Autonomous Security Infrastructure – for Self-Hosted Physical Server Operation

Most web services depend on external security gateways such as Cloudflare.
However, that means *delegating* security — not *verifying* it directly.

The server **(glitter.kr)** overcomes this structural limitation by building an **autonomous infrastructure** that proves trust at every layer by itself.

Can you abandon Cloudflare?
Let's complete trust through self-verification, not delegation.

---

1. Overview

This server is a fully autonomous security infrastructure that does not rely on any external DNS proxy or cloud gateway.
It implements directly signed **DNSSEC** and **DANE/TLSA** for end-to-end encryption, ensuring a seamless trust chain from root to application.

---

2. DNS Security Architecture

- **Self-managed nameservers**: `ns1–ns5.glitter.kr`, all independent BIND instances deployed across geographically distributed regions.
- **DNSSEC**: KSK/ZSK separation with automatic re-signing (`sign-glitter.sh`) for continuous validation.
- **DANE/TLSA integration**: Automatic TLSA record generation and distribution for `_25._tcp.mail.glitter.kr`.
- **Result**: As long as the `.kr` TLD remains signed,
  the Root → .kr → glitter.kr chain of trust stays fully intact,
  minimizing the risk of tampered or cached DNS responses in validating resolvers.

---

3. Network Layer – Direct TLS Negotiation

- No CDN/WAF proxies (Cloudflare, AWS, Akamai excluded).
- TLS sessions terminate only at **Nginx**, which connects to **FastAPI** on `127.0.0.1`.
  There are no intermediate decryption points.
- Complete security headers: HSTS (Preload), CSP, COOP/CORP, Referrer-Policy.
- Automated certificate issuance and renewal via Let's Encrypt.
- **Result**: TLS negotiation occurs *only* between the client and the server,

structurally eliminating the possibility of man-in-the-middle attacks.

---

4. Mail Layer – DANE-Enabled Secure SMTP

- Stack: **Postfix + Dovecot**.
- Policies: SPF, DKIM, DMARC, MTA-STS, TLSRPT.
- **DANE (SMTP-TLSA)** minimizes reliance on third-party certificate authorities.
- Outbound structure:
  Main MX (KR:1) → Hub (SG:1) → Relay servers (DE:1, US:1).
- **Result**: All mail traffic is transparently routed and protected by the DNSSEC-based trust chain.

---

5. Application Layer – Process Isolation & Internal Security

- Each vHost runs as an independent **FastAPI/Uvicorn** instance.
- **systemd** hardening options (`NoNewPrivileges`, `RestrictNamespaces`) minimize privilege escalation.
- Internal communication is restricted to `127.0.0.1`; external access is completely blocked.
- **Result**: Service-level isolation and secure intra-service traffic are guaranteed.

---

6. Captcha Security Module

- The server operates its own FastAPI-based captcha service (**captcha.glitter.kr**).
- Generation and verification APIs run entirely within the internal loop,
  without any dependency on external APIs or cloud services.
- In DNSSEC/DANE-validated environments,
  all request/response transactions are encrypted within the trust chain,
  preventing MITM and spoofed verification.
- Each service (PHP or FastAPI) uses
  `glitter_captcha_client.php` and `glitter_captcha_guard.php` for direct validation,
  blocking on failed verification.
- Tokens use **HMAC-SHA256** signatures, difficult to forge, and expire automatically after 120 s.
- **Rate-limit** per client IP and **App-Key** authorization prevent bot abuse and misuse.
- Shares the same security headers (CSP, HSTS, COOP/CORP) as the main infrastructure for uniform policy.
- **Result**: A fully internal trust-based captcha system — no external dependency like reCAPTCHA.

---

7. Operations

- Unified logging with `journald`, `nginx`, and `systemd`.
- Automated DNSSEC signing and certificate renewal pipelines.
  (Applicable for domains whose TLD supports DNSSEC signing.)

Summary

This server implements a **proxy-free, fully autonomous security infrastructure**.
It achieves a high level of self-verified trust without relying on commercial DNS or CDN systems.

 No Proxy / No External WAF / Full Self-Verification
 Full DNSSEC + DANE + MTA-STS Trust Chain
 Self-Managed, Self-Verified Infrastructure

> The essence of security lies in **direct control without delegation**.
> This server embodies that principle.