EVALUASI PENGGUNAAN MIKROTIK DAN LAYANAN *CLOUD* (QUAD9 VS *CLOUDFLARE GATEWAY*) DALAM MENDETEKSI *CRYPTOJACKING*

Arief Budi Pratomo
Fakultas Teknik & Informatika, Universitas Nusa Megarkencana, Yogyakarta, Indonesia
budiprato@gmail.com

ABSTRAK

Tujuan dari penelitian ini adalah untuk menguji efektivitas DNS QUAD*9 dalam mendeteksi dan memblokir ancaman keamanan seperti cryptojacking pada jaringan internet rumah. Metode eksperimen digunakan dengan mengimplementasikan DNS* QUAD*9 pada router Mikrotik dan melakukan uji coba terhadap akses ke situs yang terkait dengan cryptojacking. Sebagai perbandingan, kinerja Cloudflare Gateway juga dievaluasi, mengingat sebelumnya telah terbukti efektif dalam menangkal serangan cryptojacking menurut penelitian oleh Adhar (2023). Hasil yang diperoleh menunjukkan bahwa DNS* QUAD*9 tidak mampu memblokir akses ke situs cryptojacking, sementara Cloudflare Gateway berhasil melakukannya. Meskipun demikian,* QUAD*9 memiliki potensi untuk mendeteksi ancaman lainnya, seperti malware dan phishing, yang memerlukan pengujian lebih lanjut untuk mengevaluasi efektivitasnya. Kesimpulannya, Cloudflare Gateway lebih efektif dalam menangkal cryptojacking dibandingkan dengan DNS* QUAD*9, meskipun* QUAD*9 masih relevan untuk jenis ancaman lainnya..*

Keyword: DNS QUAD*9, Cloudflare Gateway, Keamanan Jaringan, Mikrotik*

1 PENDAHULUAN

Internet menjadi kebutuhan mendasar bagi berbagai macam kalangan, instansi dan berbagai macam organisasi memanfaatkan internet sebagai penunjang pekerjaan (Saputra, 2024). Penggunaan internet yang tidak terkontrol dapat menyebabkan berbagai macam kendala dan kerugian yang akan ditanggung oleh organisasi, selain itu internet juga dapat menjadi jalan masuk kejahatan yang akan merugikan instansi atau organisasi (Khairil, 2023).

Dalam mengamankan jaringan internet beberapa penelitian terdahulu telah memanfaatkan berbagai macam *firewall*, baik menggunakan *hardware* maupun dengan memanfaatkan *software*, untuk instansi yang memiliki sumber daya keuangan yang besar, tentunya tidak akan kesulitan dengan biaya pengadaan *hardware* dan *software*, namun untuk instansi yang terkendala keuangan akan sangat berat untuk mendapatkan perangkat yang mahal, dilain sisi keamanan jaringan internet sangat diperlukan, shingga perlu memanfaatkan layanan *firewall* yang murah dan mudah dikonfigurasi (Fikri, 2022).

Layanan *cloud* seperti *software as service (SaaS)* yang menawarkan *firewall* dengan harga yang relatif terjangkau dapat dimanfaatkan dalam rangka mengamankan jaringan internet. Salah satu layanan yang dapat digunakan adalah *Cloudflare gateway*, *cloudflare gateway* adalah SaaS yang berfungsi menangkal serangan dengan memanfaakan *Domain Name System (DNS)*. Adhar pada 2023 memanfaatkan *cloudflare gateway* yang dikombinasikan dengan *router* mikrotik untuk menangkal serangan *cryptojacking* pada jaringan internet, hasilnya *cloudflare gateway* mampu menangkal *botnet mining* (*cryptojacking*). Selain menangkal aktifitas *mining cloudflare gateway* juga mampu digunakan untuk mendeteksi aktifitas pornografi pada jaringan internet, saputra pada 2024 menjelaskan bahwa *cloudflare gateway* efektif dalam mendeteksi pornografi dan dapat meningkatkan penggunaan *bandwidth* pada kegiatan yang lebih bermanfaat.

Selain *cloudflare gateway* terdapat layanan *cloud* lain yang memanfaatkan *DNS* dalam mendeteksi serangan, selain *cloudflare gateway* terdapat beberapa *DNS firewall* yang dapat dimanfaatkan, misalnya *DNS secure* dari QUAD9, *DNS* ini hanya dipasang pada perangkat dan langsung dapat memfilter konten yang tidak aman, namun layanan ini tidak memiliki panel *control* yang dapat digunakan untuk mengidentifikasi konten apa yang diblokir. Namun keuntungan dari menggunakan *DNS secure* dari QUAD9 adalah kemudahan dalam konfigurasinya, serta tidak memerlukan jaringan dengan *dedicated* IP, dimana *cloudflare gateway* memerlukan *dedicated* IP untuk terhubung ke panel layanannya.

Dengan berbagai pertimbangan diatas, maka penelitian ini akan berfokus pada implementasi *DNS* QUAD 9, yang akan di implementasikan ke jaringan internet *shared*. *DNS* QUAD9 akan diuji untuk memblokir konten *malware*, dengan membandingkannya dengan penelitian Adhar 2023. Diharapakan dengan adanya *DNS* dari QUAD 9, jaringan internet *shared* juga dapat dilindungi dengan metode *DNS filtering*.

2 LITERATUR REVIEW

Dalam menyelesaikan penelitian ini, beberapa kajian teori dalam mendukung penelitian ini adalah sebagai berikut:

2.1 *DNS Firewall*

DNS Firewall adalah sistem keamanan jaringan yang berfungsi untuk memantau dan memfilter permintaan *DNS* (*Domain Name System*). Tujuannya adalah mencegah akses ke domain yang berbahaya, seperti situs yang terinfeksi *malware, phishing*, atau domain yang digunakan untuk aktivitas berbahaya lainnya (Marques, 2021).

DNS Firewall adalah solusi yang dirancang untuk mencegah pengguna mengakses domain berbahaya. Sistem ini memberikan perlindungan secara real-time dengan memblokir komunikasi yang tidak sah, sehingga

berkontribusi pada peningkatan keamanan siber organisasi (Hernàndez, 2022).

2.2 QUAD9

QUAD9 adalah layanan *DNS* publik yang memberikan keamanan tambahan dengan memblokir akses ke domain berbahaya menggunakan analisis ancaman berbasis data. Layanan ini gratis dan dirancang untuk melindungi pengguna dari *malware*, *phishing*, dan ancaman *online* lainnya (Chhabra, 2021).

QUAD9 adalah layanan *DNS* publik gratis yang berfokus pada keamanan dan privasi, dioperasikan oleh organisasi nirlaba dengan dukungan dari IBM, Packet Clearing House, Global Cyber Alliance, dan organisasi keamanan siber lainnya. Layanan ini memiliki beberapa keunggulan dibandingkan resolver *DNS* lainnya, termasuk tidak menyimpan *log* aktivitas pengguna, otomatis memblokir domain berbahaya seperti *phishing*, *malware*, dan *botnet*, mendukung enkripsi komunikasi melalui *DNS over* TLS dan HTTPS untuk melindungi data pengguna dari intersepsi, serta tersedia secara gratis untuk siapa saja (Sitanggang, 2024).

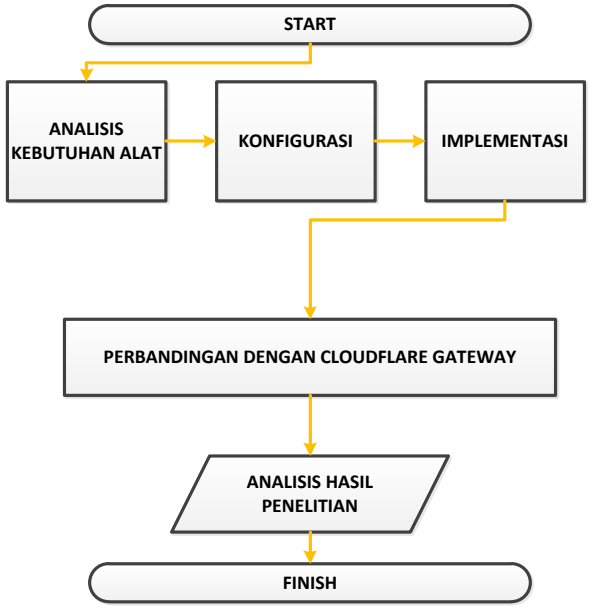
2.3 IP *shared* vs *dedicated*

layanan internet dengan *shared* IP, satu alamat IP digunakan oleh banyak pengguna atau perangkat. Hal ini sering ditemukan dalam layanan *shared hosting*, di mana beberapa website atau layanan berbagi satu alamat IP publik. Meskipun lebih hemat biaya, *shared* IP memiliki kelemahan, seperti potensi penurunan kecepatan internet jika banyak pengguna aktif atau masalah reputasi jika salah satu pengguna melakukan aktivitas yang merugikan (seperti spam). Layanan ini lebih cocok untuk pengguna rumahan atau usaha kecil yang tidak membutuhkan IP eksklusif.

Dalam hal ini, *dedicated* IP merujuk pada alamat IP yang sepenuhnya dialokasikan untuk digunakan oleh satu pengguna atau entitas tertentu. Hal ini berbeda dengan *shared* IP, di mana satu alamat IP digunakan oleh banyak pengguna. *Dedicated* IP biasanya digunakan oleh situs web atau layanan yang membutuhkan pengaturan yang lebih eksklusif, Keunggulan utama dari menggunakan *dedicated* IP adalah memberikan kontrol penuh atas pengaturan IP, stabilitas yang lebih tinggi, serta mengurangi risiko buruk yang mungkin timbul akibat aktivitas buruk dari pengguna lain yang menggunakan IP yang sama. Meskipun biaya yang terkait dengan *dedicated* IP lebih tinggi dibandingkan dengan *shared* IP, keuntungan yang ditawarkan dalam hal peningkatan keamanan, kinerja yang lebih stabil, dan reputasi yang lebih baik untuk IP tersebut menjadikannya pilihan utama, terutama bagi bisnis atau layanan yang memiliki tingkat kebutuhan yang lebih tinggi terkait keandalan dan keamanan. (NordLayer, 2024).

3 METODOLOGI

Penelitian ini menggunakan pendekatan metodologi eksperimen yang dirancang untuk menguji efektivitas dan kinerja berbagai layanan *DNS* dalam konteks pengamanan jaringan. Dalam penelitian ini, tahapan-tahapan yang terlibat dalam proses eksperimen diuraikan secara sistematis dan dapat dilihat secara visual melalui diagram yang terdapat pada Gambar 1 di bawah ini:



Gambar 1. Tahapan Penelitian

Penelitian ini bertujuan untuk menguji efektivitas penggunaan *DNS* QUAD9 dalam mendeteksi aktifitas *cryptojacking*. Sebagai perbandingan, penelitian ini akan membandingkan hasilnya dengan penelitian sebelumnya yang dilakukan oleh Adhar (2023) mengenai penggunaan *Cloudflare Gateway* dalam membatasi akses *cryptojacking*. Penelitian ini melibatkan beberapa tahapan, termasuk analisis kebutuhan, konfigurasi, implementasi, perbandingan hasil, serta analisis terhadap hasil yang diperoleh.

4 HASIL DAN PEMBAHASAN

Aplikasi ini dibagikan melalui *whatshapp* lalu di *download* oleh para siswa dan guru. Setelah itu instal aplikasi maka aplikasi sudah otomatis terpasang di android. Seperti gambar.

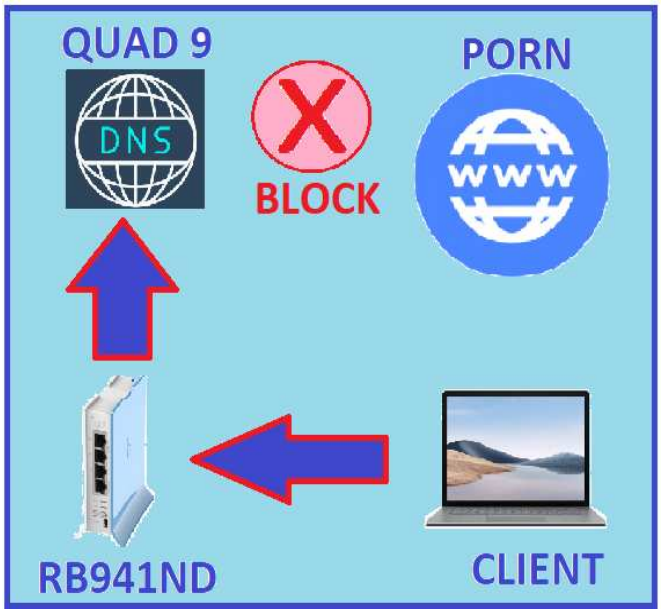
4.1 Analisis Kebutuhan Alat

Untuk mendukung penelitian ini, beberapa alat yang dibutuhkan dapat dilihat pada tabel 1 dibawah ini:

Tabel 1. Kebutuhan Alat

No	Nama Alat	Keterangan
1	Mikrotik *Router*, RB 941 ND	*Router* yang digunakan untuk mengimplementasikan QUAD9 *DNS*.
2	KABEL *UTP*	Kabel yang digunakan untuk menghubungkan *router* ke laptop (*client*).
3	Laptop	Alat yang digunakan untuk melakukan konfigurasi dan Uji coba (*client*).

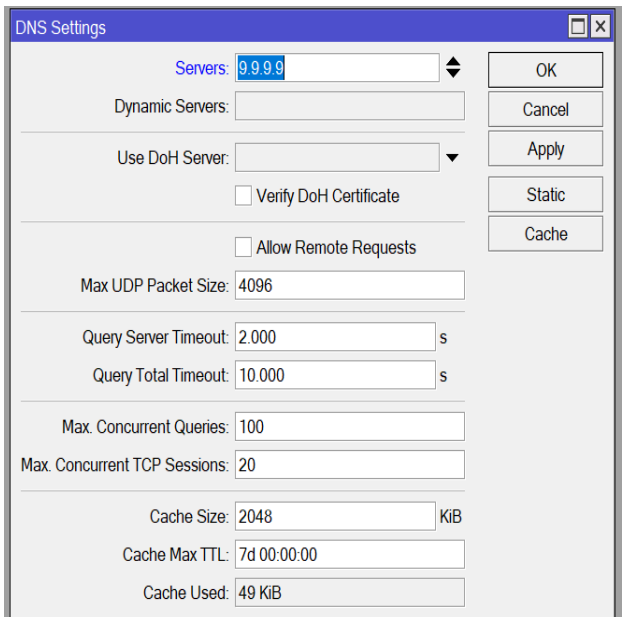
Mikrotik *Router* RB 941 ND digunakan untuk mengimplementasikan layanan *DNS* QUAD9, yang bertugas untuk memblokir akses ke domain berbahaya. Kabel *UTP* digunakan untuk menghubungkan *router* ke laptop sebagai *client*, memastikan koneksi jaringan yang stabil. Laptop digunakan untuk melakukan konfigurasi dan uji coba, serta untuk memantau dan mengevaluasi hasil implementasi *DNS* yang diterapkan. Ketiga alat ini bekerja bersama untuk menguji efektivitas penggunaan *DNS* dalam mendeteksi dan membatasi akses *cryptojacking*. Berikut ini topologi ujicoba dari penelitian ini:



Gambar 2. Topologi ujicoba

4.2 Konfigurasi

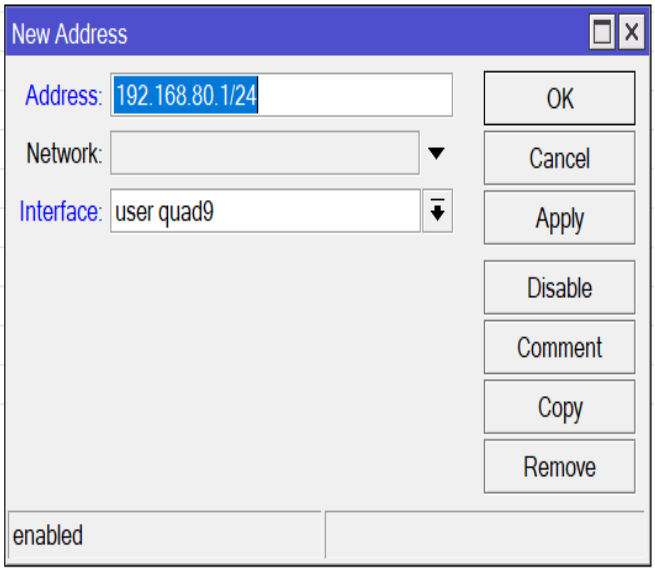
Tahap konfigurasi dilakukan pada *router* mikrotik dan laptop *client*. Laptop *client* digunakan sebagai user biasa yang terkoneksi otomatis dengan internet yang dimanajemen oleh mikrotik, sehingga pengguna akan otomatis mendapatkan alamat IP *Address*, *gateway* dan *DNS* yang diberikan oleh Mikrotik. Berikut ini gambar 3 yaitu proses konfigurasi *DNS* Pada *router* Mikrotik.



Gambar 3. Konfigurasi *DNS*

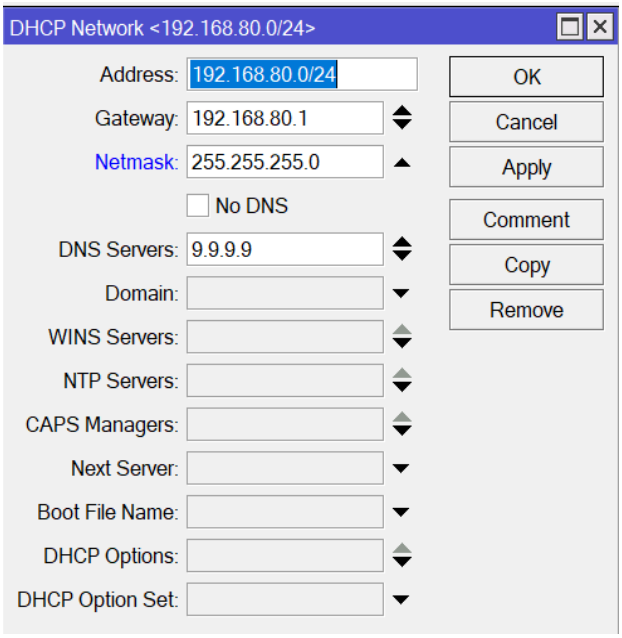
4.3 Implementasi

Langkah implementasi dimulai dengan pembuatan *address* list, yang berfungsi untuk menghubungkan perangkat atau alamat IP ke interface yang mengakses layanan *DNS* QUAD9. Proses ini dilakukan pada *router* Mikrotik dengan tujuan untuk memastikan perangkat yang terdaftar dapat terhubung ke layanan *DNS* yang telah dikonfigurasi. *Address* list ini juga memungkinkan pengelolaan perangkat yang diizinkan untuk menggunakan *DNS* QUAD9, sehingga akses yang diterima sesuai dengan kebijakan yang telah ditetapkan. Proses ini dapat dilihat pada gambar 4 di bawah ini, yang menggambarkan konfigurasi pembuatan IP *address* pada *router* Mikrotik.



Gambar 4. Konfigurasi IP *Address*

Selanjutnya, adalah proses membuat *dhcp-server*, *dhcp server* akan membagikan IP *Address*, *Gateway*, Netmask dan *DNS* ke user. *DNS* yang digunakan yaitu *DNS* dari QUAD9 yang memiliki alamat 9.9.9.9 , berikut ini gambar 5 yaitu gambar penambahan *dhcp-server*.



Gambar 5. Konfigurasi *Dhcp-server*

Selanjutnya, dilakukan proses pemeriksaan atau pengecekan pada laptop *client* untuk memastikan bahwa konfigurasi yang telah diterapkan pada DHCP server berjalan dengan baik dan benar. Proses ini sangat penting karena bertujuan untuk memverifikasi bahwa DHCP server yang telah diatur sebelumnya berhasil membagikan informasi konfigurasi jaringan kepada perangkat *client*. Informasi yang dimaksud meliputi IP *Address*, *gateway*, netmask, serta *DNS* yang akan digunakan oleh *client*. Proses ini juga bertujuan untuk memastikan bahwa laptop *client* dapat terhubung dengan baik ke jaringan yang dikelola oleh *router*, serta dapat memperoleh pengaturan jaringan secara otomatis tanpa perlu

konfigurasi manual. Berikut ini adalah gambar 6 yaitu hasil checking konfigurasi IP *Address* pada laptop *client*:

IPv4 Subnet Mask	255.255.0.0
Autoconfiguration IPv4 A...	192.168.80.254
IPv4 Subnet Mask	255.255.255.0
IPv4 Default Gateway	192.168.80.1
IPv4 DNS Server	9.9.9.9
IPv4 WINS Server	
NetBIOS over Tcpip Enab...	Yes
Link-local IPv6 Address	fe80::6919:d1b0:6348:c9e6%3
IPv6 Default Gateway	fe80::1%3
IPv6 DNS Servers	fe80::1%3
	fe80::1%3

Gambar 6. IP *client Dhcp-server*

Proses implementasi berhasil dilaksanakan dengan baik, dimana konfigurasi pada *router* Mikrotik dan penerapan *DNS* QUAD9 telah berhasil diterapkan sesuai rencana. Setelah tahap implementasi selesai, langkah selanjutnya adalah melakukan uji coba untuk menguji efektivitas dari pengaturan yang telah diterapkan. Uji coba ini bertujuan untuk mengevaluasi kinerja *DNS* QUAD9 dalam mendeteksi dan memblokir aktivitas *cryptojacking*. Untuk membandingkan hasilnya, penelitian ini merujuk pada uji akurasi yang dilakukan oleh Adhar (2023), yang menguji kemampuan *Cloudflare Gateway* dalam menangkal aktivitas *cryptojacking*.

4.4 Perbandingan Dengan *Cloudflare Gateway*

Setelah laptop *client* telah menggunakan *DNS* dari QUAD9 maka selanjutnya adalah proses ujicoba mengakses situs *mining* xmr-eu1.nanopool.org, Hasil ujicoba dapat dilihat pada gambar dibawah ini.

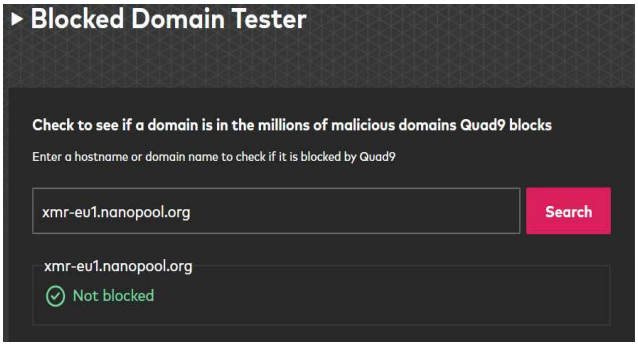
```
C:\Users\user>ping xmr-eu1.nanopool.org

Pinging xmr-eu1.nanopool.org [162.19.224.121] with 32 bytes of data:
Reply from 162.19.224.121: bytes=32 time=341ms TTL=40
Reply from 162.19.224.121: bytes=32 time=341ms TTL=40
Reply from 162.19.224.121: bytes=32 time=342ms TTL=40
Reply from 162.19.224.121: bytes=32 time=342ms TTL=40

Ping statistics for 162.19.224.121:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 341ms, Maximum = 342ms, Average = 341ms
```

Gambar 7. Ping ke alamat pool crypto tidak terblokir

Hasil ujicoba yang dilakukan pada gambar 7, *DNS* QUAD9 tidak memblokir alamat *mining*pool, artinya QUAD9 tidak dapat digunakan untuk menangkal *cryptojacking*. Hal ini juga dapat dilihat pada website resmi dari QUAD9 https://QUAD9.net/result?url=xmr-eu1.nanopool.org bahwa QUAD9 tidak memblokir alamat *mining pool* tersebut. Berikut ini gambar 8 yaitu hasil check domain pada website QUAD9:



Gambar 8. Domain block tester QUAD9 nanopool.org

4.5 Analisis Hasil Penelitian

Hasil ujicoba yang ditunjukan gambar 7 dan gambar 8, menjelaskan bahwa *DNS* QUAD9 tidak memblokir akses internet ke situs *mining* crypto, artinya *DNS* QUAD9 tidak dapat digunakan dalam mendeteksi aktivitas *cryptojacking*.

5 KESIMPULAN

Penelitian ini menunjukkan bahwa *DNS* QUAD9 tidak dapat menangkal aktivitas *cryptojacking*. Meskipun QUAD9 mengklaim dapat memblokir berbagai ancaman, pengujian membuktikan bahwa QUAD9 tidak efektif dalam memblokir situs yang terkait dengan *cryptojacking*. Sebaliknya, *Cloudflare Gateway* terbukti efektif dalam mendeteksi dan membatasi akses ke situs yang berpotensi melakukan *cryptojacking*, seperti yang dijelaskan dalam penelitian oleh Adhar (2023). Oleh karena itu, *Cloudflare Gateway* lebih dapat diandalkan dalam menangkal serangan *cryptojacking* dibandingkan dengan *DNS* QUAD9.

Namun, perlu dicatat bahwa QUAD9 memiliki potensi untuk mendeteksi ancaman lain seperti *malware* dan *phishing*. Oleh karena itu, penelitian selanjutnya sebaiknya menguji, efektifitas *DNS* QUAD9 alam mendeteksi *malware* dan phising.

REFERENSI

Adhar, S., & Saprudin, U. (2023). Implementasi *Cloudflare* Zero Trust Dalam Mendeteksi Aktivitas Cryptojcking Pada Jaringan Komputer. JTKSI (Jurnal Teknologi Komputer dan Sistem Informasi), 6(1), 23-28.

Chhabra, R., Murley, P., Kumar, D., Bailey, M., & Wang, G. (2021, November). Measuring *DNS*-over-HTTPS Performance around the World. In Proceedings of the 21st ACM Internet Measurement Conference (pp. 351-365).

Saputra, I. P. (2024). EFEKTIVITAS *CLOUDFLARE GATEWAY* DALAM MEMBATASI AKSES PORNOGRAFI SERTA PENGARUHNYA PADA KETERSEDIAAN *BANDWIDTH* . International Research on Big-Data and Computer Technology: I-Robot, 8(1).

Sitanggang, E. D., Sembiring, M., & Irawan, B. (2024). Pengembangan Layanan Pemblokiran Situs Bermuatan Negatif menggunakan *DNS* Sinkhole dan Layanan *DNS* QUAD 9 dengan Metode PPDIOO. LOFIAN: Jurnal Teknologi Informasi dan Komunikasi, 3(2), 16-24.

Khairil, K., & Sapri, S. (2023). Penerapan Squid sebagai *Filtering* Web dan Manajemen *Bandwidth* pada Jaringan Internet. MEANS (Media Informasi Analisa

dan Sistem), 112-117.
Fikri, I. M., Dzulhaq, M. I., & Setiyanto, R. (2022). Perancangan dan Implementasi Jaringan Hotspot RT RW NET Menggunakan Mikrotik. JURNAL TOPIK GLOBAL, 1(2).
Hernàndez Sànchez, M. (2022). *DNS Firewall* in Local Network.
Marques, Claudio, Silvestre Malta, and João Magalhães. "*DNS firewall* based on machine learning." Future Internet 13.12 (2021): 309.
Srebaliute, A. (2024, May 7). *Dedicated* IP vs *shared* IP: which one to use? Nordlayer.com. https://nordlayer.com/blog/*dedicated*-ip-vs-*shared*-ip-*address*/