



MENYEMBUNYIKAN ALAMAT IP WEBSERVER DENGAN PROXY DNS RECORDS CLOUDFLARE

Dzuhrizky Aryachandra¹, Ilham Fikri Yanto², Muhammad Miftahul Khair³, Muhamad Reza Sah Pahlevi⁴

Universitas Pendidikan Indonesia, Indonesia

Email: dzuhrizky007@upi.edu, ilhamfikriyanto@upi.edu, miptama@upi.edu, mrezasahf@upi.edu

Abstrak

Website menyediakan berbagai informasi, layanan, dan interaksi bagi pengguna di seluruh dunia. Website-website yang disimpan di sever pribadi rentan mengalami pencurian data seperti bocornya alamat IP webserver hingga bocornya konten didalam webserver tersebut. Hal ini sangat mungkin terjadi terutama pada webserver pribadi yang memiliki tingkat keamanan rendah. Menggunakan proxy DNS records dari Cloudflare merupakan salah satu strategi yang efektif untuk meningkatkan keamanan website. Dengan menyembunyikan alamat IP webserver, website menjadi lebih sulit untuk ditarget oleh serangan cyber yang dapat mengakibatkan pencurian data atau kerusakan lainnya. Cloudflare tidak hanya menyembunyikan informasi sensitif ini, tetapi juga menyediakan layanan tambahan seperti mitigasi DDoS, optimasi performa website, dan distribusi konten yang lebih cepat melalui CDN. Proses konfigurasi yang melibatkan pengaturan DNS dan pengujian sistem keamanan adalah langkah penting untuk memastikan bahwa alamat IP webserver terlindungi dengan baik. Kesimpulan yang diambil dari dokumen ini menegaskan pentingnya langkah-langkah keamanan ini dalam menjaga integritas dan privasi website.

Kata kunci: Proxy dns cloudflare, menyembunyikan alamat ip, Keamanan webserver

Abstract

Websites provide a variety of information, services, and interactions for users around the world. Websites stored on private sever are vulnerable to data theft such as leaking the IP address of the webserver to leaking the content on the webserver. This is very likely to happen especially on private webserver that have a low level of security. Using proxy DNS records from Cloudflare is an effective strategy to increase website security. By hiding the IP address of the webserver, the website becomes more difficult to target by cyberattacks that can result in data theft or other damage. Cloudflare not only hides this sensitive information, but also provides additional services such as DDoS mitigation, website performance optimization, and faster content distribution via CDN. The configuration process involving DNS settings and security system testing are important steps to ensure that the webserver's IP address is properly protected. The conclusions drawn from this document emphasize the importance of these security measures in maintaining website integrity and privacy.

Keywords: Cloudflare dns proxy, hide ip address, Webserver security

PENDAHULUAN

Teknologi pada saat ini telah berkembang pesat, informasi mudah sekali didapat melalui internet (Cholik 2021). Menurut penelitian terdahulu, "Internet adalah fasilitas komunikasi yang dirancang untuk menghubungkan komputer bersama-sama sehingga mereka dapat bertukar informasi digital (Iriawan 2022)." Informasi digital pada umumnya dapat diakses melalui website. Website berfungsi sebagai media untuk menyimpan dan menampilkan informasi (Nento and Masruri 2020). Website menyediakan berbagai informasi, layanan, dan interaksi bagi pengguna di seluruh dunia (Mustopa et al. 2020). Dalam pengaplikasiannya, website disimpan dalam sebuah server yang dinamakan webserver (Prasetio 2014). Webserver bertanggung jawab atas penyimpanan konten website, menjalankan skrip, mengelola basis data, dan memfasilitasi komunikasi antara server dan

perangkat pengguna (Simanjorang 2023).

Pemilik website umumnya menyewa sebuah VPS (*virtual private server*) ataupun membeli web hosting untuk dijadikan tempat menyimpan webserver mereka (Huda 2021). Keuntungan menggunakan vps yaitu dikenal dengan keandalan yang tinggi, sangat minimnya downtime, bandwidth internet yang sangat besar, serta memiliki sistem keamanan yang tinggi (Permana and Alia Nutrisiany Purnomo 2021). Akan tetapi, banyak juga pemilik website menyimpan websitenya ke dalam server pribadi yang memiliki keunggulan terbatas (Abdullah 2020).

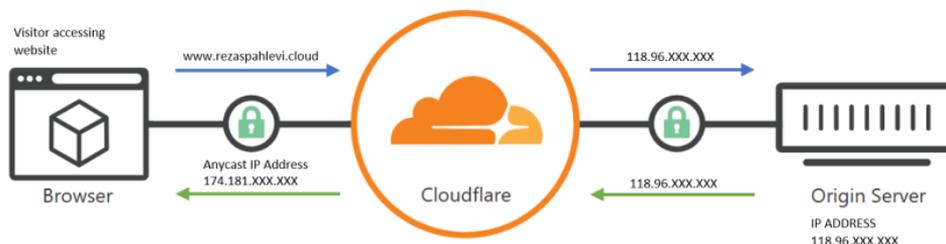
Website-website yang disimpan di server pribadi rentan mengalami pencurian data seperti bocornya alamat IP webserver hingga bocornya konten didalam webserver tersebut (Witi 2021). Hal ini sangat mungkin terjadi terutama pada webserver pribadi yang memiliki tingkat keamanan rendah. Saat alamat IP dari sebuah webserver telah diketahui, maka informasi lokasi webserver, penyedia layanan internet yang digunakan webserver juga akan dapat diketahui dengan mudah (Kurniansyah and Sinurat 2020). Maka dari itu untuk mengatasi masalah tersebut dibutuhkan sebuah sistem keamanan untuk mencegah terjadinya kebocoran alamat IP webserver.

Cloudflare merupakan salah satu penyedia layanan keamanan website untuk memaksimalkan kinerja website (Putra 2022). Cloudflare bertindak sebagai penghubung antara pengunjung dan server website. Cloudflare bisa mengoptimalkan, cache, dan melindungi semua permintaan ke aplikasi Anda, serta melindungi server asal Anda dari Serangan *DDoS*.

METODE PENELITIAN

Cara Kerja Sistem Keamanan Website dengan *Proxy DNS Records* Cloudflare

Tahap perancangan sistem ini, baiknya untuk memahami terlebih dahulu cara kerja dari sistem tersebut.



Gambar 1

Ketika pengguna mengakses sebuah website, browser tersebut akan mulai mengirimkan permintaan ke *DNS resolver*, kemudian *DNS resolver* akan mengubah nama host menjadi alamat IP. Karena domain ini menggunakan Cloudflare sebagai penyedia DNS, kueri DNS akan dirutekan ke Cloudflare, dan karena *proxy dns records* aktif, Cloudflare akan menjawab dengan alamat *IP anycast*. Selanjutnya, browser memulai permintaan kembali ke Cloudflare. Pada saat Cloudflare menerima permintaan ini, Cloudflare melakukan pencarian untuk menemukan domain dan konfigurasi akun yang cocok dan memproses permintaan yang sesuai. Cloudflare kemudian meneruskannya ke server asal yang dikonfigurasi. Proksi pada *DNS records* memengaruhi cara Cloudflare memperlakukan trafik yang masuk ke *records* tersebut.

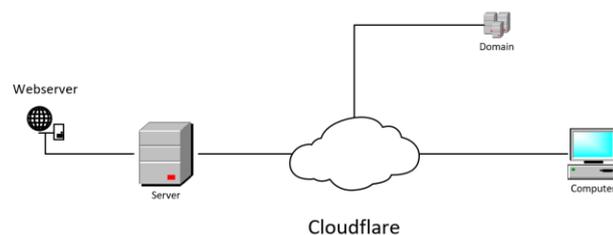
Type	Name	Content	Proxy status	TTL	Actions
A	blog	192.0.2.1	Proxied	Auto	Edit ▶
A	shop	192.0.2.2	DNS only	Auto	Edit ▶

Gambar 2

Saat proksi pada *DNS record* Cloudflare diaktifkan, trafik yang menuju domain website ini akan diselesaikan ke Cloudflare *Anycast IP* alih-alih target alamat IP aslinya. Ini berarti bahwa semua permintaan yang ditujukan untuk nama host proxy akan masuk ke Cloudflare terlebih dahulu dan kemudian diteruskan ke server asal. Perilaku ini memungkinkan Cloudflare untuk mengoptimalkan, cache, dan melindungi semua permintaan ke aplikasi Anda, serta melindungi server asal Anda dari Serangan *DDoS*.

Perancangan Sistem Keamanan Website dengan *Proxy DNS Records* Cloudflare

Dalam perancangan situs web diperlukan beberapa komponen agar situs web berfungsi yaitu, server/komputer pengganti server berfungsi sebagai perangkat utama untuk menyimpan dan menjalankan webserver dan perangkat lunak penunjang lainnya. Webserver berfungsi sebagai perangkat lunak yang menyediakan layanan penyimpanan dan pengiriman konten web kepada pengguna melalui internet. Domain berfungsi sebagai identitas dari situs web. Cloudflare berfungsi sebagai jembatan antara domain dan webserver serta sebagai pengelola sistem keamanan situs web.



Gambar 3

Selanjutnya untuk mengimplementasikan perancangan tersebut, diperlukan untuk menyiapkan beberapa komponen diantaranya

1. Server/komputer pengganti server yang sudah di instal webserver dan konten website.
2. Menyediakan domain rezaspahlevi.cloud, domain ini digunakan saat konfigurasi DNS cloudflare
3. Konfigurasi DNS cloudflare, agar website bisa diakses menggunakan domain rezaspahlevi.cloud dan bisa mengaktifkan fitur proxy dns cloudflare.

Rancangan Pengujian

Setelah sistem sudah dibangun dan dapat digunakan, selanjutnya sistem dapat diuji apakah sistem *proxy DNS records* pada cloudflare itu sudah aktif dan hasil pengujiannya akan dibahas di bab selanjutnya. Berikut rancangan pengujian yang akan digunakan.

1. Menguji apakah cloudflare sudah mengubah alamat IP asli website ke alamat *IP anycast* cloudflare menggunakan platform pihak ketiga (<https://check-host.net>).
2. Menguji menggunakan platform pihak ketiga (<https://check-host.net>), apakah alamat *IP anycast* cloudflare sudah mengganti informasi lainnya menjadi informasi yang disediakan oleh cloudflare.

HASIL DAN PEMBAHASAN

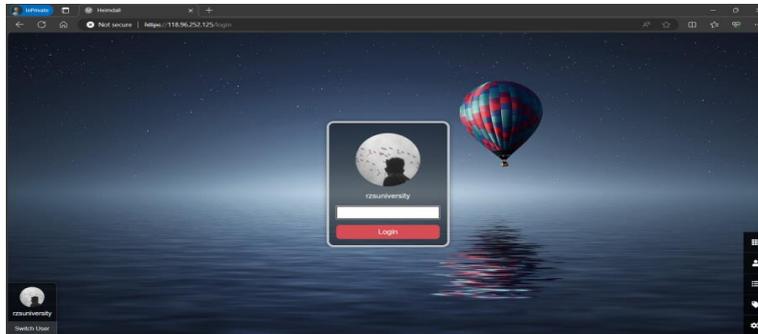
Tampilan Implementasi Perancangan Sistem Keamanan Website dengan Proxy DNS Cloudflare

Tahap Konfigurasi Webserver

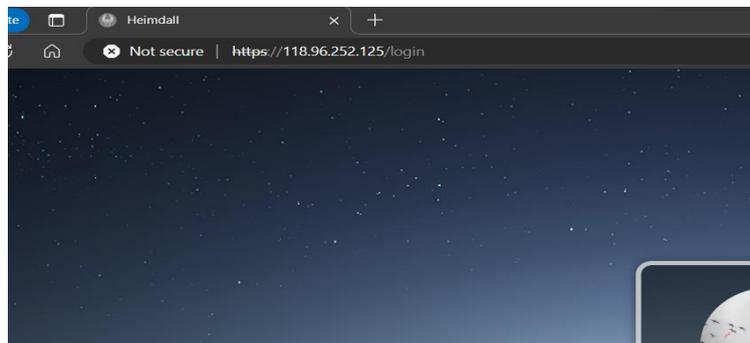
Pada tahap awal, perlu menginstal webserver di sebuah server/komputer pengganti server. Server yang dipakai untuk website biasanya menggunakan sistem operasi berbasis linux yang ringan pada saat digunakan dan kompatibel untuk banyak server/komputer pengganti server (Mair 2018). Pada gambar 4 menampilkan konten dari website tersebut sudah bisa diakses melalui browser yang

menandakan bahwa tidak ada kendala pada saat instalasi webserver.

Agar website tersebut bisa diakses secara publik, perlu dilakukan konfigurasi *port forwarding* pada router internet (Alviansyah, Lestanti, and Romadhona 2024). *Port forwarding* berfungsi meneruskan *port* yang dibuka oleh webserver ke publik. Pada gambar 5 bisa dilihat bahwa website tersebut sudah bisa diakses secara publik menggunakan alamat IP publik dari penyedia layanan internet.



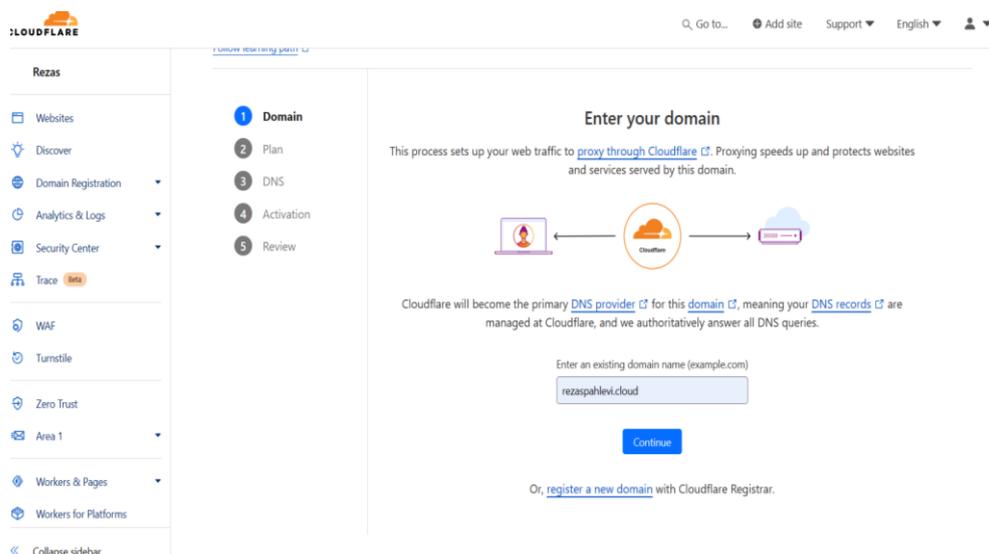
Gambar 4



Gambar 5

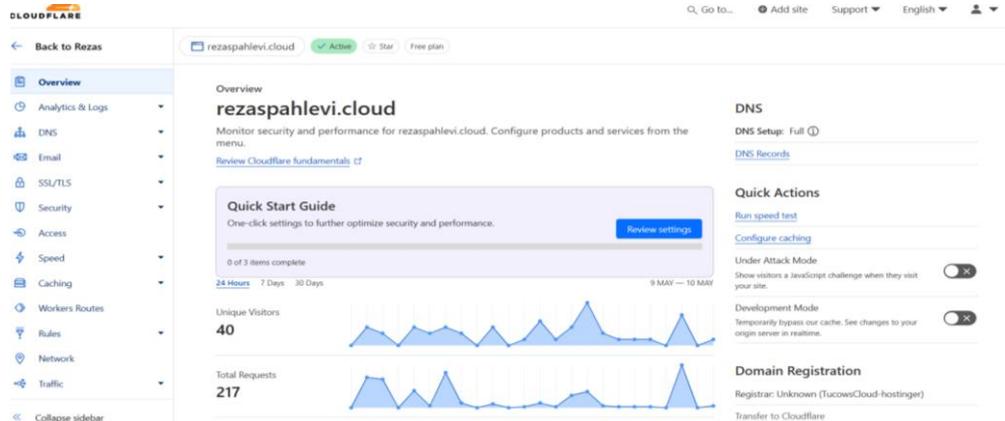
Tahap Konfigurasi Cloudflare

Pada gambar 6 merupakan tahap awal konfigurasi cloudflare. Domain yang sudah disediakan harus di registrasikan di platform cloudflare, agar ketika ada pengguna mengakses domain, permintaan dari pengguna tersebut akan diproses oleh cloudflare dan sistem keamanan dari website juga dikelola oleh cloudflare (Jayanti, Umar, and Riadi 2020).



Gambar 6

Gambar 7 merupakan tampilan dashboard dari website yang sudah di registrasikan di cloudflare. Dashboard ini menampilkan data-data statistik dari pengunjung website dari rentang waktu tertentu.



Gambar 7

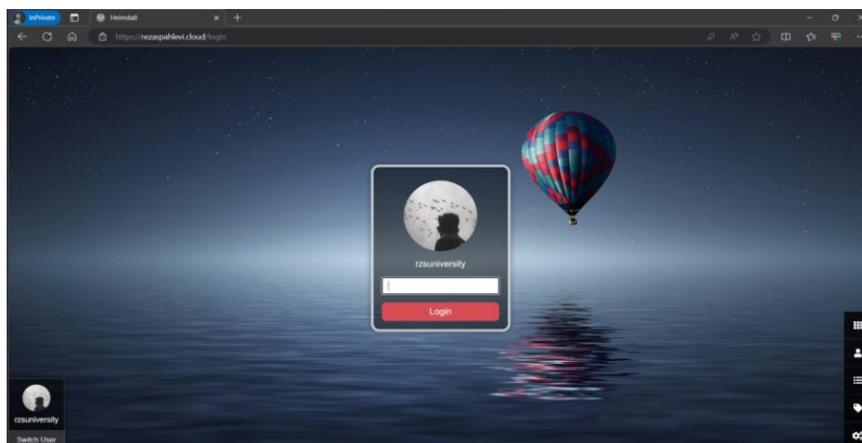
Tahap selanjutnya yaitu mengkonfigurasi DNS antara alamat IP website dengan domain yang dikenal dengan istilah *pointing domain*.

Pada gambar 8 merupakan tampilan ketika pointing domain, menggunakan dns type A, domain rezaspahlevi.cloud dikoneksikan dengan alamat IP dari website tersebut yaitu 118.96.252.125. Pastikan untuk mengaktifkan *proxy dns records* pada saat pointing agar alamat IP dari website disamarkan oleh cloudflare dan tidak terekspos secara publik.

Type	Name	Content	Proxy status	TTL	Actions
A	rezaspahlevi.cloud	118.96.252.125	Proxied	Auto	Edit
Type	Name (required)	IPv4 address (required)	Proxy status	TTL	
A	rezaspahlevi.cloud	118.96.252.125	Proxied	Auto	
Use @ for root					

Gambar 8

Semua proses konfigurasi telah selesai. Pada gambar 9 menampilkan bahwa website tersebut sudah bisa diakses secara publik menggunakan domain <https://rezaspahlevi.cloud>.



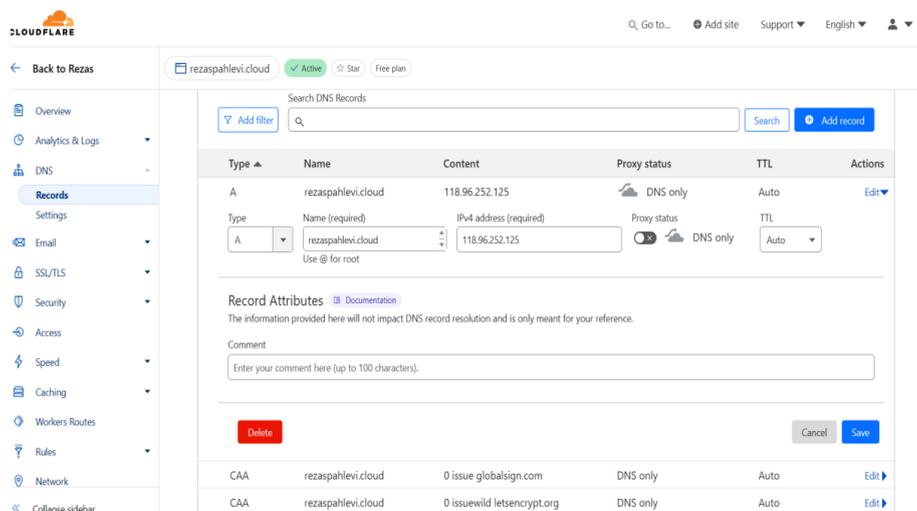
Gambar 9

Tampilan Tahapan Pengujian Proxy DNS Cloudflare

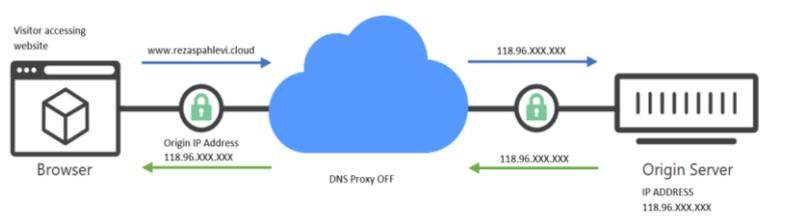
Setelah tahap konfigurasi webserver dan konfigurasi cloudflare selesai, maka selanjutnya dilakukan pengujian pada sistem *proxy dns records* yang sudah berjalan, tahapan pengujian ini memiliki dua tujuan diantaranya (1) apakah cloudflare sudah mengubah alamat IP asli website ke alamat IP *anycast* cloudflare, (2) apakah alamat IP *anycast* cloudflare sudah mengganti informasi lainnya menjadi informasi yang disediakan cloudflare. Adapun hasil pengujian Implementasi *proxy dns records* akan diuraikan dibawah ini.

Pada pengujian ini, penulis menguji *proxy dns records* sudah aktif. *Proksi dns records* cloudflare ini berperan mengubah alamat IP asli website ke alamat IP *anycast* cloudflare. Pengujian ini menggunakan platform pihak ketiga (<https://check-host.net>).

Pada gambar 10 menampilkan kondisi sebelum *proxy dns records* diaktifkan. Pada kondisi ini, semua trafik yang menuju website hanya melewati *dns resolver* pada cloudflare, cloudflare tidak merespon dengan alamat IP *anycast* nya dan trafik tersebut langsung diteruskan ke server asal.

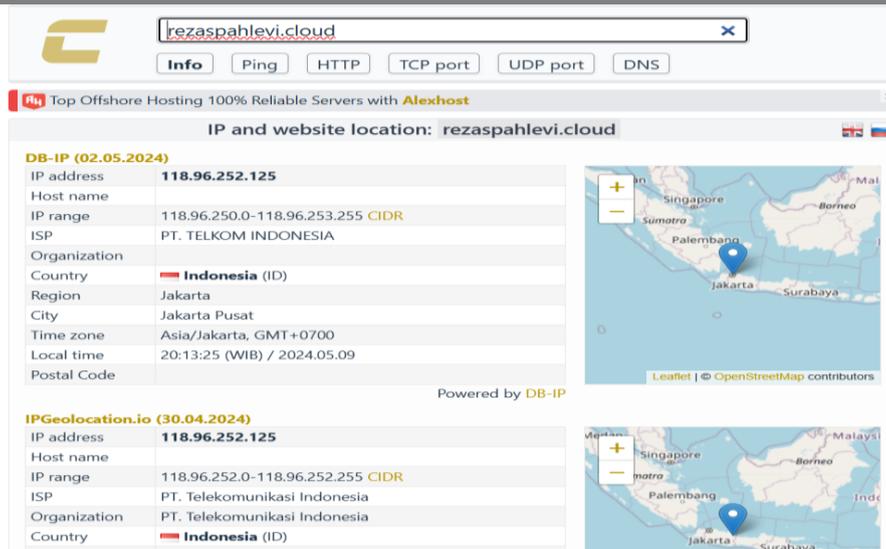


Gambar 10



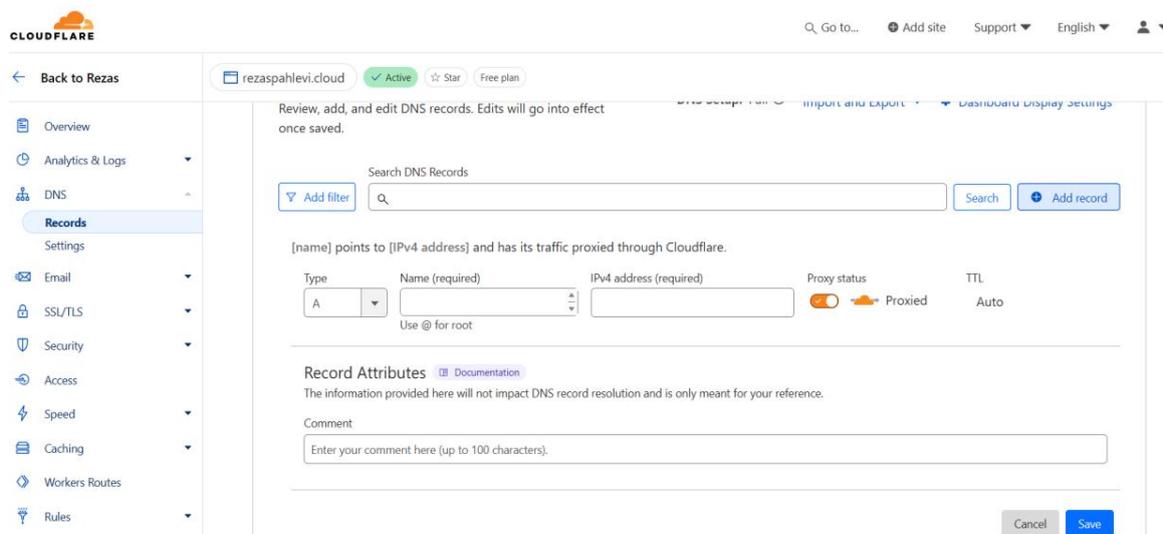
Gambar 11

Pada gambar 12 menampilkan hasil pengujian, dapat dilihat bahwa ketika *proxy dns records* dalam keadaan mati, trafik yang masuk ke domain website tersebut langsung diteruskan ke server asal tanpa diproses lebih lanjut oleh cloudflare. Konsekuensinya alamat IP pada server asal akan langsung terekspos oleh publik, dan secara tidak langsung akibat dari terekspos nya alamat IP tersebut memungkinkan untuk tereksposnya data lain seperti informasi lokasi geografis server asal, layanan internet yang dipakai oleh server asal tersebut.



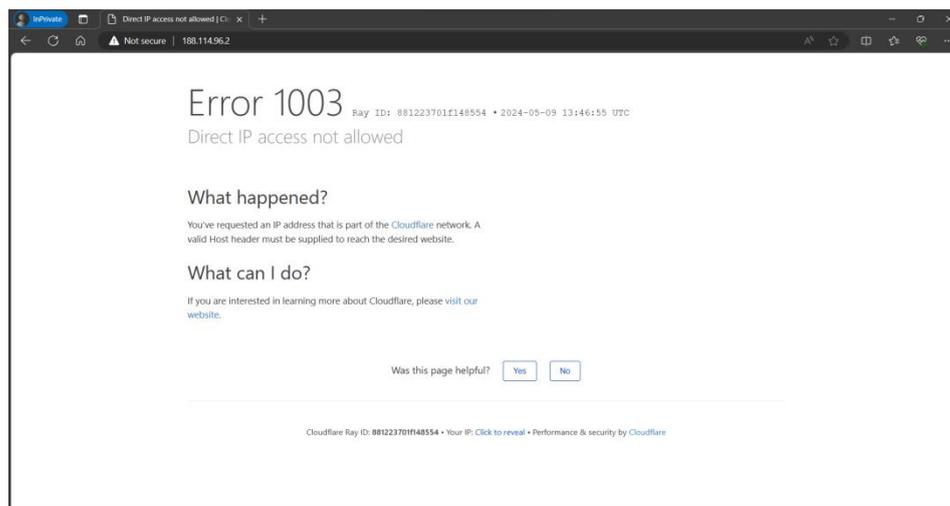
Gambar 12

Pada gambar 13 menampilkan kondisi *proxy dns records* sudah diaktifkan. Saat *proxy dns records* cloudflare diaktifkan, trafik yang menuju domain website ini akan diselesaikan oleh alamat *IP Anycast* cloudflare alih-alih target alamat IP aslinya. Ini berarti bahwa semua permintaan yang ditujukan untuk nama *host proxy* akan masuk ke cloudflare terlebih dahulu dan kemudian diteruskan ke server asal.



Gambar 13

Pada gambar 14 juga membuktikan bahwa *proxy dns records* sudah aktif dan bekerja dengan baik. Pada saat mengakses website menggunakan alamat *IP anycast* cloudflare, cloudflare memberikan informasi bahwa website tersebut tidak bisa diakses menggunakan alamat IP secara langsung dan hanya bisa diakses menggunakan domain yang sudah diregistrasikan.



Gambar 14

KESIMPULAN

Semua serangkaian konfigurasi dan serangkaian pengujian dapat disimpulkan bahwa penggunaan *proxy dns records* pada website terbukti dapat bekerja dengan baik dalam menyembunyikan alamat IP server asal. Hal ini dapat menjaga privasi dan meningkatkan keamanan pada website. Penggunaan *proxy dns records* juga dapat menjadi solusi untuk menyembunyikan alamat IP website yang diinstal pada server pribadi.

DAFTAR PUSTAKA

- Abdullah, Dahlan. 2020. "Perancangan Dan Pembuatan Aplikasi File Server Berbasis Web Menggunakan Metode Interpolation Search."
- Alviansyah, Alif, Sri Lestanti, and Rizki Dwi Romadhona. 2024. "Implementasi IP Forwarding Dengan Menggunakan IP Public Pada Alita Komputer Kota Blitar." *JOURNAL ZETROEM* 6(1):109–13.
- Cholik, Cecep Abdul. 2021. "Perkembangan Teknologi Informasi Komunikasi/ICT Dalam Berbagai Bidang." *Jurnal Fakultas Teknik Kuningan* 2(2):39–46.
- Huda, Miftahul. 2021. *Bisnis Web Hosting: Teknologi Pendukung Untuk Menjalankan Usaha Web Hosting*. bisakimia.
- Iriawan, Arya Maulana Putra. 2022. "Implementasi Sistem Sewa Mobil Pribadi Berbasis Web Untuk Usaha Mikro Kecil Menengah (UMKM)/Arya Maulana Putra Iriawan/52180253/Pembimbing: Grace Martha G. Bororing."
- Jayanti, Dewi Estri, Rusydi Umar, and Imam Riadi. 2020. "Implementation of Cloudflare Hosting for Access Speed on Trading Websites." *Sisfotenika* 10(2):227–38.
- Kurniansyah, M. Iqbal, and Sinar Sinurat. 2020. "Sistem Pendukung Keputusan Pemilihan Server Hosting Dan Domain Terbaik Untuk WEB Server Menerapkan Metode VIKOR." *Jurnal Sistem Komputer Dan Informatika (JSON)* 2(1):14–24.
- Mair, Zaid Romegar. 2018. *Teori Dan Praktek Sistem Operasi*. Deepublish.
- Mustopa, Ali, Sarifah Agustiani, Siti Khotimatul Wildah, and Maysaroh Maysaroh. 2020. "Analisa Kepuasan Pengguna Website Layanan Akademik Kemahasiswaan (LYKAN) UBSI Menggunakan Metode Webqual 4.0." *Jurnal Perspektif* 18(1):75–81.
- Nento, Khairuddin, and Anis Masruri. 2020. "Optimalisasi Penggunaan Website Sebagai Media Publikasi Informasi Sekolah SMK Koperasi Yogyakarta." *Jurnal Teknologi Informasi Indonesia (JTII)* 5(2):87–98.

-
- Permana, Pungky Indra, and S. T. Alia Nutrisiany Purnomo. 2021. *Pemrograman Web Dan Perangkat Bergerak SMK/MAK Kelas XII*. Gramedia Widiasarana indonesia.
- Prasetio, Adhi. 2014. *Buku Sakti Webmaster*. MediaKita.
- Putra, Gubtha Mahendra. 2022. "Pengujian Kinerja Web Server Atas Penyedia Layanan Elastic Cloud Compute (EC2) Pada Amazon Web Services (AWS)." *Adopsi Teknologi Dan Sistem Informasi (ATASI)* 1(1):21–35.
- Simanjorang, Anju Wahyu. 2023. "Sistem Informasi Presensi, Penggajian, Dan Pengajuan Cuti Pada Pt. Trisakti Manunggal Perkasa Internasional Berbasis Web."
- Witi, Ferdinandus Lidang. 2021. *Membangun E-Commerce: Teori, Strategi Dan Implementasi*. AMERTA MEDIA.



This work is licensed under a [Creative Commons Attribution-ShareAlike 4.0 International License](https://creativecommons.org/licenses/by-sa/4.0/)