OKTAL : Jurnal Ilmu Komputer dan Science
Volume 2, No. 2, Februari 2023
ISSN 2828-2442 (media online)
Hal 575-582

Analisis dan Implementasi Network Ad-blocking Pi-Hole di Raspberry Pi 4 Menggunakan OPNSense DHCP Dengan Metode PPDIOO (Studi Kasus Diskominfo SP Kabupaten Lebak)

Muhamad Apriyatna[1*], Ahmad Fikri Zulfikar[1]

[1]Fakultas Teknik, Teknik Informatika, Universitas Pamulang, Jl. Raya Puspiptek No. 46, Kel. Buaran, Kec. Serpong, Kota Tangerang Selatan. Banten 15310, Indonesia
Email: [1*]mapriyatna.ay@gmail.com, [2]dosen00386@unpam.ac.id
(* : coressponding author)

Abstrak−Dalam perkembangan teknologi terutama kehadiran media iklan sebagai salah satu daya tarik minat calon pembeli. Akan tetapi, semuanya tidak relevan apabila pengguna melihatnya bahkan merasa kesal karena memakan data ekstra yang berlebih dengan banyaknya iklan pada halaman web. Oleh karena itu, diperlukan suatu sistem dengan kemampuan untuk menyaring iklan yang terdapat pada halaman web dan seolah-olah menjadikan local DNS sebagai satu-satunya aliran koneksi data dengan tools Unbound DNS yang ada pada OPNSense. Local DNS yang dibuat berdasarkan pada sistem Pi-Hole yang di install ke dalam Raspberry Pi untuk menyaring data atau iklan. Selain itu tambahan keamanan ekstra dengan OPNSense yang menjadikanya sebuah DNS Resolver untuk aliran koneksi data. Seiring dengan itu, implementasi Pi-Hole di dalam Raspberry Pi dengan memanfaatkan DHCP OPNSense telah berhasil menyaring iklan dan memotong data ekstra dalam keamanan jaringan untuk memberikan perlindungan tambahan. Dengan implementasi Pi-Hole di Raspberry Pi dengan memanfaatkan DHCP OPNSense ini bertujuan memberikan solusi selain menjaga keamanan jaringan agar pengembangan sistem ini dapat berjalan dengan efisien. Pengembangan sistem menerapkan metode PPDIOO (Prepare, Plan, Design, Implement, Operate, Optimize) karena model ini sangant cocok dan mudah untuk melakukan pengembangan dan perancangan sebuah sistem.

Kata Kunci: PiHole, OPNSense, Raspberry Pi, Network Ad-blocking, PPDIOO

Abstract−*In the development of technology, especially the presence of advertising media as one of the attractions of potential buyers. However, everything is irrelevant if the user sees it even gets annoyed because it eats up extra data that is excessive with the number of ads on the web page. Therefore, we need a system with the ability to filter advertisements on web pages and make it seem as if local DNS is the only data connection stream with the Unbound DNS tools in OPNSense. Local DNS built based on the Pi-Hole system installed into the Raspberry Pi to filter data or advertisements. In addition, the extra security with OPNSense makes it a DNS resolver for the flow of data connections. Along with that, the implementation of Pi-Hole in the Raspberry Pi by utilizing DHCP OPNSense has succeeded in filtering advertisements and cutting extra data in network security to provide additional protection. By implementing the Pi-Hole on the Raspberry Pi by utilizing DHCP OPNSense, it aims to provide a solution other than maintaining network security so that the development of this system can run efficiently. The system development applies the PPDIOO (Prepare, Plan, Design, Implement, Operate, Optimize) method because this model is very suitable and easy to develop and design a system.*

Keywords*: PiHole, OPNSense, Raspberry Pi, Network Ad-blocking, PPDIOO*

1. PENDAHULUAN

Meluasnya perkembangan media iklan digital yang berupa *banner*, *Pop-up advertising*, *sponsorship*, *hyperlink* dan lain sebagainya membuat pengguna menganggap iklan tersebut tidak menyenangkan, karena dianggap tidak relevan dan umumnya terkait dengan peningkatan penggunaan daya risiko privasi dan keamanan lainnya. Masalah tersebut karena sering memunculkan iklan dan malware dalam setiap mengakses jaringan internet, ada banyak perusahaan yang beriklan diinputkan pada *web*, *blog*, *social media*, *games online* dan lain sebagainya. Hal ini mendorong banyak perangkat lunak pemblokiran iklan (*ad-blockers*) yang terus berkembang yang bertujuan untuk memblokir iklan (serta pemblokiran risiko lain, seperti *malware* atau *trackers*) sampai tingkat tertentu. Pemblokiran iklan semacam itu telah diadopsi oleh sebagian besar pengguna internet.

Untuk mengatasi banyaknya iklan yang membanjiri pengguna ketika berselancar dalam sebuah jaringan internet, Raspberry Pi adalah pilihan yang terbaik, karena memiliki fungsi dari

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 2, No. 2, Februari 2023
ISSN 2828-2442 (media online)
Hal 575-582

sebuah komputer yang sangat kompleks, sehingga dapat memproses data dengan cepat dan efisien. Sistem pemblokiran iklan berbasis Raspberry Pi 4 ini disisipkan beberapa program/*software* diantaranya dengan mengkombinasikan antara Pi-Hole dan OPNSense, yang dimana Pi-Hole merupakan sistem utama pemblokiran iklan (*ad-blocking*) pada jaringan internet, ditambah OPNSense yaitu sebagai DHCP Server untuk Pi-Hole atau sekaligus menjadi *firewall* pada jaringan lokal yang seolah-olah menjadi DNS Server satu-satunya yang ada pada jaringan.

Berdasarkan uraian di atas, penulis mencoba melakukan analisa dan perancangan sistem untuk mendukung implementasi *network ad-blocking* menggunakan metode PPDIOO, dimana penelitian ini diawali dengan menganalisis sistem yang telah digunakan hingga saat ini kemudian melakukan perancangan dan pengembangan sistem yang baru, selanjutnya menganalisis hasil model pengembangan sistem *network ad-blocking* Pi-Hole pada pada Raspberry Pi menggunakan OPNSense DHCP. Dan diharapkan dapat dimanfaatkan dengan sebaik-baiknya sebagai alat yang efektif dalam sistem pemblokiran iklan.

2. METODOLOGI PENELITIAN

2.1 Metode Penelitian

Pada penelitian ini tahapan dalam menyelesaikan permasalahan menggunakan metode *Cisco Lifecycle* PPDIOO (*prepare, plan, design, operate, optimize*) yang dikembangkan oleh Cisco (Cisco, 2010) Tahapan tersebut mendefinisikan siklus pembangunan jaringan. Metode ini memiliki 6 tahapan, yaitu persiapan (*prepare*), perencanaan (*plan*), desain (*design*), implementasi (*implementation*), operasional (*operation*), dan optimisasi (*optimize*).

Gambar 1. Metode Pengembangan PPDIOO *Network Cycle*

a. Tahap *Prepare* (persiapan). Pada tahap ini dilakukan persiapan berupa penetapan kebutuhan penelitian, konsep arsitektur, dan strategi berdasarkan penetapan sistem.
b. Tahap *Plan* (Rencana). Pada tahap ini perencanaan yang dilakukan seperti mengindentifikasi hal-hal yang harus dipenuhi dalan jaringan berdasarkan tujuan, fasilitas, kebutuhan, user, dan faktor lainnya serta melakukan analisis GAP. Analisis GAP merupakan proses dimana penelitian membandingkan kinerja yang sebenarnya dengan kinerja yang diharapkan untuk menentukan apakah memenuhi harapan dan menggunakan daya secara efektif.
c. Tahap *Desgin* (desain). Mendesain sistem jaringan dengan memperhatikan keamanan, kinerja, kehandalan, pengelolaan, skalabilitas, termasuk peralatan-peralatan jaringan.
d. Tahap *Implement* (implementasi). Pada tahap ini instalasi dan konfigurasi perangkat baru sesuai dengan spesifikasi desain. Dimana perangkat baru ini akan mengganti disertai deskripsi, rincian pedoman pelaksanaan (dokumentasi), serta perkiraan waktu pelaksanaan.
e. Tahap *Operate* (Operasional) Melakukan pengelolaan sistem jaringan seperti monitoring, *maintenance*, dan *upgrade*.
f. Tahap *Optimize* (Optimalisasi). Pada tahap ini problem solving akan dilakukan jika terdapat kesalahan dalam jaringan dan memodifikasi jika terjadi masalah yang timbul dalam jaringan.

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 2, No. 2, Februari 2023
ISSN 2828-2442 (media online)
Hal 575-582

2.1 Implementasi Metode

Pada penelitian ini tahapan dalam menyelesaikan permasalahan menggunakan metode *Cisco Lifecycle* PPDIOO (*prepare*, *plan*, *design*, *operate*, *optimize*) yang dikembangkan oleh Cisco (Cisco, 2010) Tahapan tersebut mendefinisikan siklus pembangunan jaringan. Metode ini memiliki 6 tahapan, yaitu persiapan (*prepare*), perencanaan (*plan*), desain (*design*), implementasi (*implementation*), operasional (*operation*), dan optimisasi (*optimize*).

a. Tahap *Prepare*
Dalam tahap persiapan ini hal yang perlu dilakukan yakni analisis kebutuhan yang diperlukan dalam pengembangan sistem network ad-blocking Pi-Hole dengan OPNSense baik dari segi software maupun hardware yang dijabarkan pada analisis kebutuhan yang diperlukan antara lain terdapat pada tabel:

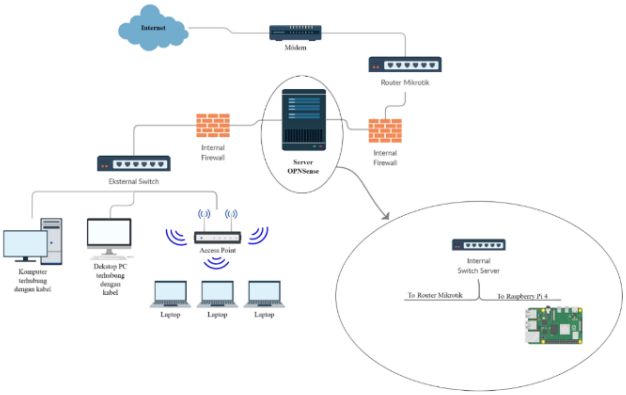
Tabel 1. Analisa Kebutuhan

Perangkat Keras (*Hardware*)	**Perangkat Lunak (*Software*)**	**Virtual Server dengan spesifikasi**
Raspberry Pi 4 Model B	Raspbian OS 64Bit	Disk Space 50 GB
Micro SD Card 32GB	Docker dan Portainer	CPU 10 vCPUs
Router Mikrotik	Pi-Hole	vMemory 16GB
Modem Internet	OPNSense	Bandwith Setting Unlimited
Server HPE ProLiant DL380 Gen10	VMware	

Selain itu beberapa tambahan seperti pengambilan data yang dilakukan peninjauan langsung ke tempat objek penelitian dan memperoleh data primer.

b. Tahap *Plan*
Dalam tahapan *plan* (perencanaan) ini merupakan perencanaan hasil yang akan dicapai dengan kebutuhan sistem yang ada baik dari segi perangkat keras ataupun perangkat lunak yang dilakukan dalam penelitian ini, tindakan ini menjelaskan skenario pengembangan sistem yang menggambarkan proses dalam penelitian yang dilakukan diantaranya yaitu studi literatur, observasi (pengamaatan), dan *action planning*.

c. Tahap *Design*
Pada tahap ini, topologi logika dirancang sesuai dengan kebutuhan sistem yang telah didefinisikan pada tahap persiapan. Hal pertama yang dilakukan adalah merancang IP Address yang akan dipakai dalam jaringan lab kecil yang telah dibuat untuk selanjutnya memakai posisi OPNSense sebagai DHCP Server, juga pengintegrasian OPNSense DHCP dengan Pi-Hole sebagai DNS lokal dalam sebuah jaringan. Berikut gambar desain rancangan yang diterapkan pada penelitian ini adalah sebagai berikut:



Gambar 2. Desain Topologi Penelitian

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 2, No. 2, Februari 2023
ISSN 2828-2442 (media online)
Hal 575-582

d. Tahap *Implement*
Pada tahap impelemtasi yaitu melakukan penerapan dari proses yang sudah dilakukan sebelumnya sehingga menghasilkan sistem yang dapat berjalan sebagaimana fungsi yang diharapkan. Meliputi instalasi sistem, konfigurasi sistem, implementasi penelitian, perhitungan kebutuhan dan keadaan, konfigurasi hardware dan software jaringan dalam sistem *network ad-blocking* Pi-Hole di Raspberry Pi menggunakan OPNSense DHCP pada Kantor Dinas Komunikasi Informatika Statistik dan Persandian Kabupaten Lebak.

e. Tahap *Operate*
Dalam tahap ini performa dan statistik dari Pi-Hole diukur serta kesalahan-kesalahan atau error yang mungkin terjadi terpantau untuk selanjutnya menjadi bahan pertimbangan di tahap optimasi. Kesalahan-kesalahan yang mungkin terjadi seperti dari sisi desain *subnet* yang ternyata membutuhkan subnet yang lebih kecil atau mungkin kesalahan pada konfigurasi dibagian OPNSense yang secara dampak tidak berjalannya sistem *network ad-blocking* pada Pi-Hole. Statistik pengguna dapat dilihat pada Dashboard Home Pi-Hole, statistik dapat berupa berapa total *queries* dari pengguna dan persentase *block* pada domain yang di adlists. Beberapa data dan tambahan informasi *client* juga dapat dilihat oleh Pi-Hole dan OPNSense yang sedang terhubung ke dalam sebuah jaringan.

a) Tahap *Optimize*
Pada tahap ini dilakukan manajemen jaringan dan sistem secara proaktif dengan tujuan untuk mengidentifikasi dan menyelesaikan masalah pada sistem keamanan jaringan khususnya *network ad-blocking*. Pada tahap ini juga dapat dilakukan modifikasi sistem yang telah dibuat jika terjadi ketidaksesuaian terhadap kebutuhan. Perawatan, pemeliharaan dan pengelolaan terhadap perangkat yang digunakan dalam sistem *network ad-blocking*.

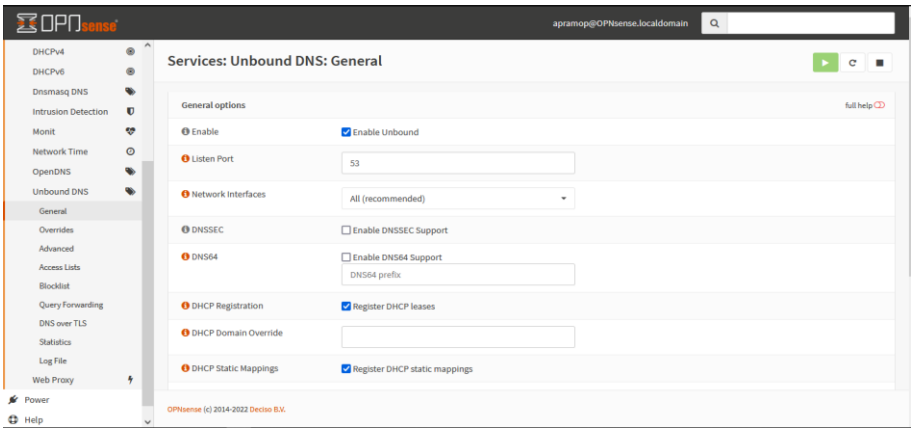
3. HASIL DAN PEMBAHASAN

2.1 Konfigurasi Dasar

Pada tahap konfigurasi ini, terdapat beberapa hal yang penting untuk pengembangan sistem network ad-blocking, layaknya router biasa OPNSense di atur sedemikian rupa agar bisa berjalan dengan baik. Berikut beberapa pengaturan pada OPNSense:

IP Address : 192.168.50.3/24
Gateway : 192.168.50.1
System DNS Server : 192.168.50.4 (Pi-Hole)
LAN DNS Server : 192.168.50.3

Sistem DNS Server yang digunakan di atas adalah IP Address yang dimiliki Pi-Hole dengan tujuan bahwa OPNSense menjadi *DNS resolver* pada sebuah jaringan LAN, selanjutnya akan diteruskan ke alamat Pi-Hole yang ada di OPNSense.

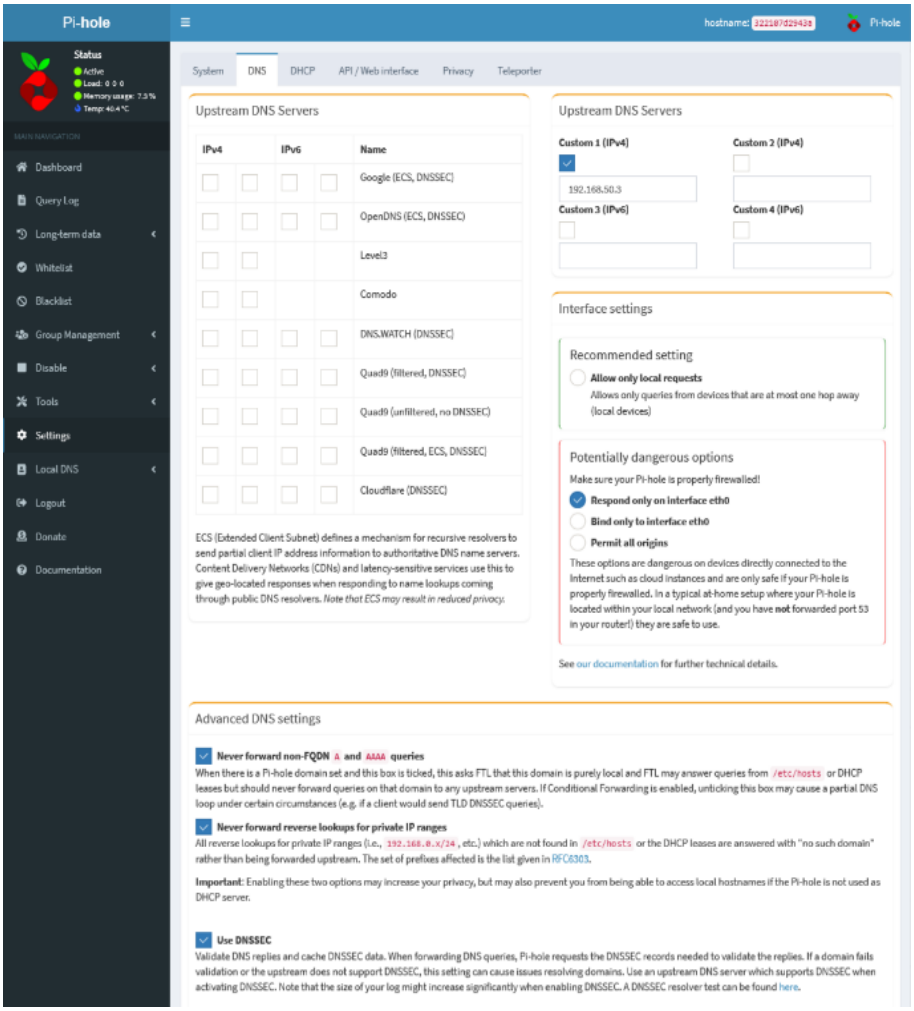


Gambar 3. Konfigurasi Unbound DNS

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 2, No. 2, Februari 2023
ISSN 2828-2442 (media online)
Hal 575-582

Setelah konfigurasi selesai, pilih *tools* bagian *services* kemudian pilih Unbound DNS, ini bertujuan agar OPNSense menjadi DNS Resolver yang mencegah kekeliruan Pi-Hole dalam tindakan yang dilakukan secara berlebihan yang dapat di *block* oleh Pi-Hole atau lebih tepatnya membuang situs sehingga gagal mengakses situs sebenarnya, dikarenakan Pi-Hole memiliki kemampuan yang sering disebut DNS *Sinkhole*.

Sebagian besar konfigurasi dilakukan pada OPNSense sehingga tidak banyak hal yang harus dikonfigurasi dari sisi Pi-Hole. Bagian konfigurasi hanya terdapat pada bagian sistem DNS yang dihubungkan kepada OPNSense, sehingga koneksi data dapat diselesaikan oleh OPNSense sebelum koneksi dikirim ke Pi-Hole atau lebih tepatnya aliran data harus melewati OPNSense kemudian baru diteruskan ke Pi-Hole lalu dikembalikan lagi kepada OPNSense.



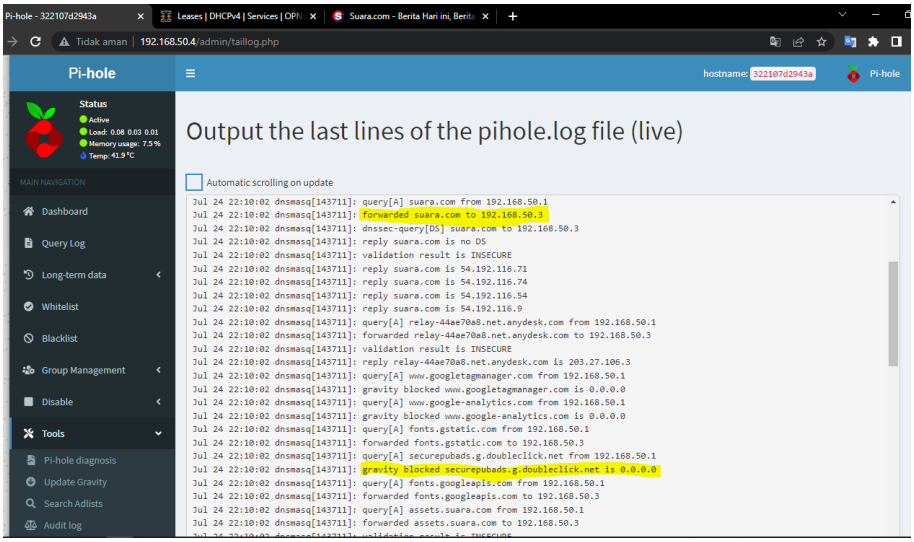
Gambar 4. Konfigurasi DNS OPNSense pada Pi-Hole

2.2 Pembahasan

Pengembangan perangkat Raspberry Pi sebagai sistem *network ad-blocking* Pi-Hole dalam sebuah keamanan jaringan yang mampu menangani lingkup jaringan area lokal hingga gedung, terlebih dengan keamanan jaringan yang dimiliki OPNSense yang mempunyai kemampuan yang *powerfull* bagi sebuah *software* yang berbasis *opensource*. Mengkombinasikan keduanya merupakan hal yang tepat bagi pengembangan sistem keamanan jaringan.

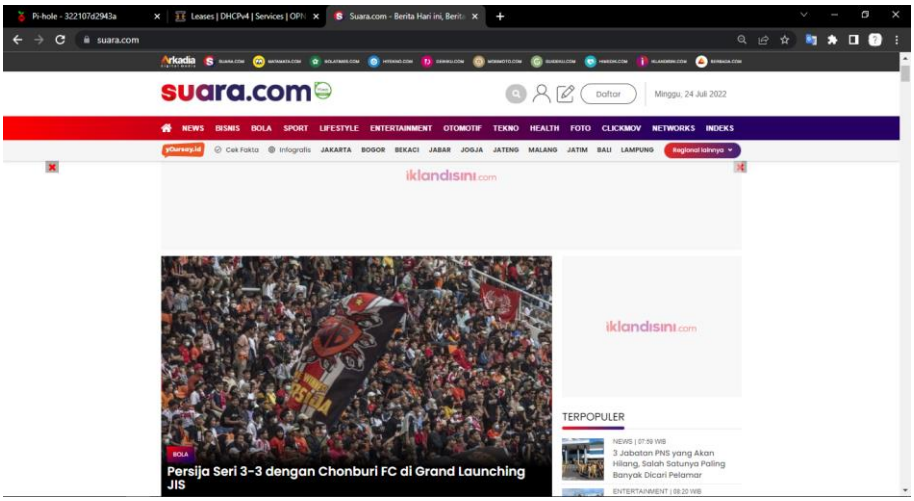
Proses dari pengembangan sistem *network ad-blocking* Pi-Hole menggunakan OPNSense DHCP yang sangat kompleks dengan melihat hasil dari *Tail piihole.log* yang memberikan informasi rute yang di lewati oleh setiap client ketika mengakses halaman web. Berikut hasil log ketika user mengakses halaman web *www.suara.com*:

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 2, No. 2, Februari 2023
ISSN 2828-2442 (media online)
Hal 575-582



Gambar 5. Hasil Tail Pihole.Log

Sementara dilihat dari hasil *client* yang telah mengunjungi web *www.suara.com* dapat dilihat pada gambar berikut ini:



Gambar 6 Hasil Tampilan dari Client

Gambar di atas menunjukkan bahwa setiap kali *client* mengakses suatu web maka akan langsung di *forward* ke *router server* OPNSense, selanjutnya akan diteruskan kepada server *Unbound* untuk memvalidasi manasaja yang ditampilkan dan yang akan di hilangkan ketika halaman web muncul, sehingga informasi yang didapat *client* lebih cepat dan tidak memakan waktu yang lama bahkan dapat memotong data ekstra.

4. ANALISA DAN IMPLEMENTASI

Hasil analisa implementasi ataupun pengujian pada pengembangan sistem *network ad-blocking* ini, analisa dan pengujian dilakukan dalam bentuk tabel yang menggunakan bantuan *browser Mozilla Firefox* dan website *www.acid3.acidtests.org* untuk mengukur performa yang mengindikasikan kesesuaian dari suatu browser atas konten-konten yang berada pada suatu halaman web. Hasil pengujian ini dilakukan pada beberapa web yang sering diakses dalam mendapatkan sebuah informasi. yaitu *detik.com, suara.com, kompas.com, sorosowan.co.id*

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 2, No. 2, Februari 2023
ISSN 2828-2442 (media online)
Hal 575-582

Hasil pengujian ini adalah dengan membandingkan data sebelum dan setelah adanya sistem *network ad-blocking*, hal ini dapat menjadi ukuran dalam efisiensi sebuah sistem dimana sistem bukan hanya dapat bekerja dengan baik juga dapat memberikan hasil yang memuaskan dari sisi penulis maupun lokasi tempat penelitian. Berikut ini dapat dilihat perbandingan data sebelum dan setelah adanya sistem *network ad-blocking* yang ada pada tabel dibawah ini:

Tabel 2. Analisa Sebelum dan Sesudah Adanya *Network Ad-Blocking*

		User 1		User 2		User 3	
		Sebelum	Setelah	Sebelum	Setelah	Sebelum	Setelah
www.detik.com	GET	33	9	37	4	38	4
	Total Transfer Data	132,99 KB	34,49 KB	355,34	55,86 KB	144,47	33,85 KB
www.suara.com	GET	42	2	44	2	48	2
	Total Transfer Data	247,34 KB	55,86 KB	285,81	72,13	209,11	55,57 KB
www.kompas.com	GET	38	5	30	3	36	3
	Total Transfer Data	144,88 KB	72,13 KB	109,12 KB	71,21 KB	117,81	71,51 KB
sorosowan.co.id	GET	26	2	33	3	30	3
	Total Transfer Data	282,80 KB	69,25 KB	313,39 KB	119,88 KB	275,34 KB	120,05 KB

5. KESIMPULAN

Berdasarkan hasil penelitian berupa analisis, pengujian dan implementasi pada bab-bab sebelumnya, maka dapat ditarik kesimpulan pada pengembangan sistem *network ad-blocking*, sebagai berikut:

a. Berdasarkan hasil implementasi *network ad-blocking* Pi-Hole menggunakan OPNSense DHCP dengan adanya fitur Sinkhole atau DNS yang telah dikonfigurasi untuk merutekan nama domain tertentu dan memfilter konten tertentu sehingga dapat gagal dalam mengakses situs yang sebenarnya pada Pi-Hole dapat disimpulkan bahwa kecepatan transfer data (*bandwidth*) yang diperlukan untuk mengakses konten pada halaman web sangat membantu meningkatkan kecepatan akses konten pada halaman web yang ditambah fitur Unbound DNS pada OPNSense.
b. Dari hasil penelitian dapat diambil kesimpulan secara menyeluruh bahwa dengan pengembangan sistem *network ad-blocking* Pi-Hole dapat meningkatkan kecepatan akses data yang dilakukan oleh user ditambah dengan menggunakan fitur *Unbound DNS* yang ada pada OPNSense untuk dapat berkomunikasi langsung dengan root DNS menjadikan pengembangan sistem keamanan jaringan yang sangat kompleks.

Berdasarkan data analisis dari pengembangan sistem ini memiliki perubahan tampilan konten halaman web setelah adanya *network ad-blocking* dapat disimpulkan bahwa terjadi perubahan tampilan terhadap dampak penyaringan iklan pada halaman web. Hal ini dapat dipengaruhi oleh tiap website yang di akses memiliki karakteristik tampilan yang berbeda, sehingga tampilan informasi dalam konten menjadi jelas dan efisien.

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 2, No. 2, Februari 2023
ISSN 2828-2442 (media online)
Hal 575-582

REFERENCES

Adha, R R Rizal, M. F., & Isma, S. J. I. (2021). *Membangun Sistem Keamanan Jaringan Berbasis Firewall Dan Ids Menggunakan Tools Opnsense*. 7(6), 2846–2856.

Ada, Lady. (2017). *Pi Hole Ad Blocker with Pi Zero W*.

Al Fatta, H. (2007). *Analisis dan Perancangan Sistem Informasi*. : Penerbit Andi.

Almas Yudistira, K. (2020). *Analisis Pencegahan Penyebaran Malware Melalui Media Iklan Menggunakan Raspberry*.

Andri Kristanto. (2018). *Perancangan sistem informasi dan aplikasinya*. Yogyakarta: Penerbit Gava Media.

Dirja Nur Ilham, R. A. C. (2018). *Analisis Celah Keamanan Jaringan Komputer Dengan Menggunakan Raspberry Pi 2*.

Habibi, R. (2022). *Optimalisasi Internet Warga Menggunakan Kombinasi Type Antrian Dan Sistem Pihole*.

Kadir. (2014). *Pengenalan Sistem Informasi*. Edisi Revisi

Lestari, K. C., & Amri, A. M. (2020). *Sistem Informasi Akuntansi (Beserta Contoh Penerapan Aplikasi Sia Sederhana Dalam UMKM)*. Dipublish. https://books.google.co.id/books?id=ShrWDwAAQBAJ

Maulana, H. (2020). *Sistem Mobile Cloud Storage Dan DNS Ad- Blocker Untuk Perlindungan Privasi Data*.

Mujiastuti, R., & Prasetyo, I. (2021). *Membangun Sistem Keamanan Jaringan Berbasis VPN yang Terintegrasi dengan DNS Filtering PIHOLE*. November 2021.

OPNSense, *https://opnsense.org/*.

Pi-Hole and OPNSense, *https://pi-hole.net/blog/2021/09/30/pi-hole-and-opnsense/*.

Portainer, *https://docs.portainer.io/*.

Setiawan, R. W. (2019). *Analisis Dan Implementasi Raspberry Pi 3 Model B + Sebagai Server E - Learning*. RESTIKOM : Riset Teknik Informatika Dan Komputer, 1(1).

Taib, A. M. (2020). *Securing Network Using Raspberry Pi by Implementing VPN, Pi-Hole, and IPS (VPiSec)*. International Journal of Advanced Trends in Computer Science and Engineering.

The PPDIOO Network Lifecyle, *http://www.ciscozine.com/the-ppdioo-network-lifecycle/*.

Thomas Krenn, *https://www.thomas-krenn.com/en/wiki/Install_OPNsense*.

Triatmoko, R. D. (2016). *Analisis Cache Dan Kompresi Proxy Pada Raspberry Pi Di Jaringan Hotspot Smk Negeri 22 Jakarta*.