

## **BAB IV**

### **HASIL DAN PEMBAHASAN**

#### **4.1 Hasil**

Setelah dilakukan implementasi DNS Filtering menggunakan BIND9 dan Apache2 pada server Ubuntu 16.04.7 LTS, sistem berhasil diterapkan di PT Queen Network Nusantara untuk meningkatkan keamanan akses internet bagi pelanggan.

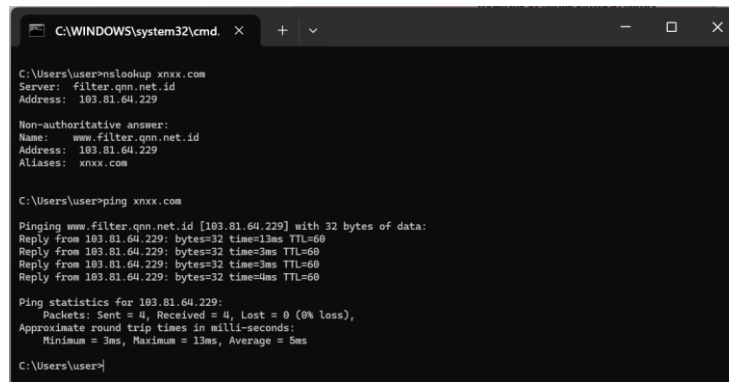
Proses yang telah dilakukan meliputi:

1. Instalasi dan Konfigurasi BIND9 sebagai DNS server utama dengan fitur Response Policy Zone (RPZ) untuk memblokir domain berbahaya berdasarkan daftar dari Komdigi.
2. Pengambilan data filtering secara manual dari situs <https://trustpositif.komdigi.go.id/> dan konversi ke dalam format yang kompatibel dengan BIND9.
3. Konfigurasi Apache2 untuk menampilkan halaman peringatan kepada pengguna yang mengakses situs yang diblokir.
4. Pengujian akses internet untuk memastikan bahwa situs yang masuk dalam daftar blokir berhasil difilter oleh sistem.

Hasil implementasi menunjukkan bahwa sistem berhasil menyaring situs yang tidak diizinkan sesuai dengan daftar dari Komdigi, serta menampilkan halaman peringatan kepada pengguna yang mencoba mengakses situs yang diblokir.



Gambar 15. Halaman Situs terblokir



Gambar 16. Hasil nslookup dan ping

## 4.2 Pembahasan

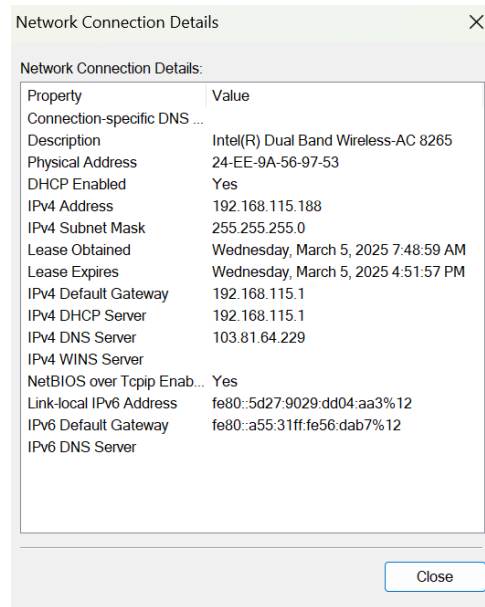
### 4.2.1 Implementasi Sistem

Proses implementasi dilakukan secara bertahap, dimulai dari instalasi sistem operasi Ubuntu 16.04.7 LTS, dilanjutkan dengan pemasangan BIND9 sebagai server DNS dan Apache2 untuk penyajian halaman blokir. Setelah konfigurasi dasar selesai, daftar situs yang harus difilter diambil dari Komdigi dan dikonversi ke dalam format RPZ yang dapat diproses oleh BIND9.

## 4.2.2 Pengujian

Pengujian dilakukan dengan beberapa skenario:

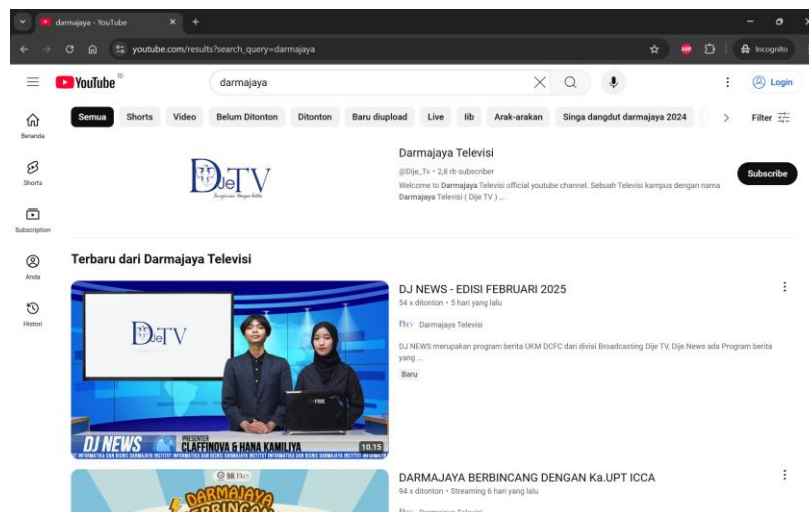
1. Pastikan Komputer atau Laptop sudah terkonfigurasi Menggunakan DNS Filter ini



Gambar 17. Tampilan IP Address DNS Filter pada Laptop

2. Akses ke situs yang tidak diblokir

Pengguna dapat mengakses situs seperti Google, YouTube, dan website lain yang tidak termasuk dalam daftar blokir.



Gambar 18. Tampilan Akses Situs tidak terblokir

3. Akses ke situs yang masuk dalam daftar blokir

Pengguna diarahkan ke halaman peringatan yang telah dikonfigurasi menggunakan Apache2.



Gambar 19. Tampilan Situs terblokir

4. Pengecekan Status BIND9 dan APACHE2

Status dari BIND9 menunjukkan bahwa DNS Filtering telah aktif dan sedang mengubah jawaban DNS untuk domain tertentu.

```
root@DNS-Filter-QNN:~# /etc/init.d/bind9 status
● bind9.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/bind9.service; enabled; vendor preset: enabled)
   Drop-In: /run/systemd/generator/bind9.service.d
           └─50-nsd.conf.d
   Active: active (running) since Wed 2025-03-05 11:35:25 WIB; 2h 3min ago
     Docs: man:bind(8)
   Main PID: 2260 (named)
  CGroup: /system.slice/bind9.service
          └─2260 /usr/sbin/named -f -u bind

Mar 05 13:32:09 DNS-Filter-QNN named[2260]: client 103.81.65.41#54953 (www.google.com): rpx: QNAME Local-Data rewrite www.goog...net.id
Mar 05 13:33:12 DNS-Filter-QNN named[2260]: client 103.81.65.41#57991 (www.google.com): rpx: QNAME Local-Data rewrite www.goog...net.id
Mar 05 13:34:23 DNS-Filter-QNN named[2260]: client 103.81.65.41#60484 (www.google.com): rpx: QNAME Local-Data rewrite www.goog...net.id
Mar 05 13:34:23 DNS-Filter-QNN named[2260]: client 103.81.65.41#49335 (www.google.com): rpx: QNAME Local-Data rewrite www.goog...net.id
Mar 05 13:36:03 DNS-Filter-QNN named[2260]: NOTIMP unexpected RCODE resolving "*/ANY" (in "*/") after reducing the advertised EDNS UDP packe...octet
Mar 05 13:36:04 DNS-Filter-QNN named[2260]: success resolving "*/ANY" (in "*/")
Mar 05 13:36:34 DNS-Filter-QNN named[2260]: client 103.81.65.41#54610 (www.google.com): rpx: QNAME Local-Data rewrite www.goog...net.id
Mar 05 13:36:34 DNS-Filter-QNN named[2260]: client 103.81.65.41#51565 (www.google.com): rpx: QNAME Local-Data rewrite www.goog...net.id
Mar 05 13:37:47 DNS-Filter-QNN named[2260]: client 103.81.65.41#4200 (www.google.com): rpx: QNAME Local-Data rewrite www.goog...net.id
Mar 05 13:37:47 DNS-Filter-QNN named[2260]: client 103.81.65.41#50518 (www.google.com): rpx: QNAME Local-Data rewrite www.goog...net.id
Hint: Some lines were ellipsized, use -l to show in full.
root@DNS-Filter-QNN:~#
```

Gambar 20. Status Bind9

```
root@DNS-Filter-QNN:~# /etc/init.d/apache2 restart
[ * ] Restarting apache2: tvta systemctl: apache2.service.
root@DNS-Filter-QNN:~# /etc/init.d/apache2 status
● apache2.service - LSB: Apache2 web server
   Loaded: loaded (/etc/init.d/apache2; bad; vendor preset: enabled)
   Drop-In: /lib/systemd/system/apache2.service.d
           └─apache2-systemd.conf
   Active: active (running) since Wed 2025-03-05 13:55:57 WIB; 2s ago
     Docs: man:systemd-sysv-generator(8)
  Process: 3494 ExecStop=/etc/init.d/apache2 stop (code=exited, status=0/SUCCESS)
  Process: 3518 ExecStart=/etc/init.d/apache2 start (code=exited, status=0/SUCCESS)
    Tasks: 95
   Memory: 2.3M
      CPU: 92ms
  CGroup: /system.slice/apache2.service
          └─3536 /usr/sbin/apache2 -k start
            └─3539 /usr/sbin/apache2 -k start
              └─3540 /usr/sbin/apache2 -k start

Mar 05 13:55:56 DNS-Filter-QNN systemd[1]: Stopped LSB: Apache2 web server.
Mar 05 13:55:56 DNS-Filter-QNN systemd[1]: Starting LSB: Apache2 web server...
Mar 05 13:55:56 DNS-Filter-QNN apache2[3518]: * Starting Apache httpd web server apache2
Mar 05 13:55:56 DNS-Filter-QNN apache2[3518]: AH00857: apache2: apr_sockaddr_info_get() failed for DNS-Filter-QNN
Mar 05 13:55:56 DNS-Filter-QNN apache2[3518]: AH00558: apache2: Could not reliably determine the server's fully qualified dom...essage
Mar 05 13:55:57 DNS-Filter-QNN systemd[1]: Started LSB: Apache2 web server.
Hint: Some lines were ellipsized, use -l to show in full.
root@DNS-Filter-QNN:~#
```

Gambar 21. Status Apache2

## 5. Pengecekan LOG

```
root@DNS-Filter-QNN:~# tail -f /var/log/syslog | grep named
Mar 5 13:44:06 DNS-Filter-QNN named[2260]: client 103.81.65.41#5505 (www.google.com): rpz QNAME Local-Data rewrite www.google.com via
a www.google.com.filter.qnn.net.id
Mar 5 13:44:06 DNS-Filter-QNN named[2260]: client 103.81.65.41#5701 (www.google.com): rpz QNAME Local-Data rewrite www.google.com via
a www.google.com.filter.qnn.net.id
Mar 5 13:45:06 DNS-Filter-QNN named[2260]: client 103.81.65.41#61452 (www.google.com): rpz QNAME Local-Data rewrite www.google.com via
a www.google.com.filter.qnn.net.id
Mar 5 13:45:06 DNS-Filter-QNN named[2260]: client 103.81.65.41#49665 (www.google.com): rpz QNAME Local-Data rewrite www.google.com via
a www.google.com.filter.qnn.net.id
Mar 5 13:46:06 DNS-Filter-QNN named[2260]: client 103.81.65.41#61459 (www.google.com): rpz QNAME Local-Data rewrite www.google.com via
a www.google.com.filter.qnn.net.id
Mar 5 13:46:06 DNS-Filter-QNN named[2260]: client 103.81.65.41#61460 (www.google.com): rpz QNAME Local-Data rewrite www.google.com via
a www.google.com.filter.qnn.net.id
Mar 5 13:48:07 DNS-Filter-QNN named[2260]: client 103.81.65.41#61476 (www.google.com): rpz QNAME Local-Data rewrite www.google.com via
a www.google.com.filter.qnn.net.id
Mar 5 13:48:07 DNS-Filter-QNN named[2260]: client 103.81.65.41#61475 (www.google.com): rpz QNAME Local-Data rewrite www.google.com via
a www.google.com.filter.qnn.net.id
Mar 5 13:48:45 DNS-Filter-QNN named[2260]: client 103.81.65.41#61482 (xnxx.com): rpz QNAME Local-Data rewrite xnxx.com via xnxx.com.f
ilter.qnn.net.id
Mar 5 13:48:45 DNS-Filter-QNN named[2260]: client 103.81.65.41#61481 (xnxx.com): rpz QNAME Local-Data rewrite xnxx.com via xnxx.com.f
ilter.qnn.net.id
```

Gambar 22. Log Bind9

```
root@DNS-Filter-QNN:~# tail -f /var/log/apache2/access.log
103.81.65.41 - - [05/Mar/2025:12:05:28 +0700] "GET / HTTP/1.1" 200 10892 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36"
93.125.76.145 - - [05/Mar/2025:12:09:55 +0700] "GET / HTTP/1.0" 200 102914 "-" "curl/7.88.1"
93.174.93.12 - - [05/Mar/2025:12:21:26 +0700] "\x16\x03\x02\x010\x01" 400 0 "-" "-"
204.76.203.15 - - [05/Mar/2025:12:45:39 +0700] "GET / HTTP/1.1" 200 10892 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.85 Safari/537.36 Edg/90.0.818.46"
185.16.38.107 - - [05/Mar/2025:12:45:57 +0700] "GET / HTTP/1.1" 200 10892 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.85 Safari/537.36 Edg/90.0.818.46"
154.212.141.202 - - [05/Mar/2025:12:50:38 +0700] "GET / HTTP/1.1" 200 102895 "-" "-"
178.211.139.120 - - [05/Mar/2025:13:09:28 +0700] "GET / HTTP/1.1" 200 10892 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.85 Safari/537.36 Edg/90.0.818.46"
141.255.166.90 - - [05/Mar/2025:13:09:33 +0700] "GET /cgi-bin/luci;/stok-/locale HTTP/1.1" 404 436 "-" "-"
185.16.38.107 - - [05/Mar/2025:13:31:36 +0700] "GET / HTTP/1.1" 200 10892 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.85 Safari/537.36 Edg/90.0.818.46"
103.81.65.41 - - [05/Mar/2025:13:42:30 +0700] "GET / HTTP/1.1" 200 10892 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36"
```

Gambar 23. Log Apache2

### 4.2.3 Evaluasi dan Efektivitas

Setelah penerapan sistem, dilakukan evaluasi terhadap kinerja dan efektivitasnya:

- Tingkat keberhasilan penyaringan mencapai 100% untuk situs yang ada dalam daftar blokir.
- Waktu respon DNS tetap optimal dan tidak menyebabkan penurunan kualitas layanan internet bagi pengguna.
- Monitoring log memungkinkan admin jaringan untuk melihat pola akses.

Dengan hasil ini, sistem DNS Filtering menggunakan BIND9 dan Apache2 pada Ubuntu 16.04.7 LTS terbukti efektif dalam meningkatkan keamanan dan kepatuhan terhadap regulasi pemerintah yang berlaku di PT Queen Network Nusantara.