ARF Agent Governance Proxy

One release rule across providers

A team adds a second coding agent for reviews. Both agents know the release process. Only one has an assignment that allows a write. The route into the provider is a practical place to ask who sent the request and what policy applies.

Define the boundary

Start with the client, the authenticated route and the destination. Agent Watchdog checks traffic on that route before forwarding it. Its policy verdict belongs to that request. If the model proposes a tool afterward, the tool's executor needs a decision for the operation it is about to perform.

This distinction matters in an incident review. A provider may have accepted a perfectly ordinary prompt before a worker tried to publish a private artifact. The provider call and the publication are two events with different audiences and different owners.

Change a permission without changing the model

In a recorded ARF command-broker run, a coding agent asked to commit. The broker refused, the repository stayed at one commit and the refusal entered the ledger. An explicit grant then permitted that tool. An operator could change the worker's permission and observe the result on the same model.

Use the same principle to exercise the proxy. Set up two configured providers behind governed routes. Submit the same scoped fixture on both. Inspect each proxy verdict, check which requests reached their provider, and keep the attempted tool effects in their own record.

Keep the evidence readable

The Watchdog capture path can digest original text before sealing selected material to named recipients. In the encryption test the matching identity recovered the original bytes and the digest still matched them. The operator can choose who reads a sensitive span while another reviewer checks the integrity of the record they received.

A rollout is ready for review when the team can name every governed route, identify the policy author, and show what happened on both a permitted and a denied request. The policy can then travel with the team when it changes vendors.

Tracing one request across providers

At this boundary	Record	Review question
Client to proxy	Authenticated route and requested destination	Which client sent the request?
Policy to proxy	Verdict returned before forwarding	Was this request permitted on this route?
Proxy to provider	Forwarding result or receiver observation	What does the receiver report?
Worker to tool	A separate effect decision	Did the grant cover the proposed commit?

Sources and evidence

Watchdog enforces configured ARF verdicts · Implementation record · Policy decisions on supported request routes · Implementation record