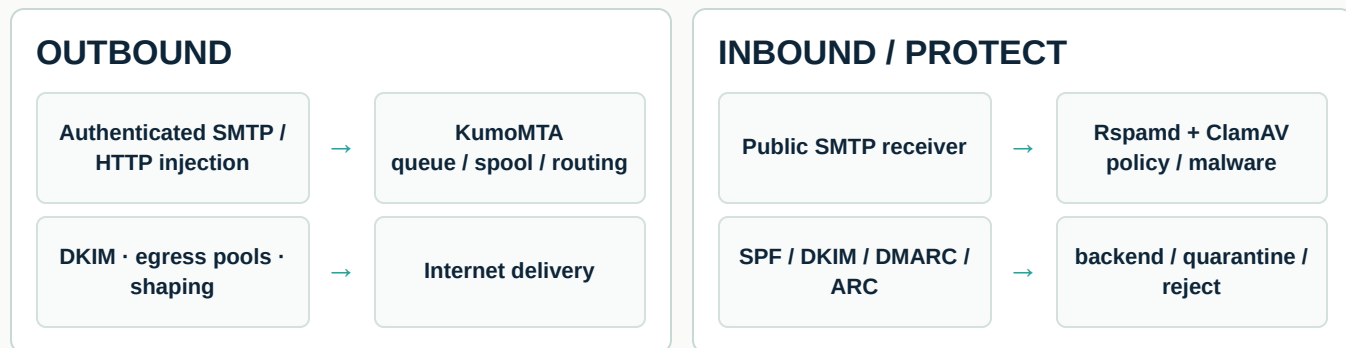
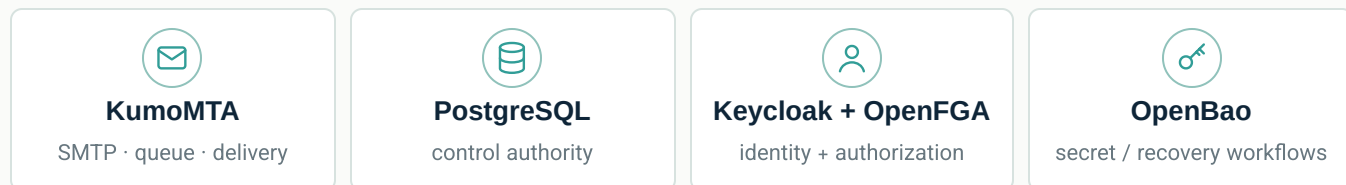


4SO Mail Gateway

Self-contained Mail Server & Gateway Platform

پلتفرم Linux/VM-first برای ارسال حجیم، دریافت محافظت‌شده، Queue/Spool، DKIM، routing، هویت و عملیات پایدار؛ با جداسازی روشن Mail Data Plane از Control Plane.



Mail Data Plane = Linux/VM workload

runtime به‌عنوان HA و DKIM hot path، KumoMTA، SMTP، queue/spool، sending IP و dependency وابسته نیستند.



Bounded Control Plane

Rust Control API، PostgreSQL، Keycloak، OpenFGA و OpenBao مسیرهای identity، authorization و durable lifecycle را مالک‌اند.

Node-local spool

Spool روی Mail Node محلی است؛ shared-spool خیالی به‌عنوان معماری محصول ادعا نمی‌شود.



PRODUCT BOUNDARY

چهار لایه؛ یک چرخهٔ عمر محصولی

SMTP runtime، inbound protection، control/identity و observability هرکدام owner روشن دارند؛ UI یا MCP جای authority های اصلی را نمی‌گیرند.

POLICY

Inbound Protection

Rspamd
mail security and policy processing



ClamAV
malware scanning



Authentication signals
SPF · DKIM · IPREV · DMARC · ARC



LINUX / VM

Mail Data Plane

KumoMTA
submission · public SMTP · delivery · queue/spool



HAProxy
stable internal transport / selected HA endpoints



Unbound + Valkey
resolver path + shared runtime authority where required



EVIDENCE

Observability & Operations

Prometheus
metrics and runtime evidence



Grafana
operational visibility



Product workflows
mail · queue · TLS · routing · deliverability state



AUTHORITY

Control & Identity

Rust Control API + PostgreSQL
durable product authority



Keycloak + OpenFGA
identity + product authorization



OpenBao
secret material / recovery workflows



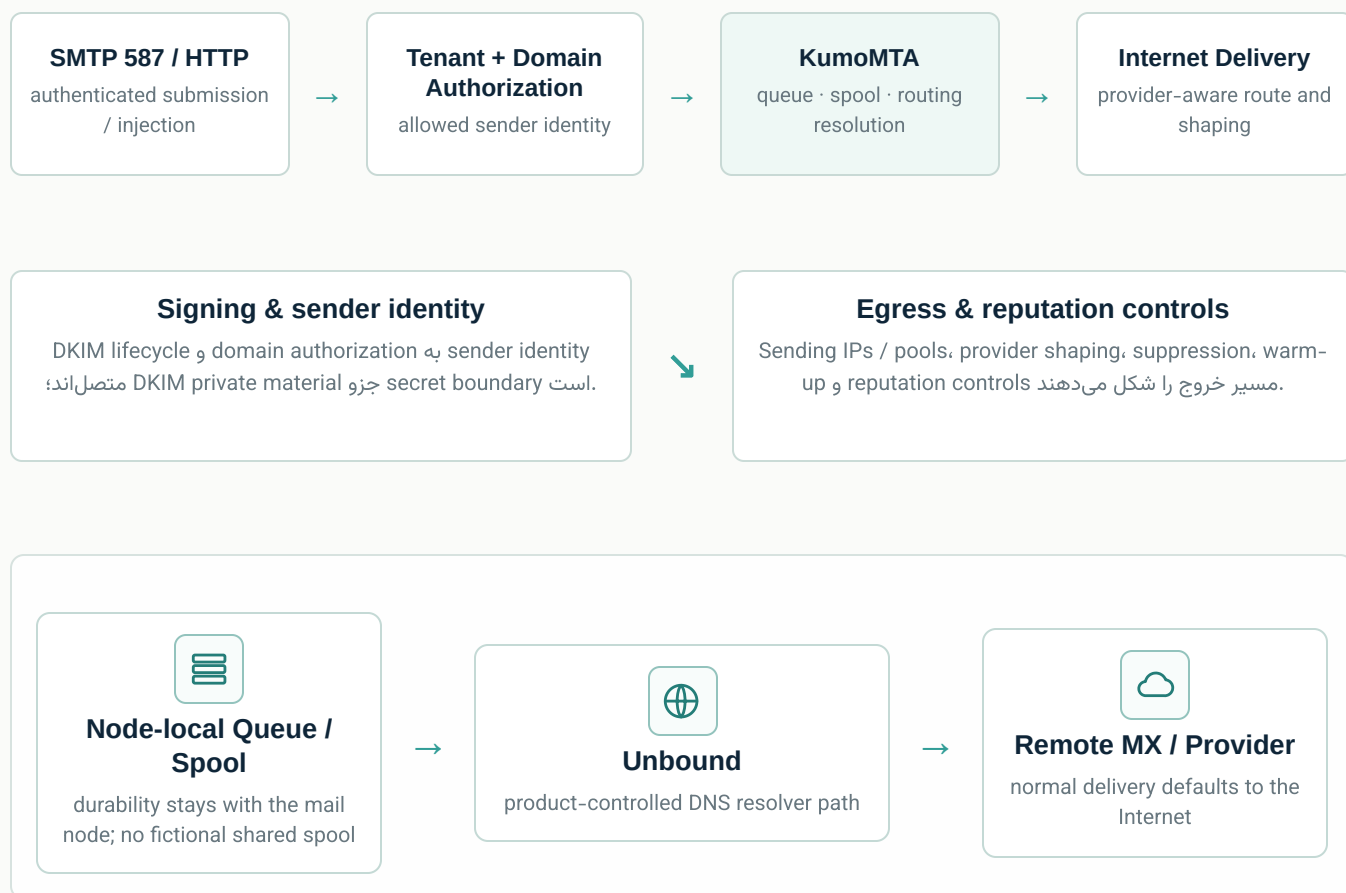
اصل مالکیت: PostgreSQL authority کنترل‌پلین را نگه می‌دارد؛ KumoMTA مالک mail hot path و node-local queue/spool است.



OUTBOUND PATH

از ارسال تا تحویل اینترنتی

Outbound path روی KumoMTA متمرکز است؛ domain authorization، DKIM، egress pool shaping قبل از delivery معنا پیدا می‌کنند، در حالی که spool روی همان Mail Node می‌ماند.



Stable transport ≠ shared spool

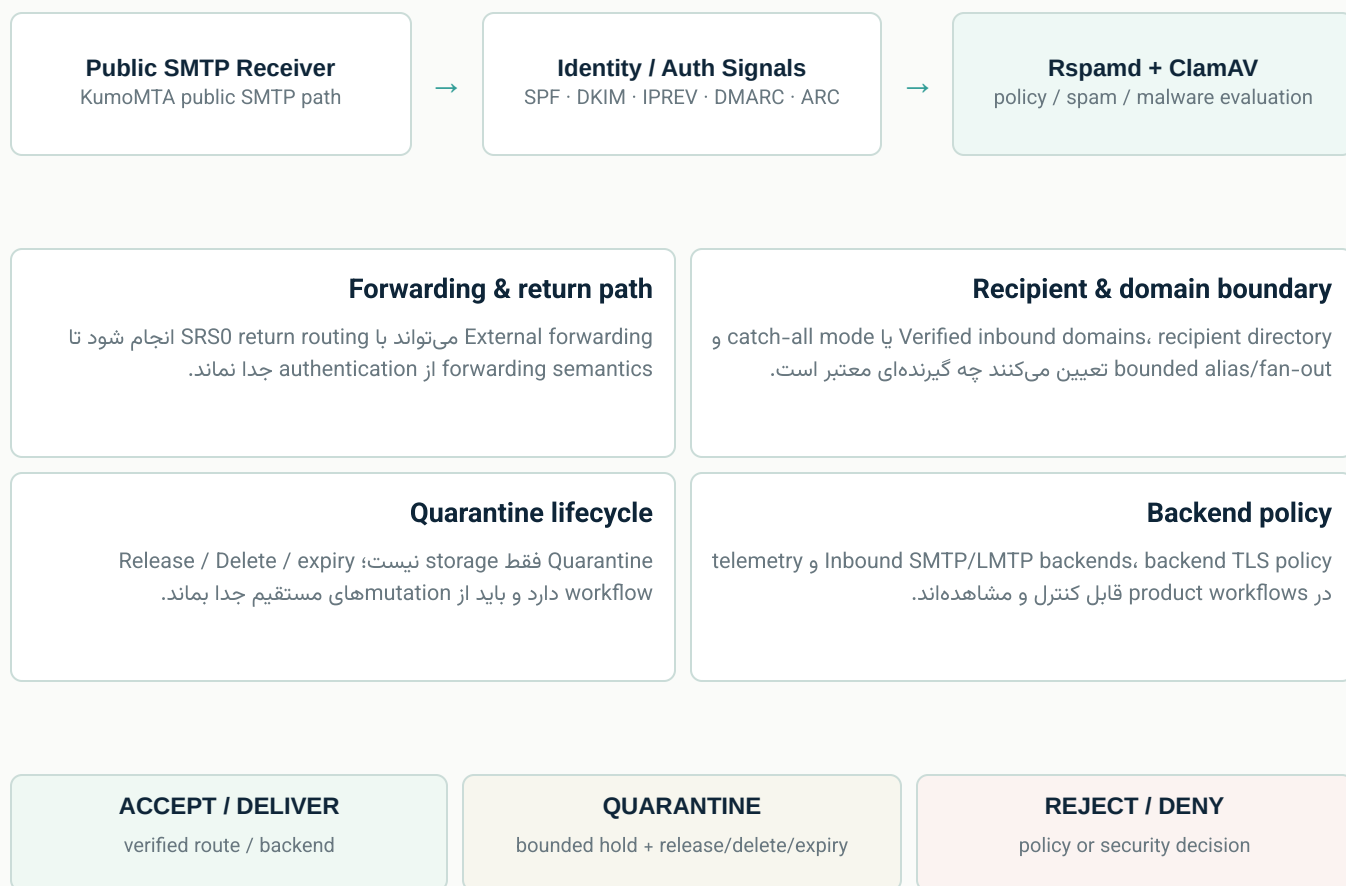
HAProxy برای selected stable transport / HA endpoints استفاده می‌شود، اما spool همچنان node-local است و از آن یک storage fabric مشترک فرض نمی‌شود.



INBOUND PROTECTION

دریافت، سیاست، بدافزار و تصمیم تحویل

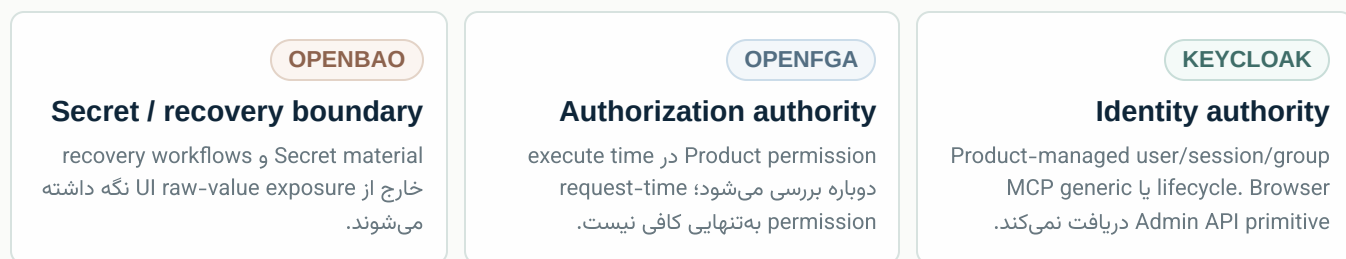
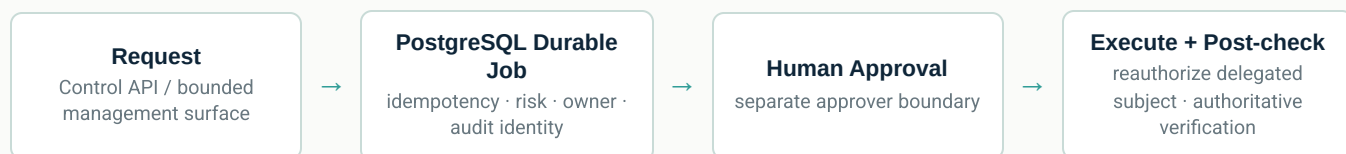
SMTP reception، authentication signals، علاوه بر Inbound path
quarantine و anti-spam، anti-malware، backend policy
lifecycle را در یک مسیر قابل مشاهده نگه می‌دارد.



HIGH-RISK IAM

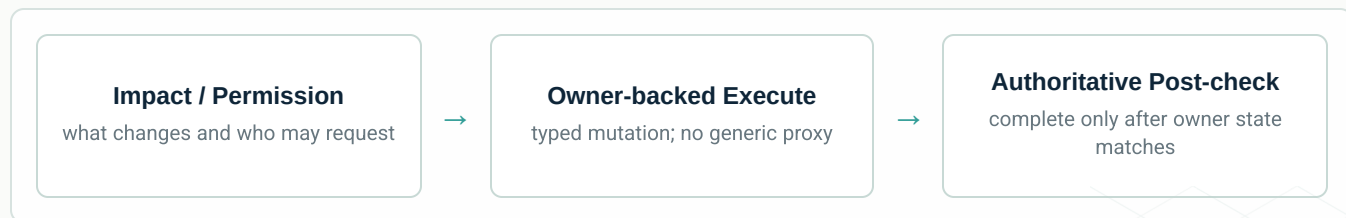
تغییر حساس بدون زنجیره تأیید میان‌بر نمی‌خورد

Identity و access mutation های حساس به durable PostgreSQL
 approval، job، انسانی مستقل، reauthorization هنگام اجرا و
 authoritative post-check متصل‌اند.



Management MCP self-approval ندارد

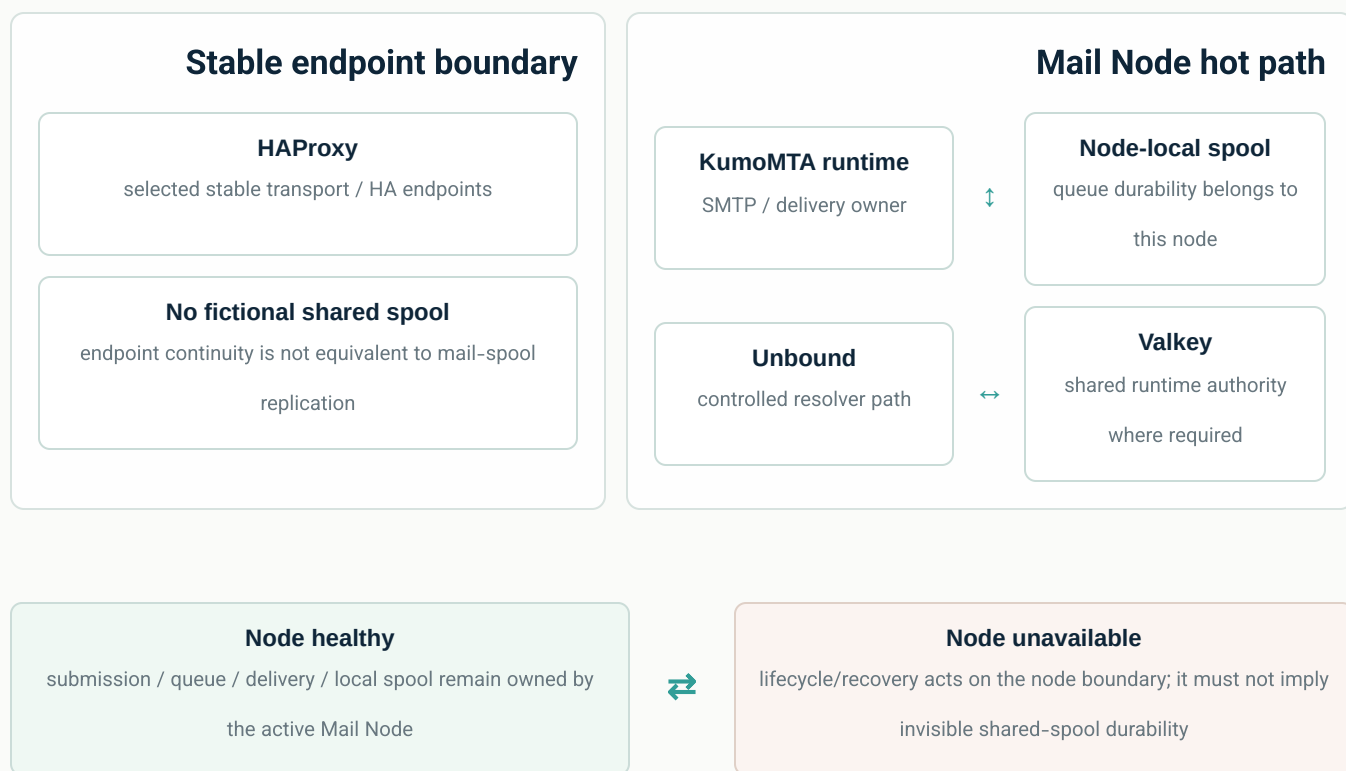
MCP می‌تواند bounded request یا read را در authority خودش انجام دهد، اما generic approve/execute bypass برای IAM mutation وجود ندارد.



QUEUE, SPOOL & FAILURE BOUNDARY

Spool محلی است؛ تداوم باید همین مرز را حفظ کند

Mail Node failure را نمی‌توان با فرض shared storage پنهان کرد.
معماری spool، product-owned، node-local را نگه می‌دارد و HA endpoint را از data durability جدا می‌کند.



Kubernetes is not Mail Data Plane runtime authority

Kubernetes ممکن است در بخش‌های دیگر delivery infrastructure استفاده شود، اما KumoMTA / SMTP / spool / HA و sending IP / DKIM hot path همچنان Linux/VM-first هستند.



OBSERVABILITY & CONTROL LOOP

وضعیت Mail باید به عملیات قابل اقدام تبدیل شود

durable و owner APIs می‌دهند؛ Grafana visibility و Prometheus Monitoring را می‌بندند. authority جای runtime authority را نمی‌گیرد.

Operational authority

Rust Control API

typed product operations

PostgreSQL

persistent control authority and durable jobs

Owner post-check

operation closes only after authoritative state verification

Audit / evidence

request, approval, execution and result stay attributable

Bundled observability

Mail / queue state

queue pressure, message activity, delivery outcomes

TLS / routing / provider state

transport and route visibility

Deliverability / reputation

suppression, feedback and provider-facing posture

Runtime health

component and evidence probes

Prometheus
runtime metrics



Grafana / Operator workflows
human visibility



Typed durable operation
owner execution + post-check

DATA PLANE SIGNALS

queue / spool / route

+

TLS / provider /
delivery

CONTROL PLANE SIGNALS

IAM / job / audit

+

fleet / lifecycle /
recovery



ACTION & OPERATIONS CATALOG

چرخه عمر Mail از مسیر پیام تا مسیر هویت

Receiver / Protect IN

public SMTP verified domains SPF/DKIM/DMARC

Rspamd ClamAV backend TLS quarantine

Policy و malware decisions به recipient/backend/quarantine workflow متصل اند.

Sender / Outbound OUT

SMTP submission HTTP injection domain auth

DKIM egress pools routing shaping

suppression

KumoMTA owner مسیر queue/spool و Internet delivery باقی می ماند.

Runtime & Operations OPS

queue/history Unbound Valkey HAProxy

Prometheus Grafana recovery

runtime owner و Visibility، durable operation boundary جدا دارند.

Identity & Sensitive Mutations IAM

Keycloak OpenFGA OpenBao durable job

human approval reauthorize post-check

هیچ generic self-approve / execute bypass برای management agent تعریف نمی شود.

معماری در یک جمله

4SO Mail Gateway یک Mail Data Plane مستقل روی Linux/VM و یک Control Plane محصولی برای lifecycle، authorization، identity و recovery است؛ نه wrapper یک hosting panel و نه یک Kubernetes-native mail runtime.

Rspamd + ClamAV inbound protection 02KumoMTA owns SMTP + queue/spool 01PostgreSQL durable control authority 04Unbound + Valkey runtime services 03Prometheus + Grafana observability 06Keycloak + OpenFGA + OpenBao 05

Own the mail path. Bound every sensitive mutation. Observe the runtime without confusing visibility with authority.

Operations و Outbound، Inbound، Identity در یک product boundary self-contained به هم متصل می شوند.

