

## **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](http://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](http://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`



```

root@DNS-Filter-QNN:~# apt update && apt upgrade -y
Hit:1 http://security.ubuntu.com/ubuntu xenial-security InRelease
Hit:2 http://us.archive.ubuntu.com/ubuntu xenial InRelease
Hit:3 http://us.archive.ubuntu.com/ubuntu xenial-updates InRelease
Hit:4 http://us.archive.ubuntu.com/ubuntu xenial-backports InRelease
Reading package lists... 80%

```

Gambar 4. Update paket ubuntu

#### 3.4.2 Instalasi dan Konfigurasi BIND9

1. Install Bind9 dan komponen pendukung :  
`apt-get install bind9 dnsutils`

```

root@DNS-Filter-QNN:~# apt-get install bind9 dnsutils
Reading package lists... Done
Building dependency tree
Reading state information... Done
dnsutils is already the newest version (1:9.10.3.dfsg.P4-8ubuntu1.19).
The following additional packages will be installed:
  bind9utils libirs141 libpython-stdlib libpython2.7-minimal
  libpython2.7-stdlib python python-minimal python2.7 python2.7-minimal
Suggested packages:
  bind9-doc python-doc python-tk python2.7-doc binutils binfmt-support
The following NEW packages will be installed:
  bind9 bind9utils libirs141 libpython-stdlib libpython2.7-minimal
  libpython2.7-stdlib python python-minimal python2.7 python2.7-minimal
0 upgraded, 10 newly installed, 0 to remove and 0 not upgraded.
Need to get 4,469 kB of archives.
After this operation, 19.6 MB of additional disk space will be used.
Do you want to continue? [Y/n] y

```

Gambar 5. Install Bind9

## 2. Konfigurasi DNS Filtering

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

```

GNU nano 2.5.3 File: /etc/bind/named.conf.options Modified
acl blok {
    103.81.64.0/22;
    10.0.0.0/8;
    172.16.0.0/12;
    192.168.0.0/16;
};

options {
    directory "/var/cache/bind";
    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk. See http://www.kb.cert.org/vuls/id/800113
    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.
    forwarders {
        8.8.8.8;
        8.8.4.4;
        1.1.1.1;
    };
    // If BIND logs error messages about the root key being expired,
    // you will need to update your keys. See https://www.isc.org/bind-keys
}

dnsssec-validation no;
recursion yes; allow-recursion {blok};
auth-nxdomain no; # conform to RFC1035
listen-on-v6 { any; };

check-names master ignore;
check-names slave ignore;
allow-query {any};
response-policy { zone "filter.qnn.net.id"; };
};

zone "filter.qnn.net.id" {
    type master;
    file "/etc/bind/db.rpz";
    allow-query {any};
};

```

Gambar 6. DNS Named Option

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

```

root@DNS-Filter-QNN:~# cd /etc/bind
root@DNS-Filter-QNN:/etc/bind# cp db.local db.rpz
root@DNS-Filter-QNN:/etc/bind# ls
bind.keys  db.255  db.root  named.conf  named.conf.options
db.0      db.empty  db.rpz  named.conf.default-zones  rndc.key
db.127   db.local  domains  named.conf.local  zones.rfc1918
root@DNS-Filter-QNN:/etc/bind#

```

Gambar 7. Buat Folder RPZ

- Unduh File Blacklist dari situs komdigi :

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

```

root@DNS-Filter-QNN:~# cd /etc/bind
root@DNS-Filter-QNN:~/etc/bind# wget https://trustpositif.komdigi.go.id/assets/db/domains
--2025-03-05 09:48:33-- https://trustpositif.komdigi.go.id/assets/db/domains
Resolving trustpositif.komdigi.go.id (trustpositif.komdigi.go.id)... 182.23.79.198
Connecting to trustpositif.komdigi.go.id (trustpositif.komdigi.go.id)|182.23.79.198|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 148585443 (142M) [application/octet-stream]
Saving to: 'domains'

domains          100%[=====] 141.70M  39.0MB/s   in 3.8s
2025-03-05 09:48:37 (37.2 MB/s) - 'domains' saved [148585443/148585443]

root@DNS-Filter-QNN:~/etc/bind# ls
bind.keys  db.127  db.empty  db.root  named.conf      named.conf.local  rndc.key
db.0      db.255  db.local  domains  named.conf.default-zones  named.conf.options  zones.rfc1918
root@DNS-Filter-QNN:~/etc/bind#

```

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

```

root@DNS-Filter-QNN:~/etc/bind# awk '{print $1" IN CNAME www"}' domains >> db.rpz

```

Gambar 9. Input File Blacklist

- Konfigurasi pada file db.rpz

```

GNU nano 2.5.3      File: db.rpz      Modified
; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA      filter.qnn.net.id. root.filter.qnn.net.id. (
;
                2          / Serial
                604800     / Refresh
                86400      / Retry
                2419200    / Expire
                604800 )   / Negative Cache TTL
;
@         IN      NS      filter.qnn.net.id.
@         IN      A       103.81.64.229
www      IN      A       103.81.64.229
p*****nisindonesia.wordpress.com IN CNAME www
c****ondibrahim.com IN CNAME www
b****idansaksi.com IN CNAME www
m*****firun.forumotion.net IN CNAME www
m*****anmuslim.com IN CNAME www
i*****neinstitute.org IN CNAME www
i****vestama.com IN CNAME www
i****ackmarket.com IN CNAME www
j*****ckmarket.com IN CNAME www
k****bm.com IN CNAME www
g*****kmarket.com IN CNAME www
a****t.pom.co.id IN CNAME www
n*****message.net IN CNAME www
k*****g9.blogspot.com IN CNAME www
v*****gratis.net IN CNAME www
x*****blogspot.co.id IN CNAME www
b*****it.blogspot.co IN CNAME www
o*****pepornchat.xxx IN CNAME www
h*****asiansex.com IN CNAME www
j****d.com IN CNAME www
p****ochilena.cl IN CNAME www
p****omexicana.com IN CNAME www
h****v.com IN CNAME www
c****cunivers.com IN CNAME www
j****ind.com IN CNAME www
t*****eyer.com IN CNAME www
j****ill.me IN CNAME www

```

Gambar 10. Konfigurasi RPZ

- Restart BIND

```

root@DNS-Filter-QNN:~/etc/bind# /etc/init.d/bind9 restart
[ ok ] Restarting bind9 (via systemctl): bind9.service.
root@DNS-Filter-QNN:~/etc/bind#

```

Gambar 11. Restart Bind9

### 3.4.3 Instalasi dan Konfigurasi Apache2

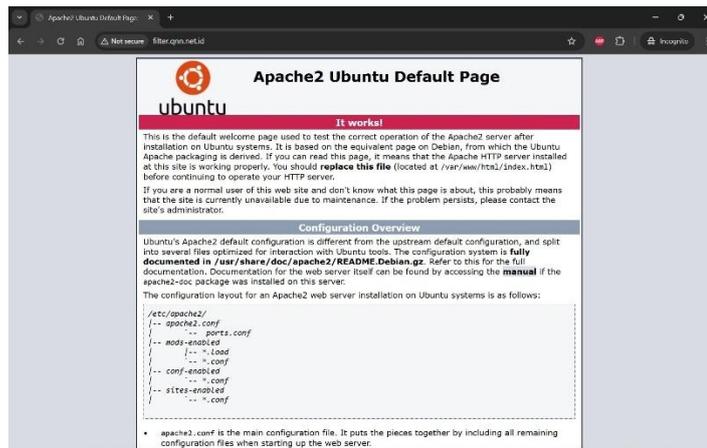
- Install apache2

apt-get install apache2 -y

```
root@DNS-Filter-QNN:~#  
root@DNS-Filter-QNN:~# 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

```
DOCTYPE html<!-- Built with Framr • https://www.framr.com/ --><html><head>  
<meta charset="utf-8">  
  
<!-- End of headStart -->  
<meta name="viewport" content="width=device-width">  
<meta name="generator" content="Framr 1249645">  
<title>Internet Sehat</title>  
<meta name="description" content="Made with Framr">  
<meta name="framer-search-index" content="https://framerusercontent.com/sites/TB87F50T7uqz50ZjL68B/searchIndex-X-W6Z-yQ7aj_jm60">  
<link rel="icon" href="https://framerusercontent.com/sites/5oms/default-favicon-v1.png">  
<!-- Open Graph / Facebook -->  
<meta property="og:type" content="website">  
<meta property="og:title" content="index">  
<meta property="og:description" content="Made with Framr">  
<!-- Twitter -->  
<meta name="twitter:card" content="summary_large_image">  
<meta name="twitter:title" content="index">  
<meta name="twitter:description" content="Made with Framr">  
  
<link href="https://fonts.gstatic.com" rel="preconnect" crossorigin=""><link rel="canonical" href="https://index.framer.website/507/style">  
<!-- End of headEnd -->  
</head>  
  
<body class="framer-body-wgIA2011">  
<script async="" src="https://events.framer.com/script" data-fid="a9094d81ba033942644d50d5db9d49fa347c978740ba056233da08c680c3ad"></script>  
  
<!-- End of bodyStart -->  
<div id="main" data-framer-hydrate-v2="1&quot;routeId&quot;;&quot;wgIA2011&quot;;&quot;localizationId&quot;;&quot;default&quot;;&quot;507/div">  
<div id="" data-framer-container=""></div>  
<script data-framer-appear-animation=""></script>  
<!-- End of bodyEnd -->  
</body></html>
```

Gambar 14. Coding halaman web pemblokiran