SELF-HOSTED EMAIL INFRASTRUCTURE

Mail Transport • Authentication • Deliverability • Reputation Controls

PROJECT OUTCOME **Designed, built, hardened, and validated a working self-hosted email platform on Ubuntu, with authenticated submission, mailbox services, TLS, SPF/DKIM/DMARC alignment, bounce-domain separation, spam/reputation controls, and inbox-deliverability testing.**

What I engineered

MAIL TRANSPORT & SUBMISSION

Postfix configured for SMTP delivery and authenticated client submission on TCP 587 using STARTTLS/SASL, with relay restrictions and queue controls.

MAILBOX & AUTHENTICATION

Dovecot-backed virtual mailbox structure using Maildir, hashed credentials, LMTP/local delivery paths, IMAP/POP3 support, and Postfix SASL integration.

SENDER AUTHENTICATION

SPF, 2048-bit DKIM signing through OpenDKIM, DMARC enforcement/reporting, aligned hostname/PTR strategy, and DNS-only mail records in Cloudflare.

DELIVERABILITY & ABUSE CONTROLS

Rspamd scanning, Postscreen/DNSBL defenses, connection/message rate limits, Microsoft-specific transport throttling, reputation checks, warm-up tracking, and unsubscribe headers.

ENCRYPTION & CERTIFICATES

Let's Encrypt certificates for the mail FQDN, TLS 1.2+ policy for Dovecot and hardened SMTP TLS settings, plus automated renewal/reload workflow.

OPERATIONS & VALIDATION

Systemd persistence, log/queue inspection, SMTP AUTH testing with OpenSSL, DKIM/SPF/DMARC DNS verification, Swaks delivery tests, and Gmail/mail-tester inbox checks.

BOUNCE-DOMAIN SEPARATION

Dedicated bounce subdomain and mailbox path to isolate return-path/bounce handling from the primary sending identity and simplify deliverability operations.

AUTOMATION & MONITORING

Shell-based DNSBL/reputation monitoring and IP warm-up state tracking via cron, with service health and blacklist checks available for ongoing operations.

Architecture snapshot

Sending application / mail client → SMTP submission :587 + STARTTLS/SASL → **Postfix** → OpenDKIM + Rspamd → Internet MX delivery

Inbound/local path → Postfix/LMTP → Dovecot Maildir → IMAP/POP3 over TLS

Key engineering decisions

- **Separate submission from server-to-server SMTP:** authenticated users submit on 587 with encrypted transport; external delivery remains on SMTP transport semantics.
- **Treat DNS identity as part of the mail system:** A/MX, SPF, DKIM, DMARC and PTR/rDNS were configured as an integrated deliverability chain rather than isolated records.
- **Protect reputation proactively:** connection/message limits, DNSBL screening, spam scanning, gradual warm-up tracking and provider-specific throttling were added to reduce abusive or bursty behavior.
- **Separate bounce handling from the primary sending identity:** a dedicated bounce subdomain and mailbox path were used to keep operational return traffic distinct.
- **Validate from protocol to inbox:** verification covered listening sockets, SMTP AUTH, TLS negotiation, DKIM keys, DNS records, Postfix queues/logs and external inbox placement.

Technical evidence at a glance

Layer	Implementation	Evidence / validation
OS / host	Ubuntu 24.04; mail FQDN; IPv4-focused mail stack	Service enablement, socket checks, systemd status
MTA	Postfix; :25 delivery; :587 submission; queue/backoff/rate controls	mailq, journal/mail.log, SMTP transaction tests
Mailbox	Dovecot; virtual vmail UID/GID; Maildir; LMTP; IMAP/POP3	doveadm auth test, mailbox directory ownership
Auth / TLS	SASL via Dovecot; Let's Encrypt certs; TLS 1.2+	openssl s_client -starttls smtp, certificate reload
DKIM	OpenDKIM; 2048-bit RSA; selector-based signing	opendkim-testkey + DNS TXT validation
SPF / DMARC	SPF policy record + DMARC quarantine/reporting	dig TXT checks; recipient "Show original" validation
Spam / abuse	Rspamd, Postscreen, DNSBL checks, relay restrictions	Rspamd listener/status; blacklist checks; logs
Deliverability	PTR alignment, bounce separation, list-unsubscribe, warm-up/reputation scripts	Gmail inbox tests, Swaks, mail-tester workflow

Security & operational hardening

- SMTP relay restricted to trusted networks or authenticated users; unauthenticated relay rejected.
- Plaintext authentication disabled outside TLS; submission configured to require encrypted authentication.
- Private DKIM keys stored server-side with restricted ownership/permissions; public selectors published in DNS.
- Inbound exposure reduced with Postscreen checks and DNSBL scoring; Rspamd integrated as a Postfix milter.
- Rate limits and queue retry/backoff settings applied to reduce abusive bursts and control delivery behavior.
- Core mail services configured to survive reboot using systemd enablement; certificate renewal reloads Postfix/Dovecot.
- Credential material shown during implementation has since been rotated; this portfolio record intentionally omits secrets and live identifiers.

Impact

END-TO-END

Owned the stack from DNS and transport through authentication, filtering, mailbox delivery and validation.

PRODUCTION-MINDED

Designed for service persistence, observability, abuse resistance, TLS, reputation hygiene and controlled sending.

PROTOCOL-LEVEL

Worked directly with SMTP, SASL, TLS, DNS, DKIM, SPF, DMARC, LMTP, IMAP/POP3 and MTA queue behavior.