Implementasi DNS Filtering berbasis RPZ Menggunakan databases DNSTrust Kominfo di PT. GN

Alimuddin Yasin

Bisnis Digital Fakultas Sains dan Ilmu Komputer, Universitas Muhammadiyah Goronralo Jl. Prof. DR. H. Masoer Pateda, Desa Pentadio Timur, Kecamatan. Telaga Biru, Kabupaten. Gorontalo,

alimuddiny@umgo.ac.id
Coresponding: alimuddiny@umgo.ac.id

ABSTRACT

In the digital age, internet access has become an integral part of daily life in Indonesia, facilitating education, entertainment, and communication. However, this growth also brings challenges such as the spread of negative content, including pornography, gambling, and malware. To address these issues, the Indonesian government, through the Ministry of Communication and Information Technology (Kominfo), introduced the Trust Positif program aimed at blocking access to sites containing prohibited content. This program is mandated for internet service providers under Regulation of the Minister of Communication and Information Technology No. 19 of 2014. DNS Filtering is a technique used to restrict access to specific websites by cross-referencing domain names with a blacklist. PT. GN, as an internet service provider, implements DNS Filtering based on the Trust Positif database to protect users from harmful content. Using Debian 12 server and BIND9 DNS server, PT. GN applies Response Policy Zone (RPZ) configuration to ensure effective blocking. Testing with tools such as dig and nslookup confirms that the RPZ configuration functions correctly, blocking access to domains listed in the Trust Positif database. The results indicate that PT. GN has successfully implemented the blocking policies, ensuring a safer digital environment for internet users and enhancing trust in their services.

Keywords: trustpositif kominfo, rpz, dns filtering

ABSTRAK

Dalam era digital saat ini, akses internet telah menjadi bagian integral dari kehidupan sehari-hari masyarakat Indonesia, memberikan kemudahan dalam edukasi, hiburan, dan komunikasi. Namun, pertumbuhan ini juga membawa tantangan berupa penyebaran konten negatif seperti pornografi, perjudian, dan malware. Untuk mengatasi masalah ini, Pemerintah Indonesia melalui Kementerian Komunikasi dan Informatika (Kominfo) meluncurkan program Trust Positif yang bertujuan memblokir akses ke situs-situs yang mengandung konten terlarang. Implementasi program ini diwajibkan kepada penyedia layanan internet berdasarkan Peraturan Menteri Komunikasi dan Informatika Nomor 19 Tahun 2014. DNS Filtering merupakan teknik yang digunakan untuk membatasi akses ke situs web tertentu dengan memeriksa nama domain terhadap daftar hitam. PT. GN, sebagai penyedia jasa layanan internet, mengimplementasikan DNS Filtering berbasis database Trust Positif untuk melindungi pengguna dari konten berbahaya. Dengan menggunakan server Debian 12 dan DNS server BIND9, PT. GN menerapkan konfigurasi Response Policy Zone (RPZ) untuk memastikan pemblokiran yang efektif. Uji coba dengan alat seperti dig dan nslookup memastikan bahwa konfigurasi RPZ berfungsi dengan baik, memblokir akses ke domain yang terdaftar dalam daftar Trust Positif. Hasilnya menunjukkan bahwa PT. GN berhasil menerapkan kebijakan pemblokiran yang sesuai, menjaga lingkungan digital yang aman bagi pengguna internet dan meningkatkan kepercayaan terhadap layanan yang disediakan.

Keywords: trustpositif kominfo, rpz, dns filtering

PENDAHULUAN

Dalam era digital saat ini, Akses internet sudah menjadi bagian dari kehidupan sehari-hari masyarakat di Indonesia [1]. Akses mudah dan cepat ke berbagai informasi menjadikan internet sebagai sarana utama untuk edukasi, hiburan, dan komunikasi [2]. Akan Tetapi, seiring dengan perkembangan yang positif ini, muncul juga tantangan

serius berupa penyebaran konten negatif, seperti pornografi, perjudian, dan konten berbahaya lainnya yang mengandung malware [3]. Konten-konten ini tidak hanya mengganggu moral masyarakat tetapi juga berpotensi membahayakan data pribadi dan keamanan pengguna internet [4].

Pemerintah Indonesia, melalui Kementerian Komunikasi dan Informatika (Kominfo), telah mengeluarkan berbagai kebijakan untuk menangani masalah ini. Salah satu inisiatif utamanya adalah implementasi sistem penyaringan konten negatif melalui program Trust Positif. Program ini bertujuan untuk memblokir akses ke situs-situs yang memuat konten terlarang, termasuk pornografi, perjudian, dan situs berbahaya yang dapat menyebarkan malware. Kebijakan ini diatur dalam Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 19 Tahun 2014, yang mewajibkan penyedia layanan internet untuk menerapkan penyaringan terhadap situs-situs yang tercantum dalam database Trust Positif [5].

DNS Filtering adalah mekanisme yang digunakan untuk memblokir akses ke situs web tertentu berdasarkan nama domainnya. Teknologi ini bekerja dengan memeriksa permintaan DNS dari pengguna untuk mengakses situs web dan membandingkannya dengan daftar hitam (blacklist) yang telah ditentukan. Jika nama domain tersebut terdaftar dalam daftar hitam, akses ke situs web akan diblokir [3]. DNS Filtering memberikan lapisan keamanan tambahan dengan mencegah pengguna mengakses konten yang tidak diinginkan atau berbahaya, serta membantu melindungi jaringan dari ancaman siber.

PT. GN, sebagai salah satu penyedia jasa layanan internet (ISP) di Indonesia, dalam mematuhi peraturan yang ditetapkan oleh Kominfo. Untuk melindungi pelanggan dari ancaman konten negatif PT. GN mengimplementasikan DNS filtering berbasis database Trust Positif [4]. Teknologi DNS filtering memungkinkan PT. GN untuk secara efisien memblokir akses ke situs-situs berbahaya, sehingga pengguna yang berada dalam jaringan mereka terlindungi dari dampak merugikan dari konten-konten tersebut.

Implementasi DNS filtering ini bertujuan tidak hanya untuk melindungi pengguna dari paparan konten negatif, tetapi juga untuk meningkatkan kepercayaan pelanggan terhadap layanan yang disediakan oleh PT. GN. Dengan menyediakan akses internet yang aman dan bersih, PT. GN berupaya berkontribusi dalam membangun lingkungan digital yang lebih sehat dan aman di Indonesia. Dalam penelitian ini menggunakan penulis menggunakan server Debian 12 yang dilengkapi dengan DNS Server Bind9. Bind9 adalah perangkat lunak server DNS yang paling umum digunakan di internet. Dikembangkan oleh Internet Systems Consortium (ISC), Bind9 menawarkan fitur lengkap dan dukungan untuk berbagai protokol DNS [6]. Bind9 memungkinkan konfigurasi yang fleksibel dan dapat diandalkan untuk mengelola dan memproses permintaan DNS, serta mendukung pengaturan kebijakan respons seperti Response Policy Zone (RPZ) untuk memblokir atau mengalihkan permintaan ke situs tertentu [7]. Dengan menggunakan Bind9, PT. GN dapat mengelola dan memodifikasi resolusi DNS secara efektif untuk menerapkan kebijakan penyaringan yang sesuai dengan peraturan Trust Positif.

METODE PENELITIAN

Penelitian ini menggunakan metode eksperimen dan studi kasus untuk mengimplementasikan dan mengevaluasi DNS filtering berbasis Trust Positif Kominfo pada PT. GN. Penelitian ini didukung oleh teori-teori jaringan komputer dan keamanan siber yang relevan. Berikut adalah langkah-langkah dan teori yang mendasari penelitian ini:

1. Teori Dasar

1.1 DNS (Domain Name System):

DNS adalah sistem terdistribusi yang mengubah nama domain yang mudah dibaca manusia menjadi alamat IP yang dapat dibaca mesin. DNS berfungsi seperti buku telepon internet, di mana nama domain seperti

www.example.com diterjemahkan menjadi alamat IP yang digunakan oleh komputer untuk berkomunikasi [8]. Dalam konteks keamanan, DNS dapat digunakan sebagai alat untuk memfilter akses ke situs-situs yang tidak diinginkan dengan mengarahkan ulang atau memblokir permintaan DNS.

1.2 DNS Filtering:

DNS filtering adalah teknik yang digunakan untuk memblokir atau mengarahkan permintaan DNS berdasarkan kebijakan tertentu. Metode ini memanfaatkan daftar domain yang diizinkan (whitelist) atau diblokir (blacklist) untuk mengontrol akses ke sumber daya internet [9]. DNS filtering sering digunakan untuk melindungi jaringan dari konten berbahaya dan memastikan kepatuhan terhadap kebijakan akses internet yang berlaku.

1.3 Response Policy Zone (RPZ):

RPZ adalah fitur dari Bind9 yang memungkinkan administrator DNS untuk mengubah respons yang diberikan kepada klien berdasarkan kebijakan tertentu. RPZ digunakan untuk memblokir, mengalihkan, atau mengubah permintaan DNS untuk domain yang ditentukan[10]. Ini sangat berguna dalam implementasi filtering, karena memungkinkan pembaruan kebijakan secara dinamis berdasarkan daftar yang disediakan oleh pihak ketiga, seperti database Trust Positif Kominfo.

1.4 Sistem Operasi Debian:

Debian adalah distribusi Linux yang dikenal karena stabilitas dan keamanannya. Debian banyak digunakan dalam lingkungan server karena ketersediaan paket perangkat lunak yang luas dan dukungan komunitas yang aktif [8]. Debian adalah platform ideal untuk mengimplementasikan layanan jaringan seperti DNS, karena menyediakan infrastruktur yang andal dan aman.

1.5 Bind9:

Bind9 adalah perangkat lunak server DNS yang paling umum digunakan di internet. Bind9 dikembangkan oleh Internet Systems Consortium (ISC) dan mendukung berbagai fitur, termasuk DNSSEC, RPZ, dan berbagai opsi konfigurasi lanjutan. Bind9 digunakan secara luas untuk mengelola dan memproses permintaan DNS dengan cara yang fleksibel dan dapat disesuaikan dengan kebutuhan organisasi [6].

2. Langkah Langkah Implementasi

Dalam Penelitian ini menggunakan metode eksperimen dengan tahapan instalasi dan konfigurasi sistem untuk menerapkan DNS filtering di PT. GN. Penelitian ini bertujuan untuk mengimplementasikan sistem penyaringan berbasis DNS yang memanfaatkan database Trust Positif Kominfo. Langkah-langkah penelitian meliputi:

2.1. Instalasi Sistem

2.1.1 Persiapan Instalasi Server:

Langkah pertama dalam instalasi Debian 12 adalah mengunduh file ISO dari situs resmi Debian, disesuaikan dengan arsitektur sistem yang digunakan, umumnya *amd64.* Setelah pengunduhan, langkah selanjutnya adalah membuat media instalasi menggunakan USB. Aplikasi seperti Rufus untuk Windows atau perintah dd pada Linux/Mac dapat digunakan untuk membuat USB yang dapat di-boot.

2.1.2 Instalasi Debian Server:

Setelah Membuat media instalas, masukkan USB tersebut ke dalam server dan lakukan boot ulang. Selama proses booting, masuk ke BIOS/UEFI dan pilih untuk boot dari USB. Setelah berhasil boot dari USB, menu instalasi akan muncul, di mana opsi *Install* harus dipilih. Proses instalasi akan dimulai dengan pemilihan bahasa yang akan digunakan, diikuti oleh pemilihan lokasi yang berfungsi untuk pengaturan lokal dan zona waktu. Selanjutnya, pilih tata letak keyboard yang sesuai dengan preferensi.

Pada tahap konfigurasi jaringan, nama host untuk server perlu dimasukkan, serta nama domain jika diperlukan. Selanjutnya, pembuatan akun pengguna dilakukan, dimulai dengan menetapkan kata sandi untuk akun root dan kemudian membuat akun pengguna baru serta menetapkan kata sandinya. Proses partisi disk adalah tahap berikutnya, di mana metode partisi *Guided - use entire disk* dapat dipilih untuk memudahkan pengaturan. Pilih disk yang akan digunakan untuk instalasi, kemudian tinjau dan konfirmasi pengaturan partisi yang telah dipilih.

Setelah pengaturan partisi dikonfirmasi, sistem akan melanjutkan dengan menginstal sistem dasar Debian, yang memerlukan waktu beberapa menit untuk diselesaikan. Setelah instalasi sistem dasar selesai, opsi untuk memilih perangkat lunak tambahan yang ingin diinstal akan diberikan, seperti *SSH Server* dan *Standard System Utilities*, yang akan menambah fungsionalitas dan utilitas sistem. Setelah semua konfigurasi selesai, komputer akan menyelesaikan instalasi dan melakukan boot ulang ke dalam sistem operasi Debian 12 yang telah diinstal.

2.1.3 Konfigurasi Jaringan Debian 12:

Setelah instalasi sistem operasi Debian 12 selesai, konfigurasi jaringan menjadi langkah krusial untuk memastikan bahwa sistem dapat terhubung dengan jaringan lokal dan internet secara efektif. Pada Debian 12, konfigurasi jaringan dapat dilakukan melalui antarmuka berbasis teks atau dengan mengedit file konfigurasi secara langsung. Sistem manajemen jaringan yang umum digunakan adalah Netplan.

Identifikasi Antarmuka Jaringan: Langkah pertama dalam konfigurasi jaringan adalah mengidentifikasi nama antarmuka jaringan. Ini dapat dilakukan dengan menggunakan perintah ip a atau ip link, yang akan menampilkan daftar semua antarmuka jaringan yang tersedia.

Mengedit File Konfigurasi Netplan: File konfigurasi untuk Netplan biasanya terletak di direktori /etc/netplan/. Untuk mengkonfigurasi jaringan, file konfigurasi seperti 01-netcfg.yaml dapat diedit dengan menggunakan editor teks seperti nano atau vim.

Contoh konfigurasi jaringan statis:

```
network:
  version: 2
  ethernets:
    eth0:
      dhcp4: no
      addresses:
        - 192.168.1.10/24
      gateway4: 192.168.1.1
      nameservers:
        addresses:
          - 8.8.8.8
          - 8.8.4.4
```

Dalam konfigurasi ini, eth0 adalah nama antarmuka jaringan, 192.168.1.10/24 adalah alamat IP statis, 192.168.1.1 adalah alamat gateway, dan 8.8.8.8 serta 8.8.4.4 adalah alamat DNS yang digunakan.

Menerapkan Konfigurasi: Setelah melakukan perubahan pada file konfigurasi, perintah sudo netplan apply digunakan untuk menerapkan konfigurasi jaringan yang telah disusun. Perintah ini akan membuat sistem menggunakan pengaturan baru yang telah ditentukan dalam file YAML.

2.2. Instalasi dan Konfigurasi Bind9

2.2.1 Instalasi Bind9:

1. Memastikan sistem operasi diperbarui dengan menjalankan sudo apt update && sudo apt upgrade.
2. Menginstal Bind9 dengan perintah sudo apt install bind9 bind9utils bind9-doc.

2.2.2 Verifikasi dan Pengaktifan Bind9:

1. Memastikan Bind9 berjalan dengan benar menggunakan sudo systemctl status bind9.
2. Mengaktifkan Bind9 untuk berjalan otomatis saat booting dengan sudo systemctl enable bind9.

2.3. Konfigurasi DNS

2.3.1 Konfigurasi Bind Options:

1. Membuka berkas konfigurasi Bind9 di /etc/bind/named.conf.options. konfigurasi berikut untuk mengaktifkan RPZ pada dns dengan mengalikan ke halaman blokir.ptgn.web.id:

```
    options {
 directory "/var/cache/bind";
 allow-query { 127.0.0.0/8; 160.*.**.0/24; };
 response-policy {
       zone "trustpositifkominfo"
       policy cname blokir.ptgn.web.id:
       max-policy-ttl 30
       log no;
 }
 recursive-only yes
 qname-wait-recurse no
 break-dnssec yes
 nsip-wait-recurse no;
 dnssec-validation auto;
 listen-on-v6 { any; };
 listen-on {any; };
};
```

1. directory "/var/cache/bind";

Direktif ini menetapkan lokasi direktori untuk penyimpanan cache DNS dan data sementara lainnya. Direktori /var/cache/bind adalah lokasi yang umum digunakan untuk menyimpan file cache DNS, yang memungkinkan BIND mengakses data yang telah di-cache untuk mempercepat proses resolusi nama domain.

2. allow-query { 127.0.0.0/8; 160.*.*.0/24; };

Pengaturan ini mengontrol akses ke server DNS dengan menentukan alamat IP yang diperbolehkan untuk melakukan kueri. Dalam hal ini:

- **127.0.0.0/8**: Mengizinkan kueri dari alamat loopback lokal, biasanya digunakan untuk komunikasi internal mesin.
- **160.*.*.0/24**: Mengizinkan kueri dari rentang alamat IP tertentu dengan subnet mask /24, yang dapat mewakili jaringan internal atau organisasi tertentu. Penulisan 160.*.*.0 adalah notasi umum yang harus diganti dengan rentang IP yang sesuai jika informasi lengkap tersedia.

3. response-policy {

- **zone "trustpositifkominfo"**: Menunjukkan zona Response Policy Zone (RPZ) yang digunakan untuk menerapkan kebijakan pemfilteran kueri DNS.
- **policy cname blokir.ptgn.web.id:**: Jika kueri cocok dengan aturan dalam zona trustpositifkominfo, permintaan akan dialihkan (diredirect) ke blokir.ptgn.web.id. Ini digunakan untuk memblokir akses ke domain tertentu dengan mengarahkan permintaan ke domain blokir.
- **max-policy-ttl 30**: Menetapkan waktu hidup maksimum (TTL) untuk kebijakan RPZ ke 30 detik, menentukan durasi seberapa lama informasi kebijakan dapat disimpan dalam cache.
- **log no;**: Menonaktifkan pencatatan aktivitas kebijakan RPZ, yang dapat membantu mengurangi volume log dan beban penyimpanan.

4. recursive-only yes

Direktif ini mengonfigurasi server BIND untuk hanya memproses permintaan rekursif, berarti server akan melakukan pencarian lengkap untuk kueri DNS dan tidak akan melayani permintaan untuk zona yang dikelola secara langsung.

5. qname-wait-recurse no

Pengaturan ini mengarahkan server untuk tidak menunggu hasil dari permintaan rekursif sebelum merespons kueri DNS. Hal ini dapat mengurangi waktu respons dalam situasi tertentu, tetapi harus dipertimbangkan dengan hati-hati agar tidak mempengaruhi keakuratan resolusi.

6. break-dnssec yes

Direktif ini mengizinkan server untuk mengabaikan validasi DNSSEC jika terdapat kesalahan dalam data DNSSEC. Ini meningkatkan fleksibilitas tetapi mengurangi tingkat keamanan dengan mengabaikan kesalahan validasi yang mungkin ada.

7. nsip-wait-recurse no;

Menetapkan bahwa server tidak harus menunggu hingga alamat IP server DNS menyelesaikan permintaan rekursif sebelum melanjutkan. Ini bertujuan untuk meningkatkan kinerja tetapi dapat mempengaruhi keandalan resolusi DNS.

8. dnssec-validation auto;

Mengaktifkan validasi DNSSEC secara otomatis, yang memungkinkan server untuk memverifikasi keaslian dan integritas data DNS jika data DNSSEC tersedia. Pengaturan auto memungkinkan server menggunakan DNSSEC bila memungkinkan.

9. listen-on-v6 { any; };

Mengonfigurasi server BIND untuk mendengarkan permintaan pada semua antarmuka IPv6. Ini memastikan bahwa server dapat merespons kueri melalui protokol IPv6.

10. listen-on {any; };

Menetapkan server BIND untuk mendengarkan permintaan pada semua antarmuka IPv4. Dengan pengaturan ini, server dapat menerima kueri dari semua alamat IPv4 yang dapat diakses.

2.3.2 Restart Layanan:

- Setelah konfigurasi selesai, merestart layanan Bind9 dengan perintah sudo systemctl restart bind9.

2.4. Konfigurasi RPZ Slave Zone:

2.4.1 Pengaturan RPZ Zone:

Menambahkan konfigurasi zone untuk RPZ di /etc/bind/named.conf.default-zones:

```
zone "trustpositifkominfo" {
        type slave;
        masters { 103.***.***.**0;***.**5.**6.202; };
        file "slave.trustpositifkominfo";
        notify explicit;
};
```

1. zone "trustpositifkominfo" {

Direktif ini mendefinisikan sebuah zona baru dalam konfigurasi BIND, dengan nama trustpositifkominfo. Zona ini merupakan bagian dari pengaturan DNS yang akan diatur oleh server BIND.

2. type slave;

Menetapkan jenis zona sebagai slave. Sebagai zona slave, server BIND akan mendapatkan data zona dari server master (server utama) yang telah dikonfigurasi untuk menyediakan data zona tersebut. Server slave tidak menyimpan salinan data zona secara lokal tetapi mendapatkan salinan dari server master.

3. masters { 103.*.***.**0; ***.**5.**6.202; };**

Bagian ini menentukan alamat IP dari server master yang menyediakan data zona untuk trustpositifkominfo. Server BIND yang dikonfigurasi sebagai slave akan mengambil data zona dari server dengan alamat IP yang tercantum. Alamat IP ini adalah placeholder dan harus diganti dengan alamat IP server master yang sebenarnya.

4. file "slave.trustpositifkominfo";

Menunjukkan nama file di direktori yang ditetapkan untuk menyimpan salinan data zona yang diterima dari server master. File ini akan berisi data zona untuk trustpositifkominfo yang dikendalikan oleh server master. Nama file ini dapat disesuaikan tetapi harus konsisten dengan pengaturan direktori di server BIND.

5. notify explicit;

Menetapkan bahwa server slave akan mengirim pemberitahuan (notify) secara eksplisit ke server master jika ada perubahan pada data zona yang diterima. Ini berarti server slave akan menginformasikan server master tentang permintaan pembaruan atau perubahan data zona, memastikan bahwa sinkronisasi antara server master dan slave tetap akurat.

Konfigurasi ini mengatur server BIND untuk bertindak sebagai server DNS slave untuk zona trustpositifkominfo, mendapatkan data zona dari server master, dan memastikan bahwa data zona diperbarui sesuai kebutuhan. Pengaturan ini memungkinkan server slave untuk berfungsi sebagai salinan data zona yang diambil dari server master, dengan sinkronisasi yang terjaga melalui pemberitahuan eksplisit.

2.4.2 Sinkronisasi dengan DNS Kominfo:

- Memastikan server dapat berkomunikasi dengan DNS master Kominfo untuk menarik pembaruan secara otomatis

Gambar 1. Proses sinkonisasi Database DNS dengan Database TrustpositifKominfo

HASIL DAN PEMBAHASAN

1. Uji Coba RPZ :

Untuk memastikan bahwa Response Policy Zone (RPZ) pada server DNS berfungsi dengan baik, kita perlu melakukan uji coba langsung menggunakan alat seperti dig dan nslookup. Berikut adalah penjelasan tentang bagaimana melakukan uji coba ini dan apa yang harus diperhatikan.

Menggunakan dig untuk Uji Coba RPZ di sisi server

Alat dig (Domain Information Groper) adalah alat baris perintah yang digunakan untuk melakukan query DNS dan mendapatkan informasi tentang domain tertentu. Ini sangat berguna untuk memeriksa bagaimana server DNS memproses permintaan dan bagaimana RPZ diterapkan.

Berikut hasil pengujian dengan menggunakan tools dig ke domain xnxx.com,

Gambar 2. Hasil outpot dari tools dig

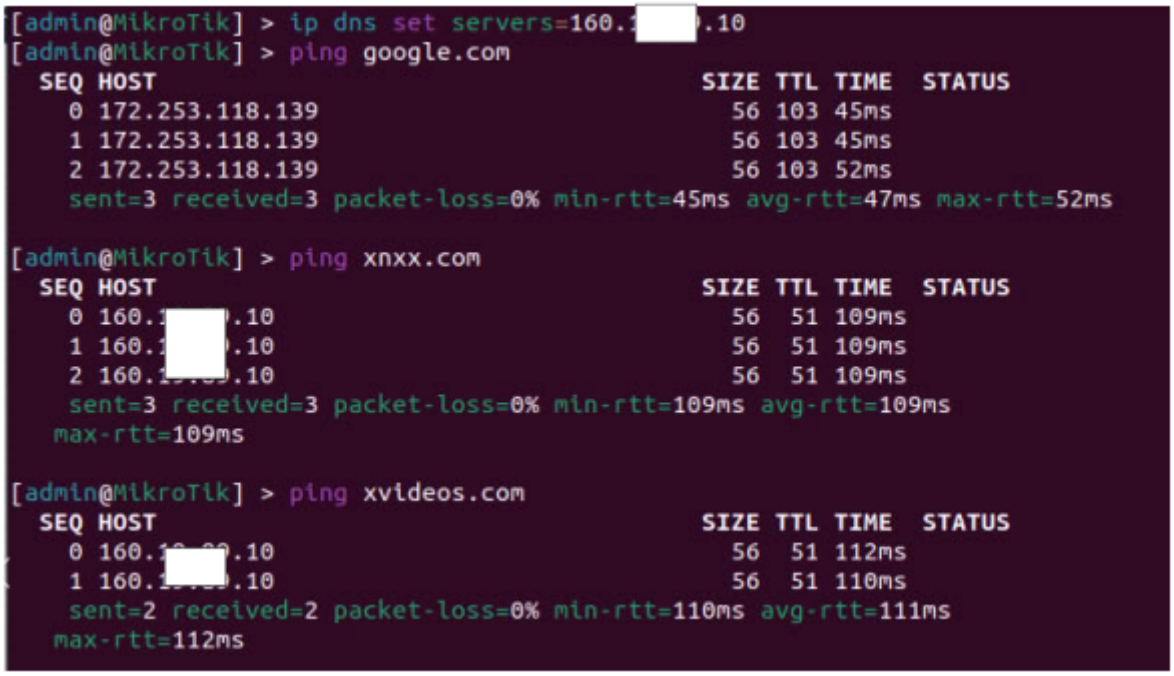
Penjelasan Hasil Dig

1. **Header**:
   - DiG 9.16.1-Debian: Versi dari utilitas dig yang digunakan. Dalam hal ini, menunjukkan bahwa perintah dig ini dijalankan pada sistem Debian.
   - xnxx.com: Domain yang sedang dicari.
2. **Global Options**:
   - +cmd: Opsi default untuk menjalankan dig dengan tampilan output standar.
3. **Got Answer**:
   - ->>HEADER<<- opcode: QUERY: Menunjukkan bahwa operasi yang dilakukan adalah query DNS.
   - status: NOERROR: Status dari query yang menunjukkan bahwa tidak ada kesalahan dalam memproses permintaan.
   - id: 34981: ID unik dari query ini.
4. **Flags**:
   - qr: Menunjukkan bahwa ini adalah jawaban dari server (query response).
   - rd: Recursion Desired, mengindikasikan bahwa resolver menginginkan recursive query.
   - ra: Recursion Available, menunjukkan bahwa server mendukung recursive queries.
5. **QUESTION SECTION**:
   - Menunjukkan domain yang di-query dan tipe record yang diminta. Dalam hal ini, xnxx.com dengan tipe record A (Address Record).
6. **ANSWER SECTION**:
   - xnxx.com. 300 IN CNAME blokir.ptgn.web.id.: Ini menunjukkan bahwa xnxx.com adalah alias (CNAME) dari blokir.ptgn.web.id, yang merupakan cara untuk mengalihkan domain ke host alternatif dalam konteks filtering.

- blokir.ptgn.web.id. 300 IN A 160.**.**.10: Menyediakan alamat IP 160.**.**.10 untuk nama host blokir.ptgn.web.id. Artinya, semua permintaan ke xnxx.com akhirnya akan diarahkan ke alamat IP ini.

7. **Query Time**:
   - Query time: 12 msec: Waktu yang dibutuhkan untuk mendapatkan jawaban dari server DNS.
8. **SERVER**:
   - SERVER: 192.168.1.1#53(192.168.1.1): Alamat IP server DNS yang digunakan untuk melakukan query, dalam hal ini adalah 192.168.1.1 pada port 53.
9. **WHEN**:
   - Tue Aug 6 16:15:00 UTC 2024: Waktu ketika query dilakukan.
10. **MSG SIZE**:
    - MSG SIZE rcvd: 87: Ukuran pesan jawaban yang diterima dalam byte.

Menggunakan Ping untuk Uji Coba RPZ di sisi Client



Gambar 3. Hasil outpot dari tools ping di sisi client

Pengujian Koneksi:

- google.com:

Ping berhasil dengan packet-loss=0%, menunjukkan koneksi ke Google berhasil. Hasil menunjukkan waktu respon (RTT) minimum 45ms, rata-rata 47ms, dan maksimum 52ms.

- xnxx.com:

Ping berhasil dengan packet-loss=0%, dengan menunjukkan koneksi ke ip 160.**.**.10 ini berhasil. di mana ip tersebut merupakan ip dns server rpz. Hasil menunjukkan waktu respon (RTT) minimum 109ms, rata-rata 109ms, dan maksimum 109ms.

KESIMPULAN

Hasil dari perintah dig menunjukkan bahwa ketika mencoba mengakses xnxx.com, domain tersebut dialihkan ke blokir.ptgn.web.id menggunakan CNAME, dan blokir.ptgn.web.id sendiri memiliki alamat IP 160.**.**.10. Ini menunjukkan bahwa sistem filtering DNS sedang diterapkan, di mana akses ke domain tertentu dialihkan ke halaman atau server lain yang mungkin memberikan informasi bahwa situs tersebut diblokir. Hal yang sama juga berlaku di sisi klien. Ketika klien terhubung ke server DNS yang telah dikonfigurasi untuk filtering, akses ke situs yang berhubungan dengan konten judi online dan porno akan diarahkan ke mesin DNS filtering yang sesuai.

DAFTAR PUSTAKA

[1] M. I. Abas, *Sistem Basis Data*. Ideas Publishing, 2018.

[2] M. I. Abas, I. Ibrahim, and S. Pakaya, "Inovasi Sistem Informasi Manajemen Zakat, Infaq dan Sedekah Lazismu Gorontalo," *JRST (Jurnal Ris. Sains dan Teknol.*, vol. 6, no. 1, p. 79, 2022, doi: 10.30595/jrst.v6i1.11939.

[3] R. Kango, N. Jamal, and M. I. Abas, "Analysis of End-to-End Delay Video Conferencing Services on a Mobile Ad Hoc Network," *J. Informatics Telecommun. Eng.*, vol. 6, no. 2, pp. 393–402, 2023, doi: 10.31289/jite.v6i2.8231.

[4] M. Januaripin, "Internet Positif Jembatan Generasi Muda Sehat Berteknologi," *KAMALIYAH J. Pendidik. Agama Islam*, vol. 1, no. 1, Art. no. 1, May 2023, doi: 10.69698/jpai.v1i1.419.

[5] "Peraturan Menteri Komunikasi dan Informatika Nomor 19 Tahun 2014." Accessed: Jul. 25, 2024. [Online]. Available: https://jdih.kominfo.go.id/produk_hukum/view/id/215/t/peraturan+menteri+komunikasi+dan+informatika+nomor+19+tahun+2014

[6] F. Firmansyah and R. A. Purnama, "Filtering Domain Name Server (DNS) untuk Membangun Internet Sehat Menggunakan Routerboard Mikrotik," *JUITA J. Inform.*, vol. 7, no. 1, p. 43, May 2019, doi: 10.30595/juita.v7i1.4164.

[7] M. Danuri, "MODEL DETEKSI DAN PEMBLOKIRAN TINDAKAN AMORAL PENGGUNA INTERNET," *J. Ilm. Infokam*, vol. 14, no. 2, Sep. 2018, doi: 10.53845/infokam.v14i2.152.

[8] "BIND 9." Accessed: Jul. 25, 2024. [Online]. Available: https://bind9.net/

[9] W. DICKY, W. Alex, and A. Eka Puji, "ANALISIS DAN IMPLEMENTASI CONTENT FILTERING TOOLS DALAM MEMBLOK SITUS NEGATIF MENGGUNAKAN METODE (RPZ) RESPONSE POLICY ZONE (Studi Kasus :Lami Komputer)," diploma, Universitas Bina Darma, 2020. Accessed: Jul. 25, 2024. [Online]. Available: https://repository.binadarma.ac.id/1083/

[10] D. Kartika, R. Riska, and Y. Mardiana, "Dns Server And Web Server Simulation With Debian Operating System On Local Area Network," *J. Media Comput. Sci.*, vol. 2, no. 1, Art. no. 1, Jan. 2023, doi: 10.37676/jmcs.v2i1.3439.