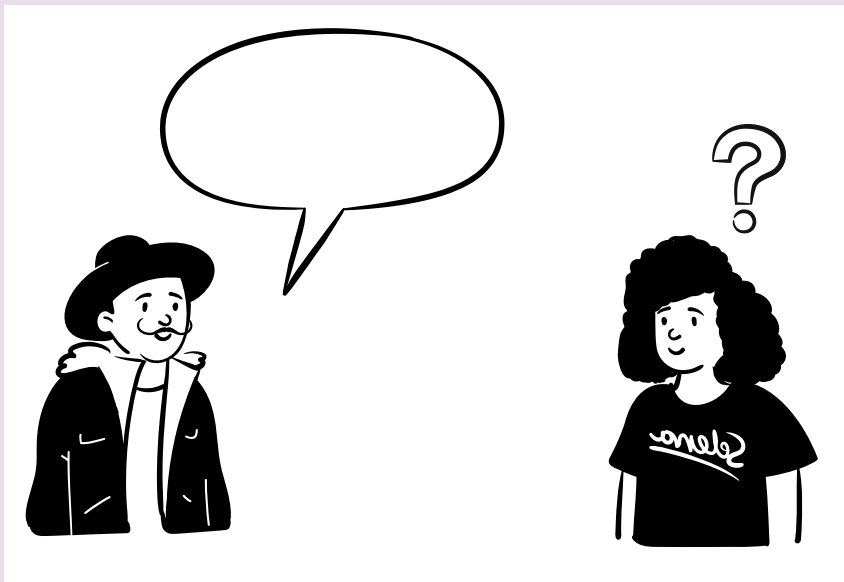


# Speaking Through Policies



# Personas

Infra Provider



Hi, I'm Ian

Cluster Operator



I'm Chihiro

App Developer



I'm Ana

# Ana: App Developer

I work with Chihiro at Evil Genius Cupcakes,  
where I am an **App Developer**.

My team **writes, deploys and maintains**  
software on **Kubernetes**, that the employees of  
our company use to operate the production of  
cupcakes.



Recently, I worked on the latest version of  
our “baker” **service**, which is ready to be  
deployed to **staging**.

# Chihiro: Cluster Operator (aka Platform Engineer)

I work with Ana at **Evil Genius Cupcakes**  
My team **maintains** the **platform** where Ana  
**deploys** her apps.

We set up **ingress gateways** that route the  
traffic to the services.

We configure the top connectivity and  
**security** of the gateways (e.g.: **DNS**, **TLS**  
**certs**, etc).

We also ensure that some company-level  
**policies** are being **enforced**.



# Ian: Infrastructure Provider

I work for the company “Infra 4 bakers”  
providing **K8S** clusters with batteries  
included, ready for their use. Including  
**Gateway API** and **Kuadrant**

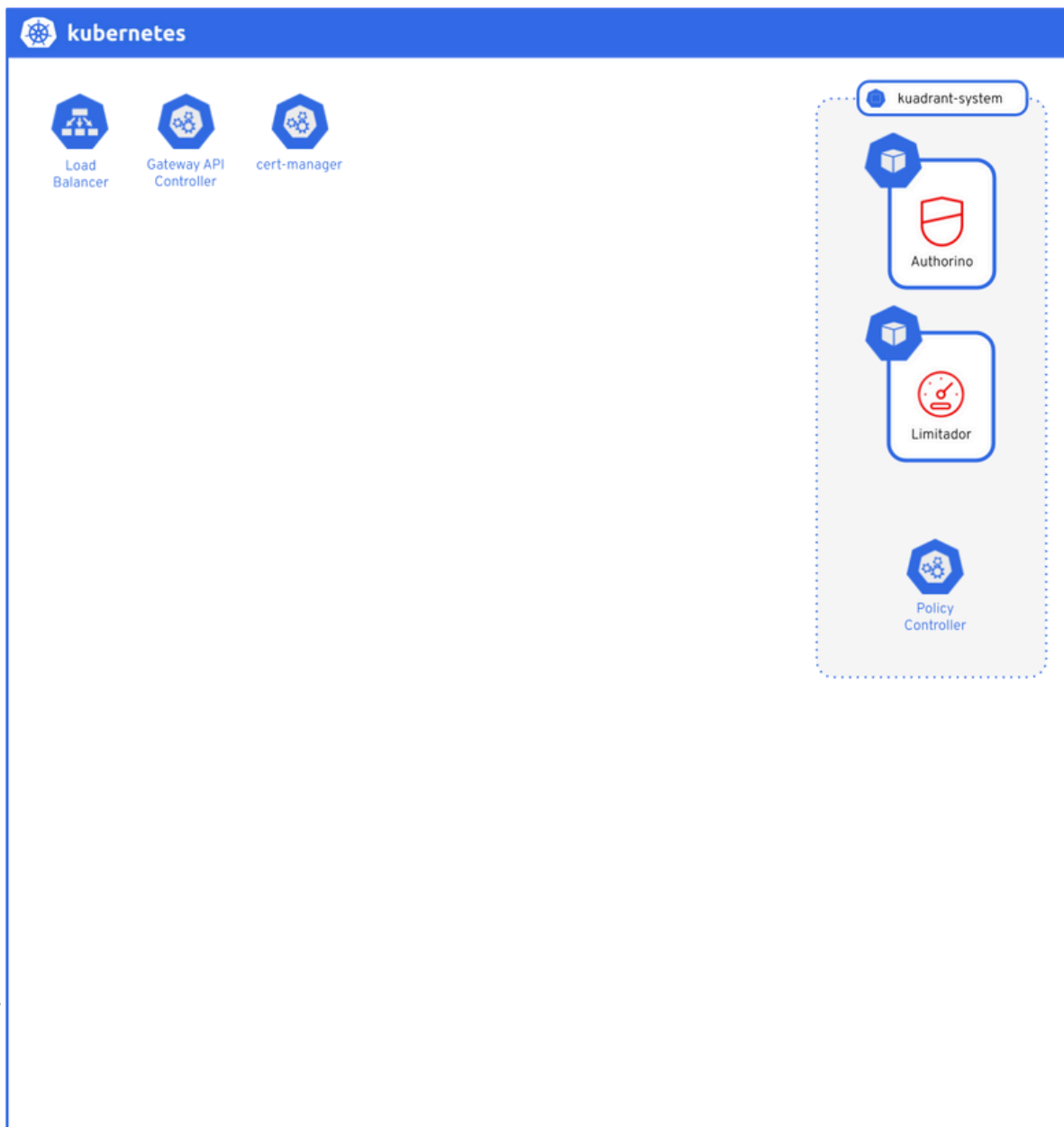


Oh, and I don't know who  
those other two people are

# Cluster Ready

Our Infrastructure provider, Ian, span up this cluster for us and installed a **gateway controller** in advance.





# Deploy Baker Service

My work depends on Chiriro's a little, because the **gateways must be there**, but once they are, we're very **autonomous** regarding how we **deploy** the apps and **roll out new versions**.

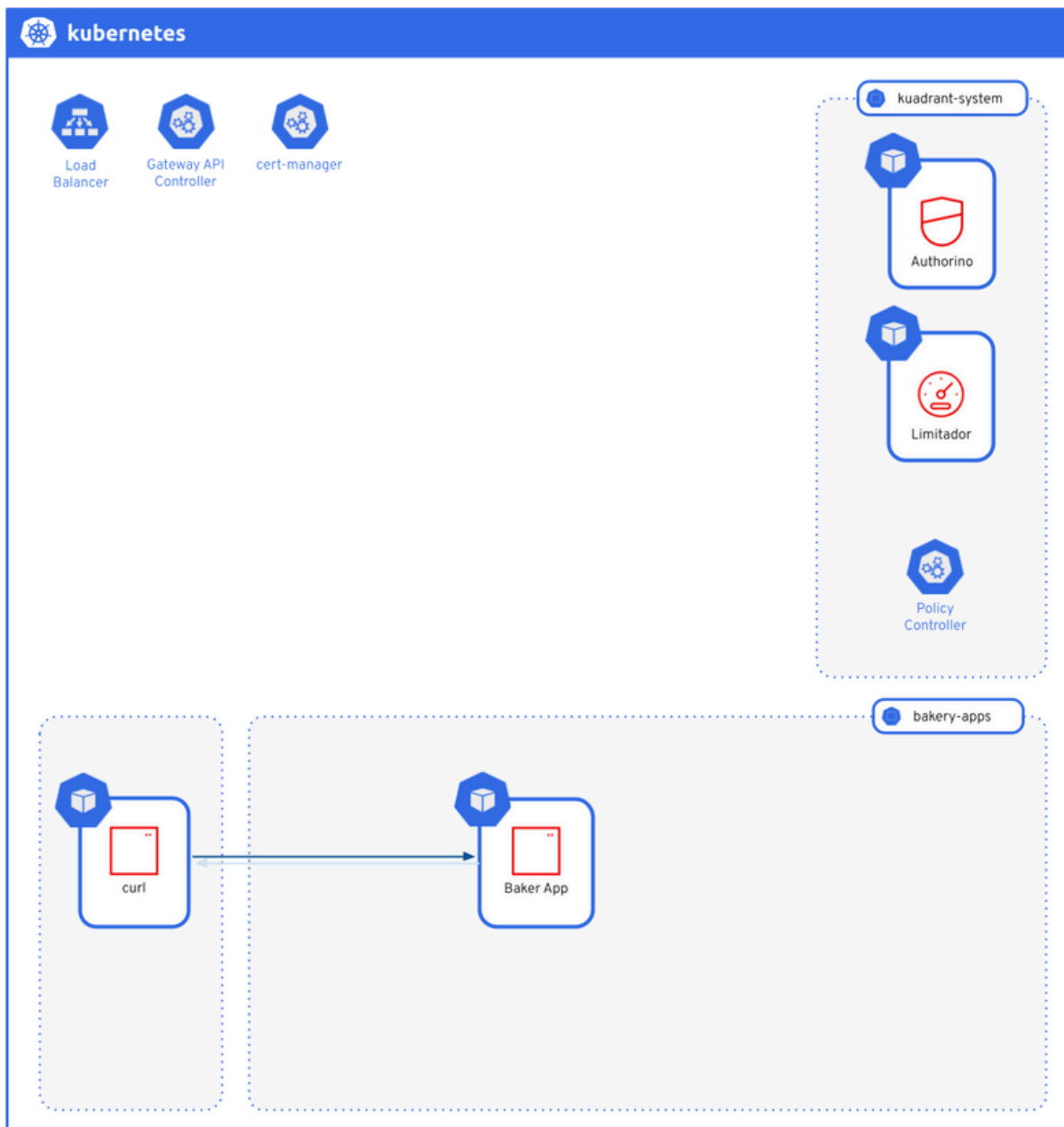
We have a **namespace** where we configure the apps.

This is typically done via automation integrated with our code repositories, but today I will be demoing my day-to-day using the **kubectl CLI** tool.

In fact, I am about to **deploy** the **`baker` service** I mentioned before.







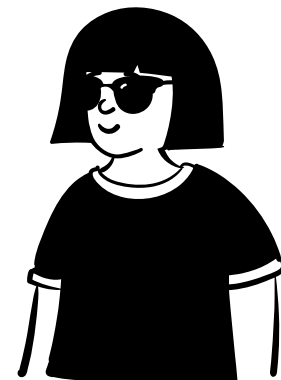
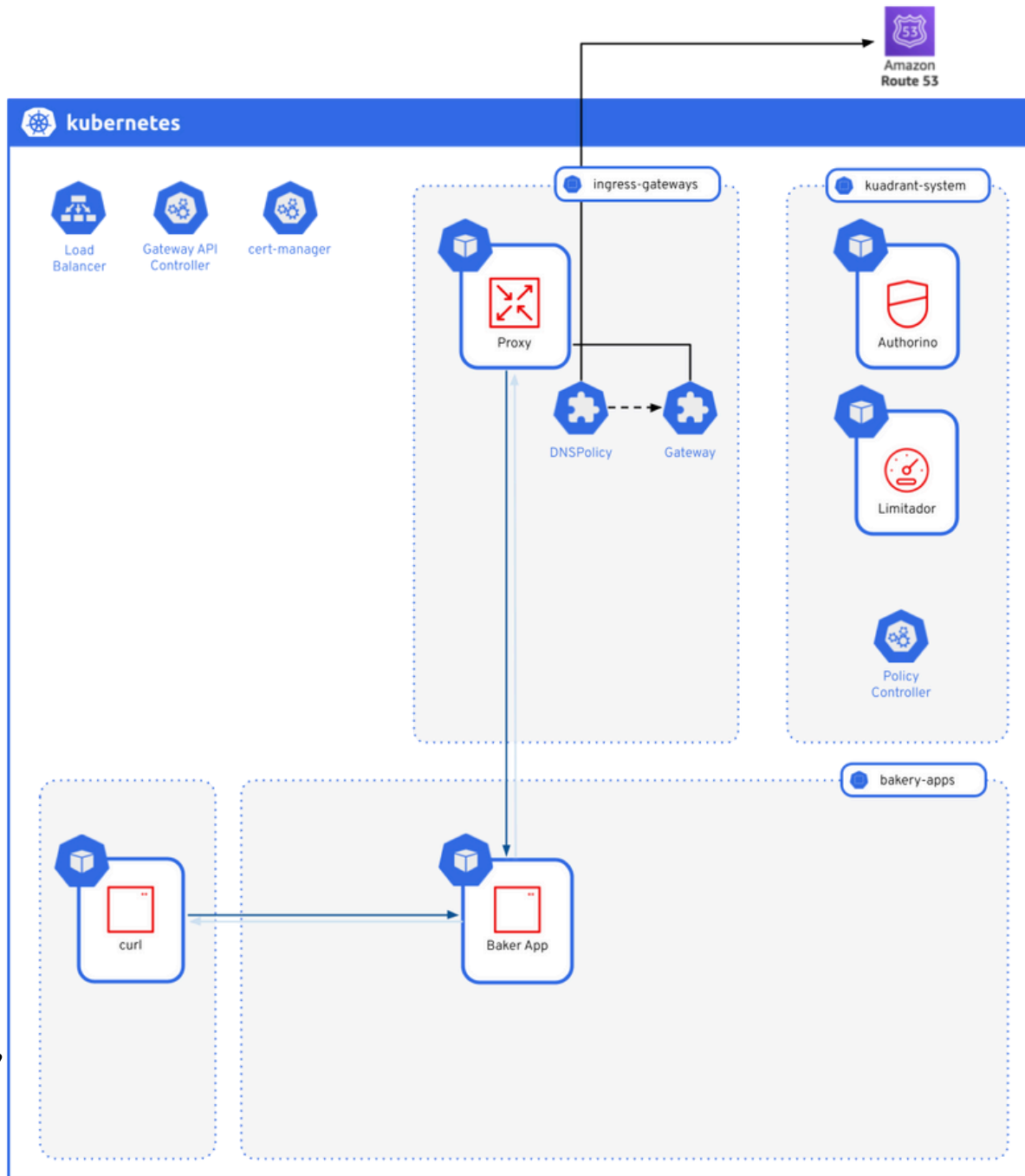
# Configure Ingress Gateway

In the meantime, I'm finishing configuring an **ingress gateway** that will be used to route the **traffic to the services**.

So now, I can focus on the gateway configuration.

This gateway is going to be a centralised point of connectivity and policy enforcement for the data plane.





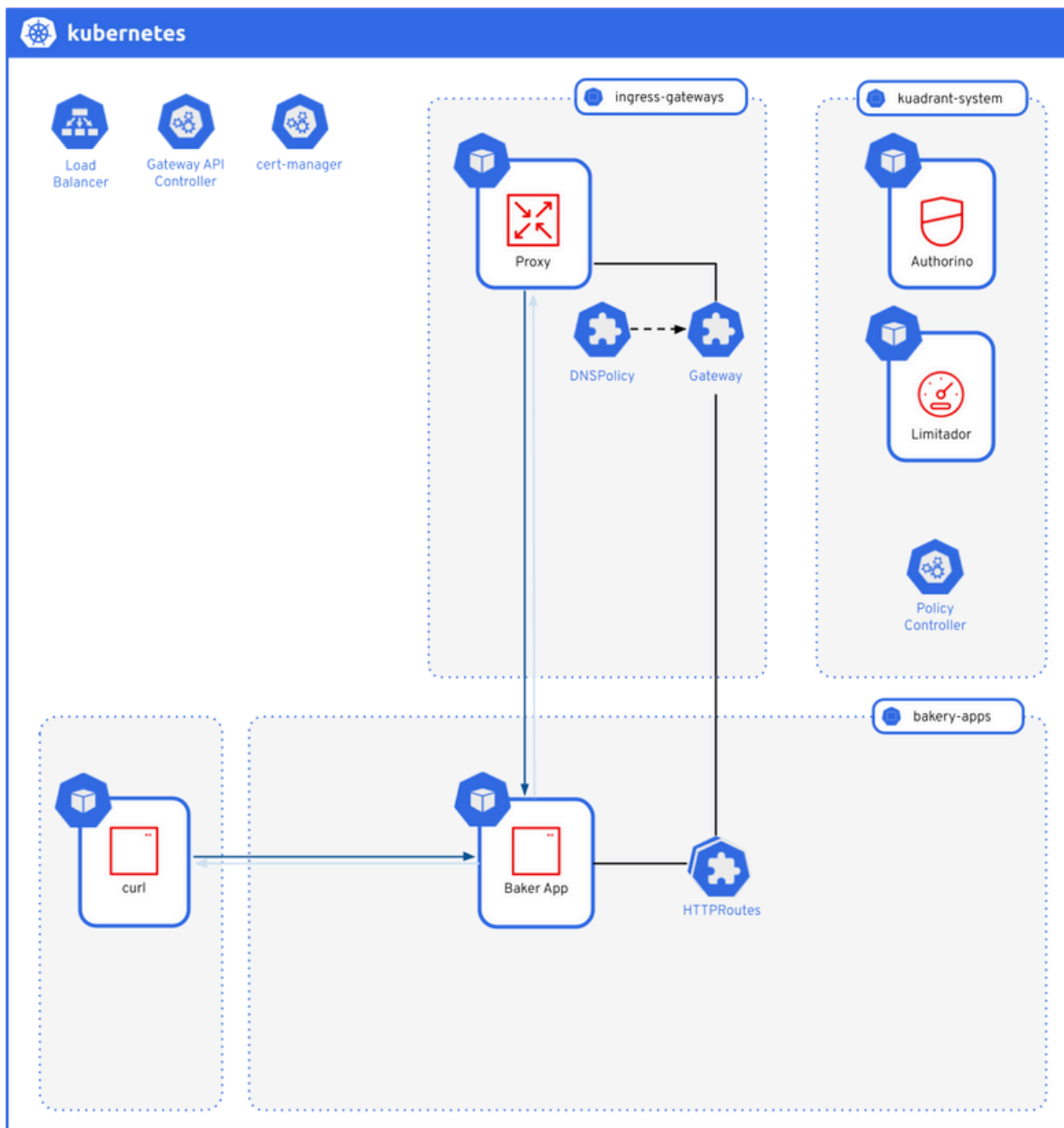
# Connecting to the Gateway



Ana, I'm going to give you **permission** to read the **status** of this **gateway**, so you can see when it's ready and grab some connectivity info you may need for your local tests.



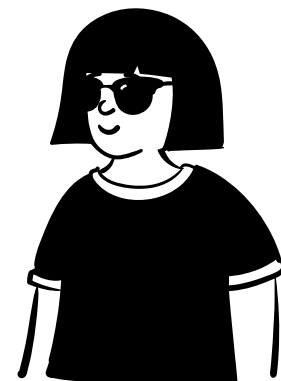
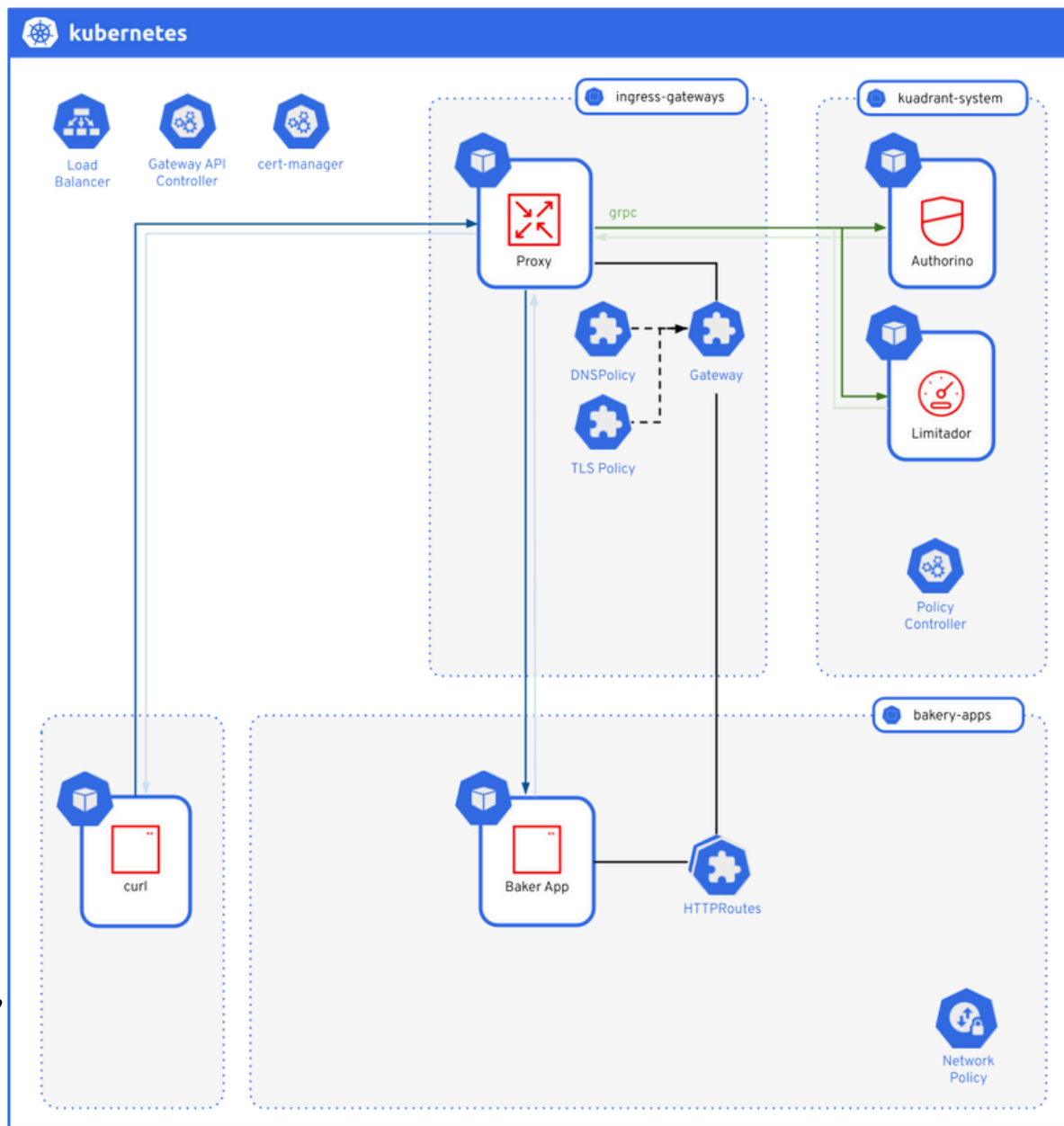
Thanks! I'll check it right away and attach some **Routes**




# Securing the Gateway

I've realised we might have traffic within the cluster hitting your apps directly. We need a **NetworkPolicy** so all the traffic goes through the ingress gateway.





# Authenticated Traffic

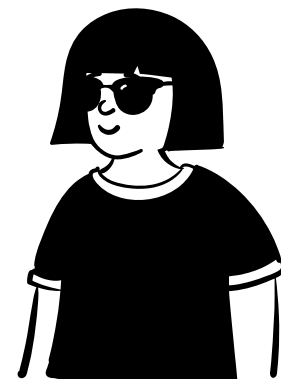
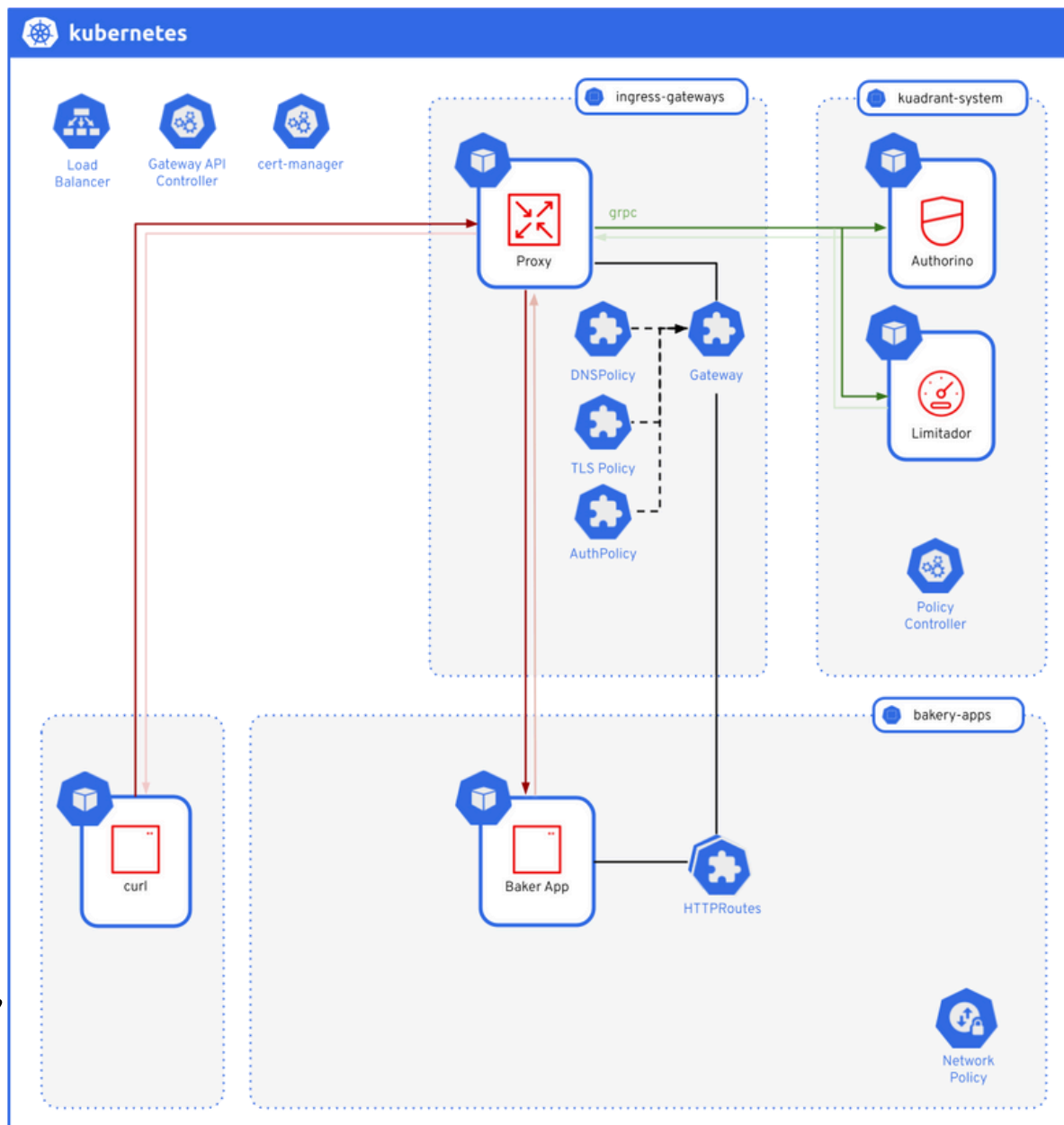


So I've attached an **AuthPolicy** to **deny all traffic**, feel free to attach one to your route to replace it and thus enforce auth as needed.




Ok, I'll setup 2 **authentication** methods, **OIDC** for **external** traffic and **K8S tokens** for pod **internal** traffic. I'll also create a **RateLimitPolicy** too.








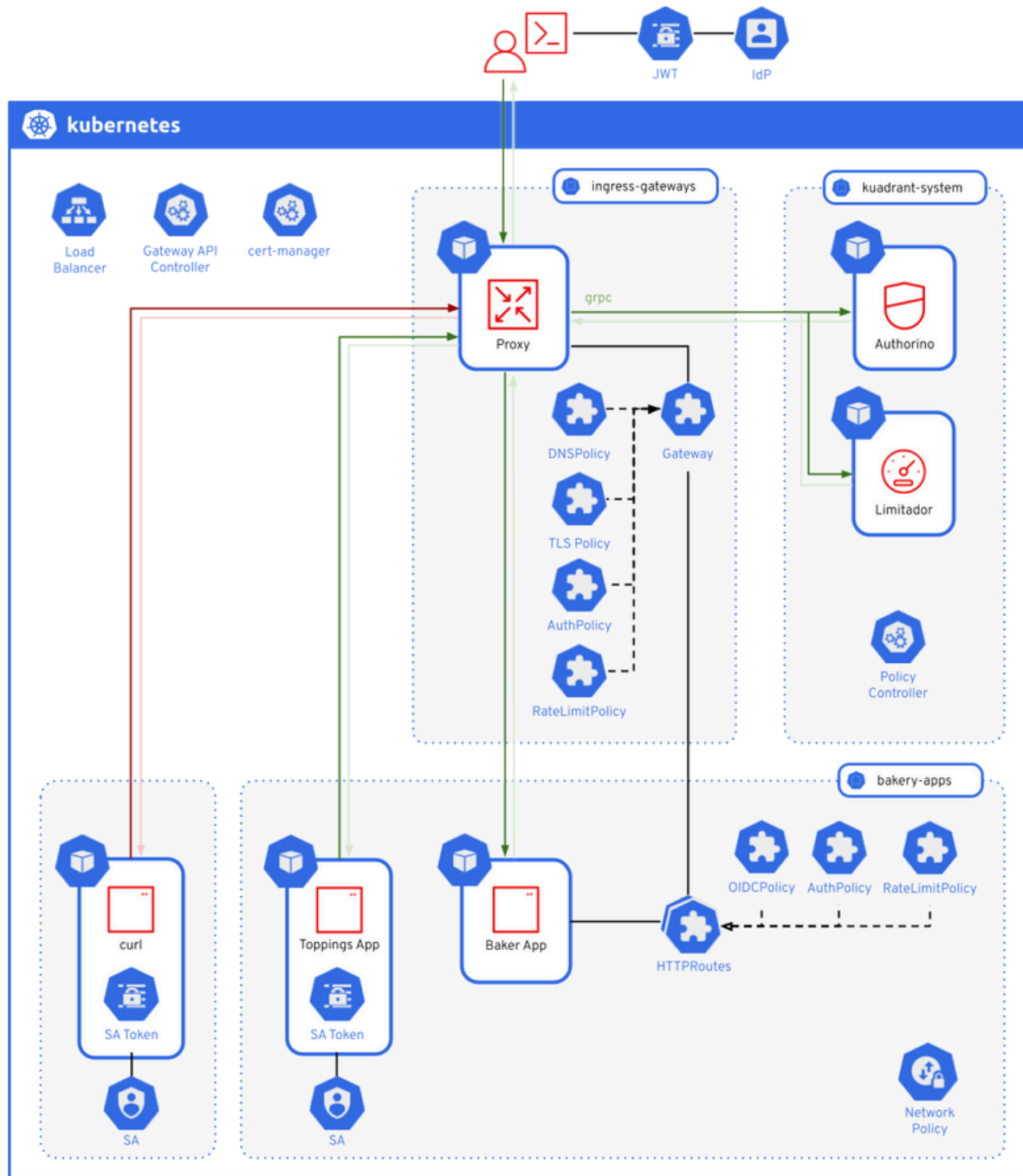
# Rate limiting



I've seen in the **HTTPRoute status** that there is another **RateLimitPolicy** in the **Gateway** affecting my rules.



Ah, yes, we've monitored more traffic that we can manage, I had to **override** yours



# Questions ?



@ddicesare



@didierofrivia



@mastodon.online/@didierofrivia



@guilherme-cassolato



@guicassolato