saat komunikasi menggunakan protokol PPPoE yaitu sebesar 3ms untuk *delay*, dan untuk nilai Jitter terbesar yang didapat dari pengujian adalah 6ms. Dari scenario pengukuran kualitas komunikasi dengan Packet Generator menggunakan metode PPPoEMPLS berhasil menurunkan nilai *delay* dan jitter menjadi sebesar 5ms

				turun 1ms dari PPPoE untuk *delay* dan 0.88ms turun 0.12ms dari PPPoE Dari scenario pengukuran kualitas komunikasi dengan menggunakan layanan video streaming, didapatkan nilai *delay* dan jitter terbesar terjadi pada resolusi video paling besar yaitu Full High Definition (1920x1080) dan dengan menggunakan protokol PPPoE, dengan nilai *delay* 126.1ms dan jitter 17.65ms. Dari data yang didapt disimpulkan bahwa penggunaan protokol PPPoE dalam jaringan *backbone wireless* akan meningkatkan nilai jitter dan *delay* dan Penggunaan MPLS dalam jaringan Wireless backbone akan menurunkan nilai jitter dan *delay*[11]

2.2.Tinjauan Teori

2.2.1. Konsep Dasar Jaringan Komputer

Network atau jaringan dalam bidang komputer dapat diartikan sebagai dua atau lebih perangkat cerdas yang dihubungkan sehingga dapat berkomunikasi, yang kemudian akan menimbulkan suatu efisiensi, sentralisasi/desantralisasi, dan optimasi kerja. Pada jaringan komputer, yang dikomunikasikan adalah data

sehingga bila ingin bertukar antar komputer, misalnya, maka kita dapat melakukan proses unduh atau unggah berkas tanpa harus membawa media penyimpanan. Ada beberapa jenis jaringan komputer bila dilihat dari cara pemrosesan data dan pengaksesannya:

1. *Host* – Terminal Dimana terdapat satu atau lebih *server* yang dihubungkan dalam suatu dumb terminal. Karena dumb terminal hanyalah sebuah monitor yang dihubungkan dengan menggunakan kabel RS-232 maka pemrosesan data dilakukan didalam *server*. Oleh karena itu, *server* tersebut haruslah sebuah sistem komputer yang memiliki kemampuan pemrosesan data yang tinggi dan pemyimpanan data yang sangat besar.
2. *Client – Server* Dimana sebuah *server* atau lebih yang dihubungkan dengan beberapa *client*. *Server* bertugas menyediakan berbagai macam layanan, misalnya pengaksesan berkas, basis data. Sedangkan *client* adalah sebuah terminal yang menggunakan layanan tersebut. Perbedaannya dengan hubungan dumb terminal adalah sebuah terminal *client* melakukan pemrosesan data di terminalnya sendiri dan hal itu menyebabkan spesifikasi dari *server* tidaklah harus memiliki performansi tinggi dan kapasitas penyimpanan data yang besar karena semua pemrosesan data yang merupakan permintaan dari *client* dilakukan diterminal *client*.
3. Peer to Peer Dimana terdapat beberapa terminal komputer yang dihubungkan denga media jaringan komputer. Secara prinsip, hubungan peer to peer ini adalah bahwa setiap komputer dapat berfungsi sebagai *server* dan *client*, keduanya dapat difungsikan dalam waktu yang bersamaan. Sedangkan bila dilihat dari sisi jangkauannya, jaringan dapat dibagi menjadi 4 jenis:
   A. Local Area Network (LAN) Adalah sebuah jaringan komputer yang bersifat lokal fisik jaringan komputernya, misalnya di satu ruang laboratorium komputer.
   B. Wide Area Network (WAN) Adalah sebuah jaringan komputer antara satu gedung dengan gedung lain yang terletak agak berjauhan.
   C. Metropolitan Area Network (MAN) Adalah jaringan komputer yang melibatkan beberapa jaringan komputer yang terhubung saru sama lain dan

secara geografis tersebar cukup jauh, namun masih dalam satu wilayah atau kota.[12]

2.2.2. Konsep Dasar Keamanan Jaringan Komputer

Keamanan jaringan adalah proses untuk mencegah dan mengidentifikasi penggunaan yang tidak sah dari jaringan komputer. Langkah-langkah pencegahan membantu menghentikan pengguna yang tidak sah untuk mengakses setiap bagian dari sistem jaringan komputer. Keamanan jaringan komputer sendiri bertujuan untuk mengantisipasi resiko pada jaringan komputer berupa bentuk ancaman fisik maupun logic baik langsung ataupun tidak langsung mengganggu aktivitas yang sedang berlangsung dalam jaringan komputer [13].

Keamanan jaringan secara umum adalah komputer yang terhubung ke network, mempunyai ancaman kemanan lebih besar dari pada komputer yang berdiri sendiri (standalone). Dengan pengendalian yang teliti, resiko tersebutdapat dikurangi. Namun network security biasanya bertentangan dengan network a ccess semakin mudah, maka network security semakin rawan dan bila network security semakin baik, network access semakin tidak nyaman. Suatu network didesain sebagai komunikasi data highway dengan tujuan meningkatkan akses kesistem komputer, sementara security didesain untuk mengontrol akses. Penyediaan network security adalah sebagai aksi penyeimbang atara open access dengan security.

2.2.3. Jenis Serangan Keamanan Jaringan

1. Serangan DoS: Serangan DoS membuat jaringan atau sistem menjadi tidak dapat digunakan dengan cara mengirimkan lalu lintas data yang berlebihan.
2. Serangan DDoS: Serangan DDoS dilakukan menggunakan banyak komputer yang terhubung ke internet secara bersamaan untuk membuat sumber daya jaringan tidak tersedia.
3. Serangan Malware: Serangan malware mengirimkan perangkat lunak berbahaya ke sistem target untuk menyebabkan kerusakan atau mencuri informasi.

4. Serangan Phishing: Serangan phishing menyamar sebagai entitas tepercaya melalui email, pesan teks, atau situs web palsu untuk mendapatkan informasi sensitif.
5. Serangan Man-in-the-Middle: Serangan Man-in-the-Middle memantau dan memodifikasi komunikasi antara dua pihak yang berinteraksi.
6. Serangan Sniffing: Serangan sniffing memonitor dan merekam lalu lintas jaringan untuk mendapatkan informasi sensitif.
7. Serangan SQL Injection: Serangan SQL injection memanfaatkan celah keamanan pada aplikasi web untuk mendapatkan akses ke database.
8. Serangan Zero-day: Serangan zero-day memanfaatkan kerentanan keamanan yang belum diketahui atau diperbaiki oleh pengembang.
9. Serangan Social Engineering: Serangan social engineering memanipulasi orang secara psikologis untuk mendapatkan informasi sensitif atau akses ke sistem.

2.3. Router Mikrotik

MikroTik adalah produsen perangkat jaringan asal Latvia yang menghasilkan berbagai jenis router, switch, dan sistem nirkabel. Router mereka terkenal karena keandalannya, fitur canggih, dan harga yang terjangkau, sehingga populer di kalangan administrator jaringan dan penyedia layanan.

Router MikroTik umumnya menggunakan sistem operasi RouterOS, yang menawarkan berbagai opsi konfigurasi dan kemampuan jaringan yang canggih. Beberapa fitur kunci dari router MikroTik meliputi:

1. Routing: Router MikroTik mendukung berbagai protokol routing seperti routing statis, OSPF, BGP, dan RIP. Ini memungkinkan pengalihan lalu lintas jaringan yang efisien antar jaringan yang berbeda.
2. Firewall dan Keamanan: Router MikroTik menyediakan kemampuan firewall yang kuat untuk melindungi jaringan Anda dari akses yang tidak sah. Mereka mendukung fitur seperti penyaringan paket, pelacakan koneksi, NAT (Network Address Translation), dan enkripsi VPN (Virtual Private Network).
3. Konektivitas Nirkabel: Router MikroTik sering dilengkapi dengan kemampuan nirkabel bawaan, memungkinkan Anda untuk membuat jaringan nirkabel

menggunakan standar seperti 802.11a/b/g/n/ac. Mereka mendukung fitur seperti mode akses poin, penghubung nirkabel (wireless bridging), dan sistem distribusi nirkabel (WDS).

4. Manajemen Bandwidth: Router MikroTik menawarkan alat yang kuat untuk mengelola dan mengontrol penggunaan bandwidth pada jaringan Anda. Anda dapat mengimplementasikan fitur seperti Quality of Service (QoS), traffic shaping, dan antrian sederhana (simple queues) untuk memprioritaskan jenis lalu lintas tertentu atau membatasi bandwidth untuk pengguna atau aplikasi tertentu.
5. *Hotspot* dan Manajemen Pengguna: Router MikroTik mendukung pembuatan *hotspot* berbasis captive portal, di mana pengguna harus melakukan autentikasi sebelum dapat mengakses internet. Mereka menyediakan fitur manajemen pengguna seperti otentikasi pengguna, waktu sesi, dan integrasi billing.
6. Pemantauan dan Manajemen: Router MikroTik dilengkapi dengan berbagai alat pemantauan dan manajemen. Sistem operasi RouterOS menyediakan antarmuka berbasis web yang disebut Winbox, serta akses melalui baris perintah melalui SSH dan Telnet. Selain itu, router MikroTik mendukung SNMP (Simple Network Management Protocol) untuk pemantauan dan manajemen jaringan.

Perlu dicatat bahwa router MikroTik memiliki kurva pembelajaran yang tinggi, terutama bagi pengguna yang belum familiar dengan konsep jaringan. Namun, mereka menawarkan solusi yang kuat dan fleksibel untuk mengelola infrastruktur jaringan. Jika Anda baru mengenal router MikroTik, disarankan untuk merujuk pada dokumentasi mereka, forum, atau mencari bantuan dari administrator jaringan berpengalaman agar dapat memanfaatkan fitur-fitur yang

2.4. PPPOE

Menurut Ongkowinoto (2021), PPPoE (Point to Point Protocol over Ethernet) adalah salah satu protokol jaringan yang sering digunakan untuk membuat koneksi antara komputer dan *server*. Salah satu keunggulan teknologi atau metode PPPoE adalah meningkatkan keamanan akses internet dengan penggunaan username dan password yang unik untuk mengatur batasan kecepatan dan melakukan filter

terhadap lalu lintas internet. Selain itu, PPPoE juga menyediakan fitur-fitur dasar seperti autentikasi, enkripsi, dan kompresi data. Oleh karena itu, PPPoE menjadi salah satu pilihan utama dalam mengelola koneksi internet, memungkinkan penyedia layanan internet untuk menawarkan berbagai jenis layanan yang berbeda.

Selain itu, PPPoE juga berguna untuk mencegah serangan dari komputer lain yang berada dalam satu router. Tanpa menggunakan PPPoE, perangkat lain dapat dengan mudah mengidentifikasi alamat MAC dan IP dari perangkat tersebut. Namun, dengan menggunakan PPPoE, baik alamat MAC maupun IP tidak terlihat karena otentikasi dilakukan melalui penggunaan username dan password.[5]

Protokol Point-to-Point over Ethernet (PPPoE) digunakan untuk mengenkapsulasi frame PPP ke dalam frame Ethernet. Pada masa pergantian abad, saat DSL menjadi populer sebagai solusi untuk mengirimkan paket melalui koneksi DSL ke jaringan IP ISP dan ke seluruh internet, PPPoE menjadi protokol yang umum digunakan. Dalam bukunya berjudul "Cisco IOS in a Nutshell", James Boney mencatat bahwa kebanyakan penyedia DSL menggunakan PPPoE untuk menyediakan otentikasi, enkripsi, dan kompresi. Penggunaan PPPoE secara umum memanfaatkan fasilitas PPP untuk mengotentikasi pengguna melalui username dan password, terutama melalui protokol Password Authentication Protocol (PAP).

2.5. Firwall

Firewall adalah perangkat keamanan atau aplikasi perangkat lunak yang berfungsi sebagai penghalang antara jaringan komputer dan dunia eksternal, seperti internet. Fungsinya utama adalah memantau dan mengendalikan lalu lintas jaringan masuk dan keluar berdasarkan aturan keamanan yang telah ditentukan.

Firewall dirancang untuk mencegah akses yang tidak sah ke jaringan pribadi maupun dari jaringan pribadi ke dunia luar, sambil memungkinkan komunikasi yang diizinkan. Hal ini dicapai dengan memeriksa setiap paket data yang mencoba melewati firewall dan membuat keputusan apakah memperbolehkan atau memblokir lalu lintas berdasarkan aturan yang dikonfigurasi.

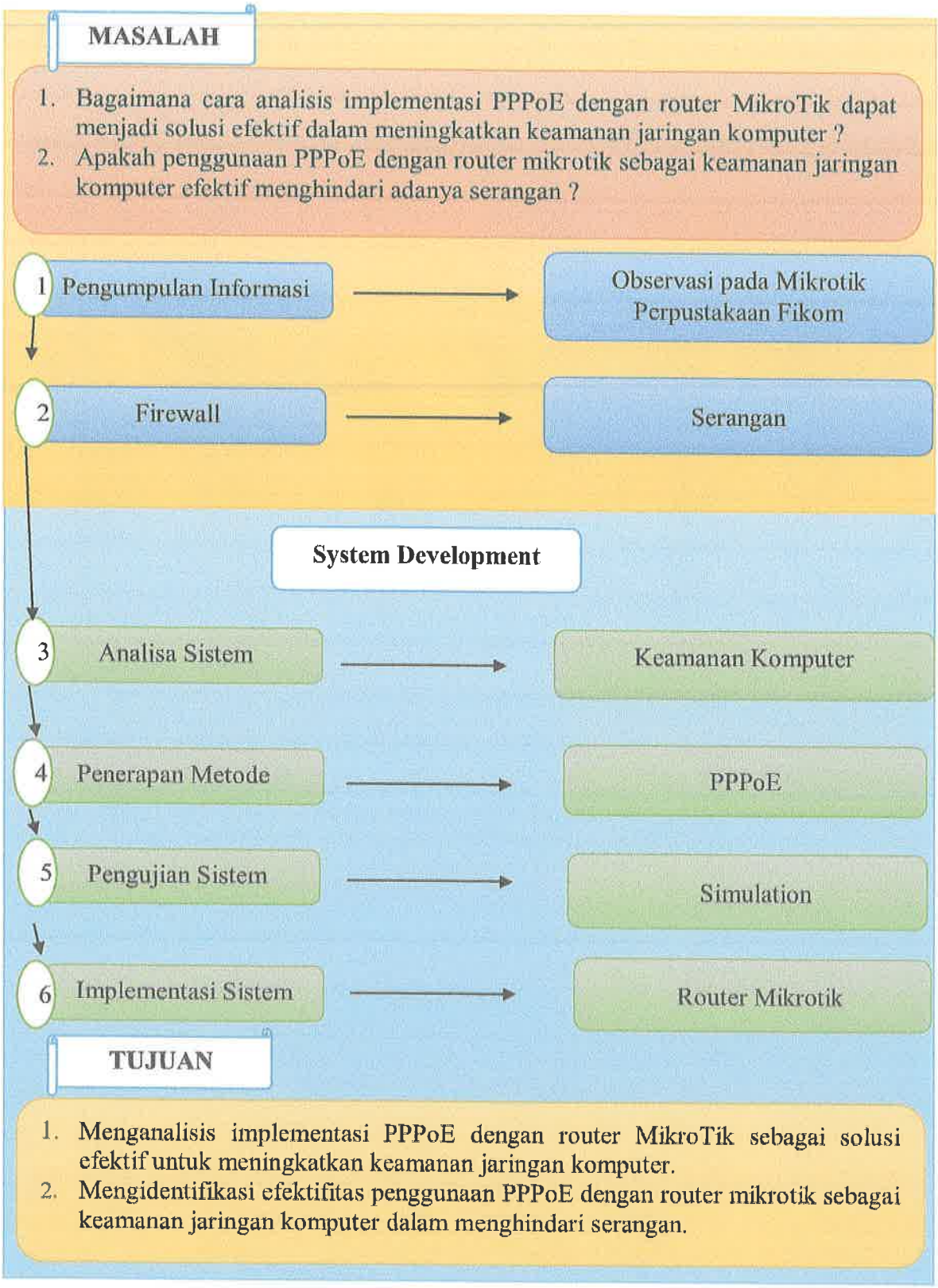
Firewall dapat diimplementasikan dengan berbagai cara, termasuk sebagai perangkat keras, program perangkat lunak yang berjalan pada komputer individu atau perangkat jaringan, atau kombinasi keduanya. Mereka dapat beroperasi pada berbagai lapisan jaringan, seperti lapisan jaringan (misalnya firewall penyaring paket) atau lapisan aplikasi (misalnya firewall proxy).

Fitur dan manfaat utama dari firewall meliputi:

1. Keamanan jaringan: Firewall memberikan lapisan pertahanan penting terhadap akses yang tidak sah dan ancaman siber dengan memantau dan menyaring lalu lintas jaringan.
2. Kontrol akses: Mereka memungkinkan organisasi untuk memberlakukan kebijakan akses dengan mengizinkan atau menolak jenis lalu lintas jaringan tertentu berdasarkan aturan yang telah ditentukan sebelumnya.
3. Pencegahan intrusi: Firewall dapat mendeteksi dan memblokir aktivitas yang mencurigakan atau berbahaya, seperti upaya peretasan, malware, atau transfer data yang tidak sah.
4. Dukungan VPN: Banyak firewall mendukung koneksi Virtual Private Network (VPN), yang memungkinkan akses jarak jauh yang aman ke jaringan pribadi melalui internet.
5. Pencatatan dan audit: Firewall sering menyimpan log lalu lintas jaringan, yang dapat digunakan untuk pemecahan masalah, analisis forensik, dan tujuan kepatuhan.
6. Segmentasi jaringan: Dengan membagi jaringan menjadi zona keamanan terpisah menggunakan firewall, organisasi dapat meningkatkan keamanan dengan mengisolasi sistem atau layanan yang sensitif dari jaringan lainnya.

Penting untuk dicatat bahwa firewall hanyalah salah satu komponen dari strategi keamanan jaringan yang komprehensif. Mereka bekerja bersama dengan langkah-langkah keamanan lainnya seperti perangkat lunak antivirus, sistem deteksi intrusi (IDS), dan pembaruan keamanan reguler untuk melindungi jaringan dan sistem dari ancaman.

2.6. Kerangka Pemikiran



Gambar 2.1 Kerangka Pikir

BAB III
METODOLOGI PENELITIAN

3.1. Jenis, Metode, Subjek, Objek, Waktu, dan Lokasi Penelitian

Penelitian ini menggunakan metode penelitian studi kasus. Dengan demikian jenis penelitian ini adalah penelitian deskriptif.

Berdasarkan latar belakang dan kerangka pemikiran seperti yang telah diuraikan diatas maka yang menjadi objek penelitian adalah analisis implementasi PPPoE dengan router MikroTik. Penelitian ini dimulai dari 01 Agustus 2023 s/d November 2023 yang berlokasi Di Universitas Ichsan Gorontalo

3.2. Pengumpulan Data

3.2.1. Data primer

Data Primer Yaitu data yang diperoleh Dengan Metode Wawancara dengan staf admin dan Observasi Langsung Pada Router Mikrotik Di Universitas Ichsan Gorontalo.

3.2.2. Data Sekunder

Data Sekunder yaitu Data diperoleh dengan cara mengumpulkan data atau keterangan melalui berbagai macam referensi seperti hasil penelitian terdahulu, buku teks, jurnal yang terkait dari internet yang berhubungan dengan mikrotik.

3.3. Pengembangan Sistem

Prosedur atau langkah-langkah pokok dalam menerapkan analisis implementasi PPPoE dengan router MikroTik pada mikrotik dan tools monitoring sistem, yang selanjutnya dilakukan simulasi untuk menguji kinerja sistemnya.

3.4. Desain Sistem

Desain sistem menggunakan pendekatan topologi dalam hal menentukan rule pada firewall.

Architecture Design, dalam bentuk :

- Topologi Jaringan

- Spesifikasi *hardwere* dan *software* yang direkomendasikan adalah:

1. Sistem Operasi : Windows 10
2. Prosesor Dengan Kecepatan Minimal 1,6GHz
3. Memori :1 GB
4. Harddisk free space 3GB
5. RAM: 2 GB

3.5. Rancangan Sistem

Gambar 3. 1 perancangan sistem

3.6. Konstruksi Sistem

Pada tahap ini dilakukan analisis implementasi PPPoE dengan router MikroTik di router mikrotik dan dan tools monitoring system di kampus Unisan Gorontalo. untuk menguji kinerja sistem menggunakan simulasi langsung pada router mikrotik dan tools monitoring sistem. Pada tahap ini penulis melakukan tahap perancangan sistem dan desain sistem sebelumnya..

3.7. Pengujian Sistem

Pada pengujian ini penulis menggunakan konsep hacking yaitu melakukan simulasi analisis implementasi PPPoE dengan router MikroTik router mikrotik dengan bantuan tools monitoring sistem untuk melihat hasil analisis kualitas bandwith.

BAB IV
HASIL PENLITIAN

4.1. Analisa dan implementasi sistem

Hasil dari penelitian ini bahwa peneliti membutuhkan beberapa perangka lunak dan perangkat keras untuk di analisa dan di implementasikan berdasarkan data yang diperoleh yang telah di olah oleh peneliti.

Analisis sistem adalah tahap awal dalam pengembangan perangkat lunak di mana tim pengembang berusaha untuk memahami secara menyeluruh kebutuhan sistem yang akan dibangun. Proses ini melibatkan pengumpulan, analisis, dan spesifikasi kebutuhan secara rinci agar dapat menghasilkan desain yang sesuai dengan kebutuhan pengguna dan tujuan bisnis perusahaan

4.1.1. Analisis kebutuhan sistem

langkah awal yang dilakukan adalah menganalisis kebutuhan terkait perangkat keras dan perangkat lunak yang akan digunakan dalam penelitian. Dalam tahap ini, fokus diberikan pada pemahaman yang mendalam tentang spesifikasi perangkat keras yang diperlukan, seperti komputer atau server, serta perangkat lunak yang dibutuhkan untuk mengimplementasikan metode penyaringan. Analisis ini bertujuan untuk memastikan bahwa semua aspek teknis yang diperlukan tersedia dan dapat mendukung efektifitas dari proses konfigurasi dan penerapan metode yang akan dilakukan.:

Tabel 4. 1 Kebutuhan Perangkat Keras

NO	NAMA PERANGKAT	SPESIFIKASI
1	LAPTOP DELL	Intel(R) Core(TM) i7-6820HQ CPU @ 2.70GHz 2.71 GHZ 8GB RAM
2	MIKROTIK ROUTERBOARD	
3	ACCESS POINT	TOTO LINK
4	KABEL LAN	

5	KONEKTOR	RJ45

Tabel 4. 2 Kebutuhan Perangkat Lunak

NO	NAMA PERANGKAT	SPESIFKASI
1	WINBOX	WINBOX64

Beberapa software yang dibutukan terdiri dari:

1. Winbox adalah perangkat lunak yang dikembangkan oleh MikroTik untuk mengkonfigurasi perangkat MikroTik RouterOS melalui antarmuka grafis (GUI). Penggunaan GUI membuat konfigurasi jaringan menjadi lebih intuitif dan mudah dipahami, terutama bagi pengguna yang tidak terbiasa dengan perintah-perintah CLI (Command Line Interface).

Dan juga terdapat hardware yang dibutuhkan untuk simulasi jaringan yaitu:

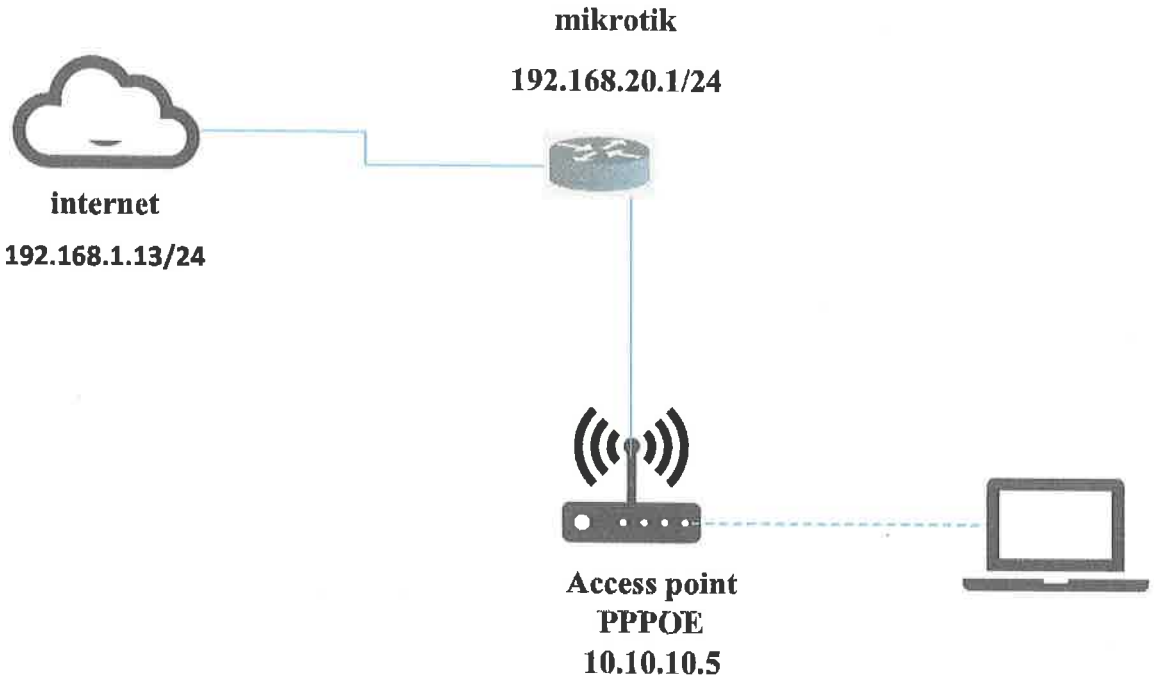
1. MikroTik wireless merupakan salah satu produk dari MikroTik yang fokus pada teknologi jaringan nirkabel atau wireless. Produk-produk ini mencakup perangkat keras (hardware) seperti router, access point, antenna, dan perangkat-perangkat lain yang mendukung konektivitas nirkabel dalam infrastruktur jaringan. Selain itu, MikroTik juga menyediakan perangkat lunak (software) yang mendukung konfigurasi dan manajemen jaringan nirkabel.
2. Laptop fungsinya dalam simulasi MikroTik yaitu dengan menggunakan laptop, pengguna dapat membuat topologi jaringan yang kompleks dalam simulasi MikroTik. Ini termasuk menghubungkan perangkat MikroTik secara virtual, menentukan jalur koneksi, dan mengatur skenario jaringan yang berbeda untuk diuji.
3. Router bertugas mentransmisikan paket data dari jaringan internet ke perangkat lain melalui proses routing, yaitu meneruskan paket data antar jaringan. Bisa

dibilang router berfungsi sebagai penghubung antara berbagai jaringan komputer.

4. Kabel LAN merupakan medium yang digunakan untuk menghubungkan perangkat-perangkat dalam sebuah jaringan lokal, seperti komputer, printer, dan perangkat jaringan lainnya. Jenis kabel ini umumnya digunakan dalam implementasi teknologi Ethernet, yang menjadi standar komunikasi data di dalam jaringan lokal. Kabel LAN tersedia dalam berbagai jenis, termasuk kabel tembaga dan serat optik, dan berfungsi untuk mentransfer data antara perangkat-perangkat dalam jarak terbatas, seperti di dalam gedung atau kantor.
5. Konektor RJ45 adalah elemen kunci dalam infrastruktur jaringan komputer yang umumnya digunakan untuk menghubungkan kabel jaringan ke perangkat seperti komputer, switch, router, atau perangkat jaringan lainnya. Dikenal karena keandalannya, konektor ini menjadi tulang punggung dalam implementasi jaringan Ethernet yang sering dipakai. Dengan desain yang mengintegrasikan delapan pin, konektor RJ45 memfasilitasi transfer data yang stabil dan aman di dalam jaringan, memastikan koneksi yang handal di lingkungan komputasi modern

4.1.2 perancangan topologi jaringan

Pada tahap perancangan ini, penulis dapat melakukan mendesain topologi jaringan dan alur kerja dari sistem dalam topologi yang dibangun yaitu tentang PPPOE



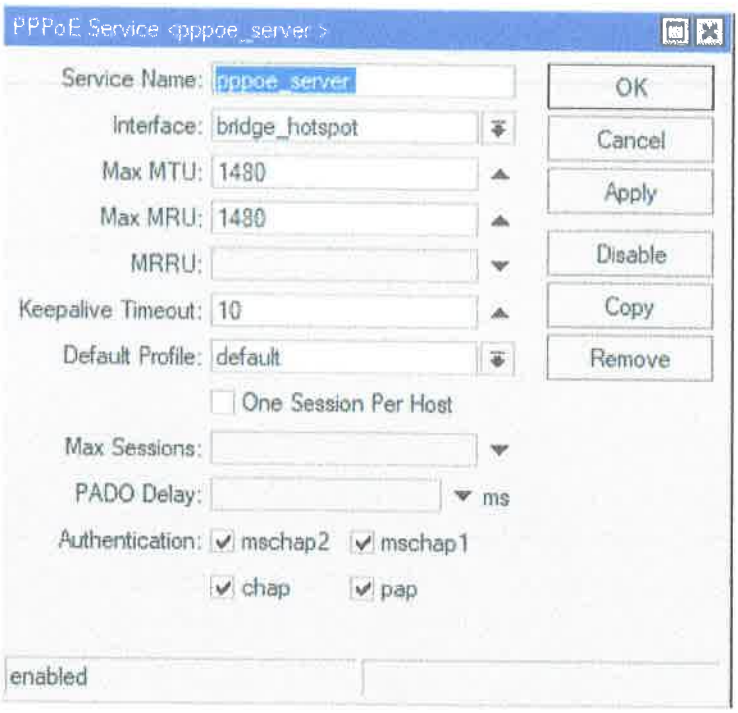
Gambar 4. 1 Topologi Jaringan

4.2. Implementasi PPPOE

Implementasi PPPOE adalah tahap menerapkan keamanan jaringan. Pada tahap ini, dilakukan konfigurasi dari sisi server dan client

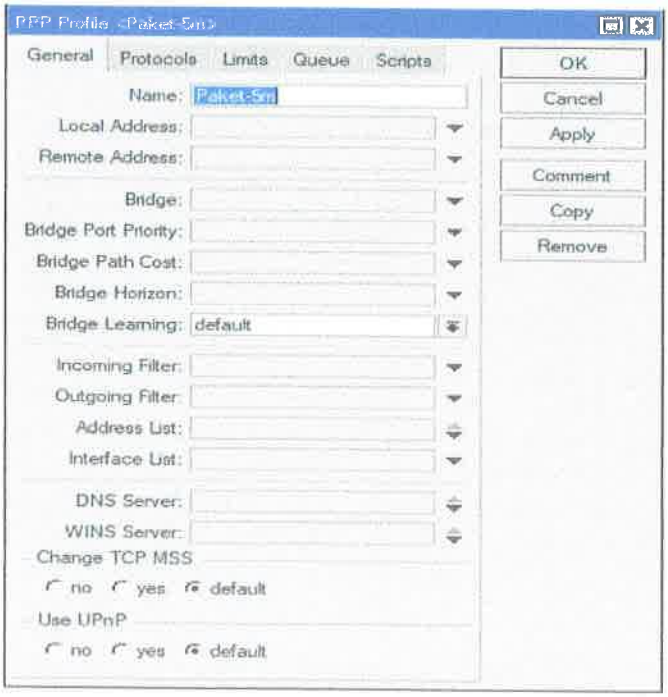
4.2.1. Perancangan seting-an PPPOE

Pada setting-an PPPoE Server ini, bridge interface dibuat sebelum membuat service PPPoE. Dengan membuat bridge, maka beberapa interface bisa digabungkan menjadi satu interface. Kemudian membuat service PPPOE server pada menu PPPoE Server. Service name diisi sesuai kebutuhan



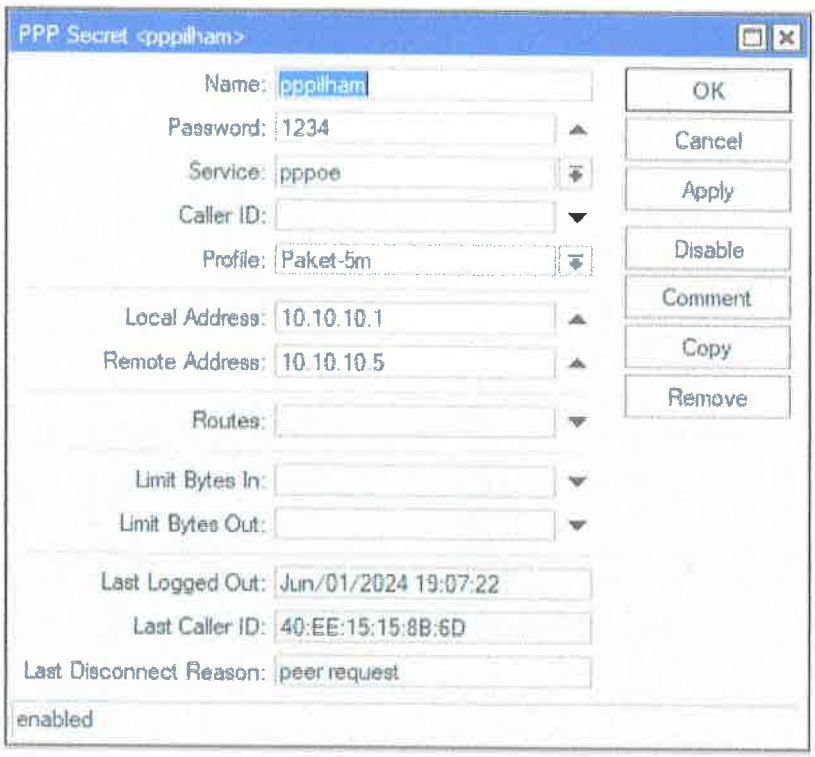
Gambar 4. 2 Konfigurasi PPPOE

Setelah itu pembuatan profile.



Gambar 4. 3 Profil PPPOE

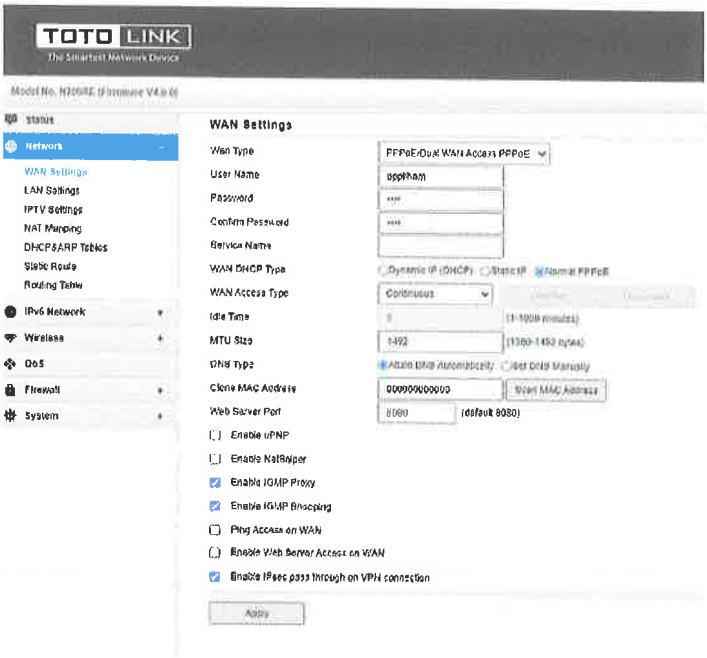
Setelah itu PPPoE akan memberikan IP secara otomatis, tetapi kinerjanya tidak seperti DHCP. Pemberian IP otomatis akan di setting dibagian secret. Di menu secret ini, bisa menentukan username dan password yang akan digunakan oleh client untuk bisa terkoneksi ke internet.



Gambar 4. 4 Secret PPPOE

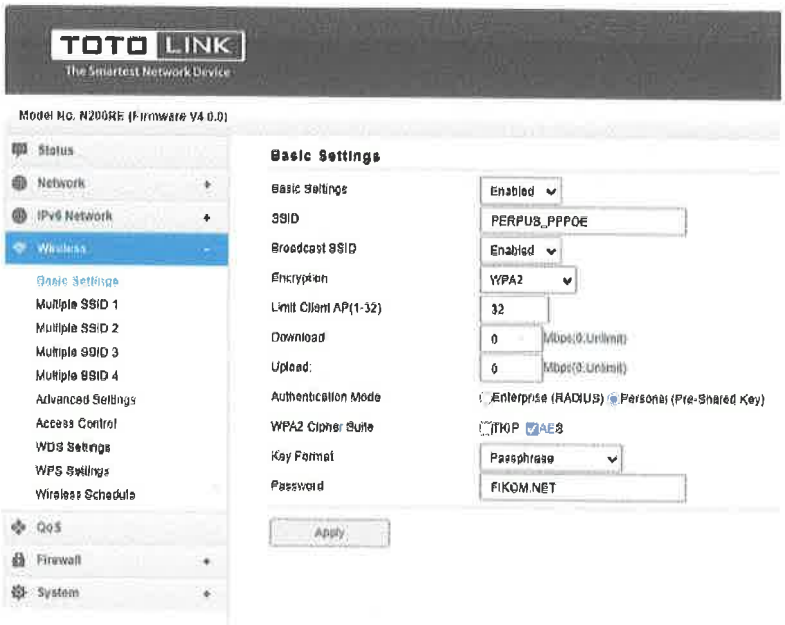
4.2.2. Perancangan seting-an access point

Pastikan juga untuk merujuk pada dokumentasi resmi dari produsen perangkat Anda karena langkah-langkah spesifik dapat bervariasi tergantung pada merek dan model access point yang Anda gunakan.



Gambar 4. 5 Konfigurasi Access Point

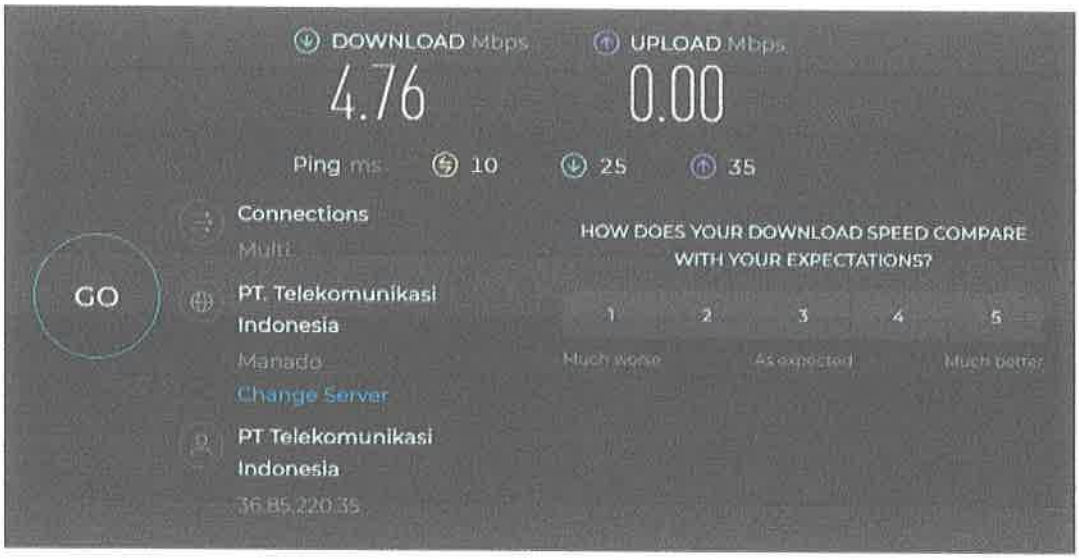
User name dan password sesuai yang ada pada mikrotik



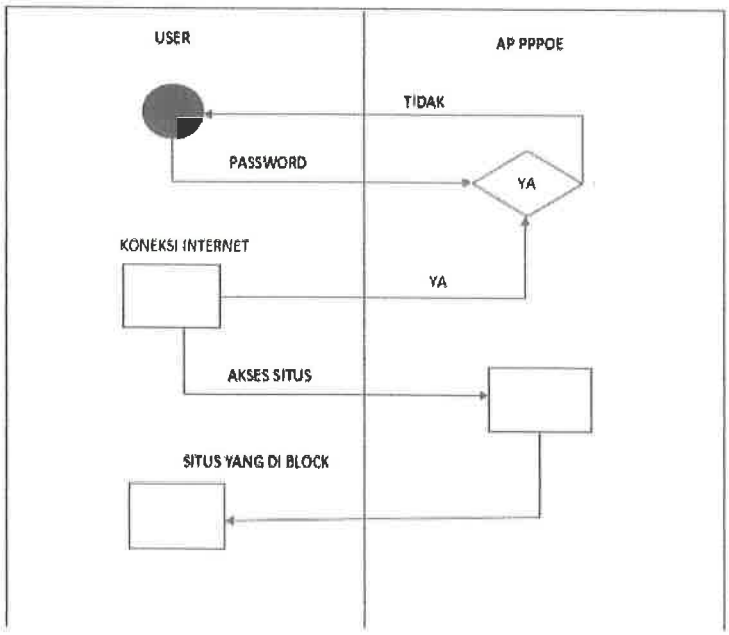
Gambar 4. 6 Konfigurasi Access Point

Pada wireless ssid di isi nama wifinya contohnya kayak pada di atas PERPUS_PPPOE Dan pada password di isi apa saja yang ingin di isi

Setelah membuat konfigurasi pppoe selesai kita akan melihat bandwith yang telah kita tentukan itu sama atau tidak dengan speedtest



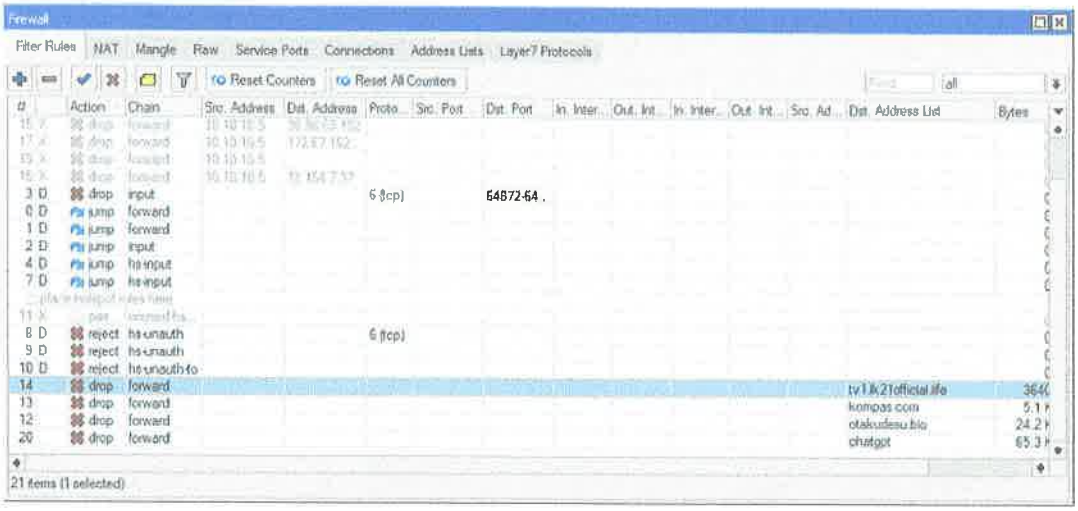
Gambar 4. 7 Spedtest



BAB V

PEMBAHASAN DAN HASIL

5.1. Perancangan seting-an mikrotik untuk keamamanan pembatasan akses situs – situs tertentu dalam perpustakaan



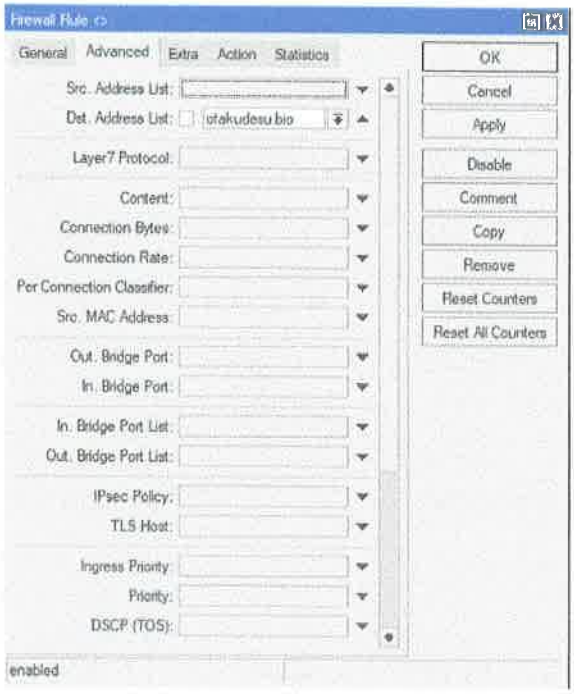
Gambar 5. 1 Tampilan Firewall

5.1.1. Perancagan sistem filters rules

Langkah awal yang harus dilakukan adalah masuk ke mikrotik yang akan di gunakan untuk pengamnannya terus masuk ke menu IP pada menu IP bayak pilihan yang bisa di pilih tapi karena sekarang membahas pengaman situ jadi masuk ke firewall

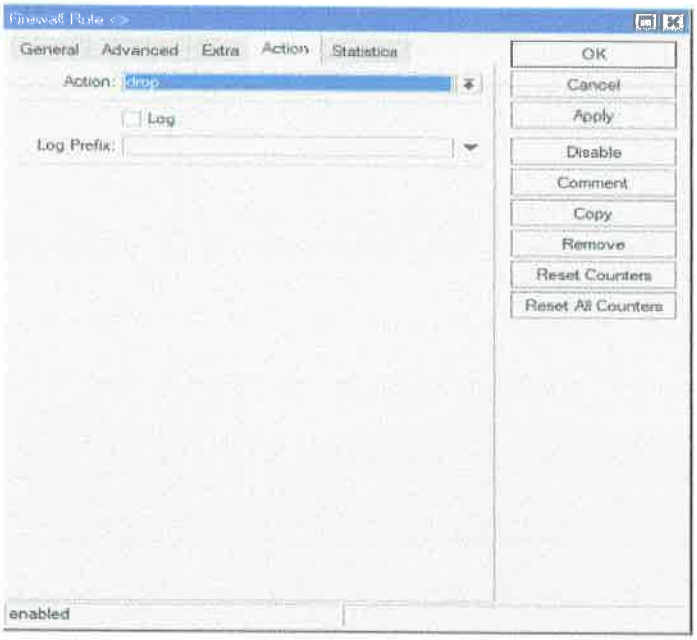
Gambar 5. 2 Menu General

Langkah ke dua pilih menu filter ruls terus pilih icon tambah dalam membuat sesuatu yang di inginkan harus menambahkan dulu sesuatu yang akan membantu pembatasan situs pada menu general pada chain harus memilih forward karena data yang akan di gunakan adalah data yang melewati routernya karena sistus yang akan kita batasi situ yang akan menggunakan wifi pada perpustakaan



Gambar 5. 3 Menu Advanced

Pada menu advanced pilih dst.address list yaitu IP tujuan yang akan di block misalnya Situs otakudesu.bio

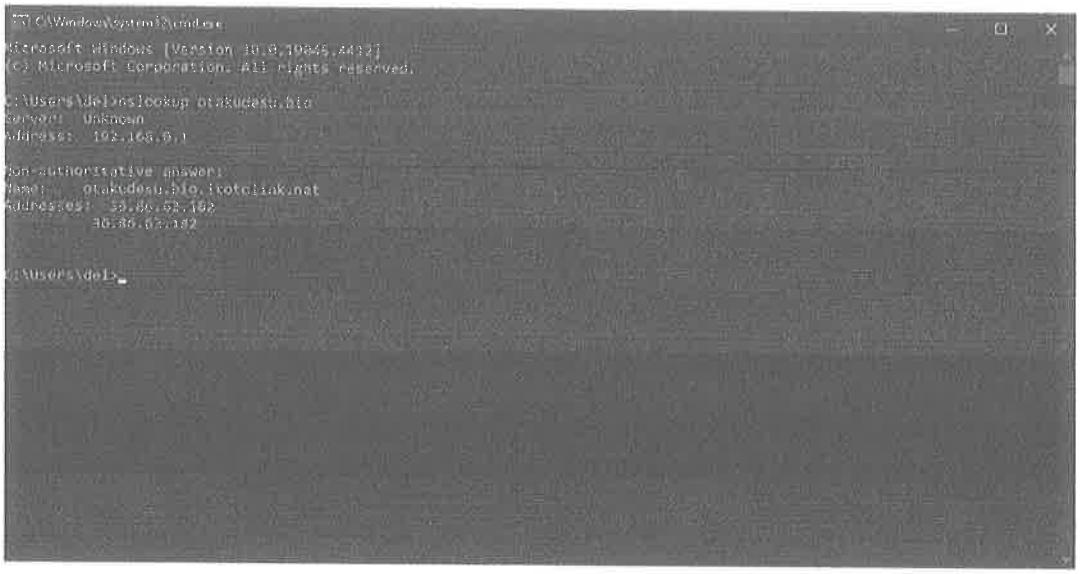


Gambar 5. 4 Menu Action

Setelah itu pada menu action pilih drop fungsinya agar domain yang mengunakan ip tadi tidak bisa mengaksess situs tersebut

5.1.2. Pencarian IP addres pada CMD

Setelah selesai menambahkan filer rule pada menu filter rules lihat IP situs yang akan kita batasi pada command prompt atau biasa di sebut cmd dengan cara nslookup misalnya situs yang akan di batasi otakudesu.bio jadi nslookup otakudesu.bio setingannya seperti berikut

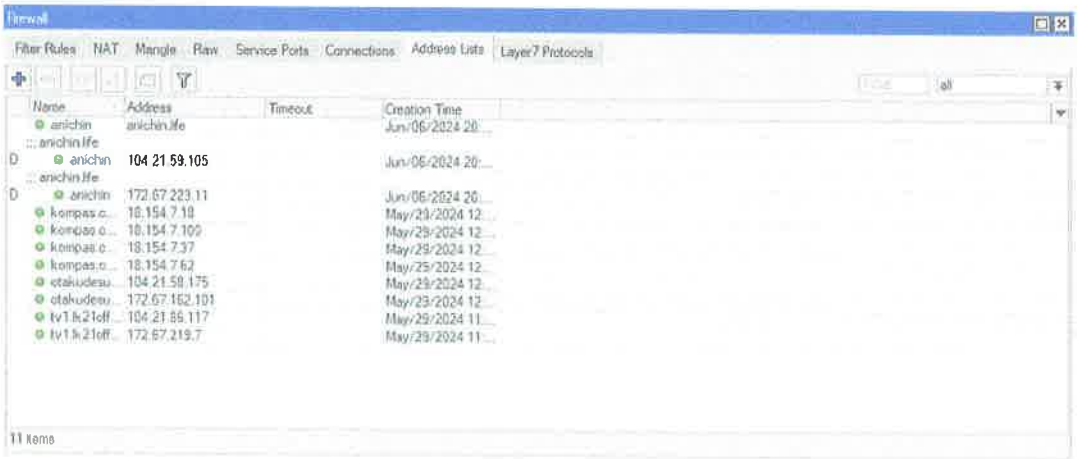


Gambar 5. 5 CMD Nslookup

Nah IP yang ada pada cmd itu yang akan di isi pada adrress list

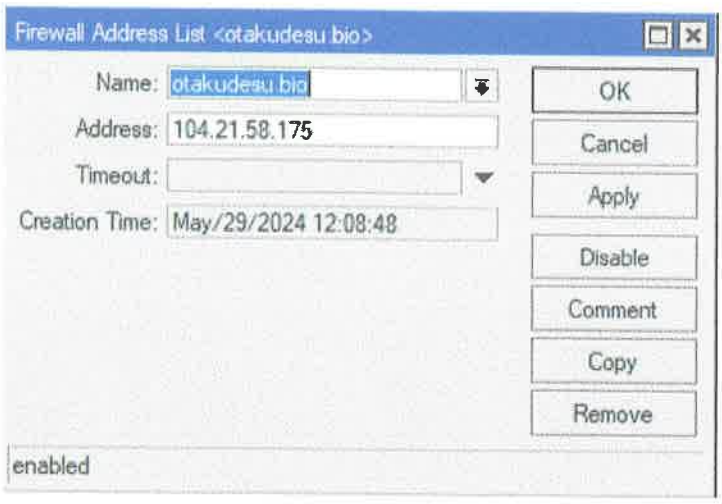
5.1.3. Perancangan sistem keamanan address list

membuat daftar alamat IP yang berfungsi sebagai kontrol akses atau untuk keperluan lain dalam konfigurasi jaringan. Anda dapat menambahkan alamat IP tunggal atau rentang alamat IP ke dalam daftar ini. Kemudian, daftar ini bisa digunakan dalam berbagai aturan firewall, NAT, atau konfigurasi routing untuk mengontrol lalu lintas jaringan, memungkinkan atau memblokir akses ke atau dari alamat IP tertentu. Dengan menggunakan Address List, Anda dapat mengelola lalu lintas jaringan dengan lebih efisien dan secara terpusat dalam router MikroTik



Gambar 5. 6 Menu Address List

Setelah memperoleh IP pada cmd masuk pada menu firewall masuk lagi pada menu address list



Gambar 5. 7 Address List

Tambahkan name dan address pada menu address list seperti nama otakudesu.bio

Terus pada address ip yang telah kita dapatan pada cmd sebanyak yang di perlihatkan pada cmd maka telah selesai pembatasan situs yang di inginkan

5.2. Hasil tampilan perancangan sistem keamanan yang sudah di block atau di batasi pada browser atau chrome

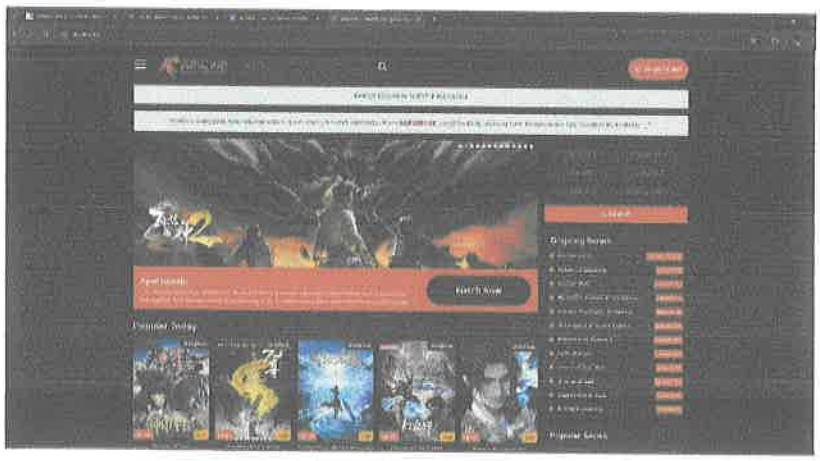
5.2.1. Hasil tampilan chrome situs yang sebelum dan sudah di block

Untuk yang sebelum tampilanya masih dapat di akses 3 situs ini

- Situs otakudesu.bio

- Situs kompas.com

- Situs anicin.life



Gambar 5. 8 Tampilan Situs yang Belum di Block

Untuk yang sudah di block tidak dapat lagi di akses atau situs ini tidak dapat di akses

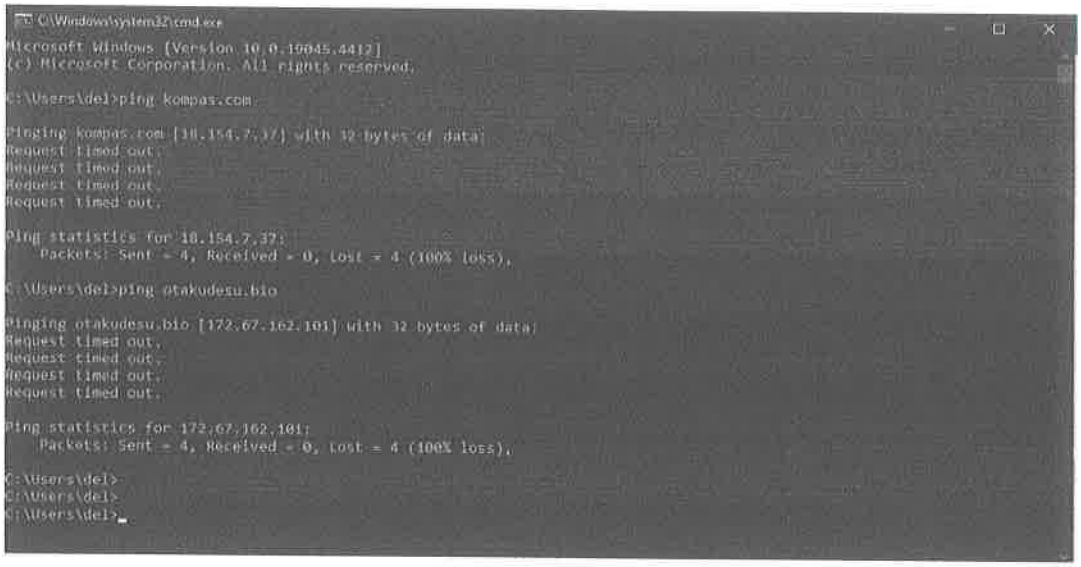
- situs kompas.com

Gambar 5. 9 tampilan situs yang telah di Block

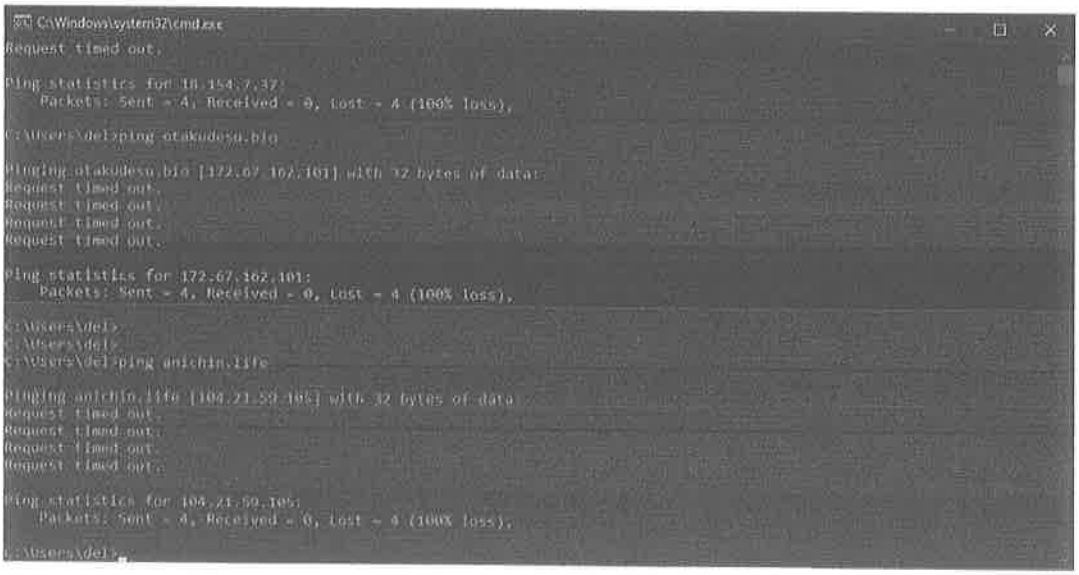
- situs otakudesu.b

5.3. hasil tampilan kemanan situs yang telah di bock pada CMD

hasil tampilan situs yang telah di block pada cmd yaitu hanya dengan mengetik test ping situs yang ingin kamu tes misalnya 'ping anichin.life'



Gambar 5. 10 Tampilan Block Pada CMD



BAB VI
PENUTUP

6.1. Kesimpulan

Penelitian ini bertujuan untuk merancang sistem keamanan pada perpustakaan dengan membatasi akses ke situs-situs tertentu menggunakan perangkat MikroTik. Metode yang digunakan meliputi perancangan sistem filter rules, pencarian IP address melalui CMD, dan perancangan sistem keamanan address list.

Langkah pertama adalah merancang filter rules pada MikroTik dengan memilih menu IP > Firewall > Filter Rules. Dalam filter rules, ditambahkan aturan untuk memblokir akses ke situs-situs tertentu dengan mengidentifikasi IP tujuan dan mengatur aksi drop.

Kemudian, dilakukan pencarian IP address situs yang akan dibatasi menggunakan CMD dengan perintah nslookup. IP address yang diperoleh kemudian diisi ke dalam address list pada MikroTik untuk mengelola akses tersebut.

Hasil tampilan dari perancangan sistem keamanan ini menunjukkan bahwa situs-situs yang telah dibatasi aksesnya tidak dapat diakses melalui browser, seperti contoh situs otakudesu.bio dan kompas.com.

Selain itu, hasil pengujian juga menunjukkan bahwa akses ke situs-situs yang telah dibatasi juga terblokir ketika diuji melalui CMD dengan perintah ping.

Kesimpulannya, penelitian ini berhasil merancang sistem keamanan pada perpustakaan dengan efektif membatasi akses ke situs-situs tertentu menggunakan perangkat MikroTik, sehingga dapat meningkatkan pengawasan dan kontrol terhadap penggunaan internet di lingkungan perpustakaan.

6.2. Saran

Setelah melakukan penelitia analisis implementasi PPPOE pada router mikrotik sebagai security jaringan komputer ada beberapa saran yan perlu di perhatikan untuk mencapai tujuan yang di harapkan yaitu sebagai berikut :

1. Tinjau kembali metode yang digunakan dalam penelitian . Pastikan bahwa proses perancangan sistem keamanan dan pengujian dilakukan secara teliti dan sistematis untuk mendapatkan hasil yang lebih akurat.
2. Dari pada mengetik manual dan harus mencari cari ip pada cmd lebih baik pada menu address list untuk name nya di isi nama singkat situsnya yang akan di block misalnya anchin pada namenya terus pada addressnya di isi full name situsnya misalnya anichin.life nanti IP situsnya akan muncul dengan otomatis semua muncul ip yang ada pada situs tersebut

DAFTAR PUSTAKA

Djusmin, V. B. (Juni 2015). *HOTSPOT* BERBASIS KONEKSI PPPoE (POINT TO POINT PROTCOL OVER ETHERNET) DENGAN OTENTIKASI USER MANAGER MIKROTIK PADA WARNET STARCOM . *Jurnal Ilmiah d'ComPutarE Volume 5.*

Djusmin, V. B. (JUNI 2015). *HOTSPOT* BERBASIS KONEKSI PPPoE (POINT TO POINT PROTCOL OVER ETHERNET) DENGAN OTENTIKASI USERMANAGER MIKROTIK PADA WARNET. *Jurnal Ilmiah d'ComPutarE Volume 5.*

fasehan, B. (2021). RANCANG BANGUN SISTEM KEAMANAN JARINGAN KOMPUTER MENGGUNAKAN FIREWALL FILTER PADA LABORATORIUM JURUSAN TEKNIK KOMPUTER .

Joefrie, Y. Y. (September 2013). PERANCANGAN PROGRAM SIMULASI PERINTAH DASAR JARINGAN KOMPUTER. *Jurnal Ilmiah Foristek Vol.3, No.2.*

Langobelen, E. S. (Desember 2019). ANALISIS DAN OPTIMASI DARI SIMULASI KEAMANAN JARINGAN MENGGUNAKAN. *Jurnal JARKOM Vol. 7 No. 2.*

Nursobah, p. a. (Januari 2023). IMPLEMENTASI JARINGAN PPPOE DAN *HOTSPOT SERVER* RT/RW NET BERBASIS MIKROTIK DENGAN FITUR MIKHMON DI ADINET SAMARINDA SEBERANG. *Jurnal INFORMATIKA, Vol.13 No.1,* .

Putra, R. R. (Agustus 2015). ANALISA QOS VPN PPPOE PADA JARINGAN *BACKBONE WIRELESS* MPLS QOS ANALYSYS OF PPPOE VPN FOR WIRELESS MPLS BACKBONE NETWORK. *e-Proceeding of Engineering : Vol.2, No.2.*

Stallings, W. (2017). *CRYPTOGRAPHY AND NETWORK SECURITY PRINCIPLES AND PRACTICE SEVENTH EDITION GLOBAL EDITION.* edinburgh: British Library Cataloguing-in-Publication Data.

sumardi, S., & zaen, m. t. (april 2018). PERANCANGAN JARINGAN KOMPUTERBERBASIS MIKROTIK ROUTER OS PADA SMAN 4 PRAYA. *JIRE (Jurnal Informatika & Rekayasa Elektronika) vol 1 no 1* .

Supendar, H. (Juni 2016). Implementasi Remote Site Pada Virtual Private Network Berbasis Mikrotik. *BINA INSANI ICT JOURNAL, Vol. 3, No.1.*

Mutaqin, A. F. ((2016)). Rancang Bangun Sistem Monitoring Keamanan Jaringan Prodi Teknik Informatika Melalui SMS Alert dengan Snort. *Jurnal Sistem dan Teknologi Informasi (JUSTIN) Vol. 1, No. 1,*.

Arif Adi Tama, F., & Panjaitan, F. (2019). Analisis Keamanan Jaringan Pada Fasilitas Internet (Wifi) Terhadap Serangan Packet Sniffing Di Kementrian Agama Provinsi Sumsel. 3, 1–5.

Megis,Jenis. 2009."Mikrotik RouterOS QoS Best Practice"

. http://mum.mikrotik.com/presentations/US09/megis_qos.pdf. Diakses pada tanggal 8 Maret 2012 pada pukul 12.30 WIB.

Noviyanto, Hendri. 2012. ANALISIS KEAMANAN WIRELESS DI UNIVERSITAS MUHAMMADIYAH SURAKARTA. Skripsi. Surakarta: FKI UMS.

JADWAL PENELITIAN

KEGIATAN	WAKTU (Tahun dan Bulan)															
	2023															
	September				Oktober				November				Desember			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Pra Penelitian																
Proposal																
Evaluasi																
Analisis Sistem																
Desain Sistem																
Konstruksi Sitem																
Pengujian Sistem																
Pembahasan																
Penyusunan Laporan Penelitian																

KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET, DAN TEKNOLOGI
UNIVERSITAS ICHSAN GORONTALO
LEMBAGA PENELITIAN
Kampus Unisan Gorontalo Lt.3 - Jln. Achmad Nadjamuddin No. 17 Kota Gorontalo
Telp: (0435) 8724466, 829975 E-Mail: lembagapenelitian@unisan.ac.id

Nomor : 5011/PIP/LEMLIT-UNISAN/GTO/I/2024
Lampiran : -
Hal : Permohonan Izin Penelitian

Kepada Yth.
Dekan Fakultas Ilmu Komputer Universitas Ichsan Gorontalo
di,-
Tempat

Yang bertanda tangan di bawah ini :

Nama	:	Dr. Rahmisyari, ST.,SE.,MM
NIDN	:	0929117202
Jabatan	:	Ketua Lembaga Penelitian

Meminta kesediannya untuk memberikan izin pengambilan data dalam rangka penyusunan **Proposal / Skripsi**, kepada :

Nama Mahasiswa	:	Muhammad Nur Ilham
NIM	:	T3120022
Fakultas	:	Fakultas Ilmu Komputer
Program Studi	:	Teknik Informatika
Lokasi Penelitian	:	FAKULTAS ILMU KOMPUTER UNIVERSITAS ICHSAN GORONTALO
Judul Penelitian	:	ANALISIS IMPLEMENTASI PPPOE DENGAN ROUTER MIKROTIK SEBAGAI SECURITY JARINGAN KOMPUTER (STUDI KASUS FAKULTAS ILMU KOMPUTER UNIVERSITAS ICHSAN GORONTALO)

Atas kebijakan dan kerja samanya diucapkan banyak terima kasih.

Gorontalo, 22 Januari 2024
Ketua,

Dr. Rahmisyari, ST.,SE.,MM
NIDN 0929117202

turnitin

Similarity Report ID: oid:25211:61182240

PAPER NAME

SKRIPSI_T3120022_MUHAMMAD_NUR_ILHAM.pdf

AUTHOR

MUHAMMAD NUR ILHAM muhilham2407@gmail.com

WORD COUNT

6525 Words

CHARACTER COUNT

46404 Characters

PAGE COUNT

50 Pages

FILE SIZE

1.4MB

SUBMISSION DATE

Jun 11, 2024 11:06 AM GMT+8

REPORT DATE

Jun 11, 2024 11:06 AM GMT+8

20% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

- 20% Internet database
- 1% Publications database
- Crossref database
- Crossref Posted Content database
- 3% Submitted Works database

Excluded from Similarity Report

- Bibliographic material
- Quoted material
- Cited material
- Small Matches (Less then 30 words)

KEMENTERIAN PENDIDIKAN, KEBUDAYAAN,RISET, DAN TEKNOLOGI
UNIVERSITAS ICHSAN GORONTALO
FAKULTAS ILMU KOMPUTER
SURAT KEPUTUSAN MENDIKNAS RI NOMOR 84/D/O/2001
Jl. Achmad Nadjamuddin No. 17 Telp (0435) 829975 Fax (0435) 829976 Gorontalo

SURAT KETERANGAN PENELITIAN

Nomor : 113 /FIKOM-UIG/SKP/V/2024

Yang bertanda tangan dibawah ini :

Nama	: Irvan Abraham Salihi, M. Kom
Jabatan	: Dekan Fakultas Ilmu Komputer

Dengan ini Menerangkan bahwa :

Nama Mahasiswa	: Muhammad Nur Ilham
NIM	: T3120022
Program Studi	: Teknik Informatika

Bahwa yang bersangkutan benar-benar telah melakukan penelitian tentang "**Analisis Implementasi PPPOE dengan Router Mikrotik Sebagai Security Jaringan Komputer (Studi Kasus Fakultas Ilmu Komputer Universitas Ichsan Gorontalo)** " Guna untuk meyelesaikan Studi pada Program Studi Teknik Informatika Fakultas Ilmu Komputer, dan bersangkutan telah menyelesaikan penelitian Tersebut pada **TGL 06 Mei 2024** sesuai dengan waktu yang telah di tentukan.

Demikian Surat Keterangan ini dibuat dan digunakan untuk seperlunya.

Gorontalo, 06 Mei 2024
Dekan,

Irvan A. Salihi, S.Kom., M.Kom
NIDN : 0928028101

KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET, DAN TEKNOLOGI
UNIVERSITAS ICHSAN GORONTALO
FAKULTAS ILMU KOMPUTER
SURAT KEPUTUSAN MENDIKNAS RI NOMOR 84/D/O/2001
Jl. Achmad Najamuddin No. 17 Telp. (0435) 829975 Fax (0435) 829976 Gorontalo

SURAT REKOMENDASI BEBAS PLAGIASI
No. 144/FIKOM-UIG/R/VI/2024

Yang bertanda tangan di bawah ini :

Nama	: Irvan Abraham Salihi, M.Kom
NIDN	: 0928028101
Jabatan	: Dekan Fakultas Ilmu Komputer

Dengan ini menerangkan bahwa :

Nama Mahasiswa	:	Muhammad Nur Ilham
NIM	:	T3120022
Program Studi	:	Teknik Informatika (S1)
Fakultas	:	Fakultas Ilmu Komputer
Judul Skripsi	:	Analisis Implementasi PPPOE Dengan Router Mikrotik Sebagai Security Jaringan Komputer

Sesuai hasil pengecekan tingkat kemiripan skripsi melalui aplikasi **Turnitin** untuk judul skripsi di atas diperoleh hasil *Similarity* sebesar **20%**, berdasarkan Peraturan Rektor No. 32 Tahun 2019 tentang Pendeteksian Plagiat pada Setiap Karya Ilmiah di Lingkungan Universitas Ichsan Gorontalo dan persyaratan pemberian surat rekomendasi verifikasi calon wisudawan dari LLDIKTI Wil. XVI, bahwa batas kemiripan skripsi maksimal 30%, untuk itu skripsi tersebut di atas dinyatakan **BEBAS PLAGIASI** dan layak untuk diujiankan.

Demikian surat rekomendasi ini dibuat untuk digunakan sebagaimana mestinya.

Gorontalo, 13 Juni 2024
Tim Verifikasi,

Mengetahui
Dekan,

Irvan Abraham Salihi, M.Kom
NIDN. 0928028101

Zulfrianto Y. Lamasigi, M.Kom
NIDN. 0914089101

Terlampir :
Hasil Pengecekan Turnitin

KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET, DAN TEKNOLOGI
UNIVERSITAS ICHSAN GORONTALO
FAKULTAS ILMU KOMPUTER
UPT. PERPUSTAKAAN FAKULTAS
SK. MENDIKNAS RI NO. 84/D/0/2001
Jl. Achmad Nadjamuddin No.17 Telp(0435) 829975 Fax. (0435) 829976 Gorontalo

SURAT KETERANGAN BEBAS PUSTAKA

No : 019/Perpustakaan-Fikom/VI/2024

Perpustakaan Fakultas Ilmu Komputer (FIKOM) Universitas Ichsan Gorontalo dengan ini menerangkan bahwa :

Nama Anggota	:	Muhammad Nur Ilham
No. Induk	:	T3120022
No. Anggota	:	M202439

Terhitung mulai hari, tanggal : Senin, 10 Juni 2024, dinyatakan telah bebas pinjam buku dan koleksi perpustakaan lainnya.

Demikian keterangan ini di buat untuk di pergunakan sebagaimana mestinya.

Gorontalo, 10 Juni 2024
Mengetahui,
Kepala Perpustakaan

Apriyanto Alhamad, M.Kom
NIDN : 0924048601

Daftar Riwayat Hidup

Nama	: muhammad nur ilham
Nim	: T3120022
Ttl	: Gorontalo, 24 Juli 2000
Alamat	: Jl. Rambutan buladu
Agama	: Islam
Warga	: Indonesia
Gmail	: muhilham2407@gmail.com

Nama Orang Tuan

Ayah : Ardasi djafar (almarhum)

Ibu : Nur Ain K. Bakrie