Terbit pada laman web jurnal : **http://ojsamik.amikmitragama.ac.id**

JURNAL JARINGAN SISTEM INFORMASI ROBOTIK (JSR)
Vol. 8 No. 2 TAHUN 2024 E - ISSN : 2579-373X

PERANCANGAN DNS FILTERING DENGAN UNBOUND PADA UBUNTU 22.04 UNTUK AKSES WEB PT. SMART TEKNOLOGI UTAMA

Muharmansyah[1], Anton[2,*]
[1,2]Fakultas Teknologi Informasi, Informatika, Universitas Nusa Mandiri, Jakarta, Indonesia
Email: [1]armansyah20y@gmail.com, [2,*]Anton@nusamandiri.ac.id

Abstrak
PT. Smart Teknologi Utama yang memiliki jaringan metro ethernet menghadapi masalah belum tersedianya sistem penyaringan yang memadai untuk mencegah akses ke situs web dengan konten negatif. Situasi ini dapat membahayakan keamanan serta integritas jaringan perusahaan. Walaupun pemerintah telah menetapkan Undang-Undang Nomor 19 Tahun 2016 yang bertujuan untuk membatasi akses ke konten negatif, implementasi filter yang efektif oleh penyedia layanan internet (ISP) masih diperlukan. Penelitian ini dilakukan untuk merancang dan menerapkan sistem penyaringan DNS menggunakan Unbound, sebuah aplikasi open-source, pada server berbasis Ubuntu 22.04. Metode penelitian mencakup tahapan studi literatur, analisis kebutuhan jaringan, perancangan topologi, serta pengujian sistem yang dirancang. Implementasi dilakukan dengan cara mengkonfigurasi Unbound agar mampu memblokir akses ke situs web yang berbahaya. Hasil pengujian menunjukkan bahwa sistem penyaringan DNS yang dibangun dapat menghalangi akses ke situs-situs negatif sesuai dengan konfigurasi yang diterapkan. Dengan demikian, penggunaan Unbound terbukti efektif dalam meningkatkan keamanan jaringan pada lingkungan PT. Smart Teknologi Utama.

Kata Kunci: ISP, Internet, DNS filtering, Unbound

Abstract
PT. Smart Technology Utama, which operates a metro ethernet network, faces the issue of inadequate filtering systems to prevent access to websites with negative content. This situation can jeopardize the security and integrity of the company's network. Although the government has enacted Law Number 19 of 2016 aimed at restricting access to negative content, effective filter implementation by Internet Service Providers (ISPs) is still required. This study was conducted to design and implement a DNS filtering system using Unbound, an open-source application, on a server based on Ubuntu 22.04. The research method includes stages such as literature review, network requirements analysis, topology design, and testing of the designed system. Implementation was carried out by configuring Unbound to block access to harmful websites. Test results show that the DNS filtering system built can effectively block access to negative sites according to the applied configuration. Thus, the use of Unbound has proven to be effective in enhancing network security in the environment of PT. Smart Technology Utama.

Keywords: ISP, Internet, DNS filtering, Unbound

1. PENDAHULUAN

Metro ethernet merupakan perkembangan dari teknologi jaringan *ethernet*, yang memiliki jarak berskala lebih luas, dengan cakupan suatu kota atau wilayah. Dapat didefinisikan sebagai jembatan antara jaringan *LAN (Local Area Network)* yang terpisah secara geografis dan menghubungkan *WAN (Wide area Network)* atau *backbone* yang dimiliki oleh suatu *ISP*[1].

Ada dua jenis layanan metro ethernet, diantaranya point to point yang menghubungkan dua titik dan *multipoint* yang menghubungkan beberapa titik. PT Smart Teknologi Utama merupakan salah satu dari banyak penyedia jasa komunikasi internet yang menggunakan teknologi jaringan *metro ethernet*. Di Indonesia, dengan adanya Undang-undang No.19 Tahun 2016 yang merupakan *update* dari Undang-undang No.11 tahun 2008 tentang informasi dan transaksi elektronik pasal 27 ayat (1) yang berbunyi "Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan. Yang dimaksud dengan "mendistribusikan" adalah mengirimkan dan/atau menyebarkan Informasi Elektronik dan/atau Dokumen Elektronik kepada banyak Orang atau berbagai pihak melalui Sistem Elektronik. Yang dimaksud dengan

"mentransmisikan" adalah mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang ditujukan kepada satu pihak lain melalui Sistem Elektronik. Yang dimaksud dengan "membuat dapat diakses" adalah semua perbuatan lain selain mendistribusikan dan mentransmisikan melalui Sistem Elektronik yang menyebabkan Informasi Elektronik dan/atau Dokumen Elektronik dapat diketahui pihak lain atau publik", sehingga selain adanya *blocking* dari pemerintah, *ISP* juga memiliki tanggung jawab untuk menghindari teraksesnya website yang memiliki konten negatif.

DNS Filtering merupakan salah satu solusi dalam teknologi keamanan jaringan yang dapat diterapkan untuk membatasi akses penggunaan layanan internet terhadap *website* yang memiliki konten negatif [2], hal ini bertujuan untuk membangun sistem *internet* sehat bagi pengguna layanan *internet* saat ini[3]. *DNS Filtering* berbeda dengan DNS server biasa, yakni *DNS server* khusus yang memiliki kemampuan untuk menyaring alamat dari sebuah *host*[4]. Untuk menggunakan teknologi *DNS Filtering* diperlukan suatu aplikasi yang memiliki fitur tersebut, penulis menggunakan aplikasi *Unbound* yang merupakan aplikasi *opensource* dari *net labs* yang memiliki fungsi untuk memvalidasi, *recursive* dan *caching DNS resolver*, memiliki tingkat kerentanan terhadap serangan *cache poison* lebih rendah karena secara *default resolver* akan melakukan kueri ulang setiap 24 Jam[5].

Beberapa penelitian sebelumnya telah mengimpelementasikan keamanan jaringan dengan melakukan block atau filtering terhadap konten negatif. Penelitian [3] menerapkan DNS filtering dengan bantuan perangkat routerboard mikrotik untuk membatasi akses internet. Penelitian [5] penelitian mengenai DNS Unbound yang memiliki fitur DNS resolver yang dapat menggunakan waktu relatif untuk keperluan caching dari pada menggunakan waktu absolut, sehingga lebih kebal terhadap serangan berdasarkan waktu dari pihak eksternal. Penelitian [6] menerapkan sistem web filtering dengan metode DNS forwarding yang diterapkan pada jaringan komputer berbasis mikrotik router OS untuk meminimalisir pengaksesan situs web dengan konten negatif. Penelitian [7] yang berfokus pada perancangan jaringan metro ethernet untuk penyebaran jaringan baik di dalam maupun hingga luar kota.

Penelitian [4] yang berfokus pada research pengetahuan mengenai internet positif pada lingkungan universitas UIN Ar-Raniry banda aceh, serta melakukan komparasi terhadap beberapa produk DNS filtering untuk mengetahui akurasinya, diantaranya seperti DNS Nawala, Open DNS dan Norton DNS. Penelitian [8] berfokus pada bagaimana pembangunan jaringan menggunakan fiber optic pada metro ethernet, penelitian [9] berfokus pada bagaimana mebangun jaringan yang dapat dikelola dengan router mikrotik.

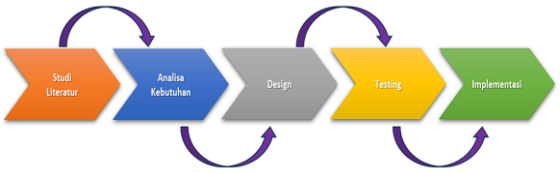
Mikrotik dikenal sebagai router yang memiliki fitur sangat lengkap, dapat dikonfigurasi lebih mudah dan memiliki harga yang relatif lebih murah. saat ini produk mikrotik sudah banyak digunakan oleh pelaku bisnis di bidang jaringan komputer, seperti warnet, *Internet Service Provider* (ISP), perusahaan kecil hingga besar, bisnis rumahan dan lain sebagainya. memiliki banyak fitur yang lebih canggih seperti *NAT, DHCP*, bahkan hingga security[10]

Jaringan komputer juga memiliki berbagai jenis topologi, jaringan metro ethernet biasanya menggunakan topologi hybrid[11], yakni topologi yang merupakan kombinasi dari dua atau lebih jenis topologi, yang mana salah satunya digunakan sebagai backbone[12].

Dari beberapa studi yang telah dijelaskan sebelumnya, *DNS Filtering* merupakan suatu teknologi penting untuk dapat membatasi akses pengguna terhadap konten negatif[13], yang mana konten negatif ini akan terus berkembang, sehingga perlu adanya penerapan *DNS Filtering* baik dari sisi pemerintah maupun *ISP*. Oleh karena itu, penelitian ini akan menerapkan *DNS filtering* menggunakan Unbound sehingga dapat melakukan *blocking* konten negatif terhadap pengguna internet pada lingkungan PT Smart Teknologi Utama.

2. METODOLOGI PENELITIAN

Tahapan dalam proses penelitian tentang perancangan *DNS filtering* dengan *unbound* pada *Ubuntu 22.04* untuk akses web PT. Smart Teknologi Utama dapat dilihat pada Gambar 1.



Gambar 1. Metode Penelitian

Tahapan Studi Literatur

Pada tahap ini dilakukan pengumpulan data dan informasi mengenai masalah saat penelitian, penulis melakukan wawancara dan observasi langsung pada PT. Smart Teknologi Utama untuk mengumpulkan informasi mengenai jaringan komputer yang berjalan, serta melakukan eksplorasi terhadap literatur yang relevan dengan topik penelitian melalui berbagai sumber seperti jurnal ilmiah, buku, artikel daring dan sumber lainnya.

Tahapan Analisa kebutuhan

Pada tahap ini penulis melakukan analisis dari insfrastruktur jaringan yang ada untuk mendapatkan kebutuhan dalam melakukan perancangan dari penelitian yang akan dibuat.

Tahapan *Design*

Pada tahap ini penulis menggambarkan topologi jaringan yang saat ini sudah terimpelementasi serta perancangan topologi dalam penelitian ini pada PT. Smart Teknologi Utama.

Tahapan *Testing*

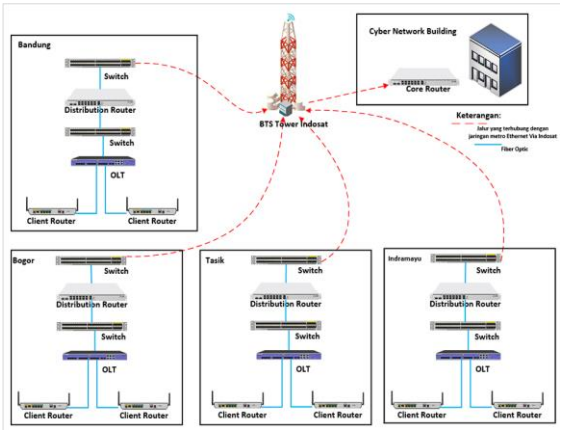
Pada tahapan ini dilakukan pengujian terhadap perancangan *DNS filtering* pada PT. Smart Teknologi Utama dengan menguji akses terhadap *website-website* berbahaya dari sisi *client.*

Tahapan Implementasi

Pada tahapan ini merupakan tahap akhir dari penelitian ini, yakni implementasi secara langsung dari *live testing* yang telah dilakukan dari perancangan yang telah dibuat untuk mendapatkan hasil yang diinginkan, yakni dari sisi *client* tidak dapat akses terhadap *website-website* berbahaya dari sisi *client.*

3. HASIL DAN PEMBAHASAN

Berdasarkan penelitian yang dilakukan pada PT. Smart Teknologi Utama, terdapat skema jaringan yang berjalan yang dapat dilihat pada gambar 2.



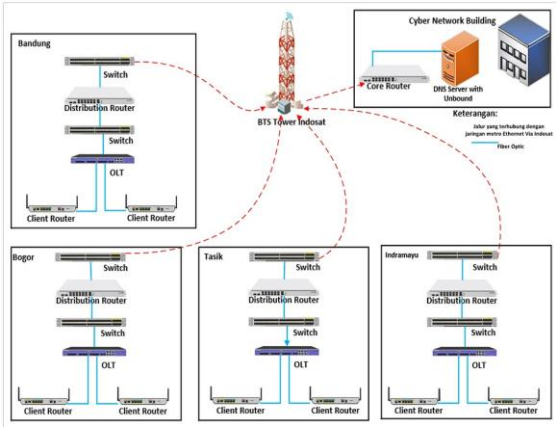
Gambar 2. Skema Jaringan Berjalan

Pada skema jaringan berjalan bisa terlihat bahwa sumber internet menggunakan pipa *via* Indosat, Dari keseluruhan Kantor Cabang topologi semua sama menggunakan topologi *Hybrid.* Yang mana koneksi dari jaringan *Metro Ethernet via* jalur *BTS* Indosat langsung masuk ke *Switch Mikrotik CSS326-24G-2S+RM* pada setiap Kantor Cabang, dari Kantor Cabang akan di ditribusikan melalui *Router Mikrotik CCR2004-1G-12S+2XS*, dari *router* akan terhubung ke *switch Nexus 36180YC-R* yang terhubung ke *OLT (Optical Line Terminal) ZTE C220.* Semua koneksi menggunakan kabel *fiber optic*. Semua perangkat keras PT. Smart Teknologi Utama yang terhubung di *router* masing-masing Kantor Cabang menggunakan IP *public* yang di distribusikan oleh *Router* PT. Smart Teknologi Utama.

Berdasarkan peraturan pemerintah yang sudah dibahas sebelumnya penulis menemukan masalah pada jaringan berjalan PT. Smart Teknologi Utama, yakni tidak adanya filtering dari sisi DNS, sehingga banyak pengaksesan berbagai situs negatif yang mana berbahaya bagi pengguna maupun jaringan bisnis PT. Smart Teknologi Utama karena rentan terhadap serangan virus.

3.1. Rancangan Jaringan Usulan

Penulis usulkan untuk PT. Smart Teknologi Utama adalah menerapkan *stand alone* DNS Server yang khusus untuk memfilter akses terhadap *website negatif[14]*, rancangan jaringan usulan yang terlihat pada gambar 3. seiring dengan kemajuan teknologi semakin banyak adanya kejahatan siber baik yang berasal dari dalam (internal) maupun yang berasal dari luar (eksternal) sistem jaringan komputer, sehingga dalam jaringan ada firewall yang berfungsi untuk memfilter ip tertentu, untuk solusi ini diperlukan juga konfigurasi dari sisi firewall internal pada router core untuk meredirect packet request ke DNS server tujuan.



Gambar 3. Rancangan Jaringan Usulan

Pada jaringan usulan, penulis tetap memanfaatkan semua insfrastruktur yang sudah ada tidak merubah keamanan jaringan yang sudah ada. dengan mengimplementasikan *DNS filtering* dengan *Unbound* yang diinstall pada *server OS Ubuntu 22.04* diharapkan dapat mencegah akses terhadap website negatif.

Berdasarkan jaringan usulan yang diusulkan oleh penulis, adapun aplikasi yang digunakan untuk mengimplementasikan sebagai berikut:

a. *Ubuntu 22.04*

Ubuntu 22.04 merupakan sistem operasi *open source* berbasis *linux*, berbasis *debian distro* yang didasarkan pada *kernel linux*. Merupakan salah satu *distro linux* yang banyak dipakai dan cocok pada banyak perangkat.

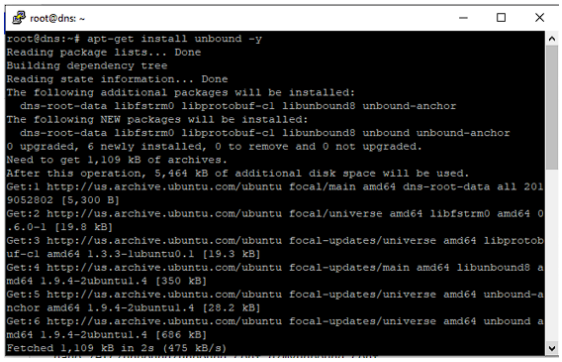
b. *Unbound*

Unbound merupakan aplikasi yang diinstall di *server* yang berfungsi untuk memvalidasi, sebagai *rekusrsif* dan juga *caching* D*NS resolver*. Yang di

design untuk bisa bekerja lebih cepat dan memiliki fitur yang lebih *modern*.

3.2 Implementasi

Implementasi yang dilakukan penginstallan OS Ubuntu 22.04 pada stand alone server dan penginstallan Unbound dapat dilihat pada gambar 4. sebagai aplikasi DNS yang akan dikonfigurasi DNS filtering.



Gambar 4. Installasi Unbound

konfigurasinya *unbound* pada file dnsunbound.conf pada direktori /*etc/unbound/unbound.conf.d/*dns*unbound.conf*

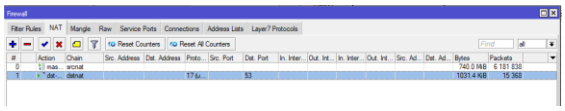
```
server:
        port: 53
        verbosity: 1
        statistics-interval: 120
        num-threads: 2
        outgoing-range: 512
        num-queries-per-thread: 1024
        msg-cache-size: 32m
        interface: 0.0.0.0
        rrset-cache-size: 64m
        msg-cache-slabs: 4
        rrset-cache-slabs: 4
        cache-max-ttl: 86400
        infra-host-ttl: 60
        infra-lame-ttl: 120
        infra-cache-numhosts: 10000
        infra-cache-lame-size: 10k
        do-ip4: yes
        do-ip6: no
        do-udp: yes
        do-tcp: yes
        #access-control: 127.0.0.0/8 allow
        access-control: 0.0.0.0/0 allow

forward-zone:
        name: "."
        forward-addr: 1.1.1.1
        forward-addr: 8.8.4.4
        forward-addr: 8.8.8.8
          include: /etc/unbound/block.conf
          chroot: ""
        username: unbound
        directory: /etc/unbound
        logfile: /var/log/unbound/unbound.log
        log-queries: yes
        use-syslog: no
        #pidfile: /etc/unbound/unbound.pid
        root-hints: /etc/unbound/named.cache
        identity: dns.rst.net.id
        server:
        local-zone: "rst.net.id." static
        local-data: "rst.net.id. 86400 IN SOA ns.rst.net.id. root 1 1D 1H 1W 1H"
        local-data: "dns.rst.net.id. IN A 0.0.0.0"
        local-data-ptr: "103.150.60.140 dns.rst.net.id."
        version: 1.4
        hide-identity: yes
        hide-version: yes
        harden-glue: yes
        do-not-query-address: 127.0.0.1/8
        do-not-query-localhost: yes
        module-config: iterator
        remote-control:
        control-enable: yes
        control-interface: 127.0.0.1
        control-interface: 0.0.0.0
        control-port: 953
        server-key-file: /etc/unbound/unbound_server.key
        server-cert-file: /etc/unbound/unbound_server.pem
        control-key-file: /etc/unbound/unbound_control.key
        control-cert-file: /etc/unbound/unbound_control.pem
```

konfigurasi untuk melakukan block terhadap website negatif terdapat pada file *File block.conf* pada directory */etc/unbound/block.conf*, pada file ini website negatif di input secara manual agar tidak dapat diakses.

```
root@dns:~# cat /etc/unbound/block.conf
server:
local-zone: "trust-positive.rst.net.id." redirect
local-data: "trust-positive.rst.net.id. 3600 IN A 103.156.17.177"
local-data: "example.com. 3600 IN MX 5 127.0.0.1"
local-data: "example.com. 3600 IN A 127.0.0.1"
local-data: "sblconference.com. 3600 IN A 103.156.17.177"
local-data: "seemedj.mefos.unios.hr. 3600 IN A 103.156.17.177"
local-data: "mackusushi.com. 3600 IN A 103.156.17.177"
local-data: "warren-pr.com. 3600 IN A 103.156.17.177"
local-data: "summerhillal.com. 3600 IN A 103.156.17.177"
local-data: "nssbexam.com. 3600 IN A 103.156.17.177"
```

local-data: "pafimimika.org. 3600 IN A 103.156.17.177"
local-data: "shcattanbark.com. 3600 IN A 103.156.17.177"
local-data: "ghostsofmarietta.com. 3600 IN A 103.156.17.177"
local-data: "soldmagny.com. 3600 IN A 103.156.17.177"
root@dns:~#

Menambahkan *rule* didalam *Core Router* RSTNet (*CCR2004-1G-12S+2XS*) dapat dilihat pada gambar 5, dengan *meredirect* semua *traffic DNS* dari semua *remote Metro Ethernet via jalur BTS Indosat* yang *Online* ke *Unbound* DNS *Server*.



Gambar 5. Penambahan rule pada core router

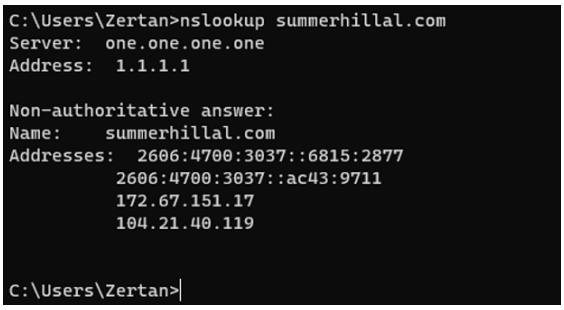
3.3 Pengujian Jaringan Usulan

3.3.1 pengujian sebelum Implementasi

Pada gambar 6 penulis melakukan *test* koneksi *internet* menggunakan jaringan *metro ethernet* PT. Smart Teknologi Utama. penulis melakukan pengujian dengan 1 buah Laptop sebagai *client*. Dan melakukan *test browsing* ke beberapa *website* yang di anggap tidak baik dan mengadung unsur sara, perjudian kekerasan atau pembajakan hak cipta, salah satu website yang dilakukan pengujian untuk akses sebelum implementasi dapat dilihat pada gambar 6.

Gambar 6. Pengujian akses web sebelum implementasi

Pada gambar 7, penulis melakukan pengujian akses langsung pada website, dengan melakukan test nslookup untuk melihat akses DNS sebelum implementasi dilakukan.



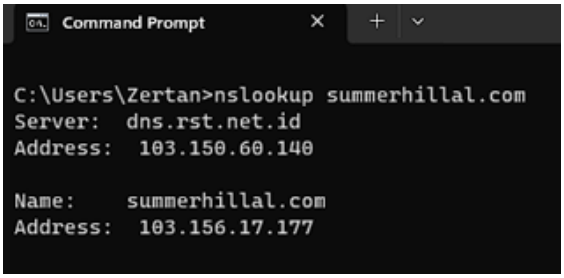
Gambar 7. Pengecekan Nslookup sebelum implementasi

3.3.2 Pengujian Setelah Implementasi

Penulis melakukan Pengujian kembali setelah implementasi dengan melakukan percobaan akses pada website sample yang sebelumnya, dengan menggunakan DNS server *Unbound* pada jaringan metro ethernet PT.Smart Teknologi Utama, dapat dilihat pada gambar 8.

Gambar 8. Hasil Block DNS server Unbound

Penulis melakukan pengujian kembali dengan nslookup untuk memastikan DNS yang dilalui sudah sesuai dengan konfigurasi pada jaringan metro ethernet PT.Smart Teknologi Utama, dapat dilihat pada gambar 9.



Gambar 9. Pengecekan nslookup stelah implementasi

Dari gambar *log* diatas terlihat bahwa *traffic* untuk *DNS* sudah melalui *unbound*, dari hasil *test* juga menunjukan setelah *implementasi* untuk *server unbound* baik dengan aplikasi, *nslookup* dan block untuk mencoba *browsing* ke *website-website* yang di anggap tidak baik untuk customer pada jaringan *metro ethernet* PT. Smart Teknologi Utama berhasil dilakukan.

4. KESIMPULAN

Berdasarkan peraturan yang dikeluarkan oleh Kominfo dalam penyediaan layanan jaringan, PT. Smart Teknologi Utama wajib untuk mematuhi ketentuan yang ada. Dengan perkembangan teknologi saat ini, banyak metode yang dapat diterapkan untuk melakukan filtering terhadap website negatif, salah satunya adalah dengan menggunakan Unbound. Hasil riset, analisis, serta implementasi yang telah dilakukan menunjukkan bahwa penggunaan Unbound untuk filtering website negatif dapat diterapkan pada jaringan metro ethernet tanpa memerlukan konfigurasi khusus dari sisi klien. Semua permintaan akses akan diarahkan oleh firewall di router inti pada jaringan metro ethernet ke DNS Server Unbound menggunakan aturan NAT. Penelitian selanjutnya dapat difokuskan pada pengembangan sistem DNS filtering yang lebih dinamis dan adaptif, seperti integrasi dengan sistem pemantauan berbasis machine learning untuk mendeteksi dan memblokir situs berbahaya secara otomatis. Selain itu, perlu dilakukan evaluasi performa dan skalabilitas Unbound pada lingkungan jaringan yang lebih kompleks dengan jumlah pengguna yang lebih besar. Penerapan teknologi DNS over HTTPS (DoH) atau DNS over TLS (DoT) [15]juga dapat menjadi topik yang menarik untuk meningkatkan keamanan transmisi data dalam konteks filtering DNS ini.

5. REFERENCES

[1] Y. Rahmawati and N. Mutiara Anjani, "Implementation of Link Failover on Metronet Network PT. Telkom Indonesia (Persero) Based on Ipv4 and OSPF," *Journal Of Informatics And Telecommunication Engineering*, vol. 6, no. 2, pp. 458–472, Jan. 2023, doi: 10.31289/jite.v6i2.8313.

[2] Md. Sohidul Islam, Md. Sajjad, M. Mahmudul Hasan, and M. Sakib Islam Mazumder, "Phishing Attack Detecting System Using DNS and IP Filtering," *Asian Journal of Computer Science and Technology*, vol. 12, no. 1, pp. 16–20, Apr. 2023, doi: 10.51983/ajcst-2023.12.1.3552.

[3] 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, May 2019, doi: 10.30595/juita.v7i1.4164.

[4] H. Mizuardy, B. Yusuf Program Studi Pendidikan Teknologi Informasi Fakultas Tarbiyah Dan Ilmu Keguruan, and U. Ar-Raniry Banda Aceh -Indonesia, "Dns Filtering: A Clean And Positive Internet Environment In Uin Ar-Raniry Banda Aceh," 2018.

[5] A. Malhotra, W. Toorop, B. Overeinder, R. Dolmans, and S. Goldberg, "The Impact of Time on DNS Security," 2019.

[6] H. Jurnal, R. I. Ramadhan, and M. Ladjamuddin, "Jurnal Informatika Dan Teknologi Komputer Perancangan Sistem Web Filtering Dengan Metode Dns Forwarding Pada Jaringan Komputer Berbasis Mikrotik Routeros," *Juli*, vol. 2, no. 2, pp. 146–157, 2022.

[7] H. Jurnal, U. P. Anggraini, Y. Ramadani, A. Pramono, and D. Aribowo, "Jurnal Ilmiah Teknik Informatika dan Komunikasi Simulasi Perencanaan Jaringan Transport Metro Ethernet Menggunakan Aplikasi Cisco Packet Tracker Pada Perusahaan Antar Cabang," vol. 3, no. 1, 2023.

[8] P. Muliandhi *et al.*, "Analisa Konfigurasi Jaringan FTTH dengan Perangkat OLT Mini untuk Layanan Indihome di PT. Telkom Akses Witel Semarang," 2020.

[9] H. Gunawan and M. Ghiffari, "Pengelolaan Jaringan Dengan Router Mikrotik Untuk Meningkatkan Efektifitas Penggunaan Bandwith Internet (Studi Kasus Smk Ki Hajar Dewantoro Kota Tangerang)," 2018.

[10] Rendra towidjojo, *Mikrotik Kungfu Kitab1*. jasacom.com, 2019.

[11] D. I. Mulyana, F. Ardiyansyah, N. Hidayat, and A. Zulfikar, "Optimasi Keamanan Jaringan Wifi dari Situs Judi Online dan Pornografi dengan DNS Filtering dan Orangepi," *MALCOM: Indonesian Journal of Machine Learning and Computer Science*, vol. 4, no. 2, pp. 647–655, Mar. 2024, doi: 10.57152/malcom.v4i2.1274.

[12] D. Putra, P. Ahmad, B. Setiawan, and R. A. Ramadhani, *JARINGAN KOMPUTER DASAR*, 1st ed. CV. Kasih Inovasi Teknologi, 2018.

[13] R. I. Ramadhan and S. M. Ladjamuddin, "Perancangan Sistem Web Filtering Dengan Metode Dns Forwarding Pada Jaringan Komputer Berbasis Mikrotik

Routeros," *Jurnal Informatika Dan Tekonologi Komputer (JITEK)*, vol. 2, no. 2, pp. 146–157, 2022.

[14] J. Bushart and C. Rossow, "Anomaly-based Filtering of Application-Layer DDoS Against DNS Authoritatives," in *2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P)*, IEEE, Jul. 2023, pp. 558–575. doi: 10.1109/EuroSP57164.2023.00040.

[15] T. Murakami, K. Shimabukuro, N. Sato, R. Nakagawa, Y. Jin, and N. Yamai, "Trustworthy Name Resolution Using TLS Certificates with DoT-enabled Authoritative DNS Servers," in *2023 IEEE 47th Annual Computers, Software, and Applications Conference (COMPSAC)*, IEEE, Jun. 2023, pp. 1121–1126. doi: 10.1109/COMPSAC57700.2023.00169.