

BUKU PANDUAN SISTEM - PT MARS DATA TELEKOMUNIKASI

DUAL STACK DNS ENGINE (ISP SCALE EDITION)

Dokumentasi ini berisi panduan operasional dan teknis untuk sistem DNS Mars Data yang telah dioptimalkan untuk skala ISP dengan topologi NAT.

1. RINGKASAN SISTEM

Sistem ini menggunakan arsitektur **Hybrid DNS High Performance** yang menggabungkan kecepatan **dnsmasq** dengan keamanan serta rekursi tingkat tinggi dari **Unbound**.

- **DNS Engine:** Hybrid (dnsmasq + Unbound) - Tuned for High Concurrency.
- **Security:** Anti-DDoS (iptables Hashlimit), Malware Shield (100k+ domains), Intelligent Self-Healing Guardian.
- **Web GUI:** Management Dashboard berbasis Flask dengan antarmuka modern dan responsif.
- **Topologi:** Mendukung **NAT Topology** (Ribuan user dibalik satu IP Public) dengan manajemen koneksi yang efisien.

2. DNS TRUST & INTERNET POSITIF

Fitur ini dirancang untuk mematuhi regulasi pemblokiran konten negatif (Internet Positif) dengan pengalaman pengguna yang mulus.

- **HTTPS Redirect:** Sistem kini mendukung redirect otomatis dari akses HTTPS ke domain terblokir menuju halaman blokir HTTP (via 302 Redirect) setelah user melewati peringatan SSL.
- **Cara Kerja:** Sistem secara otomatis mencegat trafik DNS dan HTTP/HTTPS melalui firewall (NAT) untuk mengarahkan domain terblokir ke halaman peringatan internal.
- **Konfigurasi Utama:** /etc/dnsmasq.d/smardns.conf (Single Source of Truth).
- **Status:** Jika DNS Trust "Enabled", pemblokiran aktif. Jika "Disabled", sistem tetap melakukan intersepsi namun dengan aturan yang lebih longgar.
- **Guardian:** Layanan guardian.py memastikan aturan firewall tetap aktif meskipun sistem direstart.

3. ANALISIS TRAFIK & MONITORING

Dashboard Web GUI menyediakan pemantauan real-time yang telah ditingkatkan:

- **Traffic Analysis (Live QPS):**
 - **Garis Magenta (Pink):** Menampilkan **QPS (Queries Per Second)** murni per detik.
 - **Area Biru (Cyan):** Menampilkan **Snapshot Queries** (kepadatan query terbaru).
 - **High Load Warning:** Indikator peringatan akan muncul jika QPS melebihi **90.000 QPS**.
 - **Sampling Engine:** Menggunakan *Deep Log Sampling* (200k baris) untuk akurasi tinggi pada trafik padat.
- **Combined Analysis (Baru):**
 - **SERVFAIL & Blocklist:** Grafik batang gabungan yang menampilkan domain dengan error SERVFAIL terbanyak dan domain yang paling sering diblokir dalam satu tampilan ringkas.
 - Membantu identifikasi cepat antara masalah jaringan (SERVFAIL) atau kebijakan blokir (Blocklist).
- **Hardware Monitoring:**
 - **CPU & RAM:** Beban pemrosesan real-time.
 - **HDD Usage:** Pemantauan sisa ruang penyimpanan disk.

4. FITUR BARU: RESPONSIVE FULLSCREEN MONITORING

Sistem kini dilengkapi dengan mode pemantauan layar penuh yang adaptif: - **Auto-Scale:** Grafik akan menyesuaikan ukurannya secara otomatis mengikuti orientasi dan ukuran layar perangkat. - **Mobile Friendly:** Dioptimalkan untuk iPhone dan Android dengan navigasi "Exit Fullscreen" yang mudah. - **High Performance:** Mode fullscreen menggunakan akselerasi GPU browser untuk memastikan render grafik tetap lancar tanpa membebani CPU server.

5. BATASAN PERFORMA (ISP SCALE LIMITS)

Sistem telah dikonfigurasi ulang untuk menangani topologi NAT dimana satu IP Public mewakili ribuan user:

- **Global Rate Limit: 100.000 QPS** (Perlindungan level server).
- **Per-IP Rate Limit: 20.000 QPS** (Ditingkatkan dari 1.000 QPS untuk mengakomodasi NAT).
- **Unbound Rate Limit: 20.000 QPS** per IP untuk rekursi.
- **DNS Flood Protection:** Menggunakan modul hashlimit iptables yang efisien untuk memitigasi serangan tanpa memblokir trafik legit dari NAT yang padat.

6. MANAJEMEN WHITELIST & MALWARE

- **Global Whitelist:** IP/Subnet yang ditambahkan ke Whitelist akan melewati (bypass) semua aturan pemblokiran, rate limiting, dan intersepsi.
- **Malware Shield:** Menggunakan database /etc/dnsmasq.d/malware.conf yang diperbarui secara berkala untuk memblokir situs berbahaya.

7. PEMELIHARAAN (MAINTENANCE)

- **Log System:** Sistem secara otomatis melakukan rotasi log untuk mencegah kepenuhan disk.
- **Intelligent Self-Healing:**
 - guardian.py secara aktif memonitor port DNS (53/UDP) dan Web GUI (5000/TCP).
 - Jika layanan macet atau mati, Guardian akan mencoba melakukan restart otomatis dan memperbaiki konfigurasi yang korup.
 - Mendeteksi perubahan IP Network dan secara otomatis memperbarui aturan Firewall tanpa downtime.

8. TROUBLESHOOTING WEB GUI

Jika Web GUI tidak dapat diakses:

1. **Pastikan menggunakan HTTPS (bukan HTTP):** https://IP_SERVER:5000
2. **Sertifikat Self-Signed:** Browser akan menampilkan peringatan keamanan - klik "Advanced" → "Proceed" untuk melanjutkan.
3. **Cek status layanan:** sudo systemctl status dnsmars-gui
4. **Restart Web GUI:** sudo systemctl restart dnsmars-gui
5. **Health Check:** Akses https://IP_SERVER:5000/health untuk memastikan layanan aktif.
6. **Password default:** admin (segera ganti setelah login pertama)

Dokumen ini diperbarui secara otomatis oleh System Assistant. © 2026 PT MARS DATA TELEKOMUNIKASI