

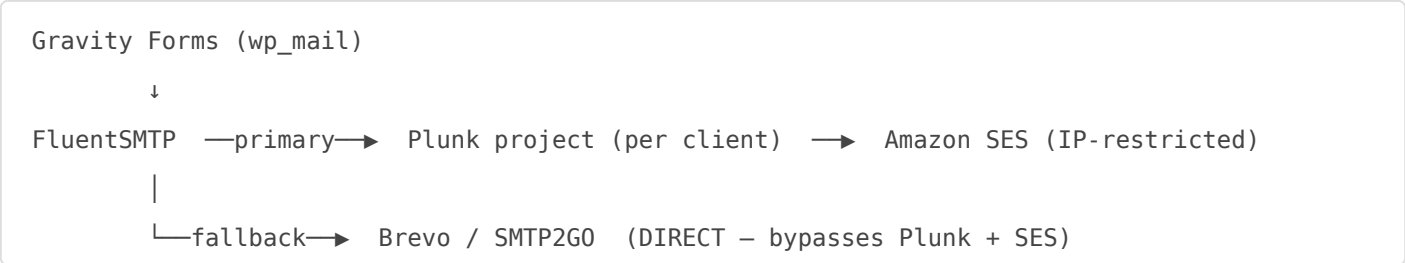
WebMarketers Client Email Protocol

Purpose: Isolate client sites from Amazon SES so one compromised site can't tank the whole account's reputation — and so we can swap providers without touching every site.

The Problem

Client mailboxes/sites get compromised → spam goes out through SES → SES flags the account for bad reputation → we're forced to reconfigure email for *all* 150+ sites at once. This protocol contains the blast radius and gives us fast rotation + fallback.

The Stack



Layer	Role
FluentSMTP	WordPress plugin. Intercepts all <code>wp_mail()</code> , handles routing, fallback, and per-site logging. Free. Replaces PostSMTP.
Plunk	Central relay over SES. One project per client (multiple domains per project). Gives per-client isolation, credential rotation, and a kill switch. Exposes standard SMTP (465/587).
Amazon SES	Actual delivery. Credentials IP-restricted to our servers via IAM <code>aws:SourceIp</code> .
Brevo / SMTP2GO	Fallback provider. Free tier, sits idle until needed. Connected directly , not through Plunk.

Key Decisions

- **Fallback goes direct, not through Plunk.** If Plunk or SES is the failure point, the site still sends. Routing fallback through Plunk would take out both paths at once.
- **Form responses stay native.** Gravity Forms notifications are `wp_mail()`, so they already flow through Plunk over SMTP automatically. No separate API integration needed.
- **Transactional ≠ marketing.** Form receipts (admin notification + visitor auto-response) are transactional. Only promote a submitter into a Plunk contact/automation on sites that actually run nurture campaigns — as a separate, consented marketing path.

Detection & Alerting

Two distinct signals — we need **both**:

- **Failure notification** (site-detected) → catches *outages* (SES down/banned). Triggers the fallback. ☐ already planned.
- **Volume/anomaly alerting** → catches the real reputation-killer: a hacked site sending spam *successfully* (returns 250 OK, looks normal). Watch Plunk per-project send spikes and/or SES CloudWatch alarms on **send rate + complaint rate**. ⚠ must add.

💡 Reminder: IP whitelisting stops *leaked-credential* abuse from outside. It does **not** stop a hacked site sending through its own legit relay — that's what the anomaly alerting is for. Prevention still lives at the source (patching, WAF, form CAPTCHA/rate-limiting).

Per-Client Setup Checklist

1. Create a Plunk **project** for the client; add their domain(s) with DKIM/SPF.
2. Point the project's upstream at the shared **IP-restricted SES** credentials.
3. On each client site, install **FluentSMTP**:
 - **Primary connection** → the client's Plunk SMTP credentials.
 - **Fallback connection** → Brevo or SMTP2GO (direct).
 - Enable **email logging**.
4. Confirm Gravity Forms notifications send and appear in the FluentSMTP log.
5. Add the site/project to **anomaly alerting** (send-rate + complaint-rate).

Blast-Radius (optional, recommended)

Split clients across **separate SES sub-accounts by risk tier** and/or **configuration sets per client**. One compromised site then degrades a segment, not all 150.

Revision #2

Created 2026-08-07 13:15:49 UTC by avelica.ws@gmail.com

Updated 2026-08-07 13:16:49 UTC by avelica.ws@gmail.com