BUKU PANDUAN SISTEM - PT MARS DATA TELEKOMUNIKASI

DNS ENGINE CYBER SECURITY (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/smartdns.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.

Captive Portal Bypass (False Positive Fix) Untuk mencegah perangkat (Android/iOS) mendeteksi jaringan sebagai "Captive Portal" palsu yang menye-

babkan popup “Sign in to network” muncul terus-menerus:

- **Mechanism:** Whitelisting domain connectivity check (misal: `connectivitycheck.gstatic.com`, `android.clients.google.com`) agar resolve ke IP asli via Unbound, bukan ke IP Block Page.
- **Firewall Policy:** Intersepsi agresif port 80/443 di Firewall telah **dinonaktifkan**. Redirect ke halaman blokir HANYA terjadi jika DNS meresolve domain ke IP Server. Trafik HTTP/HTTPS normal ke internet tidak lagi dibelokkan paksa.
- **Config:** `/home/dns/dnsMars/whitelist_domains.txt`
- **Domains Covered:** Android (Google), iOS (Apple), Windows, Firefox, **Infinix, Asus, Sony, Motorola, LG**.
- **Benefit:** User tidak akan melihat halaman blokir Internet Positif saat baru terkoneksi ke WiFi, kecuali mereka benar-benar mengakses konten terlarang.

---

3. PROTEKSI DISK DARURAT (NEW)

Guardian System kini dilengkapi dengan **Emergency Disk Protection** untuk mencegah kegagalan sistem akibat log yang membanjir:

- **Monitoring Real-time:** Guardian memantau penggunaan disk root (`/`) setiap 10 detik.
- **Critical Threshold:** Jika penggunaan disk mencapai **90%**, sistem akan masuk mode darurat.
- **Auto-Cleanup:**
  - Log aktif (`dnsmasq.log`, `access.log`) akan langsung di-truncate (dikosongkan) menjadi 0 byte.
  - File log arsip (`.gz`, `.1`) akan dihapus paksa.
  - Mencegah server crash atau Unbound gagal start karena kehabisan ruang disk.

---

4. MITIGASI SERANGAN INTERNAL & STABILITAS

Sistem kini dilengkapi dengan kernel tuning dan monitoring aktif untuk menangani ancaman kestabilan:

- **Anti-Looping:** Dnsmasq dan Unbound dikonfigurasi untuk mendeteksi DNS forwarding loops.
- **Memory Leak & Swap Thrashing:**
  - Guardian memantau penggunaan RAM dan Swap.
  - Jika RAM > 90% dan Swap penuh (Thrashing), layanan DNS akan direstart otomatis untuk membebaskan memori sebelum sistem hang (OOM).
- **UDP Drop Prevention:**

  - Kernel buffer (`rmem_default`, `rmem_max`) ditingkatkan hingga 16MB untuk mencegah paket loss saat traffic tinggi.
- **IRQ Overload:** Menggunakan `irqbalance` untuk mendistribusikan beban interupsi jaringan ke semua core CPU.
- **Botnet Mitigation:** Rate limit per-IP (20.000 QPS) mencegah satu botnet yang terinfeksi melumpuhkan seluruh server.

---

5. SYSTEM THREAT ANALYSIS (BARU)

Fitur intelijen keamanan baru untuk mendeteksi dan memblokir ancaman jaringan tingkat lanjut:

- **Integrated Traffic Analysis (3-in-1):** Grafik Web GUI kini menampilkan 3 metrik dalam satu tampilan:
  - **SERVFAIL Errors:** Indikasi masalah jaringan/DNSSEC.
  - **BLOCKED Domains:** Blokir iklan/konten negatif.
  - **CYBER THREATS:** Deteksi serangan siber aktif.
- **Log Engine Optimization:** Menggunakan teknik `tail -n 100000 | grep` untuk analisis real-time yang sangat ringan, tanpa membebani disk atau membanjiri log sistem.
- **ACS / TR-069 Botnet Detection:** Mendeteksi pola komunikasi dari perangkat yang terinfeksi botnet (Mirai, Mozi) atau protokol manajemen ISP yang tidak diinginkan (ACS).
- **Crypto Miner Blocking:** Mengidentifikasi dan memblokir trafik ke mining pool cryptocurrency yang memakan resource CPU/Bandwidth pelanggan.
- **C2 Server Blocking:** Memutus komunikasi antara perangkat terinfeksi dengan Command & Control server peretas.
- **Actionable Intelligence:**
  - **One-Click Block:** Operator dapat langsung memblokir domain berbahaya dari dashboard.
  - **Bulk Action (BARU):** Fitur seleksi massal dan pencarian (Search) memungkinkan pemblokiran banyak domain sekaligus dengan satu kali restart service.
  - **Auto-Block System (BARU):** Sistem dapat dikonfigurasi untuk secara otomatis memblokir domain berdasarkan kategori ancaman (ACS, Miner, C2) setiap 10 menit tanpa intervensi manual.
  - **Safe Blocking:** Pemblokiran ancaman ini **TIDAK** akan memutus koneksi internet pelanggan, hanya memutus jalur komunikasi malware tersebut.
  - **Recovery:** Domain yang tidak sengaja diblokir dapat dikembalikan (Unblock) melalui menu **Blacklist**.

---

6. 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.

---

7. 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.

---

8. 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.

9. 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.

---

10. PEMELIHARAAN & KEAMANAN LOG (LOG SAFETY)

Sistem telah diamankan dari risiko "Disk Full" akibat banjir log (Log Flooding):

- **Auto Log Rotation:** Log sistem (`dnsmasq.log`, `guardian.log`, `nginx`) dikonfigurasi dengan **Logrotate** yang ketat:
  - **Max Size:** 100MB per file.
  - **Rotasi:** Maksimal 3 file backup.
  - **Kompresi:** Log lama otomatis dikompres (.gz) untuk menghemat ruang.
- **Proteksi Disk Darurat:** Jika disk tetap penuh hingga 90% (misal karena serangan masif), Guardian akan otomatis **menghapus paksa** log lama agar layanan DNS tetap hidup.
- **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.

---

11. 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)
