IMPLEMENTASI FIREWALL BERBASIS MIKROTIK UNTUK INTERNET SEHAT PADA JARINGAN POLITEKNIK GORONTALO

Nursetiawati[1], Salman Suleman[2]*
[1,2]Politeknik Gorontalo
Coresponding: tia@poligon.ac.id*
Submitted: 10-01-2025; Accepted: 31-01-2025; Published: 31-01-2025

ABSTRACT

The rapid development of information technology, especially in terms of data accessibility via the internet, has become the main driver for progress in various fields of politics, health, economics and education. However, internet use also has negative impacts such as access to inappropriate content. Gorontalo Polytechnic is one of the private universities that uses the internet to support academic and student activities. However, unlimited internet use in the campus environment can provide space for users, especially students. To access negative content that can interfere with academic activities and burden the network. Therefore, this research aims to optimize network security using a Mikrotik Routerboard with a firewall method to block access to negative content on the internet network at the Gorontalo Polytechnic. It is hoped that this research can help create a more positive and supportive internet environment for users, especially students, as well as assist network operators in assisting network operators in managing and controlling internet traffic.

Keywords: Internet, firewall, negative content

ABSTRAK

Perkembangan teknolgi informasi yang pesat, terutama dalam hal aksebilitas data melalui internet telah menjadi pendorong utama bagi kemajuan dalam berbagai bidang politik,kesehatan,ekonomi, dan pendidikan. Namun, pengunaan internet juga membawa dampak negatif seperti akses terhadap konten yang tidak pantas. Politeknik Gorontalo sebagai salah satu perguruan tinggih swasta mengunakan internet untuk mendukung kegiatan akademis dan kemahasiswaan. Namun, pengunaan internet yang tidak terbatas di lingkungan kampus dapat memberi celah bagi pengguna, terutama mahasiswa. Untuk mengakses konten negatif yang dapat menggangu aktivitas akademis dan membebani jaringan. Oleh karena itu, penelitian ini bertujuan untuk mengoptimalkan keamanan jaringan mengunakan Routerboard Mikrotik dengan metode firewall untuk memblokir akses konten negatif pada jaringan internet di politeknik Gorontalo. Penelitian ini diharapkan dapat membantu menciptakan lingkungan internet yang lebih posetif dan mendukung bagi pengguna, khususnya mahasiswa, serta membantu operator jaringan dalam membantu operator jaringan dalam mengatur dan mengontrol trafik internet.

Keywords: Internet, firewall, konten negatif

1. PENDAHULUAN

Perkembangan dan kemajuan teknologi informasi sangatlah cepat [1], kebutuhan akan aksesbilitas data yang cepat dan stabil telah mendorong penggunaan teknologi internet disegala bidang mulai dari bidang politik, kesehatan, ekonomi hingga pendidikan. Teknologi internet menjadi pendukung utama untuk meningkatkan mutu dan peforma suatu bidang [2]. Kemampuan komunikasi yang tidak mengenal batasan ruang dan waktu melalui teknologi internet merupakan syarat utama disetiap bidang untuk dapat terus meningkatkan efisiensi kinerja. Penggunnaan teknologi internet menjadi pilihan terbaik untuk memaksimalkan mutu dan kualitas sistem, yang hasilnya menjadi tolak ukur suatu keberhasilan [3].

Internet merupakan salah satu teknologi komunikasi yang bisa menghubungkan dari satu komputer ke komputer lainnya di seluruh dunia [4]. Kebutuhan internet sangatlah penting bagi pengguna untuk melakukan kegiatan sehari hari [5], mulai dari mengirim dan menerima pesan, mengolah data, membeli barang secara online hingga digunakan untuk belajar dan mengajar [6]. Selain mamfaatnya yang positif, ternyata terdapat juga

dampak negatif dari penggunaan internet, contohnya seperti pengguna yang mengakses konten yang tidak pantas seperti pornography, online gambling, fraud, dan lain-lain.

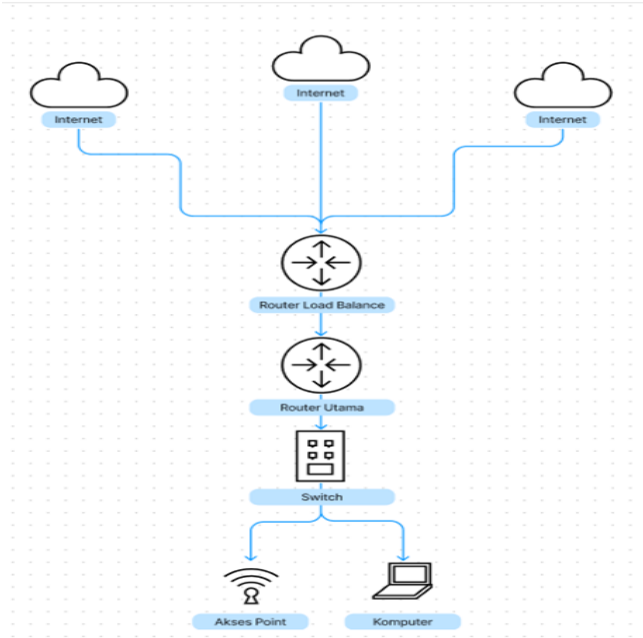
Politeknik Gorontalo merupakan perguruan tinggi swasta yang juga memamfaatkan teknologi internet untuk mendukung kegiatan kemahasiswaan dan akademis [7]. Saat ini Politeknik Gorontalo menggunakan sumber internet ISP (Internet Service Provide) dari Telkom Indonesia dengan kecepatan internet mencapai 250Mbp/s serta menggunakan Mikrotik sebagai pengelolaan management internet tersebut.

Penggunaan internet pada lingkungan kampus yang tidak dibatasi dapat memberikan celah terhadap pengguna khususnya mahasiswa [8], dalam hal ini pengguna yang tidak menggunakan fasilitas internet untuk kegiatan yang tidak baik. Hal ini dapat menyebabkan terganggunya aktivitas akademis dan juga dapat membebani FUP (Fair Usage Policy) [9]. Sehingga menyebabkan akses internet menjadi lambat. Pada jaringan internet yang berada dikampus Politeknik Gorontalo, sudah memiliki keamanan jaringan berupa TRUST+POSITIVE yang dibuat oleh KOMINFO (Kementrian Komunikasi dan Informatika Republik Indonesia) melalui perusahaan penyedia layanan internet, namun pada jaringan yang ada sekarang pada Politeknik Gorontalo belum terdapat keamanan jaringan tambahan. Oleh karena dibutuhkan sebuah solusi untuk mencegah pengguna agar tidak mengakses negative content. Salah satu upaya yang dapat diterapkan adalah dengan memamfaatkan firewall. Untuk proses implementasinya dapat menggunakan Routerboard Mikrotik Os. Mikrotik merupakan salah satu router yang banyak digunakan untuk management internet dikarenakan harganya yang terjangkau namun handal jika dibandingkan dengan produk lainnya [10]. Mikrotik cukup mudah dikonfigurasi dan memiliki fitur yang memadai untuk melakukan penapisan terhadap negatif content dengan menggunakan metode firewall dan web filtering.

2. METODE PENELITIAN

Analisis Topologi Jaringan

a. Topologi Existing



Gambar 1. Topologi Existing

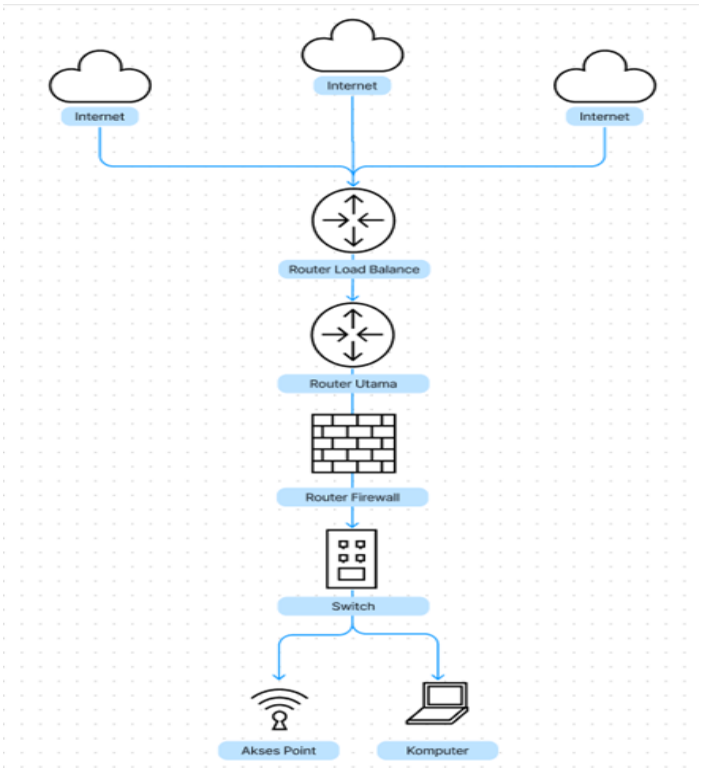
Pada *topologi* yang sedang berjalan saat ini, terdapat tiga buah sumber *internet* yang berasal dari layanan ISP (*Internet Service Provider*) dengan jenis layanan Indihome. Kemudian tiga layanan *internet* tersebut digabungkan kedalam satu wadah router untuk dimanagement menggunakan metode

load balance. kemudian *internet* tersebut di teruskan kembali ke router utama untutk di management dan dibagi ke *client* melalui perangkat switch serta *akses point*.

Berdasarkan hasil analisis topologi yang dilakukan penulis, terdapat sebuah kebebasan akses bagi pengguna internet pada kampus politeknik gorontalo khususnya mahasiswa. Hal ini disebabkan tidak adanya penghalang atau pembatas terhadap akses ke situs-situs yang tidak pantas dan ini menjadi perhatian terutama dalam lingkungan dimana akses internet terbuka degan memberikan akses tanpa hambatan pada lingkungan pendidikan.

b. Topologi yang diterapkan

Topologi yang digunakan adalah dengan menggunakan aplikasi website pengelolaan alokon sehingga dapat mempermudah petugas alokon.



Gambar 2. Topologi yang akan digunakan

Pada topologi yang akan digunakan, tidak terdapat perubahan pada topologi existing namun ditambahkan satu unit perangkat router Mikrotik yang tambahkan firewall yang terhubung antara Mikrotik utama dan switch, dimana Mikrotik tersebut dikonfigurasikan sebagai *firewall* untuk memfilter terhadap akses situs-situs yang dituju oleh pengguna.

3. HASIL DAN PEMBAHASAN

Dalam proses implementasi *firewall* berbasis *Mikrotik* berbasis *Mikrotik* pada jaringan Politeknik Gorontalo menggunakan RouterBoard RBD52G-5HacD2HnD-TC (hAP-AC2) yang sudah dibuat dalam bentuk simulasi. Simulasi ini bertujuan untuk meminimalisasi kesalahan sebelum melakukan implementasi langsung ke dalam jaringan kampus Politeknik Gorontalo. Dalam proses implementasi terdapat langkah-langkah pengerjaan di

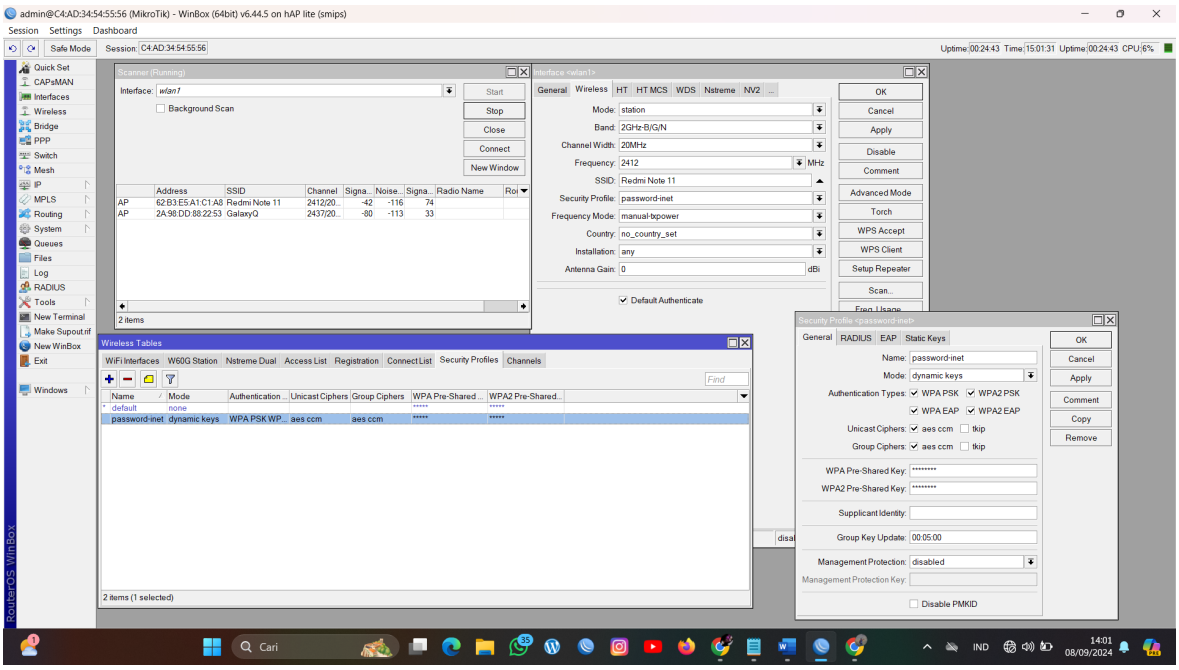
dalamnya agar proyek dapat terselesaikan dan diharapkan dapat berjalan sesuai dengan apa yang di rencanakan. Langkah-langkah pengerjaan dan tahapan konfigurasi adalah sebagai berikut.

1.1. Konfigurasi Dasar

Konfigurasi dasar pada *Mikrotik* bertujuan untuk menetapkan serangkaian pengaturan awal pada *Mikrotik*, hal ini diperlukan agar perangkat *Mikrotik* dapat berfungsi dengan baik sebagai *router* dalam jaringan dan menghubungkan perangkat dalam *jaringan*, serta memberikan akses *internet* ke pengguna.

1. Konfigurasi Wireless

Wireless merupakan alat didalam *Mikrotik* yang berfungsi untuk menyediakan konektivitas *jaringan nirkabel* kepada perangkat-perangkat yang mendukung *jaringan wireless*, seperti laptop, smartphone, dan perangkat *IoT*. *Mikrotik* memiliki fitur *wireless* yang memungkinkan *router* untuk bertindak sebagai ***Access Point***, ***client***, ***bridge***, atau ***repeater*** dalam sebuah *jaringan wireless*. Konfigurasi *wireless* pada *Mikrotik* perlu dilakukan. Dimana pada konsepnya adalah mengubah sistem *wireless* yang ada pada *Mikrotik* dari pemancar sinyal menjadi penangkap, hal ini dilakukan karena *wireless* difungsikan sebagai penangkap *Wi-Fi* layanan sumber *internet*. Dapat dilihat pada gambar 4.1 dijelaskan bahwa tahapan konfigurasi yaitu, pertama-tama pilih menu *wireless* pada *winbox*, kemudian aktifkan *wlan1*, tahap selanjutnya merubah mode *wireless* menjadi *station* Setelah itu membuat daftar *security profiles* yang baru, berupa nama password_inet, kemudian untuk autentikasi type nya dapat dipilih centangkan *WPA* dan kemudian membuat *password* yang sama dari sumber *internet*. Langkah terakhir yaitu proses *scan*, pada saat proses scan di aktifkan penulis memilih *device* yang dituju dan kemudian di hubungkan agar layanan *internet* dapat diterima.

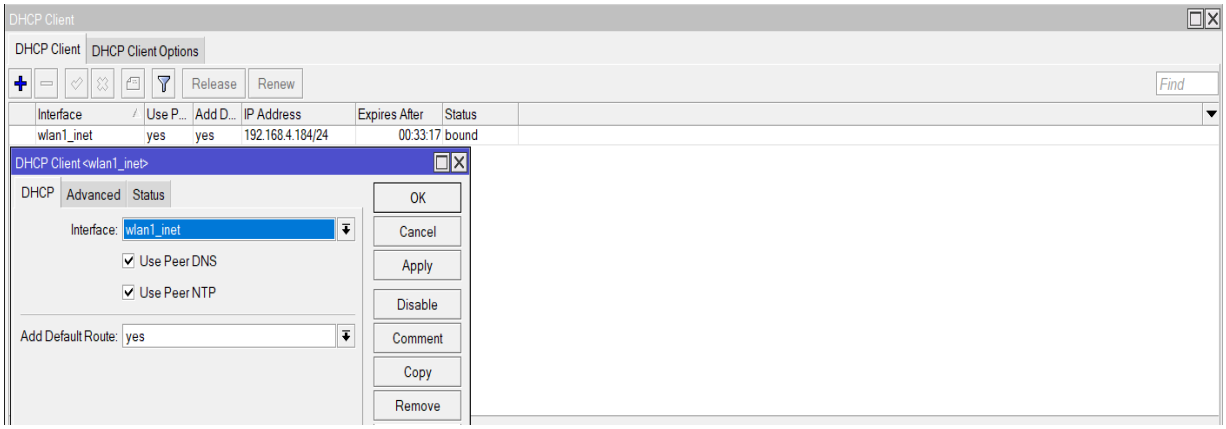


Gambar 3. Konfigurasi Sumber Internet

2. Konfigurasi layanan DHCP client

DHCP client merupakan salah satu fitur yang memungkinkan perangkat *Mikrotik* untuk secara otomatis mendapatkan konfigurasi jaringan, seperti alamat *IP*, *gateway*, *DNS*, dan informasi jaringan lainnya, dari sumber *internet*. Dengan mengaktifkan *DHCP client*, *Mikrotik* dapat berfungsi sebagai perangkat yang menerima pengaturan jaringan secara otomatis, sehingga mempermudah proses konfigurasi jaringan, terutama ketika *Mikrotik* terhubung ke jaringan dinamis seperti yang disediakan oleh *ISP*. Pada gambar 4.2 dijelaskan, untuk mengaktifkan *DHCP client* pada perangkat *Mikrotik*, pertama-tama penulis membuka

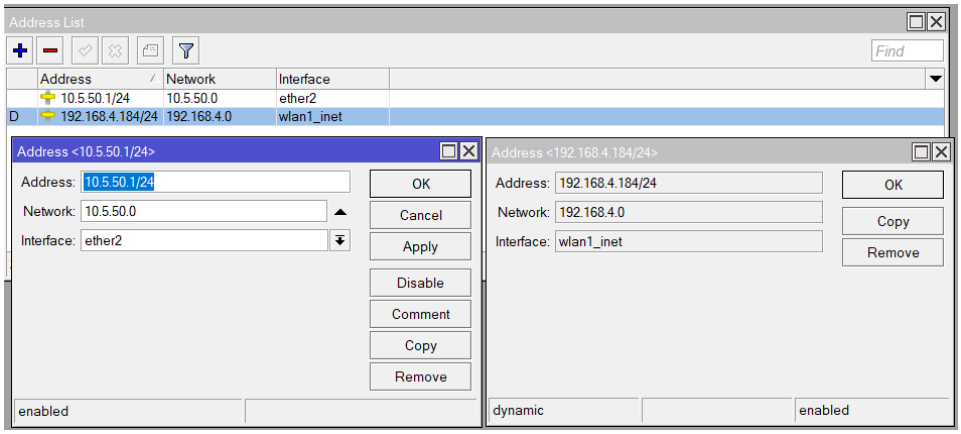
menu *IP*, kemudian memilih menu *DHCP Client*, setelah itu pilih menu tambah, dengan nama *interface wlan1*, dimana *wlan1* adalah *interface* yang digunakan sebagai akses dari seumber *internet*, yang di dapat dari konfigurasi *wireless* pada perangkat *Mikrotik*.



Gambar 4. DHCP Client

3. Konfigurasi ip address

Konfigurasi *IP Address* pada *Mikrotik* adalah tahapan untuk menetapkan identitas atau alamat pada setiap *interface Mikrotik* agar dapat berkomunikasi dengan perangkat lain di dalam jaringan lokal maupun pada jaringan eksternal. Dengan *IP Address* yang terkonfigurasi dengan benar, maka *Mikrotik* dapat berfungsi sebagai pengatur lalu lintas jaringan, penerus data antar pengguna, dan juga penghubung ke jaringan *internet*. Pada gambar 4.3 dijelaskan, bahwa untuk *IP Address* dari *interface wlan1* di dapatkan dari layanan *DHCP Client* sehingga Perangkat *Mikrotik* mendapatkan alamat IP Address secara otomatis. Kemudian penulis menambahkan IP Address untuk *interface ether2,* dimana port dari *ether2* pada perangkat *Mikrotik* berfungsi sebagai interface yang di gunakan untuk membagikan layanan ke client. Untuk alamat *IP Address* yang digunakan penulis adalah 10.5.50.1/24 dengan network 10.5.50.0.

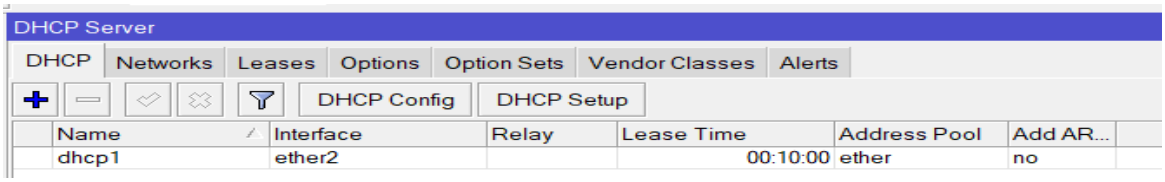


Gambar 5. Konfigurasi Ip Address

4. Konfigurasi layanan DHCP server

DHCP Server pada *Mikrotik* adalah fitur yang berfungsi untuk secara otomatis memberikan konfigurasi jaringan, seperti alamat *IP*, *gateway*, *DNS*, dan informasi jaringan lainnya, kepada perangkat yang terhubung ke jaringan. *DHCP server* di *Mikrotik* biasanya digunakan untuk jaringan lokal, di mana *Mikrotik* secara otomatis mendistribusikan alamat IP kepada perangkat client. Pada tahapan untuk konfigurasi *DHCP Server*, langkah awal penulis membuka menu IP, kemudian memilih DHCP Server, setelah itu pilih *DHCP Setup,*

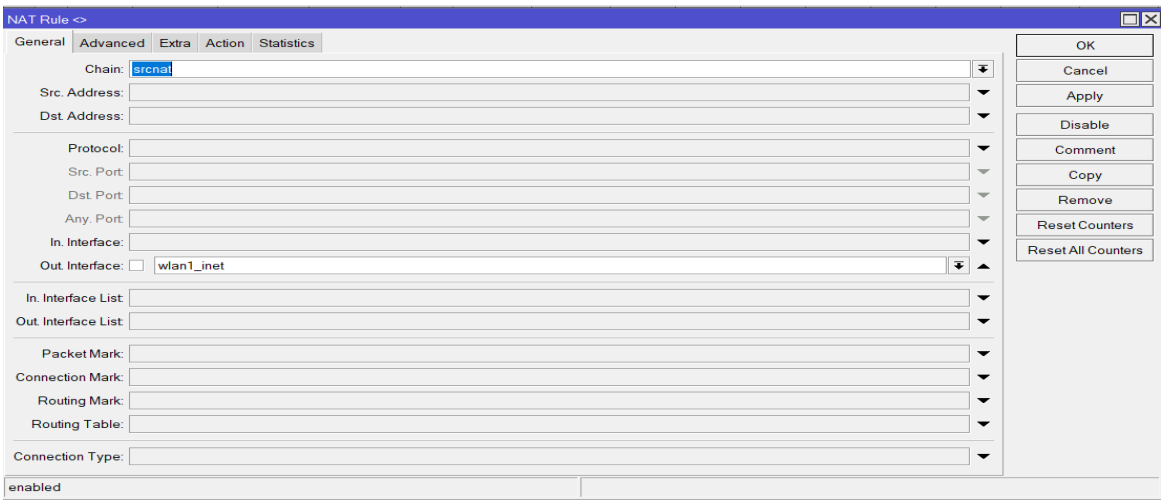
Pada DHCP Server Interface pilih ether2 sebagai interface yang mengarah ke client kemudian pilih next, pada DHCP Address Space akan mengisi otomatis *Ip Address* dari ehter2 yaitu 10.5.50.0/24 kemudian pilih next lagi, setelah itu pada *Gateway for DHCP Network* juga akan terisi otomatis dengan IP gateway dari ether2, kemudian pilih next lagi. Pada tampilan DHCP Relay, penulis mengkosongkan isi dari list tersebut, setelah itu pilih next kembali. Maka untuk konfigurasi layanan *DHCP Server* sudah berhasil, dan hasilnya akan seperti pada gambar 6.



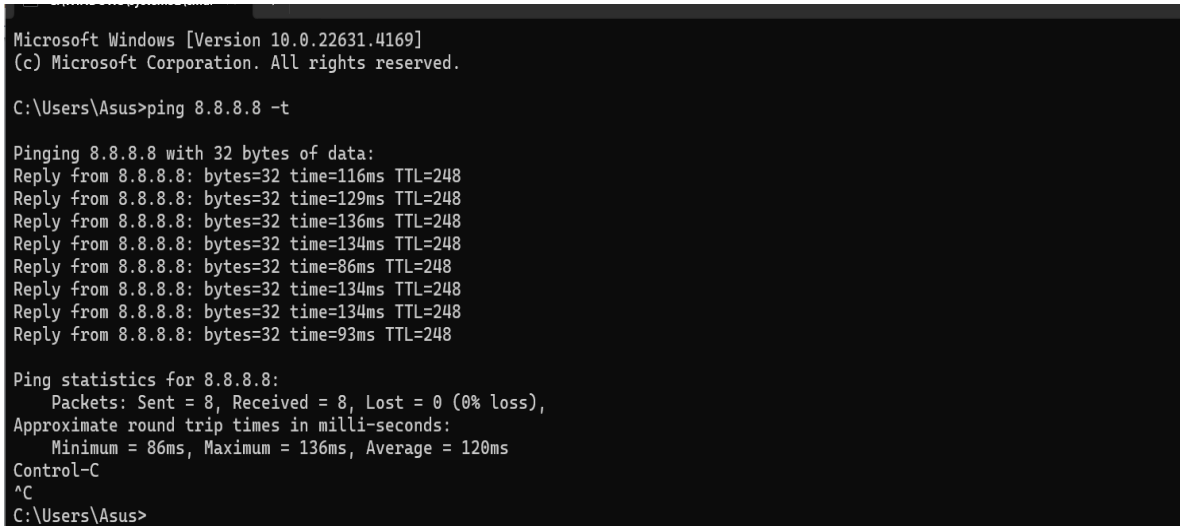
Gambar 6. DHCP Server

5. Konfigurasi NAT

NAT (Network Address Translation) pada *Mikrotik* merupakan fitur yang digunakan untuk menerjemahkan alamat *IP*, baik dari *private* ke *public* maupun sebaliknya, untuk memastikan perangkat dalam jaringan lokal dapat berkomunikasi dengan perangkat di luar jaringan, seperti *internet*. Hal ini dilakukan karena *NAT* dapat membungkus packet dan di sebarkan. Lalu memilih action masquerade dimana fungsinya agar *IP private* bisa diterjemahkan ke *IP public* sehingga bisa terhubung ke *internet*. Pada gambar 4.5 di jelaskan, langkah tahapan menyetting *NAT* di mulai dari memilih menu *IP*, kemudian membuka menu *firewall*, setelah itu memilih *NAT*. Pada pilihan general penulis memilih chain *scrnat* dengan *out_interface* yang mengarah pada *interface wlan1,* kemudian pada tab action penulis memilih action masqurade. Ketika tahapan setting *NAT* telah selesai langkah terakhir adalah menguji koneksi *internet* melalui perangkat *client*. Pada gambar di atas dijelaskan, penulis melakukan uji konektivitas *internet* terhadap perangkat *client* dengan menguji *ping* ke *dns Google*. Dapat dilihat bahwa koneksi *internet* sudah terhubung.



Gambar 7. Konfigurasi NAT



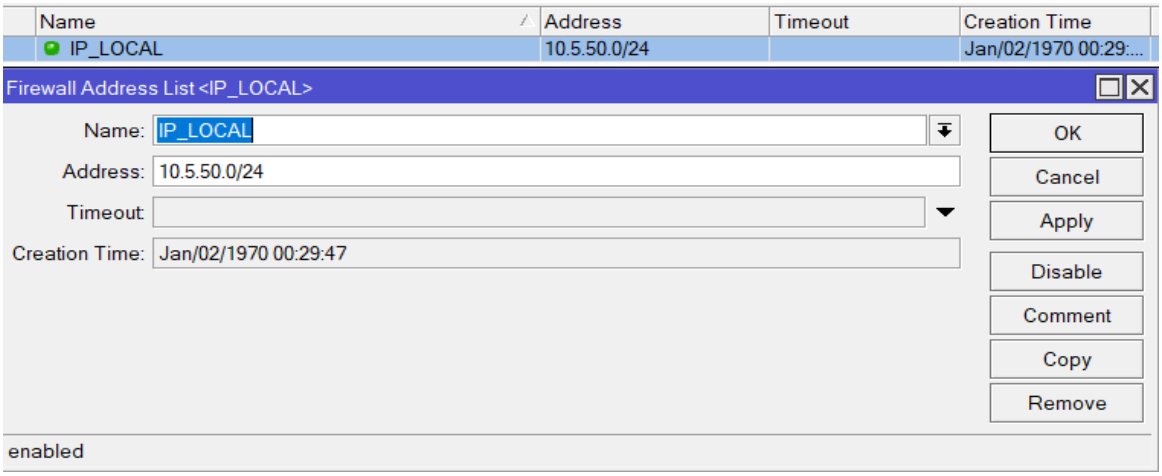
Gambar 8. Pengujian

1.2. Konfigurasi filter pada Router Mikrotik

Konfigurasi filter konten merupakan teknik yang digunakan untuk membatasi atau mengontrol jenis conten tertentu yang ada pada *internet*. Hal ini dilakukan unutk mencegah client atau pengguna tidak dapat mengakses terhadap situs, web dan layanan yang di anggap tidak sesuai, dan melanggar kebijakan instansi ataupun organisasi.

1. *Settting firewall address list*

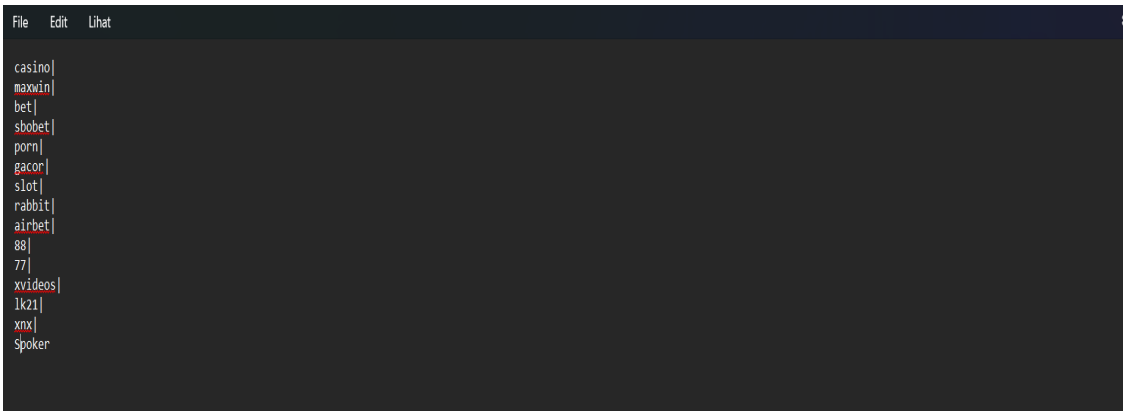
Firewall Address List pada *Mikrotik* adalah fitur yang digunakan untuk mengelola daftar alamat *IP*, baik itu alamat *IP* tunggal maupun rentang *IP*, yang akan digunakan dalam aturan *firewall*. Hal ini memudahkan manajemen *firewall* karena memungkinkan administrator untuk mengelompokkan alamat *IP* dalam satu list, yang kemudian bisa diterapkan ke berbagai aturan *firewall* secara dinamis dan efisien. Pada gambar 4.8 dijelaskan, untuk melakukan konfigurasi address list pada fitur *firewall*. Tahapan awal dimulai dari membuka menu *IP*, kemudia memilih menu *firewall* setelah itu pilih *address list*. Di dalam menu *address list* penulis membuat *address list* baru, dengan nama *IP_LOCAL* , serta alamat menggunakan *IP network* yang mengarah ke *interface ether2*.



Gambar 9. Firewall Address List

2. Membuat file yang berisi kata kunci dan domain

File yang di buat merupakan.*txt* yang berfungsi sebagai daftar *domain* dan kata kunci, hal ini dilakukan untuk mempermudah pengelolahan dan pemblokiran akses ke banyak *situs* secara otomatis. Sehingga *administrator* tidak perlu lagi menambahkan penyetingan aturan pemblokiran satu persatu ke dalam aturan *filter*. Sehingga *administrator* hanya perlu mengganti ataupun menambahkan isi dari file tersebut, yang kemudian di jalankan menggunakan *script*. Pada gambar 11 dijelaskan, bahwa penulis membuat file yang berisi daftar domain dan kata kunci ,dimana setiap satu domain serta kata kunci akan di akhiri simbol **"|"** *OR,* hal ini berfungsi sebagai batas antara domain dan juga kata kunci, serta aturan dalam *regxep* untuk memblokir domain yang banyak. Kemudian jika selesai maka langkah selanjutnya penulis mengupload file tersebut ke dalam file *local Mikrotik*.



Gambar 10. File Daftar Kata Kunci

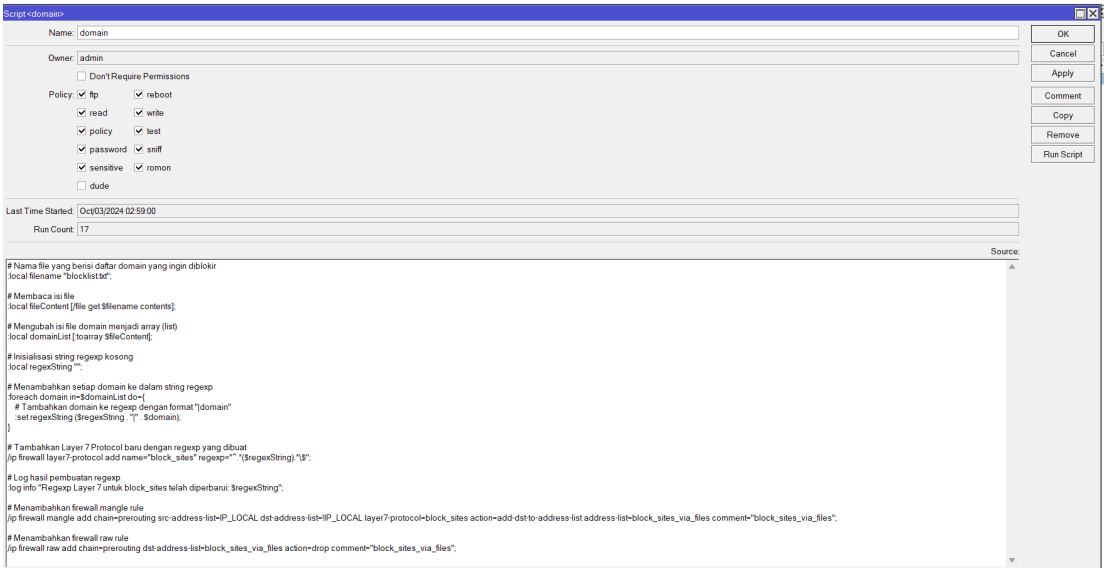


Gambar 11. File Daftar Domain

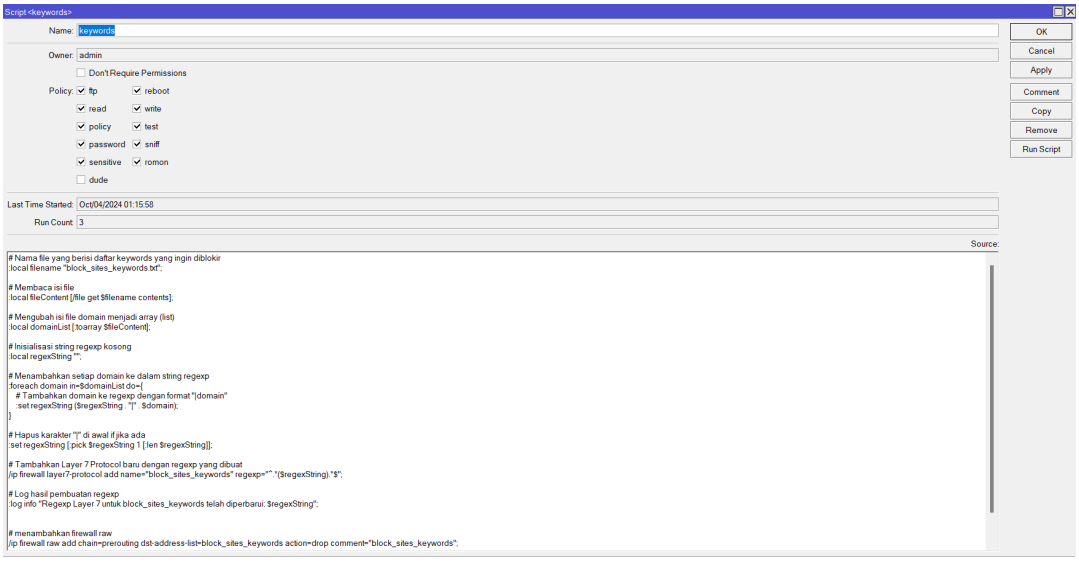
3. Membuat *script* pada mikrotik

Script bertujuam untuk memblokir domain yang terdapat pada file *local* ***Mikrotik*** dengan tujuan untuk **mendinamiskan** pemblokiran akses ke berbagai *domain* dan kata kunci yang terdaftar dalam file teks (.txt). Fungsi utama dari script tersebut adalah untuk **membaca file berisi daftar *domain* serta kata kunci**, kemudian menjalankan script tersebut untuk membuat aturan *firewall raw, mangel, dan layer7 protocol* yang dinamis agar dapat memblokir domain dan kata kunci yanga ada didalam file tersebut. Pada gambar 4.6 dan

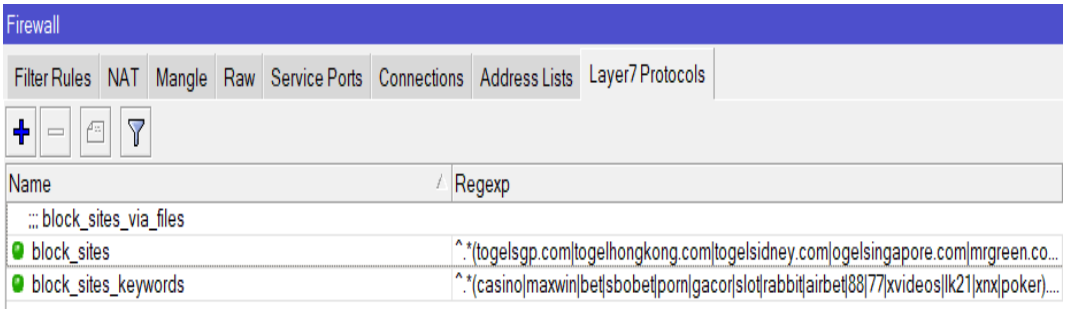
4.7 penulis membuat sebuah *script* yang bernama *domain* dan *keywords*, dijelaskan bahwa *script* diatas akan membaca sebuah file *.txt* yang terdapat pada file local pada *Mikrotik*, kemudian *script* tersebut akan mengubah file yang berupa *.txt* menjadi data *Aray*. Setelah itu *script* tersebut akan membuatkan sebuah kode *regexp* ^.*nama_domain ^.\$ didalam fitur */ip firewall layer7-protocol*, serta membuat *rule firewall mangel* untuk mengelompokan *IP* dari *domain* dan kata kunci yang didapat dari *layer7 protocol* ke dalam *firewall Address list*, dan *rule firewall raw* untuk memblokir *IP* yang telah di kelompokan oleh *rule mangel* dan *Address list* ketika perintah dijalankan dijalankan.



Gambar 12. Script Daftar Domain



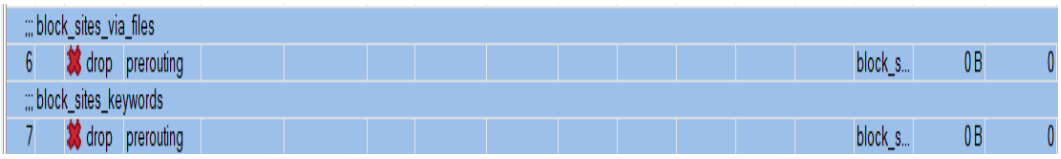
Gambar 13. Script Daftar Kata Kunci



Gambar 14. Layer7-Protocols



Gambar 15. Firewall Mangle

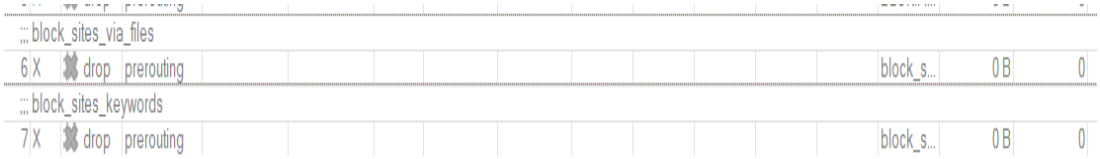


Gambar 16. Firewall Raw

2. Pengujian

Pengujian implementasi *firewall* berbasis Mikrotik perlu dilakukan agar memastikan bahwa proses implementasi sesuai dengan perencanaan. Tahap pengujian dilakukan dengan menguji akses situs yang domainnya masuk di dalam file yang menjadi p

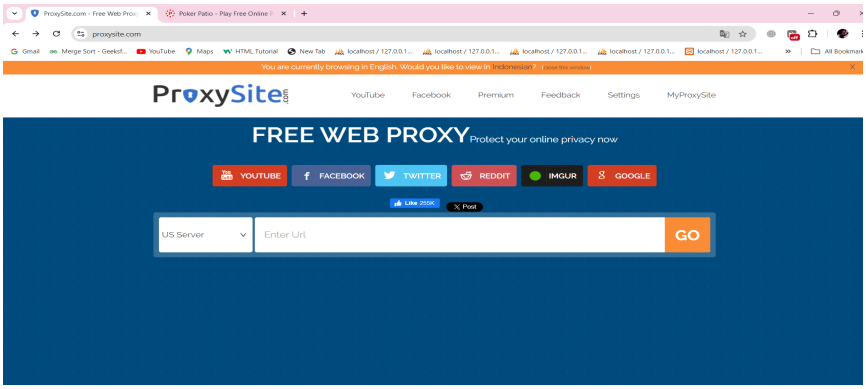
Metode pengujian menggunakan metode fungsional. Metode ini merupakan pengujian yang dikhususkan untuk menguji konfigurasi, dengan tujuan apakah pada implementasi konfigurasi yang telah dibuat, sudah berjalan dengan fungsinya. Sebelum melakukan pengujian terlebih dahulu menonaktifkan fitur *firewall raw Mikrotik* terlihat pada gambar 16 dibawah, hal ini bertujuan untuk membuka koneksifitas akses terhadap situs yang dituju. Setelah itu penulis membuka peramban *internet*, kemudia memasukan nama domain, dapat dilihat dari gambar 21 dibawah. Dijelaskan setelah dijalankan langkah di atas situs masih bisa di akses tanpa kendala serta pada *Address list IP* dari *domain* yang dituju sudah masuk dalam pengelompokan *IP*. Kemudian firewall raw diaktifkan, yang dilanjutkan mengrefresh peramban *internet*, dapat dilihat hasilnya seperti pada gambar 4.22 dibawah, dimana akses yang menuju ke daftar domain yang dituju mengalami kegagalan, dan *firewall* raw mendeteksi adanya packet yang diblokir.



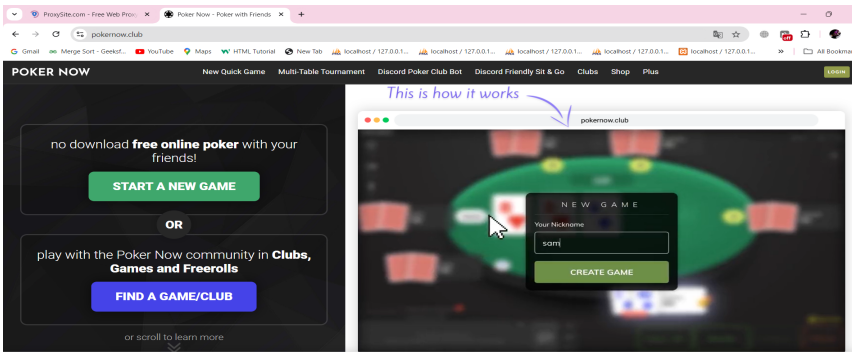
Gambar 17. Firewall Raw dinonaktifkan

	Name	Timeout	Creation Time
	IP_LOCAL		Jan/02/1970 00:29:...
	IP_LOCAL		Jan/02/1970 00:30:...
	IP_LOCAL		Oct/02/2024 23:01:...
D	block_sites_keywords	00:00:55	Oct/06/2024 00:28:...
D	block_sites_keywords	00:00:55	Oct/06/2024 00:28:...
D	block_sites_via_files	00:00:18	Oct/06/2024 00:27:...
D	block_sites_via_files	00:00:18	Oct/06/2024 00:27:...

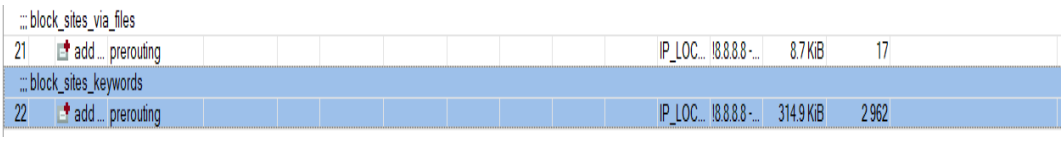
Gambar 18. Firewal Address List Dalam Posisi Berjalan



Gambar 19. Firewal Address List Dalam Posisi Berjalan



Gambar 20. Firewal Address List Dalam Posisi Berjalan



Gambar 21. Firewall Address List Dalam Posisi Berjalan

4. KESIMPULAN

Berdasarkan pembahasan yang telah diuraikan, maka dapat disimpulkan bahwa, dengan perangkat Mikrotik dengan memaksimalkan fitur *firewall Mikrotik* pada jaringan Politeknik Gorontalo dan menghasilkan sebuah rancangan jaringan *internet* sehat yang dinamis. Dalam artian, pengguna jaringan pada area Politeknik Gorontalo dapat di filter dan di kontrol sehingga menghasilkan internet yang sehat.

DAFTAR PUSTAKA

[1] M. I. Abas, I. Ibrahim, and S. Pakaya, "Inovasi Sistem Informasi Manajemen Zakat, Infaq dan Sedekah Lazismu Gorontalo," *JRST (Jurnal Ris. Sains dan Teknol.*, vol. 6, no. 1, p. 79, 2022, doi: 10.30595/jrst.v6i1.11939.

[2] M. Masri, M. I. Abas, W. Hasyim, and I. Ibrahim, "Sistem Inventarisasi Aset Universitas Muhammadiyah Gorontalo Berbasis Web," *J. Ilmu Komput.*, vol. 2, no. 2, p. 27, 2022, doi: 10.31314/juik.v2i2.1712.

[3] M. I. Abas and I. Ibrahim, "Optimasi Support Vector Machine Particle Swarm Optimization Untuk Prediksi Konsumsi Energi Listrik," *Jambura J. Informatics*, vol. 1, no. 2, pp. 47–56, 2019, doi: 10.37905/jji.v1i2.2646.

[4] R. R. Guk Guk, B. D. I. Cahya, D. Rahmayanty, and M. Regilsa, "Peran Orang Tua Dalam Mengaplikasikan Internet Sebagai Media Pendidikan Bagi Anak," *J. Pendidik. dan Konseling*, vol. 5, no. 6, pp. 45–55, 2023, doi: 10.31004/jpdk.v5i6.20182.

[5] Z. R. Rozan and A. O. P. Dewi, "Penggunaan Internet sebagai Sumber Informasi pada Generasi Baby boomer berdasarkan Kemampuan Literasi Informasi," *Anuva J. Kaji. Budaya, Perpustakaan, dan Inf.*, vol. 6, no. 1, pp. 23–42, 2022, doi: 10.14710/anuva.6.1.23-42.

[6] N. Salsabila and P. Anjani, "EFEKTIVITAS GOOGLE MEET SEBAGAI MEDIA KOMUNIKASI BELAJAR ONLINE BAGI MAHASISWA RANTAU DI DESA HEGARMANAH KABUPATEN SUKABUMI," vol. 6, no. 2, pp. 21–32, 2022, doi: 10.32832/komunika.v6i2.7106.

[7] D. Rika Widianita, "URGENSI PERGURUAN TINGGI BAGI MAHASANTRI DI ERA SOCIETY 5.0," *AT-TAWASSUTH J. Ekon. Islam*, vol. VIII, no. I, pp. 1–19, 2023.

[8] Melisa Septiani Togatorop and Mariana Simanjuntak, "Analisis Dampak Penggunaan Internet Terhadap Minat Belajar Mahasiswa," *Neptunus J. Ilmu Komput. Dan Teknol. Inf.*, vol. 2, no. 3, pp. 74–86, 2024, doi: 10.61132/neptunus.v2i3.212.

[9] A. R. Anggunani and B. Purwanto, "Hubungan antara Problematic Internet Use dengan Prokrastinasi Akademik," *Gadjah Mada J. Psychol.*, vol. 4, no. 1, p. 1, 2019, doi: 10.22146/gamajop.45399.

[10] N. N. Huri, F. Hariadi, and P. Lede, "Rancang Bangun Jaringan Hotspot Menggunakan Router Mikrotik Pada SD Inpres Kawangu 2," *... Inov. Wira Wacana*, vol. 01, no. 03, pp. 164–176, 2023, [Online]. Available: https://www.ojs.unkriswina.ac.id/index.php/inovatif/article/view/338