Implementasi *Web Content Filtering* Pada Jaringan RT/RW Net Menggunakan *Pi-Hole DNS Server*

Miftahur Rahman[1]
[1]Teknik Informatika, Fakultas Teknik, Universitas Muhammadiyah Jember
E-mail: [1]*miftahurrahman@unmuhjember.ac.id*
Coresponden Author: *miftahurrahman@unmuhjember.ac.id*

Diterima Redaksi: 07 Maret 2023 Revisi Akhir: 11 Maret 2023 Diterbitkan Online: 19 Maret 2023

Abstrak – *Penggunaan jaringan RT/RW Net supaya lebih maksimal perlu menerapkan keamanan jaringan yaitu dengan menerapkan Pi-Hole DNS Server untuk memfilter website negatif dan iklan yang tidak diinginkan. Hal ini sesuai dengan program yang dicanangkan oleh Pemerintah (Kemkominfo) yaitu penggunaan internet yang sehat dan aman. Tahapan penelitian yang digunakan adalah identifikasi masalah, studi pustaka, implementasi, pengujian dan analisis hasil atau penarikan kesimpulan. Menghasilkan penelitian bahwa penerapan Pi-Hole DNS Server terhadap topologi jaringan RT/RW Net berhasil dilakukan terbukti dapat memfilter atau menyaring website yang mengandung situs-situs negatif dan dapat memblokir iklan yang tidak diinginkan, keberhasilan dalam memfilter tersebut dikategorikan 100% efektif, serta kualitas jaringan setelah penerapan Pi-Hole DNS Server dikategorikan baik dalam metode pengujian QoS.*

Kata Kunci *— DNS Server, Internet, Mikrotik, Pi-Hole, Web Filtering*

Abstract – *RT/RW Net network infrastructure in its use, so that it is more optimal it is necessary to apply network security, namely by implementing a Pi-Hole DNS Server to filter negative websites and unwanted advertisements. This is in accordance with the program launched by the Government (Kemkominfo), namely healthy and safe internet use. The research method used is the stages of problem identification, literature study, implementation, testing and analysis of results or drawing conclusions. Resulted in research that the application of the Pi-Hole DNS Server to the RT/RW Net network topology was successfully carried out, proven to be able to filter or filter websites that contain negative sites and can block unwanted advertisements, success in filtering is categorized as 100% effective, and network quality after the implementation of the Pi-Hole DNS Server is categorized as good in the QoS testing method.*

Keywords *— DNS Server, Internet, Mikrotik, Pi-Hole, Web Filtering*

1. PENDAHULUAN

Era globalisasi modern saat ini penggunaan internet sangat dibutuhkan. Internet merupakan suatu sarana dimana sebagai sumber dari segala informasi, baik dari sektor sosial, bidang pendidikan, ekonomi dan medis serta juga IPTEK [1][2]. Pertumbuhan pengguna internet Dunia dan khususnya di Indonesia terus semakin meningkat seiring dengan perkembangan teknologi informasi dan komunikasi. Berdasarkan data yang dirilis dari situs *wearesocial.com* pada akhir Februari 2022 lalu, dari total jumlah penduduk Indonesia sekitar 277,7 juta jumlah penguna internet di Indonesia mencapai 204,7 juta orang. Hal ini, berarti jumlah pengguna internet di Indonesia meningkat sekitar 1% atau 2,1 juta pengguna dibandingkan dengan tahun 2021 yaitu 202,6 juta [3]. Internet telah mempengaruhi berbagai aspek kehidupan, baik dari sisi positif maupun sisi negatif. Dari sisi positif, salah satunya bahwa internet sangat membantu dalam mengakses informasi dan membuka wawasan masyarakat, dalam hal pekerjaan pun dengan internet dapat sangat membantu. Dari sisi negatif, salah satunya bahwa dengan adanya internet dapat berdampak terhadap ancaman masyarakat atau penggunanya [4].

Masa pandemi tahun 2020 penyebaran Covid-19 masih berlangsung di seluruh dunia, hal ini berdampak pada kebiasaan dan pola hidup sehari-hari dengan melakukan pembatasan sosial, jaga jarak, dan sebagainya, sehingga menyebabkan kegiatan seperti belajar, bekerja, belanja dan lainya yang dilakukan secara daring yaitu dengan memanfaatkan internet. Hal ini juga terjadi di daerah Krajan 1, Kasiyan Timur, Kec. Puger, Kabupaten Jember, dimana daerah tersebut masih belum terjangkau jaringan internet. Oleh karena itu, di Desa tersebut dibangun arsitektur jaringan RT/RW Net untuk memudahkan masyarakat disana supaya dapat menjalankan aktifitas sehari-hari dengan memanfaatkan jaringan internet di masa pandemi ini [1]. Namun, terdapat temuan

oleh admin jaringan RT/RW Net bahwa ada juga masyarakat yang tidak memanfaatkan jaringan internet dengan sebaik mungkin, yaitu lebih banyak meluangkan waktunya membuka situs-situs negatif, seperti porno, *game*, *social media*, dan sebagainya. Temuan lain oleh pengguna bahwa saat mengakses informasi di sebuah website sering tampil iklan, sehingga menyebabkan pemakaian *bandwith* yang semakin besar akibatnya akses menjadi lambat. Iklan yang tampil terkadang bukan iklan resmi namun iklan yang sengaja di sebar sebagai media penyebaran virus *malware*. Oleh karena itu, untuk memaksimalkan penggunaan jaringan RT/RW Net perlu menerapkan keamanan jaringan yaitu dengan menerapkan aplikasi *Pi-Hole DNS Server* untuk memfilter *website* dan iklan yang tidak diinginkan. Hal ini sesuai dengan program yang dicanangkan oleh Pemerintah (Kemkominfo) yaitu penggunaan internet yang sehat dan aman[5].

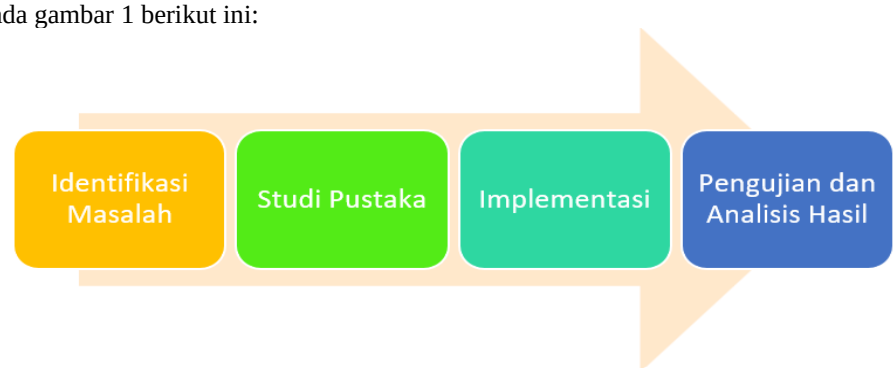
Pi-Hole sebagai *DNS sinkhole* yang dapat melindungi perangkat-perangkat jaringan dari konten web yang tidak diinginkan. *DNS Server* yang digunakan tidak seluruhnya aman. Sebab beberapa *website* yang berbahaya bisa saja lolos, dengan memanfaatkan *Pi-Hole* dapat menyaring situs-situs yang tidak aman dan juga sebagai *blokir* iklan-iklan yang tidak diinginkan [6][7]. *Web content filtering* merupakan saringan konten situs-situs yang digunakan oleh perorangan maupun kelompok atau organisasi agar tidak dapat diakses. Kendali konten perangkat lunak nantinya akan menentukan situs konten yang tersedia maupun konten yang tidak boleh diakses atau diblokir[8].

Penerapan *Pi-Hole* sebagai keamanan jaringan terbukti baik untuk memfilter situs atau iklan yang tidak diinginkan seperti penelitian yang pernah dilakukan oleh [9] yaitu menerapkan *Pi-Hole DNS Server* sebagai *Ads-Bloker* dan *system filtering* situs pada jaringan *hotspot*, menghasilkan penelitian bahwa penerapan *Pi-hole DNS Server* dapat memblokir dan memfilter iklan yang ada pada website dan tidak mengurangi kualitas pelayanan pada jaringan. Selanjutnya penelitian yang dilakukan oleh [10] tentang Implementasi dan Analisis Penerapan *Pi-Hole Network Ad-Blocking* di Laboratorium Jaringan Teknik Informatika UMMU. Perbadingan penelitian yang sudah dilakukan oleh [9][10] dengan penelitian yang akan dilakukan ini adalah sebagai pemfilteran konten website atau situs dan iklan yang bernuansa negatif sebagai keamanan jaringan, hal ini dilakukan pada topologi jaringan RT/RW Net di Desa Kasiyah Jember. Sehingga beberapa pokok yang diuraikan diatas, maka peneliti akan melakukan riset dengan topik Implementasi *Web Content Filtering* pada Jaringan RT/RW Net menggunakan *Pi-hole DNS Server*.

Manfaat pada penelitian ini adalah membantu *administrator* jaringan RT/RW Net dalam melakukan *filtering* terhadap situs-situs negatif dan iklan yang tidak diinginkan dengan menerapkan *Pi Hole DNS Server*, sehingga para pengguna internet di Desa Kasiyan Jember dapat memanfaatkan internet dengan sebaik mungkin untuk hal-hal yang positif, hal ini sesuai dengan program yang dibentuk oleh Pemerintah yaitu penggunaan internet yang sehat dan aman.

2. METODE PENELITIAN

Langkah-langkah penelitian yang akan dilakukan secara umum terdiri dari 4 (empat) tahapan, mulai dari identifikasi masalah, studi pustaka, implementasi, pengujian dan analisis hasil atau penarikan kesimpulan ditunjukkan pada gambar 1 berikut ini:



Gambar 1. Tahapan Penelitian

2.1. Identifikasi Masalah

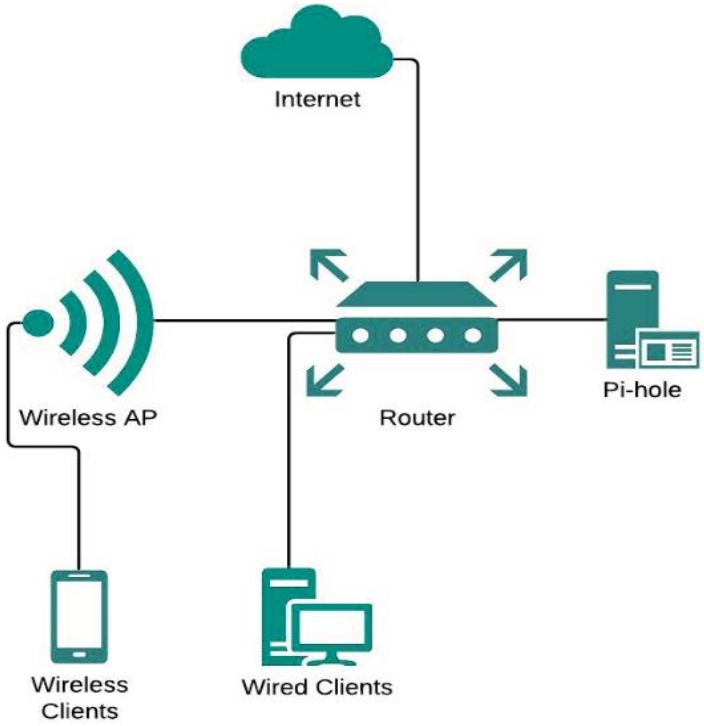
Tahapan yang pertama dalam melakukan penelitian dengan cara menganalisis masalah yang ada dan menawarkan solusi yang diharapkan dapat digunakan dalam menyelesaikan permasalah dimaksud.

2.2. Studi Pustaka

Merupakan langkah yang kedua bertujuan untuk mempelajari rujukan berupa artikel penelitian, paper, buku-buku referensi yang lain terkait dengan penelitian untuk melengkapi pengetahuan awal, guna memahami teori yang dapat digunakan untuk menunjang penelitian.

2.3. Implementasi

Tahapan ini akan mengimplementasikan *Pi-Hole DNS Server* sebagai *filtering* situs-situs negatif pada jaringan RT/RW Net dan blokir iklan yang tidak diinginkan. Gambar 2 menunjukkan topologi jaringan yang menerapkan *Pi-hole DNS server*.



Gambar 2. Topologi Penerapan *Pi-Hole*

Alur kerja pada penelitian ini adalah dengan mengalihkan lalu lintas jaringan RT/RW Net agar melewati *Pi-Hole DNS server*, sehingga lalu lintas paket data pada jaringan ini dapat diawasi oleh *Pi-Hole* dan diterapkan aturan-aturan untuk *filtering* terhadap situs-situs yang mengandung negatif dan blokir iklan yang tidak diinginkan. Berikut tahapan-tahapan yang akan dilakukan:

2.3.1. Instalasi dan Konfigurasi Ubuntu Server

Lakukan instalasi sistem operasi *linux ubuntu server*, sebab *pi-hole dns server* hanya *support* pada *os linux*. Selanjutnya lakukan konfigurasi IP *address* yaitu untuk menentukan IP dari *Network-based Intrusion Detection System (NIDS) server*.

2.3.2. Pi-hole DNS Server Configuration

Tahapan ini adalah dengan melakukan instalasi *Pi-hole* ke dalam *ubuntu server* terlebih dahulu kemudian lakukan konfigurasi *Pi-hole DNS server* untuk proses instalasinya dapat menuliskan dengan perintah:

```
[curl -sSL https://install.pi-hole.net | bash]
```

2.3.3. Router Mikrotik Configuration

Mikrotik adalah *operating system* dan *tool* yang dapat dipakai dengan tujuan menjadikan komputer biasa menjadi *router network*[11], mencakup berbagai fitur yang dibuat untuk *loacal area network* dan jaringan *wireless*, cocok digunakan oleh ISP, *provider hotspot* dan *warnet*[12][13]. Untuk menjalankan *Pi-Hole DNS Server* dapat memanfaatkan Mikrotik untuk pengaturan *DNS Server*-nya. Dalam hal ini, untuk me-*remote router mikrotik* dapat menggunakan *tool winbox.* Berikut perintah berbasis *command line*:

```
[/ip firewall nat add
chain=dstnat action=dst-nat to-addresses=IP Pi-Hole to-ports=53 protocol=udp dst-port=53
chain=dstnat action=dst-nat to-addresses=IP Pi-Hole to-ports=53 protocol=tcp dst-port=53]
```

2.4. Pengujian dan Analisis Hasil

Pengujian *filtering web* dilakukan dengan skenario sebelum dan setelah menerapkan *Pi-hole DNS Server*. Selanjutnya dilakukan analis kualitas jaringan untuk memastikan bahwa kualitas layanan pada jaringan tetap baik dengan metode *Quality of Services (QoS). QoS* merupakan sekumpulan teknologi yang bekerja pada jaringan untuk menjamin kemampuannya dalam menyediakan layanan jaringan komputer yang lebih baik, sehingga kebutuhan suatu layanan dapat terpenuhi. *QoS* merupakan metode pengukuran tentang seberapa baik jaringan dan merupakan suatu usaha untuk mendefinisikan karakteristik dan sifat dari satu servis[14]. Untuk menentukan kualitas layanan, dibutuhkan beberapa parameter pendukung antara lain *delay*, *jitter*, *packet loss*, dan *throughput* [15][16][17].

3. HASIL DAN PEMBAHASAN

3.1. Implementasi

3.1.1. Server Configuration

Konfigurasi dilakukan untuk menentukan alamat dari *NIDS server*. Untuk melakukan konfigurasi alamat IP dapat dilakukan dengan cara menuliskan perintah **ifconfig**, sesuaikan konfigurasi alamat IP dengan kebutuhan topologi jaringan yang digunakan, dalam penelitian ini menggunakan IP: 192.168.7.240/24. Berikut gambar hasil konfigurasi alamat IP pada *NIDS server*:

```
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.7.240  netmask 255.255.255.0  broadcast 192.168.7.255
        inet6 fe80::6f13:48f8:4ff5:c75f  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:8a:59:2b  txqueuelen 1000  (Ethernet)
        RX packets 43  bytes 4714 (4.7 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 103  bytes 10590 (10.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 111  bytes 9052 (9.0 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 111  bytes 9052 (9.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Gambar 3. *Alamat Server*

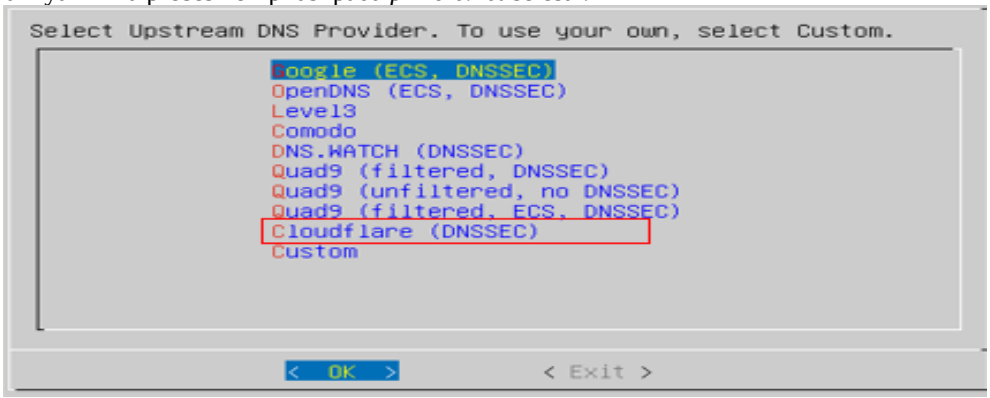
3.1.2. Pi-Hole Configuration

Pada tahap ini lakukan instalasi *Pi-Hole* ke dalam *ubuntu server* 20.04 terlebih dahulu. Kemudian lakukan instalasi *Pi-Hole DNS server* nya dengan cara mengetikkan perintah **curl -sSlhttps://install.pi-hole.net | bash** seperti berikut ini:

```
pihole@pihole-VirtualBox:~$ curl -sSL https://install.pi-hole.net | bash
```

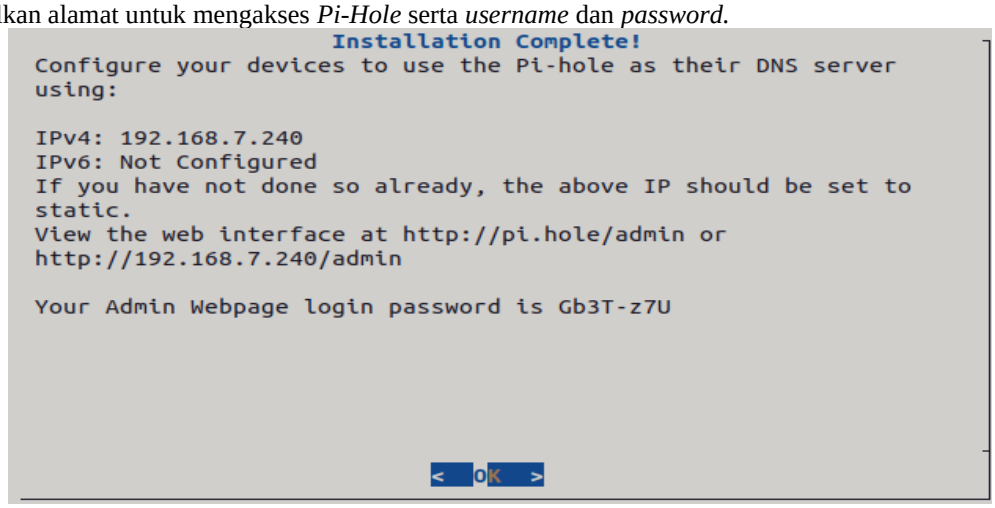
Gambar 4. Perintah *Install Pi-Hole DNS Server*

Selanjutnya ikuti langkah yang muncul saat proses intalasi berjalan, seperti yang ditunjukkan gambar 5 yakni diminta untuk memilih *upstreame DNS provider*, dalam penelitian ini menggunakan **cloudflare**. Setalah itu ikuti langkahnya hinffa proses kompilasi pada *pi-hole.net* selesai.



Gambar 5. *Select Upstream DNS Provider*

Gambar 6 berikut ini merupakan kotak dialog bahwa proses instalasi sudah selesai atau komplit dan juga menampilkan alamat untuk mengakses *Pi-Hole* serta *username* dan *password.*



Gambar 6. Tampilan *Installation Complete*

Selanjutnya untuk menyelesaikan proses tahapan instalasi dan konfigurasi pada *Pi-Hole*, maka dapat mengakses yang ditampilkan pada *form login* dengan masukkan *user* dan *password* yang sudah diberikan, selanjutnya lakukan konfigurasi untuk mengaktifkan *Pi-Hole* seperti mengaktifkan *domains on adlist* dan *group management* sehingga *Pi-Hole* siap untuk digunakan seperti yang ditunjukkan pada gambar berikut ini:

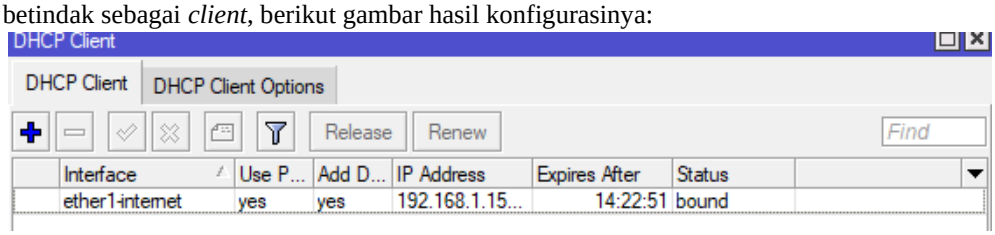
Gambar 7. Halaman *Web Admin Pi Hole*

3.1.3. Mikrotik Configuration

Perangkat Router Mikrotik RB931-2nd akan dijadikan sebagai media koneksi antara jaringan lokal ke *internet* dan juga untuk mengimplementasikan pada jaringan *hotspot*, berikut konfigurasi yang perlu dilakukan:

1) *DHCP Client Configuration*

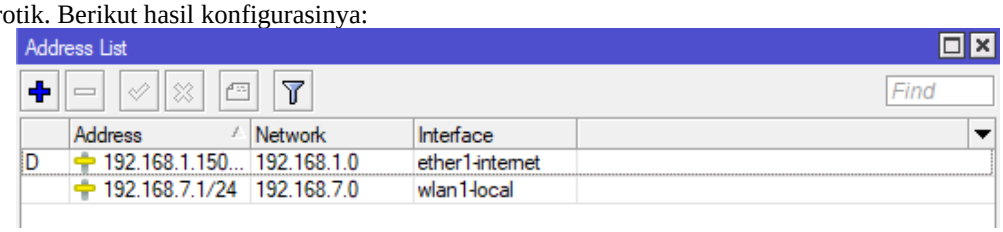
Pada penelitian ini sumber internet yang digunakan mendapatkan alokasi alamat IP secara dinamis (DHCP) yang betindak sebagai *client*, berikut gambar hasil konfigurasinya:



Gambar 8. Hasil Konfigurasi *DHCP Client*

2) *WLAN Configuration*

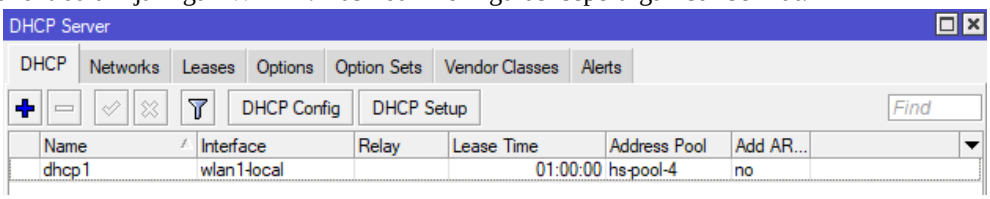
Untuk melakukan konfigurasi *wlan* pada penelitian ini dilakukan pada port *ethernet* jaringan *wlan1* dengan cara menuliskan perintah **ip address add address=192.168.7.1/24 interface=wlan1-Lokal** pada CLI *router* mikrotik. Berikut hasil konfigurasinya:



Gambar 9. Hasil Konfigurasi IP alamat wlan1-local

3) *DHCP Server Configuration*

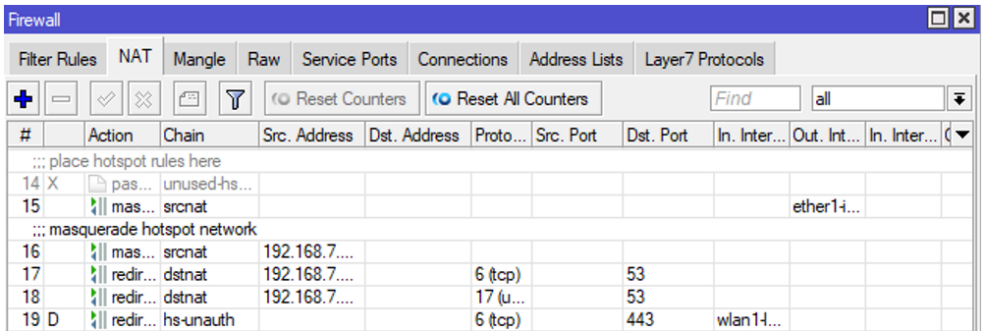
Pada penelitian ini pengaturan *DHCP Server* bertujuan untuk memberikan alokasi alamat IP secara dinamis pada *client* dalam jaringan WLAN. Hasil dari konfigurasi seperti gambar berikut:



Gambar 10. Hasil Konfigurasi *DHCP Server*

4) *Firewall NAT Configuration*

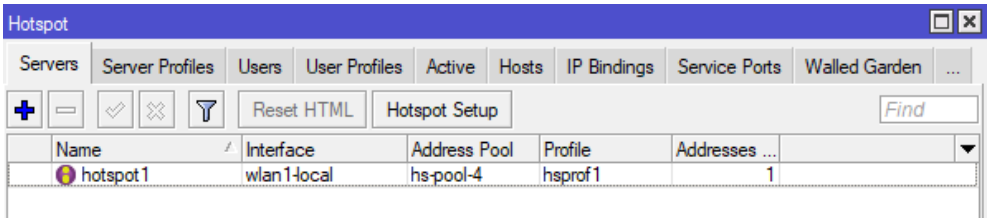
NAT atau *Network Address Translation* bertujuan untuk menerjemahkan alamat IP *public* ke alamat IP *local/private* atau sebaliknya. Berikut hasil konfigurasinya:



Gambar 11. Hasil Konfigurasi *Firewall NAT*

5) *Hotspot Configuration*

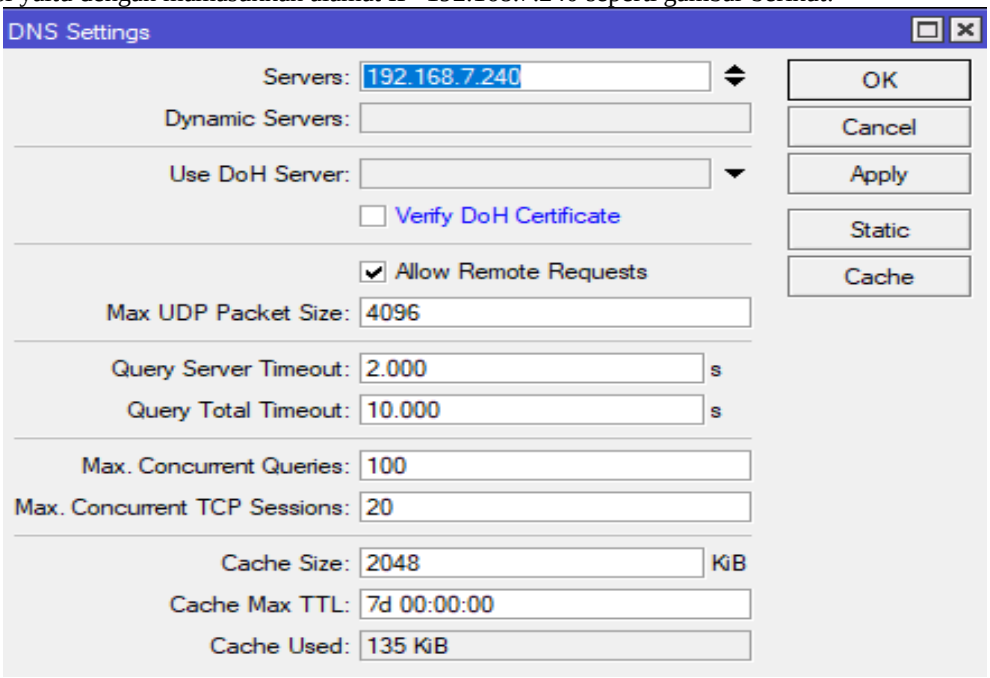
Selanjutnya konfigurasi *hotspot* di *router* mikrotik dapat dilakukan dengan cara mengklik menu IP → *hotspot* → tab menu *hotspot setup* → Pilih *hostspot interface* yaitu ether2-Lokal-WLAN → *local address* ether2-Lokal-WLAN yaitu 192.168.7.240/24 → *address pool* → *certificate (none)* → *SMTP server (default 0.0.0.0)* → *DNS* (otomatis dari sumber internet) → mengatu *local hostpot user*. Setelah konfigurasi selesai dilakukan maka *hotspot server* sudah bisa digunakan. Berikut gambar hasil konfigurasinya:



Gambar 12. Hasil Konfigurasi *Hotspot*

3.1.4. *Pi-Hole DNS Server*

Perlu dilukakan saat akan mengimplementasikan *Pi-Hole DNS server* pada jaringan *hotspot* adalah dengan cara mengubah DNS dari router menjadi alamat IP dari ubuntu server yang sebelumnya sudah dilakukan konfigurasi yaitu dengan mamasukkan alamat IP 192.168.7.240 seperti gambar berikut:



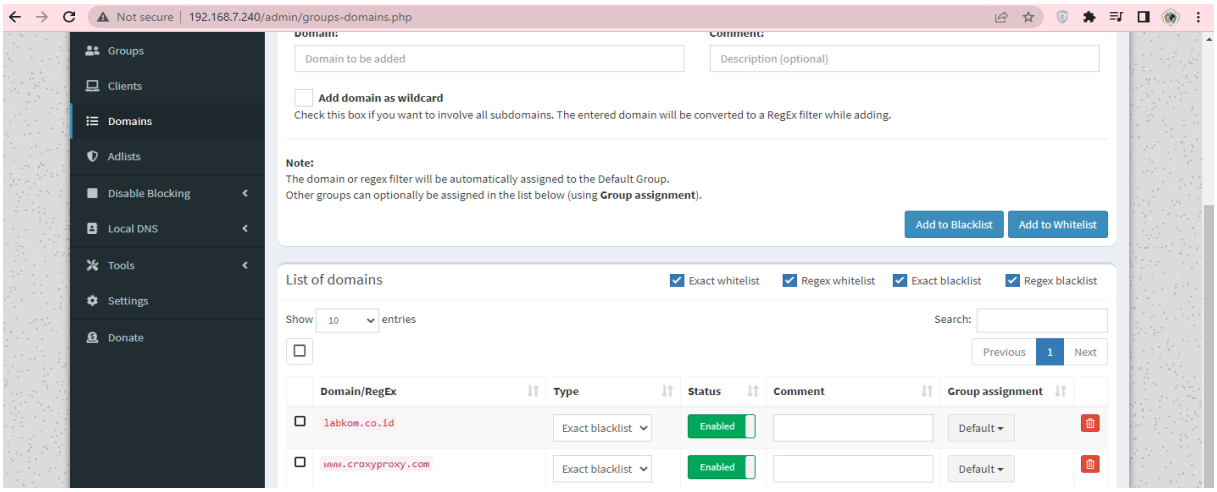
Gambar 13. Konfigurasi *DNS Router Mikrotik*

Gambar 13 diatas pada pilihan *allow remote request* untuk dicentang, supaya semuajaringanyang akan melalui *router* dapatmenggunakan layanan *Pi-HoleDNSServer*, setelah itu juga perlu dikonfigurasikan pada menu *Firewall→NAT*, untuk mamaksa *client-client* menggunakan *Pi-Hole DNS Server* atau dikenal dengan *transparent DNS*, dengan cara mengatur *chain- dst-NAT* dan *action redirect* ke *port* 53 dengan protokol *TCP* maupun *UDP* serta lakukan pengecualian pada *IP* dari *Pi-Hole DNS server* yaitu 192.168.7.240

3.2. *Pengujian dan Analisis*

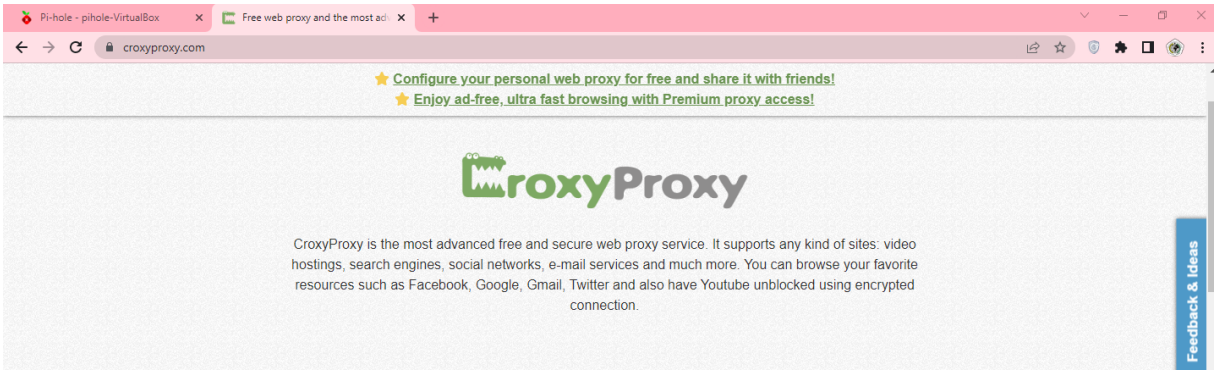
3.2.1. *Pengujian Web Filtering*

Pengujian pertama yaitu mencoba menyaring atau memblokir situs-situs yang mengandung situs negatif dari jaringan *hotspot*. Gambar 14 berikut ini menunjukkan hasil penyaringan *website*, untuk melihat hasilnya terdapat pada menu *Domains.*

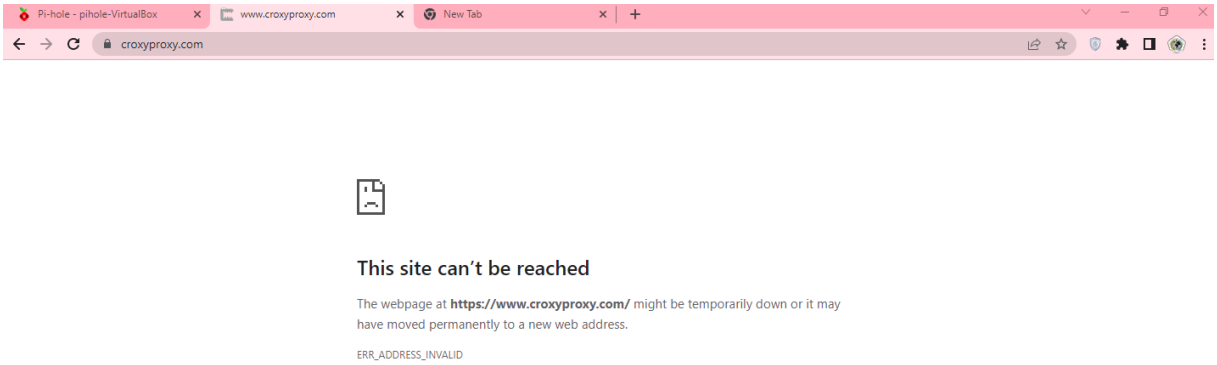


Gambar 14. Hasil Pengujian *Filtering Website*

Pengujian *web filtering* ini dilakukan pada *website* www.croxyproxy.com dengan 2 (dua) skenario, yaitu pengujian *website* sebelum difilter dan *website* setelah difilter menggunakan *Pi-Hole*. Hasil pengujian ditunjukkan pada gambar 15 yaitu tampilan *website* sebelum menerapkan *Pi-Hole DNS Server*. Sedangkan gambar 16 adalah tampilan *website* setelah menerapkan *Pi-Hole DNS Server* terlihat bahwa alamat *website* www.croxyproxy.com sudah tidak bisa diakses lagi.



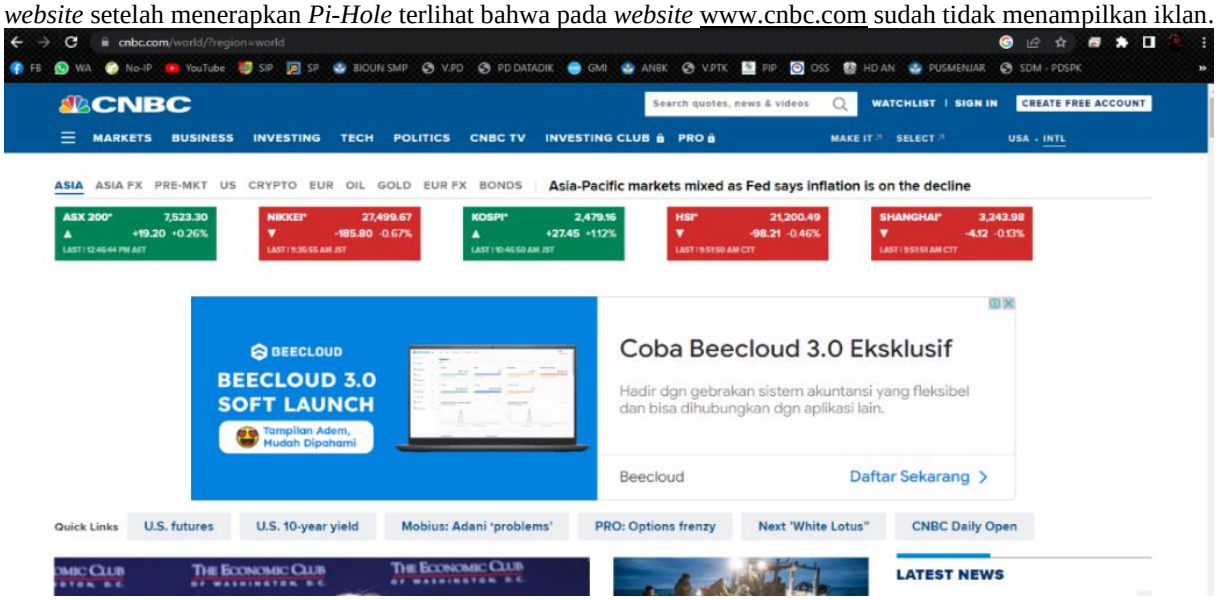
Gambar 15. Hasil Pengujian Sebelum Penerapan *Pi Hole DNS Server*



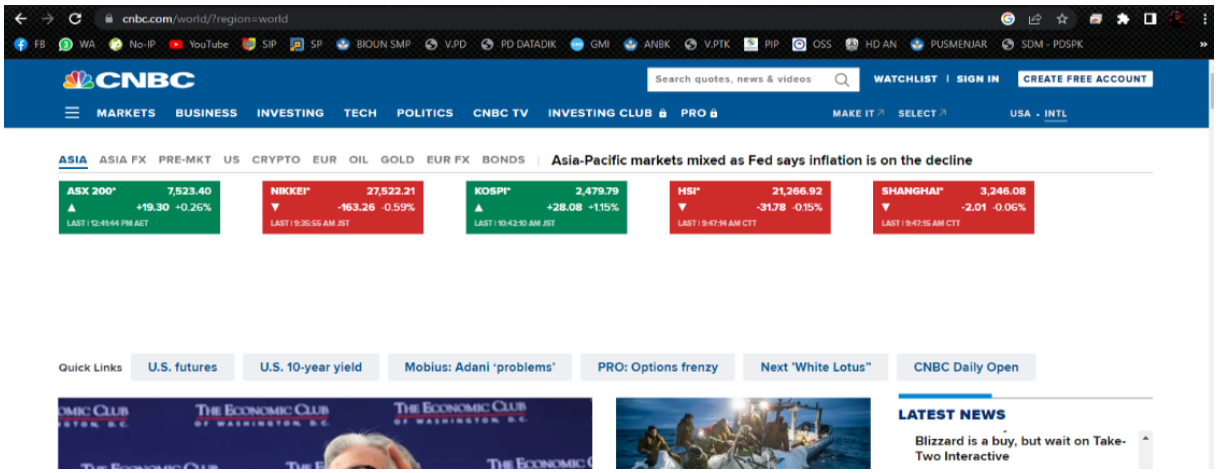
Gambar 16. Hasil Pengujian Setelah Penerapan *Pi Hole DNS Server*

3.2.2. Pengujian Blokir Iklan

Pengujian blokir iklan dilakukan pada *website* cnbc.com dengan 2 (dua) skenario, yaitu pengujian iklan sebelum diblok dan iklan setelah diblok. Hasil pengujian ditunjukkan pada gambar 17 yaitu tampilan *website* sebelum menerapkan *Pi-Hole*, pada *website* tersebut iklan masih muncul. Sedangkan gambar 18 adalah tampilan *website* setelah menerapkan *Pi-Hole* terlihat bahwa pada *website* www.cnbc.com sudah tidak menampilkan iklan.



Gambar 17. Hasil Pengujian Sebelum Penerapan *Pi Hole DNS Server*



Gambar 18. Hasil Pengujian Sesudah Penerapan *Pi Hole DNS Server*

3.2.3. *Pengujian QoS*

Pengujian *Qualty of Service (QoS)* atau kualitas jaringan dilakukan untuk mengetahui bahwa kualitas jaringan *hotspot* tetap bagus.

Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit (snaplen)
Wi-Fi	0 (0.0%)	none	Ethernet	262144 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	66393	66393 (100.0%)	—
Time span, s	30.168	30.168	—
Average pps	2200.8	2200.8	—
Average packet size, B	823	823	—
Bytes	54671023	54671023 (100.0%)	0
Average bytes/s	1812 k	1812 k	—
Average bits/s	14 M	14 M	—

Gambar 19. Hasil *ScreenshotWireshark*

Gambar 19 menunjukkan hasil *screenshot* analisis kualitas jaringan menggunakan *tool wireshark*, nilai-nilai dari hasil *screenshot* diatas digunakan sebagai dasar perhitungan secara manual pengujian *QoS* berikut ini:

1) Perhitungan *Delay*

Rerata *delay* = Total delay / Total paket yang diterima
= 30.168 s / 66393
= 0.00045 s
= 0.45 ms

2) Perhitungan *Jitter*

Jitter = Total variasi delay / (Total packet yang diterima-1)
= 2200.8 s / (66393-1)
= 2200.8 s / 66392
= 0.0331s
= 3.31 ms

3) Perhitungan *Packet Loss*

Packet Loss = ((66393-66393) : 66393) x 100%
= 0%

4) Perhitungan *Throughput*

Throughput merupakan jumlah total kedatangan paket yang sukses diamati pada sisi *client*/tujuan selama selang waktu tertentu dibagi oleh durasi selang waktu tersebut. Dari screenshot data yang telah dilakukan dengan *wireshark* maka didapatkan *throughput* dengan cara perhitungan sebagai berikut:

Throughput = (54671023 byte / 30.168 s)
= 1812,2190 byte
= 1812 k

3.3. Hasil

Setelah dilakukan implementasi *Pi Hole DNS server*, pengujian *filtering* pada situs dan blok terhadap iklan serta mengamati kualitas jaringan, ditunjukkan pada tabel berikut ini:

Tabel 1. Hasil dan Evaluasi *Filtering*

No	Pengujian	*Domain*	*Client*	*Action*	Keberhasilan
1	Website	www.croxyproxy.com	192.168.7.254	*Blacklist*	100%
2	Iklan	iklan beecloud di www.cnbc.com	192.168.7.254	*Blacklist*	100%

Pada tabel 1 dapat dijelaskaskan bahwa pengujian pada penelitian ini dilakukan terhadap 2 (dua) *website* dihasilkan keberhasilan 100% efektif dalam memfilter *website* dan memblokir iklan.

Tabel 2. Hasil dan Evaluasi Perhitungan *QoS*

No	Parameter *QoS*	Hasil
1	Rerata *delay*	0.45 ms
2	*Jitter*	3.31 ms
3	*Packet Loss*	0%
4	*Throughput*	1812 k

Pada tabel 2 dapat dijelaskaskan bahwa hasil perhitungan kualitas jaringan terhadap infrastruktur jaringan komputer yang mengimplementasikan *Pi Hole DNS Server* dapat dikategorikan baik dalam metode pengujian *Quality of Service (QoS).*

4. SIMPULAN

Bahwa implementasi *Pi-Hole DNS Server* terhadap topologi jaringan RT/RW Net berhasil dilakukan terbukti dapat memfilter atau menyaring *website* yang mengandung situs-situs negatif dan dapat memblokir iklan yang tidak diinginkan. Pada penelitian ini keberhasilan dalam memfilter tersebut dikategorikan 100% efektif, serta kualitas jaringan setelah penerapan *Pi-Hole DNS Server* berdasarkan perhitungan *QoS* dihasilkan nilai *throughput* sebesar 1812 k yang dikategorikan baik dalam metode pengujian dengan *Quality of Service (QoS).*

5. SARAN

Pada penelitian ini sudah dilakukan *filtering website* dan blokir iklan, namun masih belum ada *detail* daftar *website* dan iklan yang akan difilter. Oleh karena itu, untuk pengembagan kedepan dari penelitian ini perlu diklasifikasikan daftar situs yang perlu difilter dan iklan yang perlu diblokir. Hal ini, dapat bekerjasama dengan Kementerian Komunikasi dan Informatika (Kemkominfo) untuk mendapatkan daftar situs negatif dan iklan yang tidak diinginkan.

DAFTAR PUSTAKA

[1] A. M. Zakiyyah and M. Rahman, "Internet Service Provider (ISP) RT-RW NET," *J. Pengabdi. Masy. Ipteks*, vol. 7, no. 1, pp. 30–36, 2021.

[2] Y. I. Mukti, "Implementasi Jaringan Hotspot Kampus Menggunakan Router Mikrotik," *Indones. J. Comput. Sci.*, vol. 8, no. 2, pp. 130–138, 2019, doi: 10.33022/ijcs.v8i2.181.

[3] Wearesocial.com, "Digital 2022 Indonesia February 2022," 2022. https://datareportal.com/reports/digital-2022-indonesia (accessed Nov. 13, 2022).

[4] W. Setiawan, "Era Digital dan Tantangannya," in *Seminar Nasional Pendidikan*, 2017, pp. 1–9.

[5] Admin, "Internet Sehat dan Aman (INSAN)," *Web Kemkominfo*, 2013. https://www.kominfo.go.id/content/detail/3303/internet-sehat-dan-aman-insan/0/internet_sehat (accessed Nov. 16, 2022).

[6] Y. Sopyan, "Membahas Cara Kerja Pi-Hole," *Labkom.co.id*, 2020. https://labkom.co.id/mikrotik/membahas-cara-kerja-pi-hole (accessed Nov. 14, 2022).

[7] D. Satriawan and P. H. Trisnawan, "Implementasi Layanan DNS Sinkhole sebagai Pemblokir Iklan menggunakan Arsitektur Cloud," *Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 5, no. 2, pp. 759–768, 2021.

[8] W. Mukti and R. Widyarini, "Web Content Filtering," 2013. https://keamanan-informasi.stei.itb.ac.id/2013/10/30/web-content-filtering/ (accessed Nov. 17, 2022).

[9] O. Abdurahman, T. U. Kalsum, and Riska, "Penerapan Pi-Hole DNS Server Sebagai Ads-Blocker dan Sistem Filtering Website Pada Jaringan Hotspot," *J. Media Infotama*, vol. 18, no. 2, pp. 208–217, 2022.

[10] I. S. Ali, S. Hamza, and E. Gunawan, "Implementasi & Analisis Penerapan Pi-Hole Network Ad-Blocking Di Laboratorium Jaringan Teknik Informatika UMMU," *J-TIFA*, vol. 3, no. 1, pp. 27–31, 2020.

[11] B. K. Simpony, "Simple Queue Untuk Manajemen User dan Bandwidth di Jaringan Hotspot Menggunakan Mikrotik," *J. Inform.*, vol. 8, no. 1, pp. 87–92, 2021, doi: 10.31294/ji.v8i1.9385.

[12] E. Putra and R. A. Bugis, "Implementasi Hotspot dengan User Manager untuk Internet Wireless menggunakan Mikrotik RB-951ui di SMK Swasta Al-Washliyah Pasar Senen 2 Medan," *J. Teknol. Inf.*, vol. 3, no. 1, pp. 58–65, 2019, doi: 10.36294/jurti.v3i1.689.

[13] I. Sofana, *Jaringan Komputer Berbasis Mikrotik : Dilengkapi latihan dan contoh soal Mikrotik Training Certlfied Network Associated (MTCNA)*, Pertama. Bandung: Informatika, 2017.

[14] R. Wulandari, "Analisis QoS (Quality Of Service) Pada Jaringan Internet (Studi Kasus : UPT Loka Uji Teknik Penambangan Jampang Kulon–LIPI)," *J. Tek. Inform. dan Sist. Inf.*, vol. 2, no. 2, pp. 162–172, 2016, doi: 10.28932/jutisi.v2i2.454.

[15] T. Pratama, M. A. Irwansyah, and Yulianti, "Perbandingan Metode PCQ, SFQ, RED dan FIFO Pada Mikrotik Sebagai Upaya Optimalisasi Layanan Jaringan Pada Fakultas Teknik Universitas Tanjungpura," *J. Tek. Inform. Univ. Tanjungpura*, vol. 3, no. 1, 2015.

[16] M. Huda and Jusak, "Analisis Karakteristik Lalu Lintas Data Internet: Aplikasi Web Social Network," *J. Control Netw. Syst.*, vol. 4, no. 2, pp. 102–112, 2015.

[17] S. W. Pamungkas, Kusrini, and E. Pramono, "Analisis Quality of Service (QoS) Pada Jaringan Hotspot SMA Negeri XYZ," *J. Sist. Inf. dan Teknol. Inf.*, vol. 7, no. 2, pp. 142–152, 2018, doi: 10.36774/jusiti.v7i2.249.