LOFIAN: Jurnal Teknologi Informasi dan Komunikasi
https://ejournal.umbp.ac.id/index.php/lofian/
Vol. 3, No. 2, Pebruari 2024, Halaman 16-24

e-ISSN: 2798-9593
p-ISSN: 2798-9836

Pengembangan Layanan Pemblokiran Situs Bermuatan Negatif menggunakan DNS Sinkhole dan Layanan DNS Quad 9 dengan Metode PPDIOO

Erwin Daniel Sitanggang[1], Misdem Sembiring[2], Beny Irawan[3]

[1,2]*Universitas Mandiri Bina Prestasi*
Jl. Letjend. Djamin Ginting No. 285-287, Padang Bulan, Medan Baru, Kota Medan, Sumatera Utara, Indonesia - 20155

[3]*Institut Kesehatan Medistra Lubuk Pakam*
Jl. Sudirman No. 38, Lubuk Pakam, Kab. Deli Serdang, Sumatera Utara, Indonesia - 20512

[1]*rwins.sitanggang@gmail.com,* [2]*misdem@umbp.ac.id,* [3]*benyirawan@medistra.ac.id*

DOI: 10.58918/lofian.v3i2.240

Abstrak

Bentuk kebebasan akses internet tidaklah selalu memberikan dampak postitif dalam meningkatkan kualitas hidup manusia tetapi juga dampak negatif. Dampak negatif ini bisa didapatkan baik dengan sengaja ataupun tidak sengaja. Seperti situs yang menyediakan konten yang berisi pornografi, Juga termasuk situs yang menyediakan kegiatan ilegal lainnya seperti Abuse, Drugs, Fraud, Piracy, Gambling, Ransomware, Redirect, Malware, Phishing, Scam, Tracking. Menimbang besarnya dampak negatif dari penggunaan akses internet serta untuk melindungi penggunanya dari kegiatan ilegal. Peneliti mengembangkan usulan untuk penyediakan layanan penyaringan akses internet yang dikelola secara mandiri menggunakan DNS Sinkhole dan penyaringan di penyedia layanan DNS publik Quad 9. Sebagai tambahan menggunakan daftar blocklist DNS sinkhole dari BlockList Project. Juga menggunakan metode PPDIOO Network Lifecycle yang memiliki siklus pengembangan yaitu Prepare, Plan, Design, Implement, Operate dan Optimize. Penerapan dari DNS Sinkhole menggunakan Pi-hole sebagai layanan penyaringan akses internet yang dikelola secara mandiri bekerja dengan sangat baik. Terbukti pada hasil optimasi dan persentasi optimasi yang didapatkan rata-ratanya pada Request 60,05%, Transferred Over Network 42,30%, Resource Loaded 43,87 dan Time Loaded 69,32%.

Kata Kunci: Dampak Negatif Akses Internet, BlockList Project, DNS Sinkhole, PPDIOO.

1. Pendahuluan

Akses internet sudah menjadi bagian dari hak asasi manusia yang harus dipenuhi sesuai dengan pernyataan lembaga di bawah naungan PBB (Perserikatan Bangsa-Bangsa) yaitu ITU (International Telecommunication Union). Pernyataan tersebut tertuang dalam Declaration of Principles "Building the Information Society: a global challenge in the new Millennium" [1] yang merupakan hasil dari pertemuan World Summit on the Information Society (WSIS) yang diselenggarakan oleh PBB di Geneva, 10-12 Desember 2003 yang dihadiri oleh pemeritah beberapa negara, pebisnis, dan perwakilan warga sipil [2]. Hak atas akses internet sering dikaitkan dengan hak atas kebebasan berbicara dan berekspresi. Konten yang ada di internet dianggap sebagai hal yang harus dapat diakses oleh semua orang, tanpa atau dengan batasan seminimal mungkin. Pelanggaran atas hak ini dianggap sebagai pelanggaran hak asasi manusia oleh beberapa pihak, terutama atas kebebasan berbicara.

Bentuk kebebasan akses internet tidaklah selalu memberikan dampak postitif dalam meningkatkan kualitas hidup manusia tetapi juga dampak negatif. Dampak negatif ini bisa didapatkan baik dengan sengaja ataupun tidak sengaja [3]. Seperti situs yang menyediakan konten yang berisi pornografi, manusia dengan kesadaran yang dimilikinya dapat mengakses situs penyedianya atau tanpa disadari menemukannya pada situs-situs lainnya yang menampilkannya dalam bentuk iklan yang tidak diingikan. Juga termasuk situs yang menyediakan kegiatan ilegal lainnya [4] seperti Abuse, Drugs, Fraud, Piracy, Gambling, Ransomware, Redirect, Malware, Phishing, Scam, Tracking [5], dan lain sebagainya. Hal ini menyebabkan hilangnya akses internet yang bersih dan nyaman. Sehingga setiap manusia dalam melakukan akses internet akhirnya harus berhati-hati dan berjaga-jaga akan setiap kegiatannya dalam menggunakan akses internet yang tidaklah sepenuhnya dipahami oleh pengguna. Banyak pengguna yang masih belum bijak dan belum sesuai dengan etika atau norma yang berlaku dalam menggunakan akses internet yang membuat mereka menjadi korban dari kegiatan-kegiatan ilegal akses

e-ISSN: 2798-9593
p-ISSN: 2798-9836

internet. Pernyataan tersebut didukung oleh Laporan Bulanan Publik Desember 2022 dari Hasil Monitoring Keamanan Siber oleh ID-SIRTII/CC (Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center. Di bulan Desember 2022 terdapat sebesar 26.228.777 anomali trafik (trafik internet yang tidak sesuai dengan pola normal) yang berasal dari berbagai negara dan Indonesia menduduki penyumbang anomali trafik tertinggi sebesar 4.238.120 dengan tujuan tertinggi juga menuju Indonesia sebesar 18.309.725 anomali trafik. Dan setelah di klasifikasikan, Malware menduduki anomali terbanyak sebesar 15.828.804 diikuti oleh Information Gathering Leak sebesar 2.999.662 dan kemudian Trojan Activity dengan jumlah 4.871.407 anomali trafik [6]. Dari klasifikasi anomali trafik tersebut, yaitu malware, information gathering dan trojan activity merupakan kegiatan ilegal yang dapat langsung berhubungan dengan pengguna akses internet baik disengaja maupun tidak disengaja.

Menimbang besarnya dampak negatif dari penggunaan akses internet serta untuk melindungi penggunanya dari kegiatan ilegal baik disengaja maupun tidak, management Politeknik MBP (Mandiri Bina Prestasi) Medan merasa peduli untuk memberikan akses internet yang bersih dan nyaman pada layanan akses internet yang mereka sediakan. Management Politeknik MBP Medan kuatir akan kekurangan pahaman pengguna akses internet yaitu seluruh civitas akademika akan dampak negatif membuat mereka menjadi korban. Rasa kuatir tersebut semakin bertambah setelah dilakukan beberapa percobaan menunjukkan kondisi layanan akses internet yang dimiliki saat ini dapat mengakses internet tanpa adanya batasan. Dimana akses situs-situs terpercaya memberikan informasi-informasi yang tidak dibutuhkan.

Untuk mewujudkan keinginan manejement Politeknik MBP Medan tersebut, peneliti mengusulkan untuk menyediakan layanan penyaringan akses internet secara mandiri [4]. Usulan yang diberikan peneliti berpedoman pada peraturan yang dibuat oleh pemerintah dalam menyukseskan program INSAN (Internet Sehat dan Aman) [7]. Dimana peraturan ini ada sebagai perwujudan hak asasi manusia akan akses internet di Indonesia, serta melindungi kepentingan umum dari segala jenis gangguan sebagai akibat penyalahgunaan informasi elektronik dan untuk memberikan akses internet yang bersih dan nyaman, pemerintah melalui Kementerian Komunikasi dan Informatika telah mengeluarkan peraturan Nomor 19 Tahun 2014 tentang Penanganan Situs Internet Bermuatan Negatif [4].

Peneliti mengembangkan usulan untuk penyediakan layanan penyaringan akses internet yang dikelola secara mandiri menggunakan DNS Sinkhole [3][8][9] dan penyaringan di penyedia layanan DNS publik Quad 9 [10]. Dan sebagai tambahan dalam usulan, peneliti menggunakan daftar blocklist DNS sinkhole dari BlockList Project [11]. Peneliti juga menggunakan metode PPDIOO Network Lifecycle yang memiliki siklus pengembangan yaitu Prepare, Plan, Design, Implement, Operatedan Optimize [12]. Sehingga diharapkan dari hasil akhir penelitian ini dapat memberikan layanan akses internet yang bersih dan nyaman kepada pengguna tanpa mengurangi kualitas dari layanan akses internet itu sendiri, memudahkan network administrator dalam pengelolaan daftar blocklist dan menghindari pengguna dari kegiatan ilegal yang dapat memberikan dampak negatif akses internet.

2. Tinjauan Pustaka

Penelitian ini dikembangkan dari beberapa penelitian-penelitian sebelumnya tentang analisis dan pengembangan layanan filtering DNS. Penelitian [8] dilakukan untuk menghindari pengguna dari dampak negatif, menjaga kualitas layanan akses internet dari informasi yang tidak diinginkan dan menghindari penyebaran malware ke perangkat pengguna. Pengujian dilakukan dengan 2 skenario yaitu sebelum dan sesuadah penerapan. Hasil pengujian disebutkan 100% efektif dalam memfilter situs dan memblokir iklan serta dikategorikan baik dalam pengujian kualitas layanan akses internet. Saran dari penelitian ini agar mengklasifikasikan daftar situs-situs yang perlu difilter dan iklan yang perlu diblokir.

Penelitian selanjutnya [9] dilakukan untuk mengatasi permasalahan penyebaran iklan yang memperngaruhi kenyamanan pengguna dari kualitas kecepatan akses dan ketersediaan bandwidth internet. Peneliti menyediakan sistem filtering situs menggunakan perangkat lunak Pi-hole DNS Server. Prinsip kerja yang dilakukan dalam penelitian ini dengan mengalihkan jalur traffic pada jaringan agar melewati Pi-hole DNS Server, sehingga traffic data dapat diamati. Dari hasil pengujian dikategorikan baik. Sebagai saran dari peneliti agar diterapkan secara mendalam untuk iklan yang diperbolehkan dan menerapkan aturan untuk menampilkan nama dan jenis iklan yang sudah diblokir.

Penelitian berikutnya tentang metode PPDIOO [13], yang dilakukan untuk pemblokiran iklan yang membanjiri pengguna ketika berselancar di internet. Metode yang digunakan oleh peneliti dalam menganalisa dan perancangan menggunakan PPDIOO

e-ISSN: 2798-9593
p-ISSN: 2798-9836

Network Lifecycle. Pada tahapan prepare, dilakukan analisis kebutuhan yang diperlukan baik dari segi perangkat keras dan perangkat lunak. Tahapan plan, didefinisikan perancanaan hasil yang akan dicapai dengan kebutuhan sistem. Tahapan design, dirancang topologi sesuai dengan kebutuhan sistem yang telah didefinisikan. Tahapan implement, penerapan dari proses-proses yang sudah dilakukan sebelumnya sehingga menghasilkan sistem yang dapat berjalan sebagaimana fungsi yang diharapkan. Tahapan operate, dilakukan pengukuran performa dan statistik serta pemantauan kesalahan-kesalahan atau eror yang mungkin terjadi untuk selanjutnya dilakukan optimasi. Tahapan optimize, dilakukan manajemen jaringan dan sistem secara proaktif dan memodifikasi sistem yang telah dibuat jika terjadi ketidaksesuaian terhadap kebutuhan. Hasil pengujian menunjukkan kualitas akses internet sangat membantu meningkatkan kecepatan akses konten situs.

Dan untuk memperdalam pemahaman, peneliti memaparkan beberapa teori pendukung sebagai berikut:

2.1. Layanan Akses Internet

Layanan akses internet adalah ketersediaan dan penyediaan jalur komunikasi yang memungkinkan pengguna untuk terhubung ke World Wide Web dan sumber daya online lainnya. Seiring dengan perkembangan teknologi, layanan ini telah berkembang dari koneksi sederhana melalui telepon hingga teknologi nirkabel dan serat optik yang canggih.

Terdapat beberapa aspek yang mencakup layanan akses internet:

1. Jenis layanan akses internet, dapat berupa dial-up, broadband, nirkabel atau satelit.
2. Kecepatan dan Ketersediaan akses internet
3. Dampak Sosial dan Ekonomi
4. Inklusi Digital
5. Keamanan dan Privasi
6. Regulasi dan Kebijakan
7. Masa Depan Teknologi Informasi

Layanan akses internet terus berkembang seiring dengan kemajuan teknologi, dan tantangan seperti kesenjangan digital dan isu keamanan terus dihadapi oleh penyedia layanan dan regulator untuk menciptakan lingkungan internet yang aman, inklusif, dan efesien [14].

2.2. PPDIOO

Metode PPDIOO adalah suatu pendekatan sistematis yang digunakan dalam pengelolaan jaringan atau sistem telekomunikasi, khususnya dalam konteks Cisco Systems. Metode ini merupakan singkatan dari Prepare, Plan, Design, Implement, Operate, dan Optimize. Berikut adalah defenisi dari setiap tahapan:

1. Prepare (persiapan), dalam tahapan ini dilakukan identifikasi kebutuhan bisnis dan teknis. Mengumpulkan informasi awal dan dilakukan analisis situasional dan juga menentukan tujuan dan kebutuhan pengguna.
2. Plan (Perencanaan), tahapan membuat rencana yang mencakup kebijakan, prosedur, dan sumber daya yang diperlukan. Identifikasi resiko dan cara mengelolanya. Merencanakan kebutuhan perangkat keras, perangkat lunak dan personel.
3. Design (Perancangan), tahapan membuat desain teknis dan fungsional berdasarkan rencana. Identifikasi solusi dan teknologi yang sesuai, Perancangan arsitektur jaringan atau sistem.
4. Implement (Implementasi), tahapan menerapkan desain yang telah dibuat. Konfigurasi perangkat keras, perangkat lunak dan infrastruktur. Uji coba dan verifikasi implementasi.
5. Operate (Operasional), tahapan dalam mengelola dan operasikan sistem atau jaringan. Monitor kinerja dan lakukan pemeliharaan rutin. Menanggapi perubahan kebutuhan atau masalah yang muncul.
6. Optimize (Optimalkan), tahapan evaluasi kinerja sistem dan identifikasi area perbaikan. Tingkatkan efesiensi dan efektifitas operasional. Revisi dan perbaharui rencana dan desain sesuai kebutuhan baru.

2.3. Layanan DNS Public Quad 9

Quad 9 adalah layanan DNS public gratis yang berfokus pada keamanan dan privasi. Layanan ini dioperasikan oleh organisasi nirlaba yang digukung oleh IBM, Packet Clearing House, Global Cyber Alliance, dan organisasi keamanan siber lainnya [10].

Yang membedakan Quad 9 dengan resolver DNS lainya, antara lain:

1. Tidak menyimpan log, layanan ini tidak menyimpan catatan aktifitas penelusuran pengguna.
2. Memblokir situs berbahaya, layanan ini secara otomatis memblokir domain yang diketahui berbahaya, seperti situs phising, malware, dan botnet.
3. DNS over TLS dan HTTPS, layanan ini mendukung enkripsi untuk komunikasi antara perangkat pengguna dan server DNS, melindungi data pengguna dari intersepsi.
4. Gratis untuk digunakan, layanan ini gratis dan dapat digunakan siapapun.

e-ISSN: 2798-9593
p-ISSN: 2798-9836

2.4. Pi-hole DNS Server

Pi-hole adalah solusi perangkat lunak open-source yang dirancang untuk memblokir iklan dan pelacakan di tingkat jaringan dengan menggunakan konsep DNS Sinkhole. Umunya diimplementasikan pada perangkat seperti Raspberry Pi atau server local, Pi-hole berfungsi sebagai server DNS yang memfilter permintaan DNS dan memblokir domain yang terkait dengan iklan dan pelacakan sebelum permintaan tersebut mencapai server DNS eksternal [16].

Adapun cara kerja dari Pi-hole adalah sebagai berikut:

1. Permintaan DNS: Ketika perangkat di jaringan memcoba mengakses situs web, permintaan DNS dikirim ke Pi-hole.
2. Pemeriksaan Domain: Pi-hole memeriksa domain yang diminta terhadap daftar hitamnya yang berisi domain-domain yang dikenal terkait dengan iklan dan pelacakan.
3. Blok Iklan: Jika domain tersebut ada dalam daftar hitam, Pi-hole mengarahkan permintaan ke alamat IP local (DNS sinkhole), menyebabkan permintaan tersebut diblokir.

Terdapat beberapa keunggulan dari Pi-hole, yaitu:

1. Pemfilteran Jaringan: Pi-hole memberikan pemfilteran iklan di tingkat jaringan, sehingga setiap perangkat yang terhubung ke jaringan mendapatkan manfaatnya.
2. Kinerja dan Efisiensi: Blokir iklan terjadi di tingkat DNS, mengurangi beban lalu lintas internet dan mengingkatkan kinerja penjelajahan.
3. Antarmuka Pengguna Web: Pi-hole menyediakan antarmuka pengguna web yang memungkinakan pemantauan aktivitas jaringan dan statistik penggunaan.

2.5. Situs Bermuatan Nefatif

Situs bermuatan negatif menjadi fenomena yang semakin menonjol dalam ekosistem digital saat ini. Istilah ini mencakup situs web atau platform online yang menyajikan konten yang merugikan, meresahkan, atau melanggar etika dan norma tertentu. Jenis konten tersebut bisa beragam, mulai dari berita palsu dan propaganda hingga materi kebencian, tindakan kekerasan, atau pornografi yang melibatkan anak-anak. Dampak dari situs bermuatan negatif tidak hanya mempengaruhi individu secara langsung, tetapi juga dapat merusak tatanan sosial secara lebih luas.

Keberadaan berita palsu dan propaganda di situs-situs ini dapat memperkeruh persepsi masyarakat terhadap isu-isu tertentu, menghasut konflik, atau bahkan merusak reputasi individu dan lambaga. Materi kebencian, yang sering kali merusak hubungan antar-kelompok, meningkatkan ketidaksertaan, dan memicu konflik sosial, juga dapat dengan cepat menyebar melalui media sosial dan situs berita online. Ancaman terhadap keamanan individu juga muncul, terutama ketika situs-situs ini digunakan untuk menyebarkan informasi pribadi atau mengorganisir kegiatan kriminal [16].

2.6. DNS Forwarding

DNS Forwarding adalah proses dimana server DNS mengirimkan permintaan DNS dari klien ke server DNS lainnya untuk resolusi nama domain. Saat klien membuat permintaan DNS, server DNS lokal dapat meneruskannya ke server DNS yang lebih tinggi dalam hierarki untuk mencari informasi yang diperlukan. Ini membantu dalam mempercepat proses resolusi DNS dan dapat digunakan untuk memperkuat keamanan atau menerapkan kebijakan khusus.

Konfigurasi DNS Forwarding umumnya digunakan di server DNS lokal, di mana server tersebut dapat diatur untuk meneruskan permintaan DNS ke server DNS eksternal atau upstream. Ini dapat membantu mengurangi beban server lokal dan memanfaatkan server DNS yang memungkinkan memiliki cache yang lebih besar atau akses yang lebih cepat ke sumber daya DNS eksternal [17].

2.7. Network Address Translation (NAT)

Network Address Translation (NAT) adalah teknik yang digunakan dalam jaringan komputer untuk mengonversi alamat IP privat menjadi alamat IP publik dan sebaliknya. Hal ini umumnya diterapkan di router atau firewall untuk mengatasi keterbatasan jumlah alamat IP yang tersedia di internet.

Cara kerja dari NAT sendiri yaitu saat perangkat di jaringan lokal mengirim paket ke internet, NAT mengganti alamat IP privat dengan alamat IP publik sebelum paket mencapai internet. Saat balasan dari internet tiba, NAT mengonversi alamat IP publik kembali menjadi IP privat dan mengirimkannya ke perangkat yagn sesuai di jaringan lokal.

Keuntungan dari NAT berupa konservasi alamat IP yaitu mengatasi keterbatasan alamat IP publik dengan memungkinkan banyak perangkat di jaringan lokal menggunakan satu alamat IP publik. Keamanan yaitu menyembunyikan struktur jaringan lokal dari internet karena hanya alamat IP publik yang terlihat di luar jaringan [18].

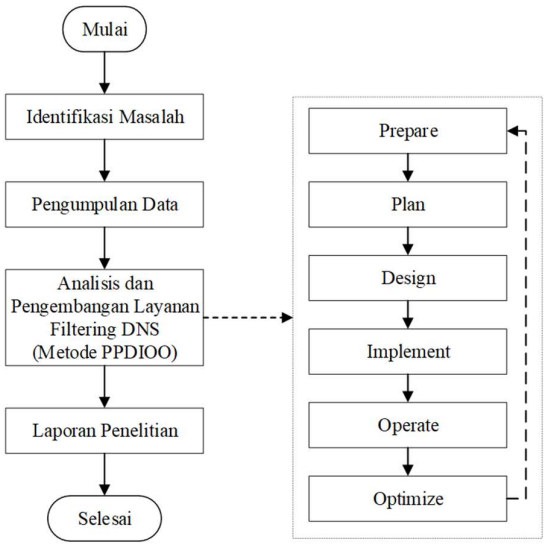
e-ISSN: 2798-9593
p-ISSN: 2798-9836

3. Metodologi Penelitian

Dalam menyelesaikan permasalahan penelitian ini, ditetapkan tahapan-tahapan yang menjelaskan proses penelitian ini dari awal hingga permasalahan yang dirumuskan terselesaikan.

3.1. Kerangkat Kerja

Adapun kerangka kerja dari penelitian yang digunakan dalam menyelesaikan permasalahan dalam penelitian ini, terlihat pada Gbr. 1.



Gbr. 1. Kerangka Kerja Penelitian

3.2. Uraian Kerja

Terdapat 4 tahapan dari kerangka kerja dalam membangun layanan Filtering DNS yang dapat melakukan penyaringan akses ke domain. Adapun tahapan-tahapan tersebut adalah sebagai berikut:

1. Identifikasi Masalah
   Tahapan yang pertama dilakukan dalam penelitian ini adalah mendefenisikan masalah pada sistem yang sedang berjalan. Sehingga dapat ditemukan penyelesaian dari permasalahan tersebut.
2. Pengumpulan Data
   Untuk mendukung dalam penyelesaian masalah, dilakukan pengumpulan data berupa teori dan konsep pendukung yang bersumber dari buku, publikasi penelitian-penelitian sebelumnya yang berhubungan dengan penelitian ini. Sehingga dalam penyelesaian masalah dari penelitian ini memiliki landasan dan keilmuan yang baik dan sesuai.
   Adapun metode yang digunakan dalam pengumpulan data pada penelitian ini adalah:
   a. Wawancara, Metode ini digunakan untuk pengumpulan data dari pihak-pihak terkait. Pihak tersebut adalah pengambil keputusan dan pengelola jaringan di Politeknik MBP Medan.
   b. Observasi, Metode ini dilakukan dengan mengamati secara langsung layanan akses internet di Politeknik MBP Medan.
   c. Studi Pustaka, Metode ini digunakan bertujuan untuk pengumpulan data dengan mempelajari dari rujukan dari buku-buku, artikel-artikel penelitian dan publikasi-publikasi ilmiah yang berhubungan dengan penelitian ini. Metode ini digunakan untuk melengkapi pengetahuan awal, guna memahami teori yang dapat digunakan untuk menunjang penelitian.
3. Analisis dan Pengembangan Layanan Pemblokiran
   Dari sejumlah model pengembangan siklus hidup perencanaan jaringan yang ada, dalam penelitian ini menggunakan metode PPDIOO dari Cisco.
4. Laporan Penelitian
   Pada tahapan ini, seluruh hasil yang didapat selama melakukan penelitian dirangkunm dan kemudian ditarik kesimpulan dan saran sehingga menjadi laporan penelitian yang utuh.

3.3. Lokasi Penelitian

Penelitian ini dilakukan di Jaringan Komputer gedung Politeknik Mandiri Bina Prestasi Medan tepatnya pada perangkat Router.

3.4. Data Pengujian

Adapun data yang akan dijadikan ujicoba perbandingan ada website berita yang paling banyak diakses berdasarkan dari Similar Web (diakses 13 Juni 2023) [19].

Tabel 1.
Data Testing

No.	Website	Pengunjung
1.	tribunnews.com	147.3M
2.	detik.com	145.0M
3.	kompas.com	132.3M
4.	suara.com	59.6M
5.	pikiran-rakyat.com	53.4M

4. Analisis dan Perancangan

4.1. Prepare

Pemaparan kondisi jaringan, topologi jaringan. Penggunaan layanan DNS dan kecepatan akses internet.

a. Penyediaan layanan internet

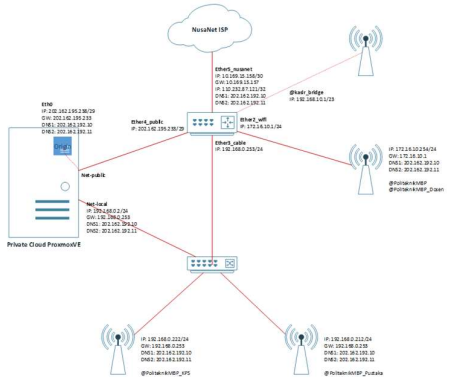
e-ISSN: 2798-9593
p-ISSN: 2798-9836

Penyediaan layanan internet kepada pengguna yang ada di Gedung Politeknik Mandiri Bina Prestasi Medan dibagi kedalam 4 segment. Pembagian ini berasal dari Router utama. Adapun segment- segment tersebut adalah:

1. Segment yang pertama ada di port Ether4_public. Melalui media kabel UTP, port ini langsung terhubung ke komputer server yang menyediakan Private Cloud (Proxmox Virtual Environment) pada port Ethernet_1. Di komputer server ini juga telah ada sebuah server virtual.
2. Segment yang kedua ada di port Ether3_cable. Segment ini terhubung menggunakan media kabel UTP ke Switch Jaringan. Satu port dari Switch Jaringan ini akan terhubung ke ke port Ethernet_2 komputer server. Satu port dari Switch Jaringan terhubungan dengan WAP (Wireless Access Point) dengan SSID @PoliteknikMBP_KPS menggunakan media Kabel UTP. Kemudian Satu port dari Switch Jaringan terhubungan dengan WAP dengan SSID @PoliteknikMBP_Pustaka menggunakan media Kabel UTP. Selanjutnya port-port yang ada di Switch Jaringan terhubung di komputer-komputer yang ada di ruangan masing-masing civitas akademi.
3. Segment yang ketiga ada di port Ether2_wifi. Segment ini terhubung langsung melalui media kabel UTP ke satu perangkat WAP yang memiliki 2 SSID @PoliteknikMBP dan @PoliteknikMBP_Dosen.
4. Segment yang keempat ada port wlan1_kasir dan wlan2_kasir yang terhubung secara bridge di port @kasir_bridge. Dari port menyediakan SSID @PoliteknikMBP_Kasir.

b. Topologi Jaringan

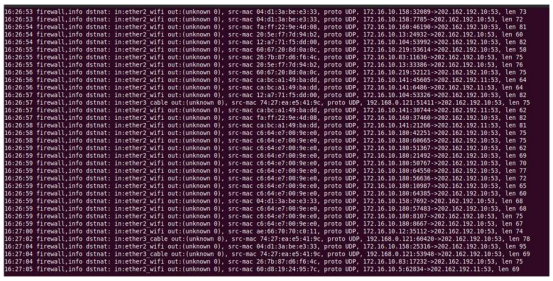
Hubungan antara perangkat-perangkat yang dimiliki saat ini hingga dapat menyediakan layanan internet yang ada di Gedung Politeknik Mandiri Bina Prestasi Medan digambarkan dalam topologi berikut.



Gbr. 2. Topologi Jaringan Sebelum dikembangkan

c. Penggunaan Layanan Akses Internet

klien dapat menggunakan layanan internet di Gedung Politeknik Mandiri Bina Prestasi Medan tanpa ada pembatasan. Klien dapat terhubung ke jaringan komputer menggunakan IP Statik maupun IP Dinamis melalui media Kabel mapun Nirkabel (Wireless). Seluruh perangkat yang adi jaringan komputer akan menggunakan DNS yang disediakan oleh ISP NusaNet dengan alamat DNS1: 202.162.192.10 dan DNS2: 202.162.192.11 atau diubah ke layanan DNS lainnya.



Gbr. 3. Log port 53 di Router penggunaan DNS dari klien

d. Kecepatan Akses website

Akses kepada 5 website berita yang paling banyak dikunjungi berdasarkan Tabel 1.

Tabel 2.
Akses Website

No.	Request	Tranfered Over Network (kB)	*Resourc Loaded (kB)*	*Time Loaded (s)*
1.	994	6400	16200	48,02
2.	497	3500	8900	46,65
3.	728	6900	17900	45,99
4.	481	4800	11300	34,33
5.	256	4200	11100	44,58

4.2. Plan

Pada tahapan ini, dipaparkan konsep yang akan digunakan, data-data yang digunakan untuk pengujian.

a. Konsep Pengembangan

Ketika pengguna akses terhubung ke jaringan, perangkat yang digunakan akan mendapatkan IP Address secara dinamis atau manual namun untuk DNS servernya akan menggunakan IP Address dari server Pi-hole. Kemudian setiap akses ke internet dari pengguna akan dialihkan terlebih dahulu ke server Pi-hole walaupun pengguna menggunakan DNS dari layanan lainnya. Pemaksaan ini akan dilakukan di router menggunakan NAT. Filtering akses internet akan dilakukan di server Pi-hole, untuk akses ke internet

e-ISSN: 2798-9593
p-ISSN: 2798-9836

yang terdaftar di server Pi-hole akan otomatis di blok dan yang tidak akan diteruskan ke pengguna.

b. Data Pengujian

Adapun data yang akan dijadikan ujicoba perbandingan ada website berita yang paling banyak diakses berdasarkan dari https://www.similarweb.com/ (diakses 13 Juni 2023).

Tabel 2.
Data Testing

No.	Website	Pengunjung
1.	tribunnews.com	147.3M
2.	detik.com	145.0M
3.	kompas.com	132.3M
4.	suara.com	59.6M
5.	pikiran-rakyat.com	53.4M

c. Daftar Blocklist

Dalam melakukan filtering, peneliti menggunakan daftar blocklist yang sudah disediakan oleh komunitas-komunitas yang sudah dikategorikan berdasarkan jenis.

Tabel 3.
Daftar Blocklist

No.	Jenis	Pengunjung
1.	Abuse	https://blocklistproject.github.io/Lists/abuse.txt
2.	Advertising	https://blocklistproject.github.io/Lists/ads.txt
3.	Crypto	https://blocklistproject.github.io/Lists/crypto.txt
4.	Drugs	https://blocklistproject.github.io/Lists/drugs.txt
5.	Fraud	https://blocklistproject.github.io/Lists/fraud.txt
6.	Gambling	https://blocklistproject.github.io/Lists/gambling.txthttps://zerodot1.gitlab.io/CoinBlockerLists/hosts_browser
7.	Malware	https://blocklistproject.github.io/Lists/malware.txt
8.	Phishing	https://blocklistproject.github.io/Lists/phishing.txt
9.	Piracy	https://blocklistproject.github.io/Lists/piracy.txt
10.	Porn	https://blocklistproject.github.io/Lists/porn.txt
11.	Ransomware	https://blocklistproject.github.io/Lists/ransomware.txt
12.	Redirect	https://blocklistproject.github.io/Lists/redirect.txt
13.	Scam	https://blocklistproject.github.io/Lists/scam.txt
14.	Torrent	https://blocklistproject.github.io/Lists/torrent.txt
15.	Tracking & Telemetry	https://blocklistproject.github.io/Lists/tracking.txt
16.	YouTube	https://raw.githubusercontent.com/kboghdady/youTube_ads_4_pi-hole/master/youtubelist.txt
17.	Suspicious	https://raw.githubusercontent.com/PolishFiltersTeam/KADhosts/master/KADhosts.txt
18.	Malicious	https://raw.githubusercontent.com/DandelionSprout/adfilt/master/Alternate%20versions%20Anti-Malware%20List/AntiMalwareHosts.txt

d. Perangkat Keras Tambahan

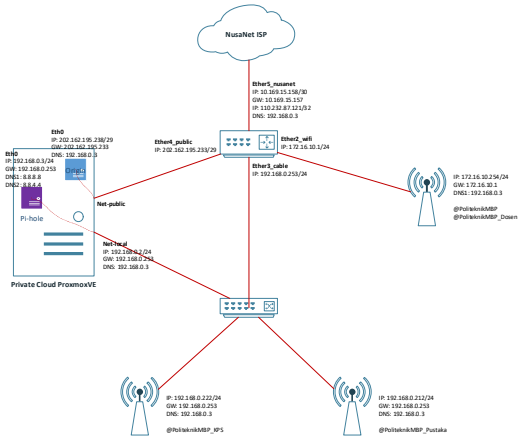
Untuk menerapkan filtering membutuhkan perangkat server baru dengan minimal spesifikasi, sebagai berikut:

Tabel 4.
Spesifikasi minimum perangkat server Pi-hole

No.	Item	Size
1.	Processor	1 CPU
2.	RAM	512MB
3.	Storage bebas	2GB
4.	OS	Rocky Linux 8

4.3. Design

Untuk dapat menerapkan usulan perubahan, peneliti melakukan perubahan topologi jaringan menjadi sebagai berikut:



Gbr. 3. Topologi Jaringan Usulan Perubahan

Pada topologi jaringan usulan perubahan akan ditambahkan server baru yang difungsikan sebagai Pi-hole dengan IP Address 192.168.0.2 dan DNS menggunakan layanan public dari Quad 9 dengan DNS1: 9.9.9.9 dan DSN2: 149.112.112.112.

4.4. Implement

Penerapan dari usulan perubahan dilakukan dalam beberapa tahap, yaitu:

1. Instalasi Server
   Untuk sistem operasi yang digunakan adalah Rocky Linux 8 dengan mode text (minimal instalation) dan partisi /boot, / dan swap.
2. Setting IP

e-ISSN: 2798-9593
p-ISSN: 2798-9836

Server terhubung ke internet dengan setting IP Address sebagai berikut:

Tabel 5.
Setting IP Address Server Pi-hole

IP Address	192.168.0.2
Netmask	255.255.255.0
Gateway	192.168.0.253
DNS1	9.9.9.9
DNS2	149.112.112.112

3. Instalasi Pi-hole
   Instalasi Pi-hole dilakukan di dalam Server Rocky Linux 8 dengan perintah:

   curl -sSL https://install.pi-hole.net | sudo PIHOLE_SKIP_OS_CHECK=true bash

4. Konfigurasi Pi-hole
   Untuk konfigurasi Pi-hole dilakukan melalui control panelnya yang diakses di http://192.168.0.2/admin. Seluruh blocklist yang ada di table 3 dimasukkan di bagian Adlists sebagai daftar domain yang akan di blok.
5. Setting DHCP Server Router
   Perangkat dari pengguna akan mendapatkan setting IP Address dan DNS secara otomatis. Perubahan dilakukan di Router dengan setting DHCP Server sebagai berikut:

Tabel 6.
Setting DHCP Server

Name	Address	*Gateway*	*DNS Servers*
dhcp_civitas	192.168.0.0 /24	192.168. 0.253	192.168.0.2
dhcp_kasir	192.168.10. 0/24	192.168. 10.1	192.168.0.2
dhcp_wifi	172.16.10.0 /24	172.16.1 0.1	192.168.0.2

6. Setting NAT Router
   Kondisi sebelumnya mengijinkan pengguna untuk mengubah DNS Server yang digunakan secara bebas. Konfigurasi di Router akan memaksakan permintaan melalui port 53 akan dialihkan ke server Pi-hole, dengan perintah:

   ip firewall nat chain=dstnat action=dst-nat to-addresses=192.168.0.2 to-ports=53 protocol=udp dst-port=53 log=no log-prefix=""

5. Hasil dan Pembahasan

5.1. Operate

Hasil dari pengoperasi dari penerapan perubahan ditampilkan pada Table 7.

Tabel 7.
Tabel Analisa Pengoperasian

No.	Request	Tranfered Over Network (kB)	*Resourc Loaded (kB)*	*Time Loaded (s)*
1.	615	5400	14000	19,58
2.	150	1900	3700	6,19
3.	234	3500	7700	10
4.	185	3500	7300	11,37
5.	95	1100	5000	19,84

5.2. Optimize

Hasil optimasi yang didapatkan ditampilkan pada Table 8 dan Tabel 9.

Tabel 8.
Hasil Optimasi

No.	Request	Transfered Over Network (kB)	*Resource Loaded (kB)*	*Time Loaded (s)*
1.	379	1000	2200	28,44
2.	347	1600	5200	40,46
3.	494	3400	10200	35,99
4.	296	1300	4000	22,96
5.	161	3100	6100	24,74

Tabel 9.
Persentasi Hasil Optimasi

No.	Request (%)	Transfered Over Network (%)	*Resource Loaded (%)*	*Time Loaded (%)*
1.	38,13	15,63	13,58	59,23
2.	69,82	45,71	58,43	86,73
3.	67,86	49,28	56,98	78,26
4.	61,54	27,08	35,40	66,88
5.	62,89	73,81	54,95	55,50
Rata[2]	60,05	42,30	43,87	69,32

6. Kesimpulan dan Saran

Penerapan dari DNS Sinkhole menggunakan Pi-hole sebagai layanan penyaringan akses internet yang dikelola secara mandiri bekerja dengan sangat baik. Terbukti pada hasil optimasi dan persentasi optimasi yang didapatkan rata-ratanya pada Request 60,05%, Transferred Over Network 42,30%, Resource Loaded 43,87 dan Time Loaded 69,32%.

Sebagai saran pengembangan dari penerapan penelitian ini, untuk menambahkan data blocklist dari komunitas penyedia lain dan selalui di update secara berkala.

Referensi

[1] WSIS: Declaration of Principles. (n.d.). https://www.itu.int/net/wsis/docs/geneva/official/dop.html
[2] Kontributor dari proyek Wikimedia. (2022). Hak atas akses internet. Wikipedia Bahasa Indonesia, Ensiklopedia Bebas. https://id.wikipedia.org/wiki/Hak_atas_akses_internet
[3] S.Ali, I., Hamza, S., & Gunawan, E. (2020). Implementasi & Analisis Penerapan Pi-Hole Network Ad-Blocking Di Laboratorium Jaringan Teknik Informatika UMMU. In Jurnal Teknik Informatika (J-Tifa) (Vol. 3, Issue 1, pp. 27–31). Universitas Muhammadiyah Maluku Utara. https://doi.org/10.52046/j-tifa.v3i1.1110
[4] Republik Indonesia. 2014. Undang-Undang Republik Indonesia Nomor 19 Tahun 2014 tentang Penanganan Situs Internet Bermuatan Negatif. Kementerian Komunikasi dan Informatika. Jakarta.
[5] BlockList:Project. (n.d.). https://blocklist.site/
[6] Badan Siber dan Sandi Negara. 2022. Laporan Bulanan Publik Hasil Monitoring Keamanan Siber Desember 2022. Available at: https://cloud.bssn.go.id/s/GfpcGJNQqSZRgDE (Accessed 21 Juni 2023).
[7] Kontributor dari proyek Wikimedia. (2023). Internet Sehat dan Aman. Wikipedia Bahasa Indonesia, Ensiklopedia Bebas. https://id.wikipedia.org/wiki/Internet_Sehat_dan_Aman
[8] Miftahur Rahman. (2023). Implementasi Web Content Filtering Pada Jaringan RT/RW Net Menggunakan Pi-Hole DNS Server. Generation Journal, 7(1), 50-60. https://doi.org/10.29407/gj.v7i1.19818
[9] Abdurahman, Okky, Kalsum, T., & Riska, R. (2022). Penerapan PI Hole DNS Server Sebagai ADS-Blocker Dan Sistem Filtering Website Pada Jaringan Hotspot. JURNAL MEDIA INFOTAMA, 18(2), 208-217. https://doi.org/10.37676/jmi.v18i2.2658
[10] Quad9 | A public and free DNS service for a better security and privacy. (n.d.). Quad9. https://www.quad9.net/
[11] BlockList:Project. (n.d.-b). https://blocklist.site/
[12] Nirwana, A., Hasibuan, M., & Hediyanto, U. (2018). Perancangan Network Structure Data Center Untuk Meningkatkan Availability Jaringan Di Pemerintah Kabupaten Bandung Menggunakan Standar TIA-942 Dengan Metode PPDIOO Life-cycle Approach. Jurnal Rekayasa Sistem & Industri (JRSI), 5(01), 8-14. doi:10.25124/jrsi.v5i01.314
[13] Muhamad Apriyatna. (2022). Analisis dan Implementasi Network Ad-blocking Pi-Hole di Raspberry Pi 4 Menggunakan OPNSense DHCP Dengan Metode PPDIOO Studi Kasus Dinas Komunikasi Informatika Statistik dan Persandian Kabupaten Lebak. OKTAL: Jurnal Ilmu Komputer Dan Sains, 1(11), 1943–1950. Retrieved from https://journal.mediapublikasi.id/index.php/oktal/article/view/811
[14] Moore, M., & Tambini, D. (Eds.). (2018). Digital dominance: The power of Google, Amazon, Facebook, and Apple. New York, NY: Oxford University Press.
[15] Eckersley, P. (2018). The Pi-hole Ad Blocker. California. No Strach Press.
[16] Klimburg, A. (2017). The Darkening Web: The War for Cyberspace. London. Penguin Books.
[17] Liu, C. and Albitz, P. (2017). DNS and Bind. Massachusetts. O'Reilly Media.
[18] IT Starter Series. (2021). Cisco CCNA Networking For Beginners: 3 in 1-Threee Books in One (CCNA, Networking, IT Security). Illinois. Independently published.
[19] Website Traffic - Check and Analyze Any Website. (n.d.). https://www.similarweb.com/