BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil implementasi dan evaluasi sistem DNS Filtering dengan BIND9 dan Apache2 di Ubuntu 16.04.7 LTS pada PT Queen Network Nusantara, dapat disimpulkan bahwa:

1. DNS Filtering berhasil diterapkan dengan menggunakan BIND9 untuk menyaring akses ke situs yang masuk dalam daftar blacklist dari Komdigi. Situs-situs yang dilarang dapat diblokir secara efektif, sehingga mengurangi risiko keamanan siber seperti malware, phishing, dan akses ke konten ilegal.
2. Halaman blokir menggunakan Apache2 berfungsi dengan baik dalam memberikan informasi kepada pengguna mengenai alasan pemblokiran. Ini membantu pelanggan memahami kebijakan pemblokiran dan meminimalkan keluhan terkait akses situs yang dibatasi.
3. Kinerja layanan internet tidak mengalami gangguan signifikan, berdasarkan hasil evaluasi latensi DNS. Sistem tetap responsif dan tidak menyebabkan perlambatan yang berarti bagi pengguna jaringan.
4. Monitoring dan logging efektif dalam memantau aktivitas DNS Filtering, sehingga administrator dapat dengan mudah mengevaluasi efektivitas pemblokiran dan melakukan perbaikan jika diperlukan.

Dengan implementasi ini, PT Queen Network Nusantara dapat lebih mudah mematuhi regulasi pemerintah dan meningkatkan keamanan serta kualitas layanan internet yang diberikan kepada pelanggan.

5.2 Saran

Untuk meningkatkan efektivitas sistem DNS Filtering dan meningkatkan kualitas layanan bagi pelanggan, beberapa saran perbaikan dan pengembangan yang dapat dilakukan adalah:

1. Otomatisasi Pembaruan Daftar Blokir
    - Implementasi skrip otomatis yang berjalan secara terjadwal (cron job) untuk mengambil data terbaru dari Komdigi dan memperbarui konfigurasi BIND9 tanpa perlu restart manual.
    - Menggunakan mekanisme incremental update untuk menghindari downtime atau gangguan layanan saat daftar blokir diperbarui.
2. Pengelolaan Whitelist yang Lebih Baik
    - Menyediakan mekanisme whitelist management agar situs yang diblokir secara tidak sengaja dapat dikembalikan berdasarkan kebutuhan pelanggan.
    - Melibatkan tim support atau feedback dari pelanggan untuk mengevaluasi apakah ada domain yang perlu dikecualikan dari pemblokiran.
3. Penggunaan Sistem Logging dan Monitoring yang Lebih Canggih
    - Mengintegrasikan sistem monitoring seperti Grafana dan Prometheus untuk memvisualisasikan lalu lintas DNS dan mempermudah analisis performa filtering.
    - Menerapkan alert system yang dapat memberikan notifikasi jika terjadi anomali dalam layanan DNS Filtering.
4. Sosialisasi ke Pengguna Mengenai Kebijakan Filtering
    - PT Queen Network Nusantara dapat memberikan edukasi kepada pelanggan mengenai kebijakan pemblokiran yang diterapkan. Ini dapat dilakukan melalui email, pemberitahuan di portal pelanggan, atau informasi pada halaman blokir.
    - Menyediakan kanal komunikasi bagi pelanggan yang ingin memberikan masukan terkait daftar situs yang diblokir atau yang perlu dibuka kembali.