BUKU PANDUAN SISTEM
INTELLIGENT DNS MANAGEMENT

PT MARS DATA TELEKOMUNIKASI

Versi 2.0 - Februari 2026

Security, Speed, and Reliability

1. Pendahuluan

Sistem DNS MARS DATA adalah solusi manajemen DNS tingkat lanjut yang dirancang untuk infrastruktur ISP dan Enterprise. Sistem ini menggabungkan kecepatan resolusi DNS dengan lapisan keamanan berlapis untuk melindungi pengguna dari ancaman siber dan serangan DDoS.

2. Arsitektur Sistem (Hybrid DNS)

Sistem ini menggunakan pendekatan **Hybrid** untuk memaksimalkan performa:

- **Dnsmasq (Frontend):** Menangani caching cepat, manajemen whitelist/blacklist, dan filtering domain malware.
- **Unbound (Backend):** Bertindak sebagai *Recursive Resolver* yang aman dengan dukungan DNSSEC, memastikan validitas data DNS dari root server.

> **Alur Query:**
> Client → Dnsmasq (Cache Check) → Unbound (Recursive Lookup) → Internet

3. Keamanan & Proteksi (Guardian Engine)

Guardian.py adalah jantung dari sistem penyembuhan mandiri (self-healing) dan deteksi serangan:

- **Deteksi Flood:** Memantau log secara real-time untuk mendeteksi anomali query (DDoS).
- **Auto-Banning:** Secara otomatis memblokir IP penyerang melalui `iptables` jika melewati ambang batas 1.500 QPS.
- **Self-Healing:** Memantau status layanan `dnsmasq` dan `unbound`. Jika layanan mati, Guardian akan melakukan perbaikan dan restart otomatis.

4. Firewall & Network Hardening

Konfigurasi `setup_firewall.sh` menerapkan aturan keamanan ketat:

Fitur	Deskripsi
Anti-DDoS UDP	Membatasi query DNS maksimal 1.500 QPS per IP menggunakan `hashlimit`.
NAT Interception	Memaksa semua trafik port 53 untuk masuk ke server lokal (mencegah bypass DNS).
Access Control List (ACL)	Hanya IP/Subnet di `whitelist.conf` yang bisa mengakses SSH (22) dan Web GUI (5000).

5. Manajemen Web GUI

Dashboard modern berbasis Flask menyediakan kontrol penuh:

- **Monitoring Real-time:** Grafik trafik query dan status layanan.
- **Global Whitelist:** Antarmuka untuk menambah IP/Subnet terpercaya tanpa perlu restart manual.
- **Security Logs:** Melihat riwayat serangan dan aktivitas sistem.

6. Internet Positif & Captive Portal

Sistem ini mendukung regulasi konten dan pengalaman pengguna mobile:

- **Halaman Blokir:** Tampilan kustom PT MARS DATA untuk domain yang dilarang.
- **Redirect HTTP (302):** Pengalihan otomatis untuk akses HTTP yang lebih cepat ke halaman blokir.
- **Popup Android/iOS:** Memicu notifikasi "Sign in to network" pada perangkat mobile saat mencoba mengakses situs terblokir melalui teknik *Captive Portal Detection*.