E-ISSN : 2827-9425
P-ISSN : 2828-4666

Penerapan *Proxy Server* Pada Mikrotik Untuk *Blocking* Situs Negatif Di Jaringan Komputer

Rahmat Rafli Suleman[1], Irvan Abraham Salihi[2], Warid Yunus[3]

[1]Fakultas Ilmu Komputer, Program Studi Teknik Informatika, Ichsan Gorontalo, Kota Gorontalo, Indonesia.
[1]Fakultas Ilmu Komputer, Program Studi Teknik Informatika, Ichsan Gorontalo, Kota Gorontalo, Indonesia.
[1]Fakultas Ilmu Komputer, Program Studi Teknik Informatika, Ichsan Gorontalo, Kota Gorontalo, Indonesia.
Email: [1]rahmatid39@email.com, irvanabrahams@gmail.com, warid.dsn@gmail.com

Abstrak - Penelitian ini bertujuan untuk mengatasi masalah akses terhadap situs negatif di Laboratorium Fakultas Ilmu Komputer Universitas Ichsan Gorontalo melalui penerapan *proxy server* pada Mikrotik. Masalah yang dihadapi adalah banyaknya mahasiswa yang membuka situs dengan konten negatif, seperti *pornografi* dan perjudian, yang dapat mengganggu proses pembelajaran dan suasana akademis. Metode yang digunakan dalam penelitian ini meliputi beberapa tahapan: analisis kebutuhan sistem, perancangan dan konfigurasi router Mikrotik, pembuatan *proxy server* menggunakan perangkat lunak Squid, serta pengujian sistem yang telah diimplementasikan. Dalam tahap analisis, dilakukan identifikasi terhadap situs-situs negatif yang sering diakses dan kebutuhan perangkat keras dan perangkat lunak yang diperlukan. Selanjutnya, tahap implementasi mencakup konfigurasi Mikrotik untuk memblokir akses VPN dan penetapan *proxy server* untuk menyaring konten negatif. Pengujian sistem dilakukan dengan membandingkan kondisi sebelum dan sesudah penerapan konfigurasi, serta pengamatan terhadap efektivitas pemblokiran situs dan akses VPN. Hasil penelitian menunjukkan bahwa kombinasi antara Mikrotik dan proxy server terbukti efektif dalam memblokir situs negatif dan mengurangi akses melalui VPN hingga 80%. Hal ini disebabkan oleh kemampuan Mikrotik dalam mengidentifikasi dan memblokir IP address VPN yang sering digunakan, serta efisiensi *proxy server* dalam menyaring lalu lintas internet. Kesimpulan dari penelitian ini adalah bahwa penerapan konfigurasi tersebut dapat meningkatkan keamanan dan kenyamanan penggunaan internet di lingkungan pendidikan, serta memberikan acuan untuk pengembangan sistem keamanan jaringan yang lebih efektif di masa mendatang. Penelitian ini diharapkan dapat memberikan kontribusi signifikan dalam upaya pengelolaan akses internet yang aman dan terkendali di institusi pendidikan.

Kata Kunci: Proxy Server, Mikrotik, Situs Negatif, Jaringan Komputer, Blokir VPN

Abstract - *This research aims to overcome the problem of accessing negative sites in the Laboratory of the Faculty of Computer Science, Universitas Ichsan Gorontalo by applying a proxy server on Mikrotik. The problem faced is that many students opensites with negative content, such as pornography and gambling, which can disruptthe learning process and academic atmosphere. The method used in this research includes several stages, namely the system needs analysis, Mikrotik router's designand configuration, development of a proxy server using Squid software, and testingthe implemented system. The analysis stage includes the identification of negative sites often accessed and the hardware and software required to carry out. Furthermore, the implementation stage includes configuring Mikrotik to block VPNaccess and establishing a proxy server to filter the negative contents. System testingis done by comparing the conditions before and after the implementation of the configuration, as well as observing the effectiveness of site blocking and VPN access. The results show that the combination of Mikrotik and proxy servers is proven to be effective in blocking negative sites and reducing access via VPN by 80%. It is due to Mikrotik's ability to identify and block frequently used VPN IP addresses and the efficiency of proxy servers in filtering internet traffic. The conclusion of this research is that the application of these configurations can improve the security and comfort of internet use in an educational environment andprovide a reference for a more effective network security system development in thefuture. This research is expected to make a significant contribution to efforts to manage secure and controlled internet access in educational institutions.*

Keywords: *Proxy Server, Mikrotik, negative sites, computer network, VPN blocking*

E-ISSN : 2827-9425
P-ISSN : 2828-4666

1. PENDAHULUAN

Kemajuan teknologi komunikasi sangat pesat, namun dimanfaatkan oleh pihak tidak bertanggung jawab untuk bisnis ilegal seperti pornografi, penipuan, perdagangan narkoba, dan jual beli senjata. Hal ini berdampak negatif pada masyarakat, terutama pada anak-anak dan orang dewasa, serta mengganggu proses pendidikan. Meskipun internet membawa dampak positif dalam pendidikan, juga terdapat risiko paparan konten negatif yang merugikan, seperti berita palsu dan kekerasan.[1] Di Fakultas Ilmu Komputer Universitas Ichsan Gorontalo, akses internet yang digunakan untuk pembelajaran sering disalahgunakan untuk mengunjungi situs terlarang, mengganggu suasana akademis. Menurut KOMINFO, dari Januari hingga Oktober 2017, konten pornografi mendominasi pemblokiran dengan 16.902 kasus, dan data 2022 menunjukkan konten pornografi masih tertinggi dengan 1.142.010 pemblokiran.[2] KOMINFO berupaya memerangi situs merugikan, namun akses tetap dimungkinkan melalui VPN.[2] Peneliti di Fakultas Ilmu Komputer akan memblokir IP VPN dan mengonfigurasi router mikrotik serta proxy server untuk membatasi akses ke situs negatif. Kombinasi mikrotik dan proxy server akan menciptakan lapisan keamanan yang efektif untuk mengelola akses internet, menghindari konten berbahaya.

2. TINJAUAN PUSTAKA

2.1 Analisa

Analisis, juga dikenal sebagai "analisis", adalah proses menguraikan ide ke dalam bagian yang lebih kecil sehingga struktur logisnya menjadi jelas.

2.2. Jaringan Komputer

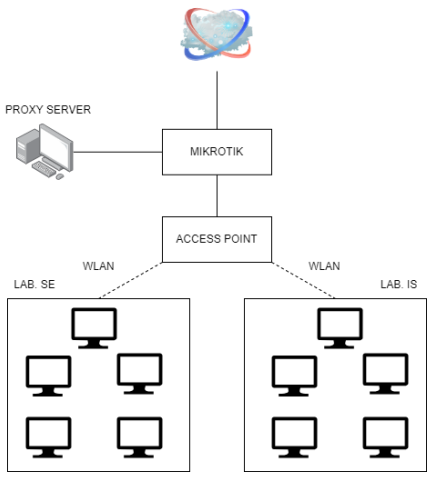
Menurut pengertian yang ada, jaringan komputer merujuk pada sekumpulan interkoneksi antara beberapa komputer. Dalam istilah yang lebih sederhana, jaringan komputer adalah gabungan beberapa komputer dan perangkat seperti router dan switch yang saling terhubung melalui berbagai jenis media, seperti media kabel atau nirkabel.[3] Melalui media ini, informasi berupa data dapat mengalir dari satu komputer ke komputer lainnya atau bahkan dari satu komputer ke perangkat lain. Hasilnya, komputer-komputer yang saling terhubung ini dapat saling bertukar data dengan lancar.[4]

2.3. Firewall

Firewall, juga dikenal sebagai "tembok api", adalah sistem yang melindungi jaringan dari ancaman dengan menggunakan aturan khusus untuk menentukan tindakan terhadap paket data. Efektivitas firewall bergantung pada kebijakan keamanan yang diterapkan. Semakin ketat kebijakan, semakin kompleks konfigurasi jaringan, dan sebaliknya, kebijakan yang lemah memungkinkan lebih banyak akses namun meningkatkan risiko keamanan.[5]

2.3. Proxy Server

Proxy server berfungsi sebagai perantara antara komputer pengguna dan server tujuan di internet. Ketika pengguna menggunakan *proxy server* untuk mengakses internet, permintaan mereka akan diarahkan terlebih dahulu ke *proxy server*, yang kemudian meneruskannya ke server tujuan. Setelah menerima tanggapan dari server tujuan, *proxy server* akan meneruskannya kembali ke pengguna.[6]



Gambar 2. 1. Rancangan Topologi Jaringan

E-ISSN : 2827-9425
P-ISSN : 2828-4666

3. METODE PENELITIAN

3.1 Pengumpulan Data

a. Data Primer

Data primer dikumpulkan melalui observasi langsung pada router Mikrotik di Laboratorium Fakultas Ilmu Komputer Universitas Ichsan Gorontalo dan wawancara dengan karyawan bagian jaringan. Metode ini memungkinkan pengumpulan data langsung dari sumbernya, yaitu staf berpengalaman dalam manajemen jaringan dan perangkat Mikrotik, serta memberikan pemahaman praktis tentang pengaturan dan pengelolaan jaringan laboratorium. Data ini menjadi landasan utama untuk analisis penelitian.

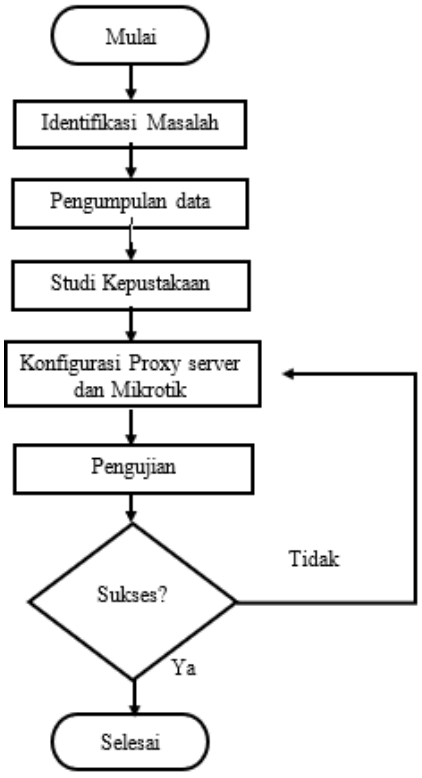
b. Data Sekunder

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

3.2 Desain Sistem

Untuk melindungi jaringan komputer dari situs web negatif, sistem yang direncanakan menggabungkan MikroTik Router dan *proxy server*. Komputer klien terhubung ke router MikroTik sebagai gateway, yang kemudian mengarahkan lalu lintas HTTP dan HTTPS ke *proxy server*. mikrotik berfungsi sebagai perantara antara klien dan internet, dan konfigurasi dilakukan untuk memastikan bahwa lalu lintas HTTP dan HTTPS diblokir dengan benar. Untuk memastikan kinerja dan keamanan sistem, uji coba dan pemeliharaan dilakukan, yang mencakup pemantauan kinerja jaringan dan pembaruan berkala terhadap daftar situs yang dilarang. Akibatnya, sistem ini menjaga pengguna dari konten yang tidak diinginkan atau berbahaya sambil mengontrol lalu lintas internet di jaringan.

3.3 Pemodelan



Gambar 3. 1. Alir Penelitian

3.4 Pengujian Sistem

Pengujian sistem dalam penelitian ini difokuskan pada evaluasi efisiensi penerapan *proxy server* dan router MikroTik. Proses pengujian melibatkan pemantauan kinerja *proxy server* dalam memblokir situs web berbahaya, serta melakukan filtrasi terhadap lalu lintas internet. Evaluasi juga mencakup penilaian kemampuan *Proxy server* dan MikroTik dalam mengatur akses internet di lingkungan Fakultas Ilmu Komputer, Universitas Ichsan Gorontalo. Aspek yang di uji tingkat keberhasilan pemblokiran situs web yang telah diidentifikasi sebagai potensial merugikan. Selain itu, pengujian ini juga mengevaluasi sejauh mana kombinasi kedua *proxy* tersebut dapat mengurangi penggunaan VPN yang umumnya digunakan untuk mengakses konten terlarang. Dengan

E-ISSN : 2827-9425
P-ISSN : 2828-4666

harapan bahwa hasil pengujian dapat memberikan pemahaman mendalam terkait performa dan keamanan sistem *proxy server* yang diImplementasikan.

4. HASIL DAN PEMBAHASAN

4.1. Analisis dan Implementasi Sistem

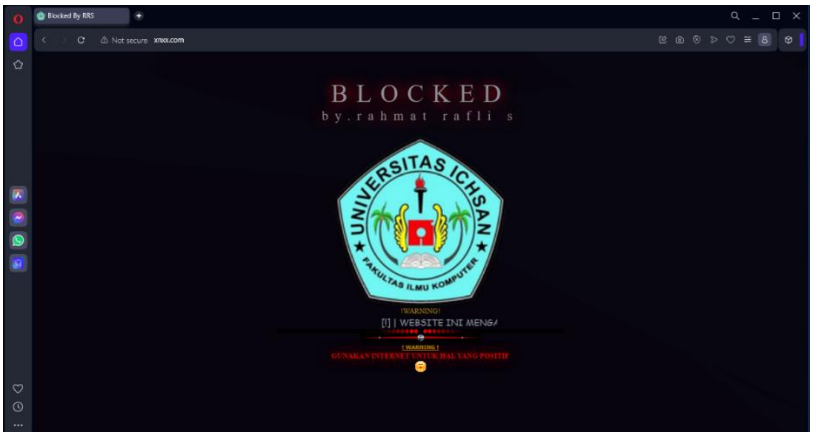
Analisis kebutuhan sistem mencakup perangkat keras dan perangkat lunak yang diperlukan untuk mengimplementasikan proxy server dan router Mikrotik. Sistem ini bertujuan untuk meningkatkan keamanan jaringan dan mengontrol akses internet. Implementasi dilakukan melalui beberapa tahap, yaitu:

a. Konfigurasi proxy server penetapan daftar situs blokir dengan Squid di sistem operasi Ubuntu.
b. Konfigurasi Mikrotik untuk mengelola lalu lintas data dan akses VPN.

4.2. Pengujian Imlementasi sistem

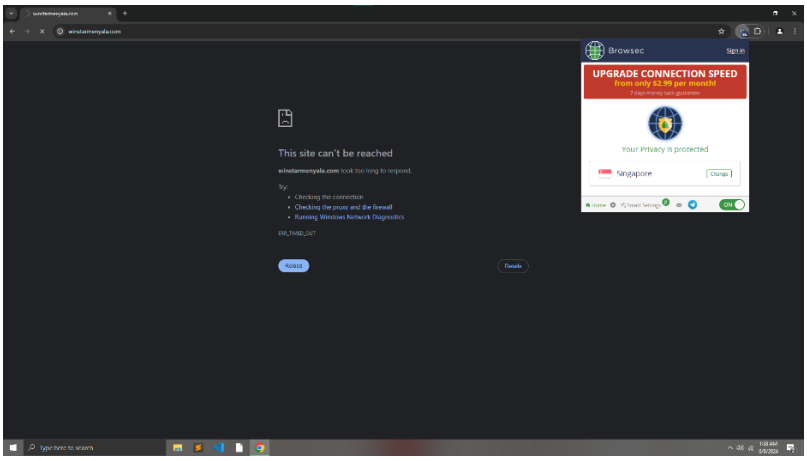
Pengujian dilakukan untuk mengevaluasi efektivitas penerapan proxy server dan Mikrotik. Beberapa pengujian meliputi:

a. Pengujian sesudah menerapkan proxy server menunjukkan keberhasilan proxy server dalam memblokir situs.



Gambar 4. 1. Hasil Blokir Proxy Server

b. Pengujian VPN sesudah menerapkan konfigurasi Mikrotik menunjukkan keberhasilan dalam memblokir VPN.



Gambar 4. 2. Hasil Blokir Mikrotik

E-ISSN : 2827-9425
P-ISSN : 2828-4666

4.3. Pembahasan Sistem

4.3.1. Tabel Penetapan Address List VPN

Tabel ini menyajikan hasil penetapan alamat IP untuk VPN yang telah dikumpulkan melalui cache DNS.

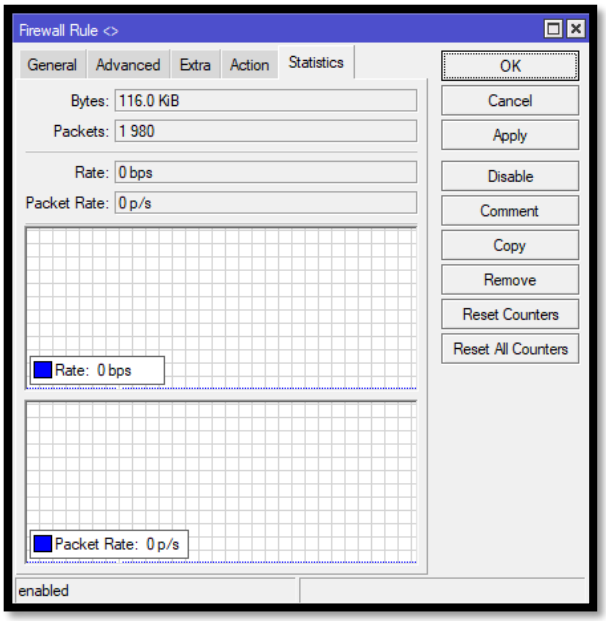
Tabel 4. 1. Penetapan Address List VPN

Nama List	IP Address	Status Akses
Blacklist VPN	162.210.0.0/16	Drop
Blacklist VPN	207.244.0.0/16	Drop
Blacklist VPN	161.35.0.0/16	Drop
Blacklist VPN	50.7.0.0/16	Drop
Blacklist VPN	23.106.0.0/16	Drop
Blacklist VPN	83.136.0.0/16	Drop
Blacklist VPN	94.237.0.0/16	Drop
Blacklist VPN	95.111.0.0/16	Drop
Blacklist VPN	209.94.0.0/16	Drop
Blacklist VPN	185.123.0.0/16	Drop
Blacklist VPN	167.71.0.0/16	Drop
Blacklist VPN	157.245.0.0/16	Drop
Blacklist VPN	178.128.0.0/16	Drop
Blacklist VPN	198.16.0.0/16	Drop

Data tersebut merupakan hasil sementara yang akan divalidasi melalui prosedur capture DNS untuk memastikan akurasi.

4.3.2. Hasil Tampilan Statistik Sebelum Akses VPN Masuk

Tampilan monitoring statistik menunjukkan bahwa sebelum implementasi VPN, tidak ada aktivitas trafik data yang terdeteksi.



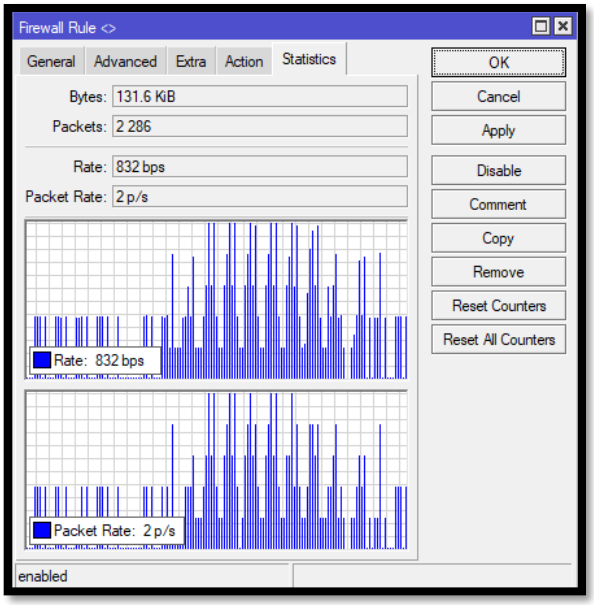
Gambar 4. 3. Statistik Sebelum Akses VPN

Ini berarti komputer tidak mengirim atau menerima data melalui firewall rule sebelum VPN diimplementasikan.

E-ISSN : 2827-9425
P-ISSN : 2828-4666

4.3.3. Hasil Tampilan Statistik Saat Akses VPN Masuk

Setelah akses VPN dimulai, tampilan statistik menunjukkan adanya trafik data yang signifikan.



Gambar 4. 4. Statistik setelah Akses VPN

Ini menandakan bahwa konfigurasi VPN berhasil dan mulai mengarahkan lalu lintas data melalui jalur yang aman.

4.3.4. Tabel Hasil Log Akses Real-Time pada Squid

Log akses real-time pada Squid menunjukkan data aktivitas pengguna secara langsung. Ini membantu dalam memantau dan mengontrol akses ke situs-situs yang telah diblokir.

Tabel 4. 2. Log Akses Real Time

Log akses		Status Akses	Keterangan
IP Address PC	**Situs web**		
192.168.200.241	x.com	Denied	Media Sosial
	youtube.com	Allow	Platform Vidio
192.168.200.244	xnxx.com	Denied	Situs Dewasa
	alsoporn.com		Situs Dewasa
	maha168heya.com		Judi Online
192.168.200.239	pornhub.com	Denied	Situs Dewasa
	winstarmenyala.com		Judi Online
192.168.200.235	tiktok.com	Allow	Platform vidio
192.168.200.252	x.com	Denied	Media Sosial
	youtube.com	Allow	Platform vidio
	alsoporn.com	Denied	Situs Dewasa
192.168.200.247	xnxx.com	Denied	Situs Dewasa
	alsoporn.com		Situs Dewasa
	maha168heya.com		Judi Online
192.168.200.246	pornhub.com	Denied	Situs Dewasa
	xnxx.com		Situs Dewasa
192.168.200.234	tiktok.com	Allow	Platform vidio
192.168.200.236	x.com	Denied	Media Sosial
	instagram.com	Allow	Media Sosial
	alsoporn.com	Denied	Situs Dewasa

E-ISSN : 2827-9425
P-ISSN : 2828-4666

4.3.5. Tabel Hasil *Capture* DNS Oleh Script

Capture DNS memastikan validitas dan akurasi data alamat IP dengan menangkap dan memverifikasi permintaan DNS secara langsung saat terjadi. Ini memberikan gambaran lebih akurat tentang konfigurasi jaringan dan kinerjanya.

Tabel 4. 3. Hasil Capture DNS

Browsec VPN		**Status Akses**		
IP Location	**IP Address**	**Chrome**	**Opera Browser**	**Microsoft Edge**
Singapure	23.106.249.35	Drop	Drop	Drop
	23.106.249.34	Drop	Drop	Drop
	23.106.249.39	Drop	Drop	Drop
	23.106.249.36	Drop	Drop	Drop
	23.106.249.53	Drop	Drop	Drop
	23.106.249.52	Drop	Drop	Drop
	23.106.249.44	Drop	Drop	Drop
	23.106.249.54	Drop	Drop	Drop
	23.106.249.37	Drop	Drop	Drop
United Kingdom	23.106.56.12	Drop	Drop	Drop
	23.106.56.54	Drop	Drop	Drop
	23.106.56.13	Drop	Drop	Drop
	23.106.56.52	Drop	Drop	Drop
	23.106.56.36	Drop	Drop	Drop
	23.106.56.14	Drop	Drop	Drop
	23.106.56.19	Drop	Drop	Drop
	23.106.56.11	Drop	Drop	Drop
	23.106.56.53	Drop	Drop	Drop
	23.106.56.43	Drop	Drop	Drop
	23.106.56.22	Drop	Drop	Drop
	23.106.56.35	Drop	Drop	Drop
	23.106.56.37	Drop	Drop	Drop
	23.106.56.51	Drop	Drop	Drop
United Stated	162.210.194.1	Drop	Drop	Drop
	207.244.71.82	Drop	Drop	Drop
	207.244.89.161	Drop	Drop	Drop
	207.244.71.80	Drop	Drop	Drop
	207.244.89.166	Drop	Drop	Drop
	162.210.194.4	Drop	Drop	Drop
	162.210.194.3	Drop	Drop	Drop
	162.210.194.2	Drop	Drop	Drop
	207.244.71.79	Drop	Drop	Drop
	207.244.71.84	Drop	Drop	Drop
	207.244.71.81	Drop	Drop	Drop

E-ISSN : 2827-9425
P-ISSN : 2828-4666

5. KESIMPULAN

1. Sistem yang dirancang berhasil dan mampu memblokir akses ke situs web negatif secara efektif. Penggunaan *proxy server* berhasil memblokir situs-situs yang dianggap peneliti merugikan atau tidak pantas, seperti x.com dan porn*ub.com, sehingga tidak dapat diakses melalui jaringan laboratorium.
2. Sistem yang diterapkan juga menunjukkan kemampuan dalam mengurangi penggunaan VPN untuk mengakses konten terlarang. Analisis DNS *capture* menunjukkan bahwa filter rules yang diterapkan membuat penggunaan VPN untuk mengakses situs negatif menjadi kurang efektif.

DAFTAR PUSTAKA

[1] W, Y., Fitriana, Y. B., Susanto, A., Susanto, E. S., & Hamdani, F. (2022). Implemetasi *Filtering* Alamat Website Pada *Proxy Server* Menggunakan Raspberry-Pi. *Jurnal Informatika: Jurnal Pengembangan It (Jpit), Vol.7, No.1*.

[2] Ferrissa, W. (2017, November 30). *Ini Konten Negatif Yang Dominan Di Indonesia*. Retrieved From Kementerian Komunikasi Dan Informatika Ri: Https://Www.Kominfo.Go.Id/*Content*/Detail/11711/Ini-Konten-Negatif-Yang-Dominan-Di-Indonesia/0/Sorotan_Media

[3] Drajana, I. C. R., & Bode, A. (2021). Simulasi Jaringan Menggunakan Cisco Packe Tracer. *Simtek: Jurnal Sistem Informasi Dan Teknik Komputer*, *6*(1), 24-27.

[4] Bangun, Cindya Novira. "Jaringan Komputer." (2022).

[5] Tangahu, R. A., Bode, A., & Taliki, S. (2024). Analisa Kualitas Layanan Jaringan Internet Pada Wireless Lan Menggunakan Metode Qos (Quality Of Service). *Jurnal Ilmiah Ilmu Komputer Banthayo Lo Komputer*, *3*(1), 23-30.

[6] Towidjojo, R. (2023). *Mikrotik Kung Fu: Kitab 1 (Edisi 2019)*. Jasakom.