Institut Riset dan Publikasi Indonesia (IRPI)
MALCOM: Indonesian Journal of Machine Learning and Computer Science
Journal Homepage: https://journal.irpi.or.id/index.php/malcom
Vol. 4 Iss. 2 April 2024, pp: 647-655
ISSN(P): 2797-2313 | ISSN(E): 2775-8575

Network Security Optimization Against Online Gambling and Pornography Sites Using DNS Filtering and Orangepi

Optimasi Keamanan Jaringan Wifi dari Situs Judi *Online* dan Pornografi dengan DNS *Filtering* dan Orangepi

Dadang Iskandar Mulyana[1*], Ferry Ardiyansyah[2], Nurhikmah Hidayat[3], Ahmad Zulfikar[4]

[1,2,3,4]Program Studi Teknik Informatika,
Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika, Indonesia

E-Mail: [1]mahvin2012@gmail.com, [2]ardiyansyahferry@gmail.com,
[3]nurhikmahhidayay@gmail.com, [4]ahmadzulfikar662@gmail.com

Received Jan 02nd 2024; Revised Feb 05th 2024; Accepted Mar 17th 2024
Corresponding Author: Dadang Iskandar Mulyana

Abstract

In this digital era, internet usage has become a basic necessity. Despite its significant benefits, internet usage is often abused, particularly concerning access to adult and online gambling sites. Additionally, network security is a crucial concern due to potential digital crimes like data theft and malware dissemination that can harm users. Therefore, the author conducted research by implementing DNS filtering as a solution. This study aimed to restrict access to sites with negative content and those prohibited by religious or legal standards. To achieve a positive internet environment, the researcher studied DNS filtering systems applied to the WIFI network of Balaiwarga RW 32 in North Bekasi. The DNS filtering method functions by filtering network traffic, and if unauthorized website access is detected, the system restricts access to that website. The research yielded positive results, effectively limiting internet access. During December 24-31, 10,102 ad logs, 65 online gambling site logs, and 16 adult site logs were blocked. It is concluded that this network security optimization effectively restricts community internet activities by blocking negative content, including pornography, and online gambling sites.

Keyword: DNS Filtering, Negative Site Filter, Orange Pi, RW 32 Bekasi, WIFI Network Security Optimization

Abstrak

Di era digital ini, penggunaan internet telah menjadi kebutuhan pokok. Meskipun internet memberikan manfaat yang besar, penggunaannya seringkali disalahgunakan, terutama terkait dengan akses ke situs dewasa dan judi *online*. Selain itu, keamanan jaringan juga menjadi perhatian penting mengingat adanya potensi kejahatan digital, seperti pencurian data dan penyebaran malware yang dapat merugikan pengguna. Oleh karena itu, penulis melakukan penelitian dengan menerapkan metode DNS *filtering* sebagai solusi. Penelitian ini bertujuan untuk membatasi akses situs-situs yang memiliki konten negatif dan yang tidak diperbolehkan oleh agama maupun secara hukum negara. Dalam mewujudkan internet positif ini peneliti melakukan penelitian sistem DNS *filtering* yang diterapkan pada jaringan WIFI Balaiwarga RW 32 Bekasi Utara. Kinerja dari dari metode DNS *filtering* adalah dengan melakukan *filtering* pada lalu lintas jaringan dan jika ditemukan akses ke *website* yang tidak diperbolehkan maka sistem melakukan pembatasan *website* tersebut. Hasil penilitian berjalan dengan baik dapat melakukan pembatasan akses internet, dalam rentan waktu tanggal 24-31 Desember ditemukan log yang ter-blokir yaitu sebanyak 10.102 *Log* Ads, 65 *Log* situs judi *online*, dan 16 *Log* situs dewasa. Maka disimpulkan bahwa optimasi keamanan jaringan ini efektif melakukan pembatasan aktivitas masyarakat dalam mengakses internet dengan memblokir konten negatif termasuk pornografi, dan situs perjudian *online*.

Kata Kunci: DNS Filtering, Filter Situs Negatif, Optimasi Keamanan Jaringan WIFI, Orange Pi, RW 32 Bekasi

1. PENDAHULUAN

Pada era digital saat ini, akses internet telah menjadi kebutuhan utama bagi masyarakat Indonesia. Pemanfaatan internet telah mengubah pola hidup dan budaya manusia dalam berkegiatan sehari-hari, seperti belajar, bekerja, berkomunikasi, berbelanja, dan aspek lainnya [1]. Berdasarkan data dari APJII, penetrasi internet di Indonesia pada tahun 2022 mencapai 77,1%. Angka ini menunjukkan bahwa semakin banyak

masyarakat Indonesia yang menggunakan internet. Pemanfaatan internet di Indonesia didominasi oleh kalangan usia muda, yaitu 13-18 tahun (99,16%) dan 19-34 tahun (98,64%) [2][3]. Kelompok usia ini memanfaatkan internet untuk berbagai keperluan, seperti belajar, bekerja, dan hiburan. Internet memiliki banyak manfaat, namun juga memiliki risiko, seperti penyalahgunaan internet untuk mengakses konten negatif, seperti pornografi, judi, dan *phishing*. Remaja adalah kelompok yang paling rentan terhadap penyalahgunaan internet [4]. Oleh karena itu, perlu ada upaya serius untuk memberikan pengetahuan dan keterampilan yang benar dalam memanfaatkan kemajuan teknologi internet. Jaringan WIFI merupakan sarana yang penting bagi masyarakat saat ini [5]. Namun, jaringan WIFI juga rentan terhadap ancaman keamanan, salah satunya adalah akses ke situs judi *online* dan pornografi.

Dalam masa lalu, permainan judi mengharuskan pemainnya bertemu secara langsung, mungkin dengan orang yang nyata, dan membayar dengan uang tunai. Namun, saat ini permainan judi dapat dilakukan melalui jaringan internet, atau dunia maya. Oleh karena itu, permainan dilakukan secara *online* tanpa mengharuskan para pemainnya bertemu secara langsung [6]. "Dikutip dari halaman similarweb.com" pada bulan Oktober 2023 pada data *Top 20 Visit Website* Ranking Indonesia kategori gambling di mana untuk jumlah *visit* dari *website* category gambling dengan data terendah sebanyak 806,928 sedangkan data tertingi jumlah *visit* mencapai 7,914,745 [7].

Keamanan merupakan hal yang penting dalam kehidupan sehari-hari. Faktor keamanan merupakan peran yang sangat penting bagi manusia. Tidak hanya keamanan dalam beraktifitas, namun keamanan juga sangat dibutuhkan untuk menjaga suatu benda atau tempat yang dianggap berharga sehingga tidak semua orang dapat mengaksesnya. Berbagai bentuk pengamanan telah banyak dilakukan untuk melindungi barang penting atau keselamatan seseorang untuk mencegah penanganan illegal [8].

Situs-situs tersebut dapat menimbulkan dampak negatif bagi individu dan masyarakat [9]. Oleh karena itu, perlu dilakukan upaya untuk meningkatkan keamanan jaringan WIFI dari akses ke situs-situs tersebut. Salah satu upaya yang dapat dilakukan adalah dengan menggunakan DNS *filtering* [10] DNS *filtering* adalah teknik yang digunakan untuk memblokir akses ke situs tertentu berdasarkan nama domain. DNS *filtering* dapat dilakukan dengan menggunakan perangkat lunak atau perangkat keras [11].

Perangkat lunak DNS *filtering* yang umum digunakan adalah OpenDNS dan Comodo DNS. Perangkat keras DNS *filtering* yang umum digunakan adalah Orange Pi [12]. Selain itu, iklan yang muncul saat berselancar di internet juga mengganggu karena beberapa di antaranya menghalangi tampilan *website* dapat memperlambat waktu pemuatan *website* dan juga mengganggu pengguna [13]. Umunya Ketika kita membuka satu halaman website, secara otomatis muncul *pop-up* yang mengandung iklan, sebagian besar iklan tersebut mengandung pornografi. Jika kita mengklik iklan tersebut, sistem komputer kita mungkin terinfeksi *malware* lainnya [14].

Pada penelitian sebelumnya yang berjudul "Membangun Sistem Keamanan Jaringan Berbasis VPN yang Terintegrasi dengan DNS Filtering PIHOLE" menunjukkan bahwa saat berselancar di internet, pengguna berisiko mengalami kerugian akibat penyadapan data oleh pihak yang tidak bertanggung jawab dan munculnya iklan *online* yang mengganggu [15].

Selanjutnya pada penelitian sebelumnya telah dilakukan oleh [10] dimana dalam penelitian tersebut peneliti menerapkan sistem 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. Namun, dalam penelitian tersebut untuk melakukan pemblokiran situs perlu memasukan nama *domain* atau *database* secara manual dan belum ada klasifikasi daftar situs yang difiltrasi atau diblokir secara otomatis oleh sistem.

Perbedaan pada penelitian ini peneliti menerapkan sistem DNS *filtering* menggunakan NxFilter pada Orange Pi, dimana perbedaan penelitian ini dibandingkan dengan penelitian sebelumnya adalah tidak perlu melakukan *update database blacklist* nama *domain* yang ingin diblokir secara berkala dan terus menerus. Pada penelitian ini sistem akan melakukan filtrasi dan mengklasifikasi nama domain secara otomatis tanpa perlu melakukan update *database blacklist* secara terus menerus. Hal ini dikarenakan sistem *NxFilter* sudah mempunyai *database* sendiri yang telah disediakan dan juga *Nxfilter* juga melakukan pembatasan berdasarkan isi konten atau parameter pada *website* yang akan diakses. Jika dalam sebuah website terdapat konten yang termasuk ke dalam parameter seperti *Ads*, *Porn* dan *Gambling* makan sistem akan melakukan pembatasan.

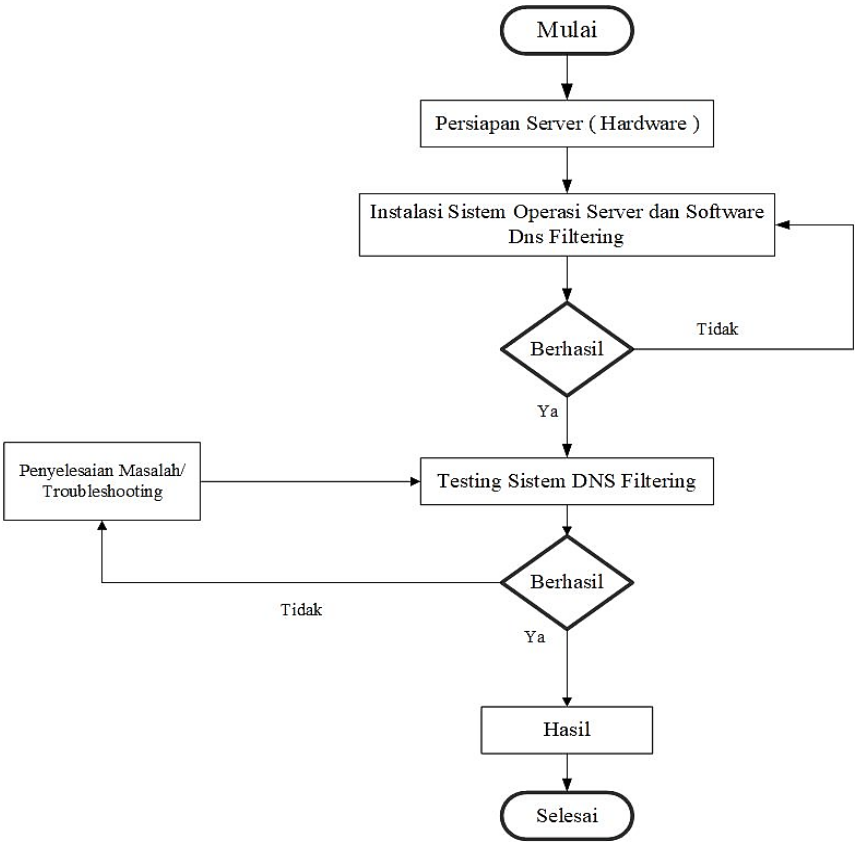
2. METODOLOGI PENELITIAN

Metodologi merupakan ilmu-ilmu atau cara yang digunakan untuk memperoleh kebenaran menggunakan penelusuran dengan tata cara tertentu dalam menemukan kebenaran, tergantung dari realitas yang sedang dikaji [16]. Alur penelitian dijelaskan pada Gambar 1 Metodologi Penelitian.

Gambar 1. Metodologi Penelitian

2.1. Rancangan Pengujian

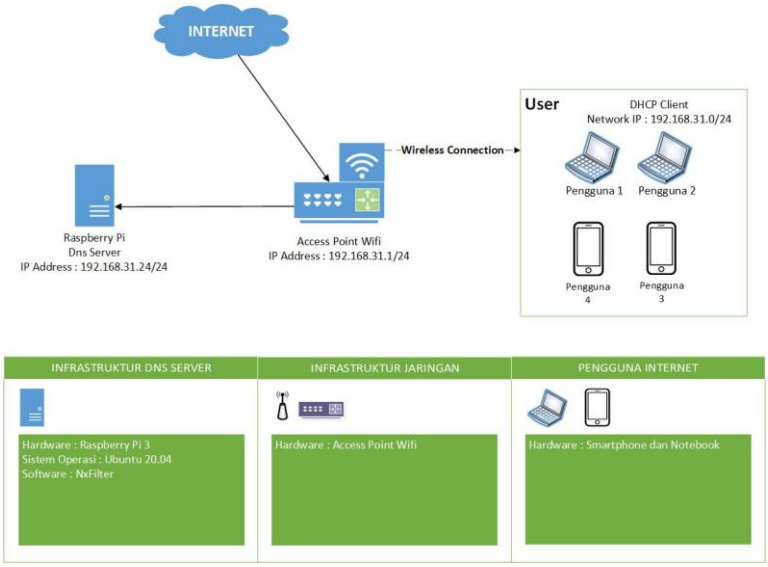
Gambar 2 merupakan alur pengujian sistem DNS *filtering* yang diimplementasikan pada balai warga RW 32 Bekasi Utara.



Gambar 2. Alur Pengujian

2.2. Topologi

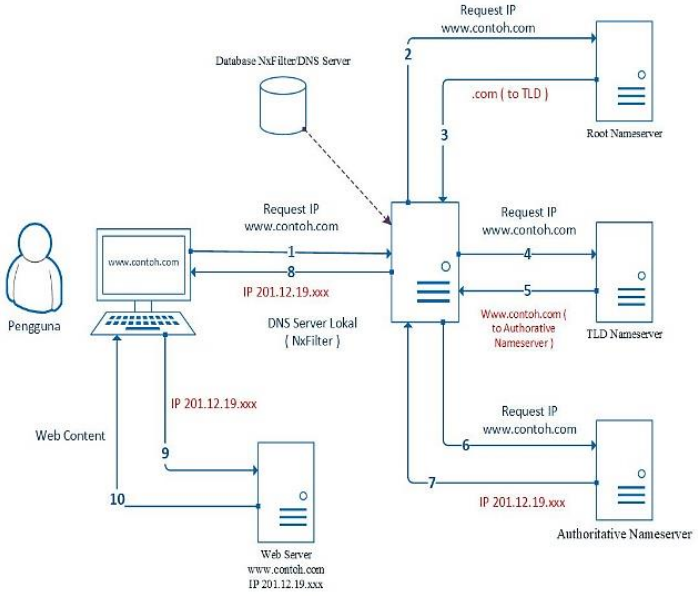
Pada tahapan ini peneliti melakukan tahapan perancangan topologi jaringan seperti yang ada pada Gambar 3. Pada perancangan topologi disesuaikan dengan kondisi infrastruktur jaringan yang sudah ada pada lokasi dengan sumber internet dari penyedia internet dan modem internet sebagai *router* jaringan. Pada skema jaringan ini *server* OrangePi 3 bertugas sebagai DNS *server* lokal yang didalamnya sudah dipasang sistem operasi Linux Ubuntu dan NxFilter sebagai aplikasi *filtering* akses internet pengguna. Terdapat juga *Access Point* yang bertugas sebagai *router* dan *access point* jaringan LAN yang akan mendistribusikan IP ke pengguna yang terkoneksi ke WIFI atau sebagai DHCP *server*. Setelah itu *router* akan mengalihkan DNS ke *server* DNS Orange PI tersebut.



Gambar 3. Topologi

2.3. Alur Sistem DNS *Filtering*

Sistem *filtering* DNS ini mengalihkan lalu lintas akses internet melewati DNS *server*, setelah itu DNS *server* akan membaca *log* akses internet, jika permintaan akses internet tersebut masuk kedalam kategori yang diblok maka akses internet tidak bisa dilewatkan [17].



Gambar 4. Alur Sistem DNS *Filtering*

3. HASIL DAN PEMBAHASAN

3.1. Alat Penelitian

Alat penelitian yang di butuhkan dalam optimasi keamanan jaringan WIFI dari situs judi *online* dan pornografi dengan DNS *filtering* pada balai warga rw 32 bekasi utara yaitu membutuhkan *hardware* , *software* dan *network* ditunjukkan pada tabel 1 sampai dengan tabel 3.

Tabel 1. Spesifikasi Perangkat Keras

No.	Perangkat Keras	Spesifikasi	Sistem Operasi
1	Mini *Server*	Orange Pi Zero3 Allwinner H618 Quad-core Cortex-A53 Processor, GPU Arm mail-G31 MP2, Ram 2Gb, Micro Sd Sandisk Ultra 32Gb	Linux Ubuntu
2	Laptop	Lenovo Thinkpad T470 Processor: 15 Gen 7 Ram: 8Gb	Windows 10
3	Kabel Jaringan	UTP Cat6	

Tabel 2. Spesifikasi Perangkat Lunak

No.	Perangkat Lunak
1	NxFilter
2	Zerotier One
3	Putty

Tabel 3. Sumber Internet

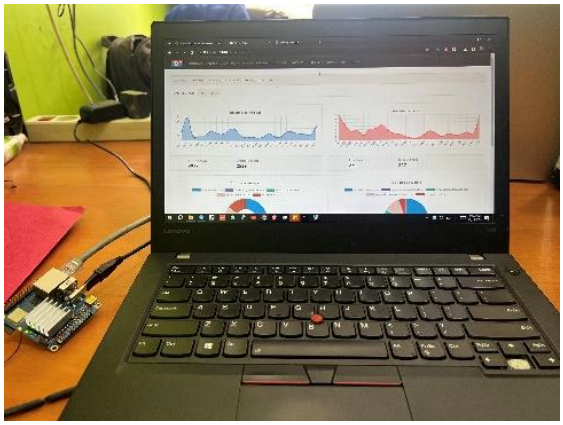
No.	Network	Penyedia Layanan
1	Broadband Internet	MyRepublik
2	Thetering Hotspot	Jaringan Seluler

3.2. Implementasi dan Pengujian

Dalam proses implementasi Keamanan Jaringan WIFI dari Situs Judi *Online* dan Pornografi Dengan DNS *Filtering* dan OrangePi Pada Balai Warga Rw 32 Bekasi Utara, peneliti melakukan tahap lanjutan pemasangan dari hasi rancangan pengujian yang sebelum nya sudah di paparkan pada bab sebelumnya tentang rancangan pengujian.

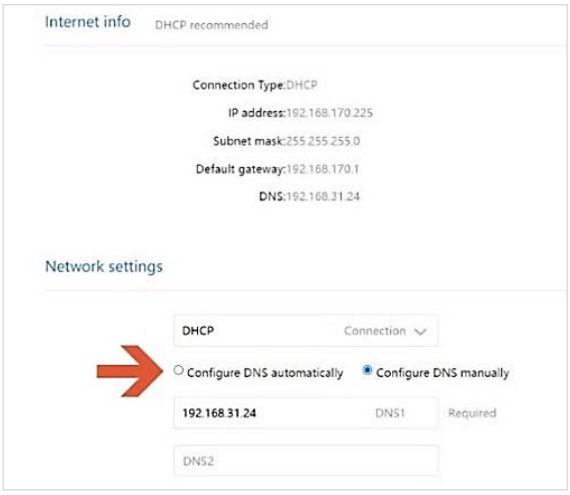
Gambar 5. Pemasangan *Server* Orange Pi

Pada gambar 4 adalah proses pemasangan *server* Orange Pi yang sudah di konfigurasi sebagai DNS *resolver* dan di hubungkan dengan router balai warga rw 32 bekasi utara.



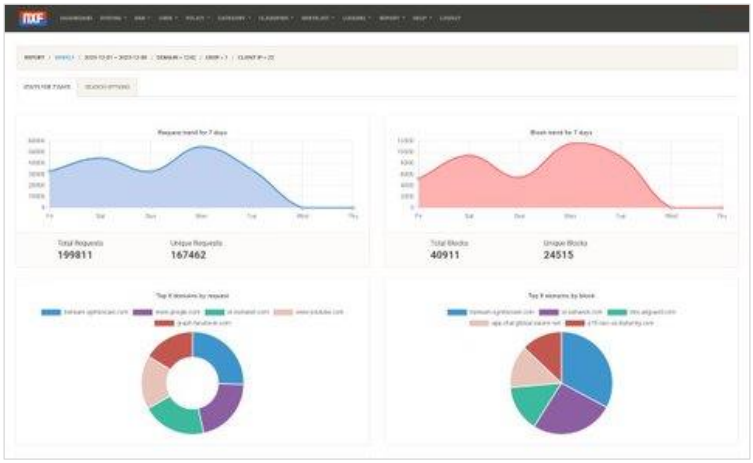
Gambar 6. Konfigurasi OrangePi dan NxFilter

Pada gambar 5 adalah proses konfigurasi ip DNS *server* dari Orange Pi ke ip DNS router, berikut setingan dari konfigurasi yang di lakukan dapat dilihat di gambar 6 dimana dalam konfigurasi ini peneliti mengalihkan alamat DNS agar menuju ke *IP DNS resolver Orange Pi.*



Gambar 7. Konfigurasi DNS Router

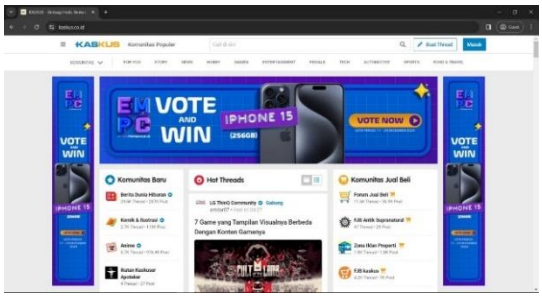
Setelah proses konfigurasi selesai Nxfilter sebagai DNS *resolver* dapat mulai melakukan *monitoring activity user* yang terkoneksi dengan jaringan WIFI balai warga rw 32, dapat dilihat dari gambar 8 dimana nxfilter sudah mulai mengambil data *activity*.



Gambar 8. *Dashboard Monitoring* NxFilter

Setelah melakukan instalasi dan konfigurasi OrangePi dan NxFilter selesai , dalam tahap pengujian peneliti melakukan testing ke salah satu situs judi *online* dan pengoptimalan *ads* atau iklan yang sering muncul di halaman situs, Berikut lampiran kondisi sebelum dan sesudah DNS filter terkonfigurasi.

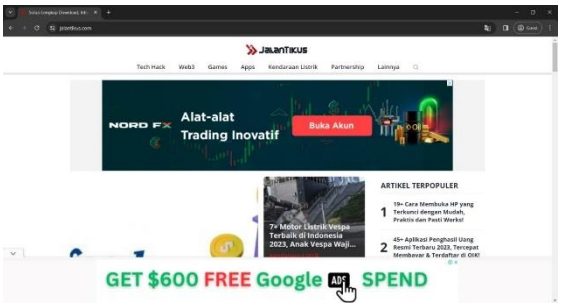
Sebelum mengaktifkan fitur DNS *filtering*:



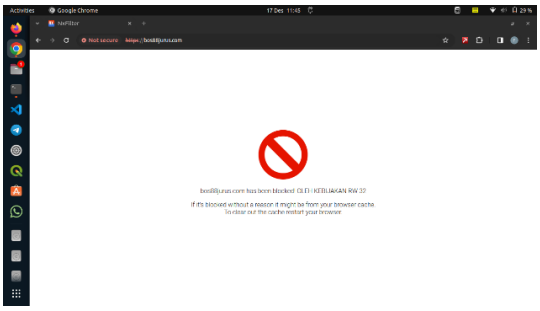
Gambar 9. Tampilan *Website* Sebelum DNS *Filtering ON*

Gambar 10. Akses Situs Judi *Online* Sebelum DNS *Filtering* ON

Sesudah Mengaktifkan DNS *Filtering*:



Gambar 11. Tampilan W*ebsite* Setelah DNS *Filtering ON*



Gambar 12. Akses Situs Judi *Online* Setelah DNS *Filtering ON*

Dapat di simpulkan dari kedua gambar di atas untuk tahapan pengujian berjalan dengan baik di mana sistem bekerja sesuai dengan apa yang di harapkan. Dalam hal pengujian ini peneliti juga mengambil sampel data *log* dalam situasi ketika tanpa mengaktifkan sistem DNS *filtering* dan ketika di aktifkan kembali fitur DNS *filtering* guna untuk melihat serta memantau *activity* pengguna yang terkoneksi dengan WIFI balai warga rw 32 bekasi utara setelah di lakukannya optimasi keamanan jaringan menggunakan Orange Pi dan DNS *filtering*.

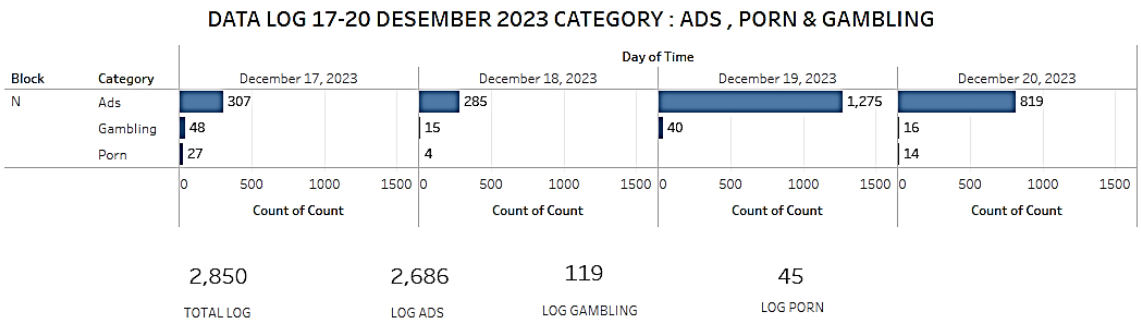
3.3. Hasil Akhir Pengujian

Hasil akhir pengujian terkait Optimasi Keamanan Jaringan WIFI dari Situs Judi *Online* dan Pornografi dengan DNS *Filtering* dan OrangePi pada Balaiwarga Rw 32 Bekasi utara peneliti mengambil *log activity* pengguna yang terkoneksi pada WIFI Balai Warga RW32 sebelum dan sesudah mengaktifkan DNS *filtering*.

Tabel 4. DNS *Log Before* Periode 17-20 Desember 2023

No	Data	Time	Block	Domain	Category
1	DNS *Log*	12/20/2023	N	Nekopoi.care	*porn*
2	DNS *Log*	12/20/2023	N	Pragmaticplay.com	*Gambling*
3	DNS *Log*	12/20/2023	N	Pornhub.com	*porn*
…	…		…	…	…
2850	*Ads Log*	12/17/2023	N	Find.api.micloud.xiaomi.net	*Ads*

Dalam penarikan *log before* diambil dalam rentan waktu 4 hari pada tanggal 17 Desember 2023 – 20 Desember 2023 dalam rentan waktu terebut dapat dilihat pada table 4 mendapatkan total *log activity* sebanyak 2.850 *log* dengan memfilter 3 kategori yang di tarik yaitu *Ads*, *Porn* & *Gambling*. Berikut hasil data *log* di tampilkan secara visual pada Gambar 13 *Log Activity DNS Filtering OFF*.



Gambar 13. *Log Activity DNS Filtering OFF*

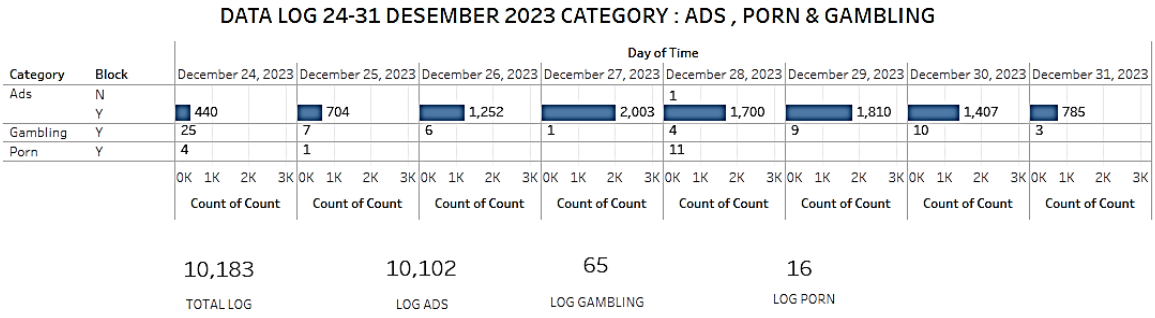
Hasil dari penarikan data *before* selama 4 hari terdapat *activity* user mengakses situs berkategori *Porn* & *Gambling* di setiap harinya khususnya untuk kategori *gambling* selalu ada pengaksesan situs judi *online* dan banyak juga data *log* kategori *ads* atau iklan yang masuk disetiap harinya, dari hasil *log before* tersebut peneliti menarik kesimpulan untuk kemanan jaringan WIFI dari penyedia layanan internet pada balaiwarga rw 32 bekasi utara masih belum optimal, lalu pada tanggal 23 Desember 2023 peneliti mulai melakukan pengaktifan fitur DNS *filtering* menggunakan NxFilter dengan pemblokiran 3 kategori yaitu *Ads*, *Porn* & *Gambling*, dalam penarikan *log after* peneliti menarik selama 8 hari pada rentan waktu atau periode tanggal 24 Desember 2023

– 31 Desember 2023 Berikut hasil data *log after* dapat dilihat pada tabel 5 terkumpul sebanyak 10.183 data *log*.

Tabel 5. DNS *Log After* Periode 24-31 Desember 2023

No	Data	Time	Block	Domain	Category
1	DNS *Log*	12/31/2023	Y	adx.ads.vungle.com	*Ads*
66	DNS *Log*	12/31/2023	Y	dga.pragmaticplaylive.net	*Gambling*
9411	DNS *Log*	12/24/2023	Y	pragmaticplay.com	*Gambling*
….	….	….	….	….	….
10183	*Ads Log*	12/31/2023	Y	mdp-appconf-sg.heytapdl.com	*Ads*

Dari hasil penarikan *log after* periode 24 - 31 Desember 2023 di atas, dibuatkan tampilan visual pada Gambar 14 *Log Activity DNS Filtering ON.*



Gambar 14. *Log Activity DNS Filtering ON*

Dan dari data *log after* mengaktifkan DNS *filtering* dengan memfilter 3 kategori yaitu : *Ads*, *Gambling* & *Porn* dapat dilihat untuk selama periode 24-31 Desember terdapat pengaksesan situs judi *online* yang masuk ke kategori *gambling* dan di setiap harinya selama pengaksesan berhasil di *block* oleh sistem DNS *Filtering*, lalu terbilang cukup efektif di mana dapat dilihat pada Gambar 14 *Log Activity DNS Filtering ON* sebagai pembanding data ketika sebelum dan sesudah dilakukan pengamanan menggunakan DNS *filtering* dimana dari data *after* untuk pengaksesan situs kategori *Ads*, *Gambling* & *Porn*, 100% terblokir , dan dapat dilihat terjadinya penurunan untuk percobaan akses ke situ-situs yang masuk ke dalam kategori *Porn* & *Gambling*.

4. KESIMPULAN

Penelitian ini bertujuan untuk mengimplementasikan konfigurasi keamanan jaringan WIFI di Balai Warga RW 32 Bekasi Utara menggunakan DNS *Filtering* dan OrangePi. Analisis data *log activity* pengguna sebelum konfigurasi menunjukkan prevalensi akses ke situs judi *online*, pornografi, dan iklan. Setelah penerapan konfigurasi, terjadi peningkatan yang signifikan dalam pemblokiran akses ke situs-situs tersebut. Hanya terdapat 65 *log activity* terkait judi *online*, 16 *log activity* terkait pornografi, dan 10.102 *log activity* berkategori iklan dari total 10.183 *log activity*.

Kesimpulan utama dari penelitian ini adalah bahwa optimasi keamanan jaringan WIFI dengan DNS *Filtering* dan OrangePi efektif dalam membatasi aktivitas pengguna dalam mengakses internet, khususnya dalam mengatasi akses ke situs judi *online*, pornografi, dan iklan yang tidak diinginkan. Sistem ini tidak hanya mampu memberikan perlindungan terhadap konten negatif, tetapi juga dapat meningkatkan kecepatan pengaksesan halaman web dengan pemblokiran iklan. Meskipun implementasi konfigurasi berhasil mengatasi kelemahan keamanan jaringan WIFI sebelumnya, diperlukan langkah-langkah lanjutan. Pemantauan berkala terhadap aktivitas pengguna, edukasi intensif terkait keamanan jaringan, dan perhatian terhadap pembaruan sistem menjadi kunci untuk menjaga tingkat keamanan yang optimal.

Kelebihan daripada penelitian ini adalah sistem *NxFilter* sudah mempunyai *database* sendiri yang telah disediakan dan juga *Nxfilter* juga melakukan pembatasan berdasarkan isi konten atau parameter pada *website* yang akan diakses. Jika dalam sebuah website terdapat konten yang termasuk ke dalam parameter seperti *Ads*, *Porn* dan *Gambling* makan sistem akan melakukan pembatasan.

Kelemahan pada penelitian ini adalah belum efektif dalam melakukan pembatasan akses sebuah website yang menggunakan *IP Public* dikarenakan sistem yang digunakan bekerja pada protokol *domain name system* (DNS). Saran untuk penelitian sebelumnya diharapkan melakukan peningkatan keamanan mencakup penguatan *firewall* di tingkat *router* guna mencegah akses yang lolos berdasarkan DNS maupun *IP Address*, pembatasan penggunaan VPN untuk mengurangi risiko, dan penelitian lanjutan untuk terobosan baru dalam keamanan jaringan WIFI. Meningkatkan pemahaman pengguna tentang risiko VPN dan perlunya kepatuhan terhadap kebijakan keamanan juga menjadi aspek penting untuk diperhatikan. Diharapkan hasil penelitian ini

dapat memberikan kontribusi yang substansial terhadap penerapan keamanan jaringan di ruang publik. Kesinambungan dalam upaya meningkatkan sistem keamanan jaringan diharapkan dapat menciptakan lingkungan internet yang lebih aman dan produktif di ruang publik Balai Warga RW 32 Bekasi Utara.

REFERENSI

[1] O. P. Beban *et al.*, "Optimasi Pembagian Beban Dan Keamanan Network Menggunakan OpenVPN Virtual Private Network Menggunakan OSPF Routing Protocol……Oky Tria Saputra".

[2] M. Agreindra Helmiawan Dosen Jurusan Teknik Informatika STMIK Sumedang, "INTERNET POSTIF DENGAN METODE WEB FILTERING LAYER 7 PADA JARINGAN WIRELESS (STUDY CASE HOTSPOT RT4 CIPEUTEUY BARU SUMEDANG)."

[3] Reza Pahlevi, "Penetrasi Internet di Kalangan Remaja Tertinggi di Indonesia," databoks.katadata.co.id. Accessed: Jan. 25, 2024. [Online]. Available: https://databoks.katadata.co.id/datapublish/2022/06/10/penetrasi-internet-di-kalangan-remaja-tertinggi-di-indonesia

[4] F. Firmansyah and R. A. Purnama, "Filtering Domain Name Server (DNS) untuk Membangun Internet Sehat Menggunakan Routerboard Mikrotik," *JUITA : Jurnal Informatika*, vol. 7, no. 1, p. 43, 2019, doi: 10.30595/juita.v7i1.4164.

[5] S. Jayanto, A. Tantoni, H. Asyari, P. Studi, T. Informatika, and S. Lombok, "Jurnal Ranah Publik Indonesia Kontemporer Implementasi Keamanan Jaringan dengan Packet Filtering Berbasis Mikrotik Untuk Internet Positif Di SMKN 1 Praya." [Online]. Available: https://rapik.pubmedia.id/index.php/rapik

[6] A. Sahata Sitanggang, R. Sabta, and F. Yuli Hasiolan, "Triwikrama: Jurnal Ilmu Sosial PERKEMBANGAN JUDI ONLINE DAN DAMPAKNYA TERHADAP MASYARAKAT: TINJAUAN MULTIDISIPLINER," vol. 01, pp. 50–60, 2023.

[7] similarweb, "Most Visited Gambling," similarweb.com. Accessed: Jan. 25, 2024. [Online]. Available: https://www.similarweb.com/top-websites/indonesia/gambling/gambling/

[8] D. I. Mulyana, A. Wulandari, F. N. Huda, R. F. Putra, and R. Wanandi, "Implementasi Sistem Keamanan RFID pada Lingkungan Rukun Warga 015 Tegal Alur Jakarta Barat," *Jurnal Pengabdian Nasional (JPN) Indonesia*, vol. 4, no. 1, pp. 230–237, Jan. 2023, doi: 10.35870/jpni.v4i1.150.

[9] D. Novianto, "Optimasi Waktu Query Dan Filtering Nama Domain Pada Dns Server Lokal Menggunakan Bind 9," *Jurnal Ilmiah Informatika Global*, vol. 8, no. 2, 2018, doi: 10.36982/jiig.v8i2.320.

[10] M. Rahman, "Implementasi Web Content Filtering Pada Jaringan RT/RW Net Menggunakan Pi-Hole DNS Server," *Generation Journal*, vol. 7, no. 1, pp. 50–60, 2023.

[11] S. Muhlison, "Analisa Dan Implementasi Dns Server Sebagai Filtering Konten Negatif Menggunakan Metode Rpz (Response Policy Zone) Di Pt. Time Excelindo," *Jurnal Ilmiah DASI*, vol. 16, no. 1, pp. 49–54, 2015, [Online]. Available: http://whois.domaintools.com

[12] "Aplikasi Monitoring Server Menggunakan Device Orange Pi".

[13] "IMPLEMENTASI PEMANFAATAN PI-HOLE SEBAGAI DNS SERVER PADA RUMAH UNTUK MEMONITORING TRAFFIC INTERNET DAN MEMBLOKIR IKLAN."

[14] T. Wahyu and A. Sanjaya, "STUDI SISTEM KEAMANAN KOMPUTER," no. 2, 2008.

[15] R. Mujiastuti and I. Prasetyo, "Membangun Sistem Keamanan Jaringan Berbasis VPN yang Terintegrasi dengan DNS Filtering PIHOLE," 2021. [Online]. Available: www.google.com

[16] R. A. Putra, H. Supendar, and R. Fahlapi, "Perancangan Virtual Private Network Dengan Metode PPTP Menggunakan Mikrotik," *Jurnal Komputer Antartika*, vol. 1, p. 2023, [Online]. Available: https://ejournal.mediaantartika.id/index.php/jka

[17] M. Rahman, "Implementasi Web Content *Filtering* Pada Jaringan RT/RW Net Menggunakan Pi-Hole DNS Server," *Generation Journal*, vol. 7, no. 1, pp. 50–60, 2023.