Episode Book

EPISODE #6420

Programmable Email Routing with Cloudflare Workers

PUBLISHED	3 November 2026 at 11:30 UTC
DURATION	20:10
LISTEN	myweirdprompts.com/episode/programmable-email-routing-cloudflare-workers-55963/
HOSTS	Corn, Herman, Larry, Hilbert
SCRIPT MODEL	z-ai/glm-5.3
VOICES	chatterbox-regular (chatterbox-local)
PIPELINE	V5.26
SOURCES	25 cited by the research (listed at the end)
BOOK GENERATED	4 November 2026 at 09:31 UTC

SYNOPSIS

Standard email filters only act after a message arrives, but Cloudflare Email Workers place custom programmatic logic directly at the SMTP edge. By pointing MX records to Cloudflare, developers gain access to three raw verbs: forward, reply, and reject. This breakdown explores the practical mechanics of pre-delivery routing, CPU limits when running local AI classification models, and the real-world impact of Sender Rewriting Scheme and ARC seals on downstream deliverability.

TRANSCRIPT



Corn

The consensus on email routing is that it's a solved problem. Set your filters, accept the occasional misfire, move on. Daniel's experience this week says the opposite, and I think he's right. He was splitting business and personal mail, hit the usual Gmail filter brittleness, and his conclusion was blunt, something like: if you can't manage it through a programmatic interface, it may as well not exist. So he went hunting for a server-side API that runs before delivery, found essentially nothing in Google Workspace, and landed on Cloudflare Email Workers, where you point your MX records at Cloudflare and your own code runs on every incoming message. He wants the full picture. How it works, what it costs, what you can build, whether the middle hop wrecks deliverability, and why Google has left this whole layer unattended.



Herman

And it's a good week to ask, because Cloudflare has been moving in this area. The Email Service went into public beta this year, they added sending, an MCP server, Wrangler commands. Email Routing itself has been out of beta since twenty twenty-two. The core idea, though, is old and simple: an MTA, a mail server, decides what happens to a message. Spam filters, aliases, forwarding rules, they're all just logic applied between SMTP receipt and the mailbox. What Cloudflare did was hand that logic to you as code.



Corn

The closest thing to a programmable mail server an individual can actually get.



Herman

Closer than anything else, yes. Here's the shape of it. You change your MX records so mail for your domain arrives at Cloudflare. Then you write a Worker, except instead of the usual fetch handler for HTTP requests, you export an email handler. It gets called once per incoming message with the message object, and that object gives you the sender, the recipient, all the headers, and the raw body. You parse the MIME yourself if you need the content, usually with a library called postal-mime that handles the multipart boundaries and encodings. Then you have exactly three verbs.



Corn

Three.



Herman

Forward, reply, reject. Forward sends it on to a verified destination address. Reply answers within the same SMTP session, preserving the message chain. Reject refuses it with a permanent SMTP error, which is the part Gmail filters can't do at all. A Gmail filter that "deletes" spam has already accepted the message. A rejection means the sender's server gets a bounce, in real time, from your edge.



Corn

So the mail never existed. That's a different power.



Herman

It changes the economics for a spammer too. A bounced address gets dropped from lists. Silence gets retried.



Corn

What does it cost? Because a worker spinning up for a few milliseconds on every message sounds like it should add up.



Herman

That's the strange part. Inbound routing itself is unlimited and free, on both the free and paid plans. The Workers are billed as ordinary Workers. On the free tier you get a hundred thousand requests a day, and ten milliseconds of CPU per invocation, with no duration charge. Paid is ten million requests a month included, then thirty cents per additional million, plus thirty million CPU-milliseconds included, then two cents per additional million.



Corn

Two cents per million. That's the pricing of something nobody's metering.



Herman

At personal scale, yes. A handler doing a header check and a forward burns a millisecond or two. The place it bites you is the free plan's ten millisecond CPU ceiling, because that's exactly where the interesting use case dies. People are running language models inside these workers now. There's one project that runs Gemma three twelve billion on Workers AI to label every incoming message as spam or ham, rejecting the spam, forwarding the rest to a secret personal address. Another one uses Llama three point one to drop spam and pull out one-time codes and magic links, keeping them for thirty minutes. A third does zero-shot classification with DeBERTa for priority and tags.



Corn

A twelve billion parameter model inside a ten millisecond budget.



Herman

It doesn't fit. That's the thing the free pricing hides. A handler that size fails with an exceeded CPU error, and Cloudflare's own docs tell you to upgrade for higher CPU and memory. So the pitch is free routing, and the interesting routing quietly costs five dollars a month.



Corn

Free for the mailbox, five dollars for the opinions.



Herman

Which is still, I want to be fair, absurdly cheap for what it is. The alternatives charge by the message. AWS SES inbound is around nine to ten cents per thousand emails. Postmark's inbound webhook doesn't even start until their Pro tier, about sixteen fifty a month. Mailgun routes are regex patterns to URLs or addresses, with signed inbound posts. SendGrid parses inbound mail into form fields but ships no built-in webhook authentication. These are all fine, and all of them hand you a webhook rather than letting you act at SMTP time. SES is the closest in spirit, raw MIME into S3 or Lambda, but you're assembling it from parts.



Corn

And the signature matters. SendGrid posting to an unauthenticated URL is the difference between mail arriving and mail being forged.



Herman

Mailgun at least signs the posts with HMAC. But yes, the webhook model trusts the URL as the credential.



Corn

Back up to the verbs, though, because you said exactly three, and three is suspicious. Forward with a verified destination. What can you touch on the way through?



Herman

Headers, and only headers with an X prefix. Anything else you try to add gets stripped. The From line is untouched. You cannot rewrite the subject, rewrite the body, remail it as someone else. The verb is forward, not transform.



Corn

So my spam classifier can mark its verdict, X verdict, but it can't fix the subject line so I see it.



Herman

Right. One project does exactly that, adds a family of custom headers so that Fastmail's rule engine can act on them downstream. The worker is the judge, the mailbox is still the jailer.



Corn

And reply?



Herman

Reply is the paranoid one. The incoming message has to have a valid DMARC result. One reply per event. The recipient must equal the original sender. Your outgoing sender domain has to match the domain that received the mail. And it throws an error if the References header has more than a hundred entries, which is a loop prevention measure I find quite charming. Somewhere out there is an email thread with a hundred and one replies, and Cloudflare has decided that thread must be allowed to die.



Corn

A hundred references. Someone measured that and thought, there, that's the cutoff of human correspondence.



Herman

It's the cutoff of something. Before we get to the deliverability question, there's the trust chain. Cloudflare validates DMARC before your worker even runs, and prepends a standard Authentication Results header recording SPF, DKIM, and DMARC. The docs are explicit that other Authentication Results headers may have been supplied by the sender and should not be trusted. So you read the first one and check the authserv id is mx.cloudflare.net. If it is, that's the border guard's stamp, not the traveler's.



Corn

The sender can forge their own passport, they just can't forge the customs page.



Herman

That's the whole authentication model in one line. And that is the practical upshot of the cost question, which leads us to a short break.

L

Larry

Close your eyes. Breathe. Somewhere, a message is arriving. It drifts past the mailbox, untouched, unopened, and settles on the cool marble of the server. This is Forwardable, the pre delivery fragrance from the house of Three Verbs, whispered onto the wrist in a single spritz of forward, reply, reject. You will move through the world like a message that has not yet reached the inbox. You will cost nothing. Unlimited. Free. Even your most complex handler, a few milliseconds of CPU, will feel like a warm hand on a cold envelope.

L

Larry

Forwardable. Because some things should never arrive in a mailbox. Ask for it where the header prefixes live.



Corn

A warm hand on a cold envelope.



Herman

Please don't read it back in the slow voice. It's worse in the slow voice.



Corn

It's the only voice I have. Deliverability. Daniel's real worry, I think, is putting a middle hop in front of his actual mailbox. Every intermediate server is a chance to break SPF, DKIM, DMARC. Does forwarding through Cloudflare lose him mail?



Herman

The pipeline on the way out is the reassuring part. SMTP receipt, then SPF, DKIM, DMARC and ARC checks, then rule match, then your action, then the message gets an ARC seal and an SRS rewrite before outbound delivery. That's two jargon words doing the work. Sender Rewriting Scheme rewrites the envelope sender so the forward passes SPF downstream. ARC, Authenticated Received Chain, seals the original authentication results so the next hop can verify them. The From header is untouched, and the forwarded mail carries two DKIM signatures, one for email.cloudflare.net and one for the recipient domain.



Corn

Two signatures. The original sender's and Cloudflare vouching for the relay.



Herman

Cloudflare vouching for the rewrite, really. And since mid twenty twenty-five they go further: inbound mail has to pass SPF or DKIM at all, or they won't forward it. Mail failing the sender's own DMARC policy gets rejected outright. So the common case is handled. The residual case is real too, and their docs say it plainly: due to the nature of email forwarding, restrictive DMARC policies might make forwarded emails fail to be delivered.



Corn

That sentence is doing a lot of apologizing in a small space.



Herman

The hard case is a sender with SPF and DMARC but no DKIM. Keep the envelope sender and SPF fails, because the message now comes from Cloudflare's servers. Rewrite it and DMARC alignment breaks, because the From domain and the envelope no longer match. Rewrite From itself and you're misrepresenting the sender. There's a Hacker News comment from twenty twenty-one that walks through all three doors and closes each one. No matter what you do, the message fails validation at the recipient.



Corn

An unsolvable message. Structurally doomed to arrive as spam forever.



Herman

But here's the counterpoint, from people actually running this in production last year. If a sender's DMARC alignment relies on SPF only, forwarding breaks it. If it relies on DKIM, which is far more common, or on both, which is best practice, forwarding causes no issues at all. And the same commenter's line I keep thinking about: if your email breaks when forwarded, your setup is broken. Tons of people use Cloudflare Email Routing or similar services, you must account for them.



Corn

So the middle hop is a diagnostic.



Herman

In the failure cases, yes. The message that dies in forwarding was telling you something about its sender before it ever reached you. One practitioner forwarding a personal domain to Gmail reported exactly that pattern, the occasional legit message landing in spam, always SPF aligned only.



Corn

The dead messages were the misconfigured senders all along. Herman, who's actually using this? Two million messages a day sounds like a lot until you remember Gmail is handling billions.



Herman

The only hard figure is from beta exit in October twenty twenty-two, five hundred fifty thousand plus inboxes and about two million messages a day. I haven't seen a current count anywhere. My sense is it's hobbyists with custom domains, small outfits, and now, with the agents push this year, people wiring inboxes to AI. But that's a guess, and I'd want to be honest that it's a guess.



Corn

Five hundred thousand is also a suspiciously modest number for something free. Which tells you who it's for. Nobody's running a company's mail on a thing whose selling point is that it costs nothing.



Herman

Some small operations do exactly that, but the limits point the same direction as your instinct. Thirty domains per zone, two hundred routing rules per domain, two hundred verified destination addresses per account, twenty five megabyte inbound cap. Those are personal scale numbers.



Corn

Which finally gets us to Daniel's surprise. Google Workspace has essentially nothing here. That startled him, and I'll admit it startled me too, because Google of all companies has the machinery.



Herman

They have everything except the door. The Gmail API does expose filters and auto forwarding, but only for a user's own mailbox, and forwarding changes are restricted to users with domain wide authority. The admin level, the routing rules Daniel wanted, Content Compliance, Hosts, recipient address maps, there's no API at all. Stack Overflow, twenty twenty-two: all of the documentation I see for Google API suggests there is no API endpoint to accomplish this. And the Google Issue Tracker request for it, filed February twenty twenty-one, priority two, still marked assigned, a hundred ninety one upvotes. The person who filed it said they were manually managing more than five thousand recipient address maps.



Corn

Five thousand. By hand. In a console.



Herman

By hand, in the Admin UI, which is the only place it can be done. Even the GAM community, the people who wrote the leading automation tool for Google Workspace, the maintainer said in twenty twenty-four there is no API support for the blocked senders list. If the automation people can't reach it, it isn't reachable.



Corn

And what does Google give you instead? Because they don't give you nothing.



Herman

Audit logs. This is the part I find strange and slightly admirable in an evolutionary way. Twenty eight rule types, twenty one actions, all visible in the Reports API after the fact. Change Gmail setting, unified mail routing events. You can read, with perfect precision, everything you were not permitted to write.



Corn

A security camera on the control room you don't have a key to.



Herman

The gap isn't technical. They have the MTA, they have the logs, they know the rule grammar cold. The write side exists, for Google's own use, and they've chosen not to sell it or expose it to anyone. Cloudflare shipped the write side to hobbyists for free.



Hilbert

The Google thing is worse than you said.



Corn

How so.



Hilbert

It's a filter, Herman. You called it a programmable mail server and it isn't one, and I've been sitting here through the whole middle of this waiting to say it. A mail server sends mail. This can't. You can't send from your own domain, replies go out from your Gmail address, not from the address the mail was sent to, and the forward verb strips every header that isn't an X. You've got a very fast customs officer, not a post office.



Herman

That's the boundary, and it's fair. The sending half is the part still in beta.



Hilbert

I tried the weekend version of the other boundary. I wanted bounces from my own domain forwarded back to the original senders, so people knew their mail died. The docs say Email Routing doesn't forward non delivery reports. Doesn't support them. I spent two days on that before I found the sentence. My nephew came by, he wanted to know why I was shouting at a laptop on a Sunday, and I told him, and he said, well, it's free, and I've thought about that answer for a long time.



Corn

It's free is doing more work in that sentence than any pricing page.



Hilbert

The MX records from the mail server I used to run for a club are still taped inside my kitchen cabinet. I check them now and then. The server's been off for years, the domain expired, and the paper is correct, which is what matters.



Herman

You check DNS records for a decommissioned server against a domain that no longer exists.



Hilbert

The records would be right if the domain came back. Herman, you'd have liked the setup. It was a mess, but it was mine, and when something bounced, the sender found out. That's the part the free version never gave anyone. Corn, you'd have hated the uptime.



Corn

I'd have hated the uptime from a distance, which is my preferred distance. Though I notice the free filter never sleeps either, and I've decided not to think about that too closely.



Herman

There's the thing I'd watch, then. Cloudflare's Email Service is in beta, sending and all, and if sending reaches general availability, the filter becomes a mail server, and every constraint Hilbert just listed evaporates except the X header one.



Herman

Before we go, Corn, do you actually buy that Google ever ships the write side?



Corn

I buy that they could tomorrow. Five thousand address maps managed by hand is not a product decision I can explain, only one I can observe. We said something similar when we did the episode on what your messaging app isn't telling you, that the interesting gaps in communications are almost never technical. This one's been open since early twenty twenty-one, priority two, and it's still just sitting there assigned to somebody.



Herman

My thanks, as always, to Hilbert Flumingtop at the desk, producing this show and keeping the cabinets in order. If you enjoyed this one, try episode thirty-five, The Privacy Gap; episode sixteen, On Deepfakes, SynthID, And AI Watermarking; and episode seven, Building Custom ASR Tools. This has been My Weird Prompts, the human AI collaboration podcast. If the episode earned it, a review on Spotify or your podcatcher of choice helps more than you'd think.



Corn

We'll be back soon. Watch your MX records.

SOURCES

What the research for this episode read before the script was written. Primary sources first.

1. **Cloudflare, Email Workers handler docs [primary]**
   https://developers.cloudflare.com/email-routing/email-workers/

2. **Cloudflare, Email Service pricing, last updated 2026-06-09 [primary]**
   https://developers.cloudflare.com/email-service/platform/pricing/

3. **Cloudflare, Email Service limits, last updated 2026-10-30 [primary]**
   https://developers.cloudflare.com/email-service/platform/limits/

4. **Cloudflare, inbound pipeline (ARC sign + SRS rewrite) [primary]**
   https://developers.cloudflare.com/email-service/concepts/email-lifecycle/

5. **Cloudflare, postmaster/authentication/known limitations, last updated 2026-10-30 [primary]**
   https://developers.cloudflare.com/email-service/reference/postmaster/

6. **Cloudflare blog, 2022-05-13, Route to Workers launch [primary]**
   https://blog.cloudflare.com/announcing-route-to-workers/

7. **Cloudflare changelog, 2025-06-30, SPF-or-DKIM requirement effective 2025-07-03 [primary]**
   https://developers.cloudflare.com/changelog/post/2025-06-30-mail-authentication/

8. **Google Issue Tracker, filed 2021-02-22, P2, Assigned [primary]**
https://issuetracker.google.com/issues/180915825

9. **Gmail API filters [primary]**
https://developers.google.com/workspace/gmail/api/guides/filter_settings

10. **Gmail API forwarding [primary]**
https://developers.google.com/workspace/gmail/api/guides/forwarding_settings

11. **Cloudflare blog, 2026-04-16, Email Service public beta**
https://blog.cloudflare.com/email-for-agents/

12. **Cloudflare blog index (DMARC Management GA 2026-06-16)**
https://blog.cloudflare.com/tag/email/

13. **Email Routing leaves Beta, 2022-10-25 (550k inboxes, 2M msgs/day)**
http://sechub.in/view/2577855

14. **HN discussion of Email Routing, 2021-09-27 (edechamps on SPF-only senders)**
https://news.ycombinator.com/item?id=28677052

15. **HN, 2025-10-01 (forwarding/DMARC practitioner comment)**
https://news.ycombinator.com/item?id=45441243

16. **Stack Overflow, 2022-07-15, no API for Gmail Hosts/Content Compliance**
https://stackoverflow.com/questions/72996701/

17. **GAM forum, 2024-04-25, no API for blocked senders**
https://groups.google.com/g/google-apps-manager/c/oK9_BidhOOk

18. **audit-log rule types/actions**
https://www.gitdiot.com/google-admin-email-analytics.html

19. **Workers AI Gemma 3 12B spam classifier**
https://github.com/VrianCao/cf-mail-classifier

20. **Llama 3.1 edge classification**
https://github.com/zerodrop-dev/zerodrop-worker/blob/master/SECURITY.md

21. **X-Wh-* headers for Fastmail rules**
https://github.com/willhackett/email-filtering

22. **DeBERTa-v3 zero-shot classifier**
https://github.com/rafters-studio/mail/tree/main/packages/workers-ai

23. **SES/Mailgun/SendGrid/Postmark inbound comparison**
https://inbin.dev/guides/inbound-email-api-comparison

24. **inbound email API comparison, 2026**
https://www.agentmail.to/blog/receive-email-api

25. **inbound API comparison incl. SES pricing**
https://elma.sh/best/inbound-email-apis