BAB III
PERMASALAH PERUSAHAAN

3.1 Analisa Permasalahan yang dialami Perusahaan

PT Queen Network Nusantara sebagai perusahaan yang bergerak di bidang Internet Service Provider (ISP) menghadapi berbagai tantangan dalam menjaga keamanan dan pengelolaan akses internet bagi penggunanya. Sebagai penyedia layanan internet, perusahaan tidak hanya bertanggung jawab untuk memberikan koneksi yang cepat dan stabil, tetapi juga memastikan bahwa pelanggan dapat mengakses internet dengan aman dan nyaman. Salah satu permasalahan utama yang dihadapi adalah pengendalian akses ke situs web yang mengandung konten berbahaya, ilegal, atau tidak sesuai dengan kebijakan yang ditetapkan oleh pemerintah maupun perusahaan.

Dalam dunia digital yang semakin kompleks, banyak pelanggan yang tidak menyadari risiko dari mengakses situs berbahaya, seperti malware, phishing, atau konten ilegal yang dapat membahayakan data pribadi dan perangkat mereka. Oleh karena itu, PT Queen Network Nusantara perlu memastikan bahwa setiap pelanggan, baik individu maupun bisnis, mendapatkan perlindungan optimal tanpa mengurangi kenyamanan dalam berinternet.

Sebagai solusi, diperlukan sistem DNS Filtering yang mampu menyaring akses ke situs web berdasarkan daftar yang telah ditentukan, tanpa mengganggu pengalaman pengguna dalam mengakses layanan yang sah. Sistem ini bertujuan untuk melindungi pelanggan dari ancaman siber seperti pencurian data, penyebaran virus, hingga eksploitasi siber lainnya, sesuai dengan regulasi yang berlaku. Selain itu, DNS Filtering juga membantu perusahaan memenuhi peraturan pemerintah terkait pemblokiran konten negatif, yang dikeluarkan melalui Kominfo dan Komdigi.

Dengan menerapkan DNS Filtering yang efektif dan efisien, PT Queen Network Nusantara dapat meningkatkan kepercayaan pelanggan terhadap layanan yang diberikan.

Pelanggan akan merasa lebih aman dalam menggunakan internet, baik untuk keperluan bisnis, pendidikan, maupun hiburan, tanpa khawatir terhadap ancaman dari situs berbahaya. Selain itu, sistem ini juga dapat meningkatkan kualitas layanan (QoS) ISP dengan mencegah lalu lintas tidak produktif yang membebani jaringan, sehingga koneksi internet dapat tetap cepat, stabil, dan aman.

3.1.1 Temuan Masalah

Beberapa permasalahan yang diidentifikasi di PT Queen Network Nusantara antara lain:

1. Akses ke situs berbahaya dan ilegal – Tanpa sistem filtering yang efektif, pengguna dapat mengakses situs yang berpotensi membahayakan keamanan jaringan.
2. Kurangnya kontrol terhadap lalu lintas DNS – Tidak adanya sistem pengelolaan DNS Filtering menyebabkan perusahaan kesulitan dalam membatasi akses ke domain yang tidak diinginkan.
3. Kepatuhan terhadap regulasi pemerintah – Pemerintah melalui Kominfo dan Komdigi telah mengeluarkan daftar situs yang harus diblokir. PT Queen Network Nusantara perlu memastikan bahwa daftar ini diterapkan dalam sistemnya.
4. Ancaman malware dan phishing – Banyak situs berbahaya yang dapat mencuri data pengguna, menyebarkan virus, atau melakukan penipuan online.

3.1.2 Perumusan Masalah

Berdasarkan temuan di atas, permasalahan utama dapat dirumuskan sebagai berikut:

1. Bagaimana cara mengimplementasikan sistem DNS Filtering menggunakan BIND9 agar sesuai dengan kebutuhan PT Queen Network Nusantara?
2. Bagaimana mengambil data filtering dari situs trustpositif.komdigi.go.id dan menerapkannya secara manual dalam konfigurasi BIND9?
3. Bagaimana mengelola dan memperbarui daftar blokir agar selalu terkini dengan regulasi pemerintah dan ancaman baru yang muncul?

4. Bagaimana menampilkan halaman informasi bagi pengguna yang mengakses situs yang diblokir menggunakan Apache2?

3.1.3 Kerangka Pemecahan Masalah

Untuk menyelesaikan masalah tersebut, solusi yang diusulkan adalah:

1. Instalasi dan Konfigurasi Ubuntu 16.04.7 LTS sebagai server filtering, yang akan menjadi platform utama untuk menjalankan layanan DNS Filtering.
2. Implementasi DNS Filtering menggunakan BIND9, yaitu sistem open-source yang dapat dikonfigurasi untuk menyaring akses berdasarkan daftar domain yang telah ditentukan.
3. Pengambilan data filtering secara manual dari situs trustpositif.komdigi.go.id, di mana daftar domain yang diblokir akan diperbarui secara berkala dengan mengunduh dan memasukkannya secara manual ke dalam konfigurasi BIND9.
4. Pembaruan daftar blokir secara rutin, dengan melakukan pengecekan berkala terhadap daftar domain yang dilarang.
5. Menampilkan halaman informasi blokir menggunakan Apache2, sehingga pengguna yang mencoba mengakses situs terblokir akan diarahkan ke halaman pemberitahuan.

3.2 Landasan Teori

3.2.1 Pengertian Sistem Operasi Ubuntu 16.04.7 LTS

Ubuntu 16.04.7 LTS adalah versi sistem operasi berbasis Linux yang stabil dan banyak digunakan dalam implementasi server. Ubuntu memiliki dukungan komunitas yang luas serta berbagai fitur keamanan yang memungkinkan administrator jaringan mengelola layanan dengan lebih baik.

3.2.2 Pengertian DNS Filtering

DNS Filtering adalah teknik yang digunakan untuk membatasi akses ke situs tertentu dengan cara memblokir permintaan DNS ke domain yang masuk dalam daftar hitam (blacklist). Filtering ini berguna untuk mencegah akses ke situs yang berbahaya, ilegal, atau tidak sesuai kebijakan perusahaan. DNS Filtering dapat dilakukan dengan berbagai cara, salah satunya adalah menggunakan Response Policy Zone (RPZ) pada BIND9.

3.2.3 Pengertian BIND9 (Berkeley Internet Name Domain)

BIND9 adalah salah satu server DNS open-source yang paling banyak digunakan. BIND9 memungkinkan administrator jaringan untuk mengonfigurasi berbagai fitur, termasuk:

- DNS Caching untuk meningkatkan kecepatan akses
- Zone Management untuk mengelola domain secara internal
- ACL (Access Control List) untuk membatasi akses ke domain tertentu
- Response Policy Zone (RPZ) sebagai mekanisme filtering DNS

3.2.4 Apache2 sebagai Halaman Informasi Blokir

Apache2 adalah perangkat lunak server web yang digunakan untuk menampilkan halaman informasi kepada pengguna yang mengakses situs yang telah diblokir oleh sistem DNS Filtering. Dengan menggunakan Apache2, administrator dapat menampilkan pesan pemberitahuan yang menjelaskan bahwa situs yang diakses telah diblokir sesuai dengan kebijakan perusahaan dan regulasi pemerintah.

3.2.5 Sumber Data Filtering dari Trustpositif Komdigi

Trustpositif (Kominfo Digital) menyediakan daftar domain yang harus diblokir sesuai dengan regulasi pemerintah Indonesia. Daftar ini biasanya diperbarui secara

berkala dan berisi situs yang dianggap ilegal, berbahaya, atau tidak sesuai kebijakan. PT Queen Network Nusantara akan mengambil data ini secara manual dari situs https://trustpositif.komdigi.go.id/ untuk diterapkan dalam konfigurasi BIND9.

3.3 Metode yang Digunakan

Untuk mengimplementasikan DNS Filtering di PT Queen Network Nusantara, metode yang digunakan meliputi:

1. Instalasi Ubuntu 16.04.7 LTS sebagai sistem operasi utama server.
2. Instalasi dan Konfigurasi BIND9
    - Menginstal BIND9 di server yang akan digunakan sebagai DNS resolver utama.
    - Mengonfigurasi Response Policy Zone (RPZ) untuk menyaring akses ke domain tertentu.
3. Instalasi dan Konfigurasi Apache2
    - Menginstal Apache2 untuk menampilkan halaman informasi ketika pengguna mencoba mengakses situs yang telah diblokir.
    - Membuat halaman statis atau dinamis untuk menampilkan pesan blokir.
4. Pengambilan Data Filtering secara Manual dari Trustpositif Komdigi
    - Mengunjungi situs https://trustpositif.komdigi.go.id/ secara berkala.
    - Mengunduh dan menyalin daftar domain yang diblokir ke dalam konfigurasi BIND9.
5. Penerapan dan Pengujian
    - Menerapkan konfigurasi di lingkungan PT Queen Network Nusantara.
    - Melakukan pengujian filtering untuk memastikan bahwa situs yang masuk daftar hitam berhasil diblokir.
6. Monitoring dan Pembaruan Manual

- Melakukan pengecekan daftar domain di situs Trustpositif Komdigi secara berkala.
- Memperbarui daftar domain yang diblokir dengan memasukkan data ke dalam konfigurasi BIND9 secara manual.

3.4 Rancangan Program

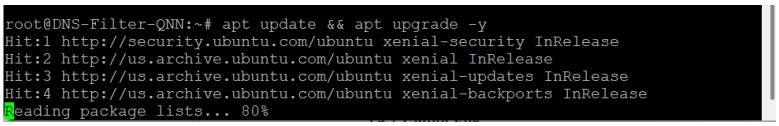
Berikut adalah rancangan implementasi DNS Filtering menggunakan BIND9 di PT Queen Network Nusantara:

3.4.1 Instalasi Ubuntu 16.04.7 LTS

- Unduh Ubuntu 16.04.7 LTS dari situs resmi Ubuntu :

  https://releases.ubuntu.com/16.04/ubuntu-16.04.7-server-amd64.iso
- Buat bootable USB menggunakan Rufus atau di Linux.
- Boot dari USB dan ikuti langkah instalasi hingga selesai.
- Perbarui sistem setelah installasi selesai dilakukan :

  apt update && apt upgrade -y

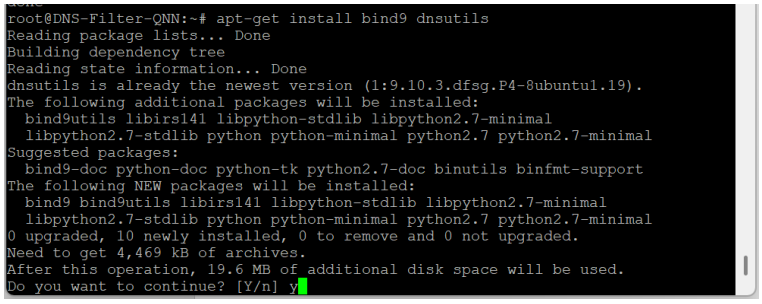


Gambar 4. Update paket ubuntu

3.4.2 Instalasi dan Konfigurasi BIND9

1. Install Bind9 dan komponen pendukung :

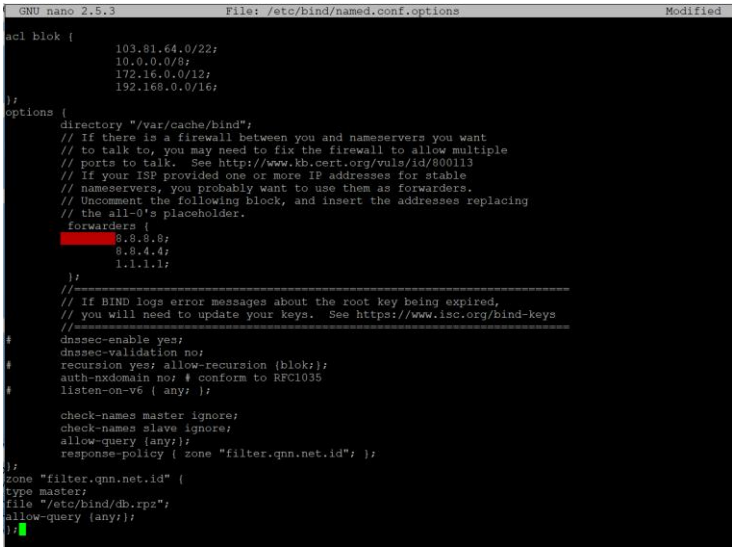
   apt-get install bind9 dnsutils



Gambar 5. Install Bind9

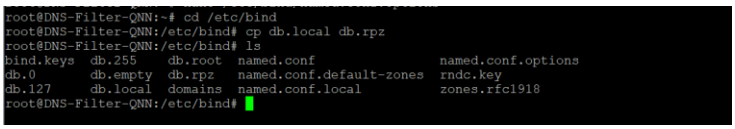
2. Konfigurasi DNS Filtering

- Konfigurasi DNS Option pada /etc/bind/named.conf.options



Gambar 6. DNS Named Option

- Buat File db.rzp dengan mengcopy file db.local



Gambar 7. Buat Folder RPZ

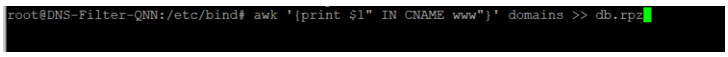
- Unduh File Blacklist dari situs komdigi :

  https://trustpositif.komdigi.go.id/assets/db/domains

Gambar 8. Unduh File Blacklist Komdigi

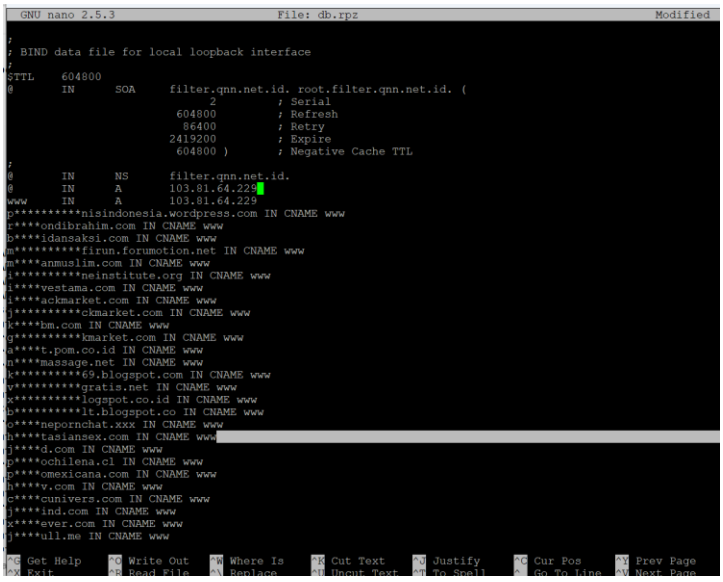
- Masukkan file Blacklist domains ke db.rpz

awk 'length($1) <= 63 {print $1" IN CNAME www"}' domains >> db.rpz



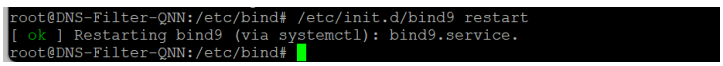
Gambar 9. Input File Blacklist

- Konfigurasi pada file db.rpz



Gambar 10.Konfigurasi RPZ

- Restart BIND

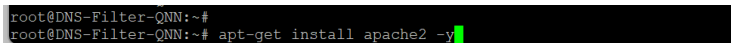


Gambar 11. Restart Bind9

3.4.3 Instalasi dan Konfigurasi Apache2

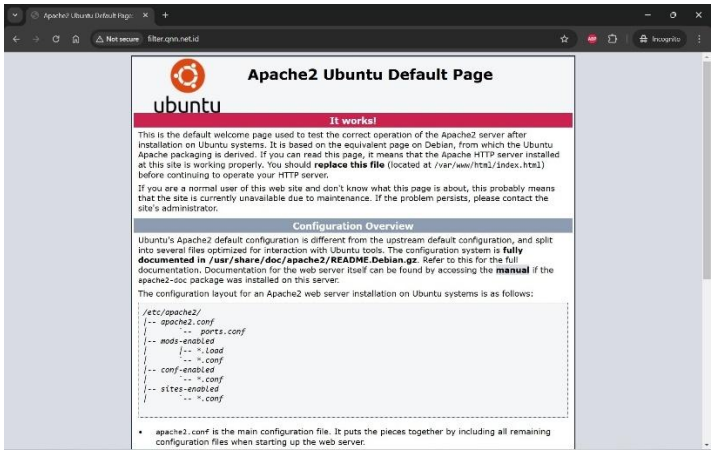
- Install apache2

  apt-get install apache2 -y



Gambar 12. Install Apache2

- Tampilan Setelah apache2 sudah terinstall



Gambar 13. Halaman web Apache2

3.4.4 Membuat Halaman Blokir untuk DNS Filtering

- Konfigurasi pada /var/www/html/index.html

Gambar 14. Coding halaman web pemblokiran