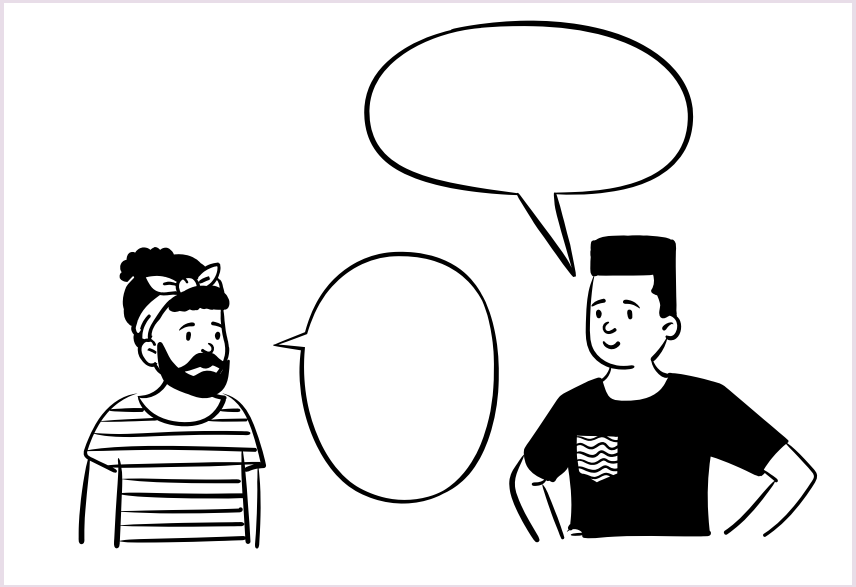
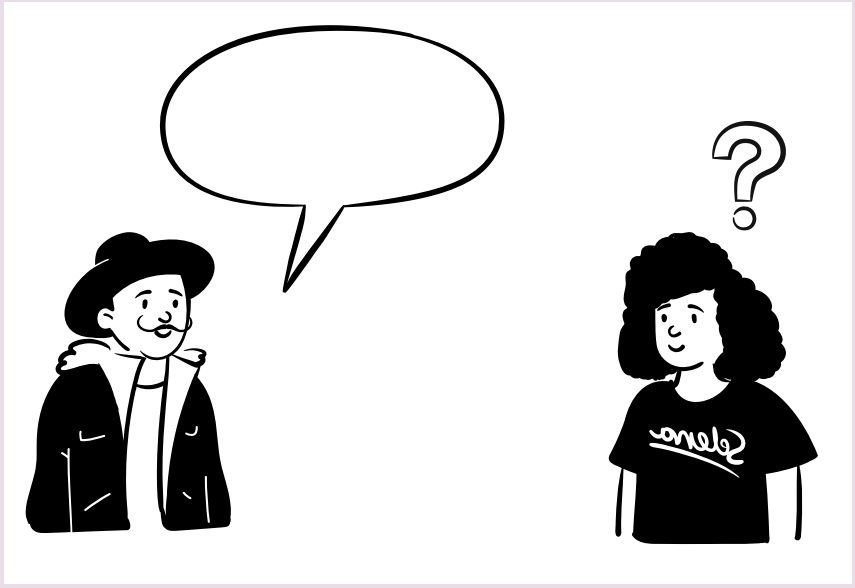
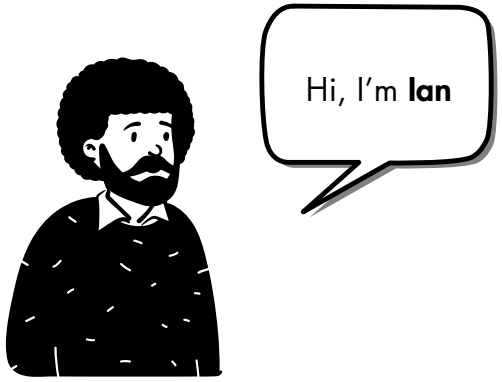


Speaking Through Policies



Personas

Infra Provider



Cluster Operator

App Developer

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**.

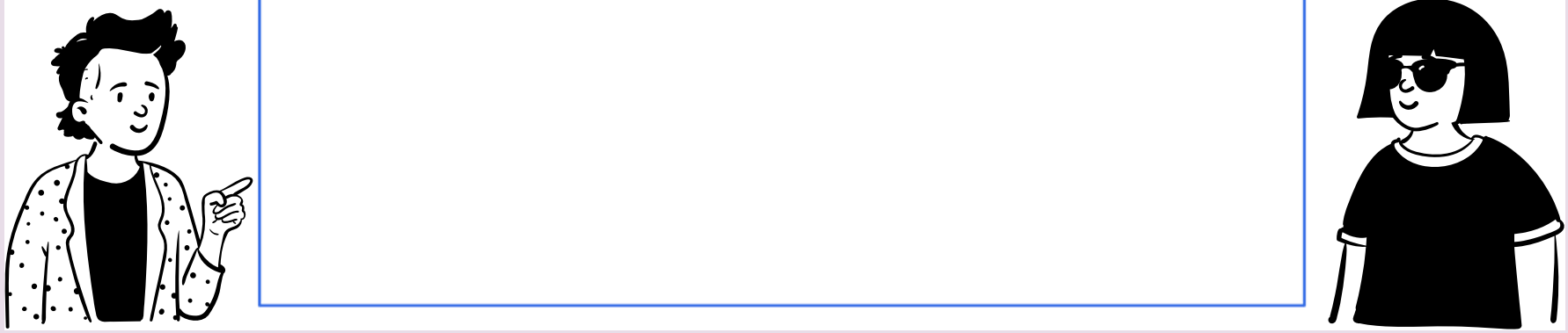
Ian: Infrastructure Provider

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.


kubernetes
Load Balancer
Gateway API Controller
cert-manager
kuadrant-system
Authorino
Limitador
Policy Controller

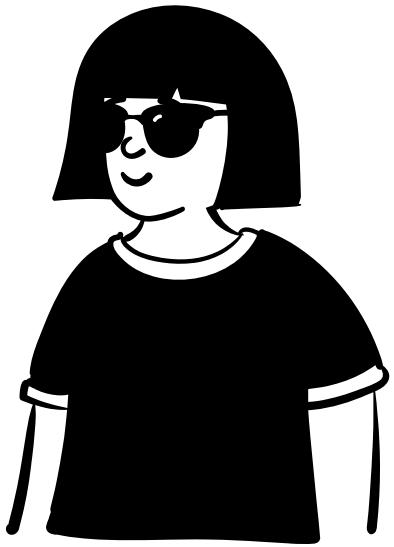
Deploy Baker Service

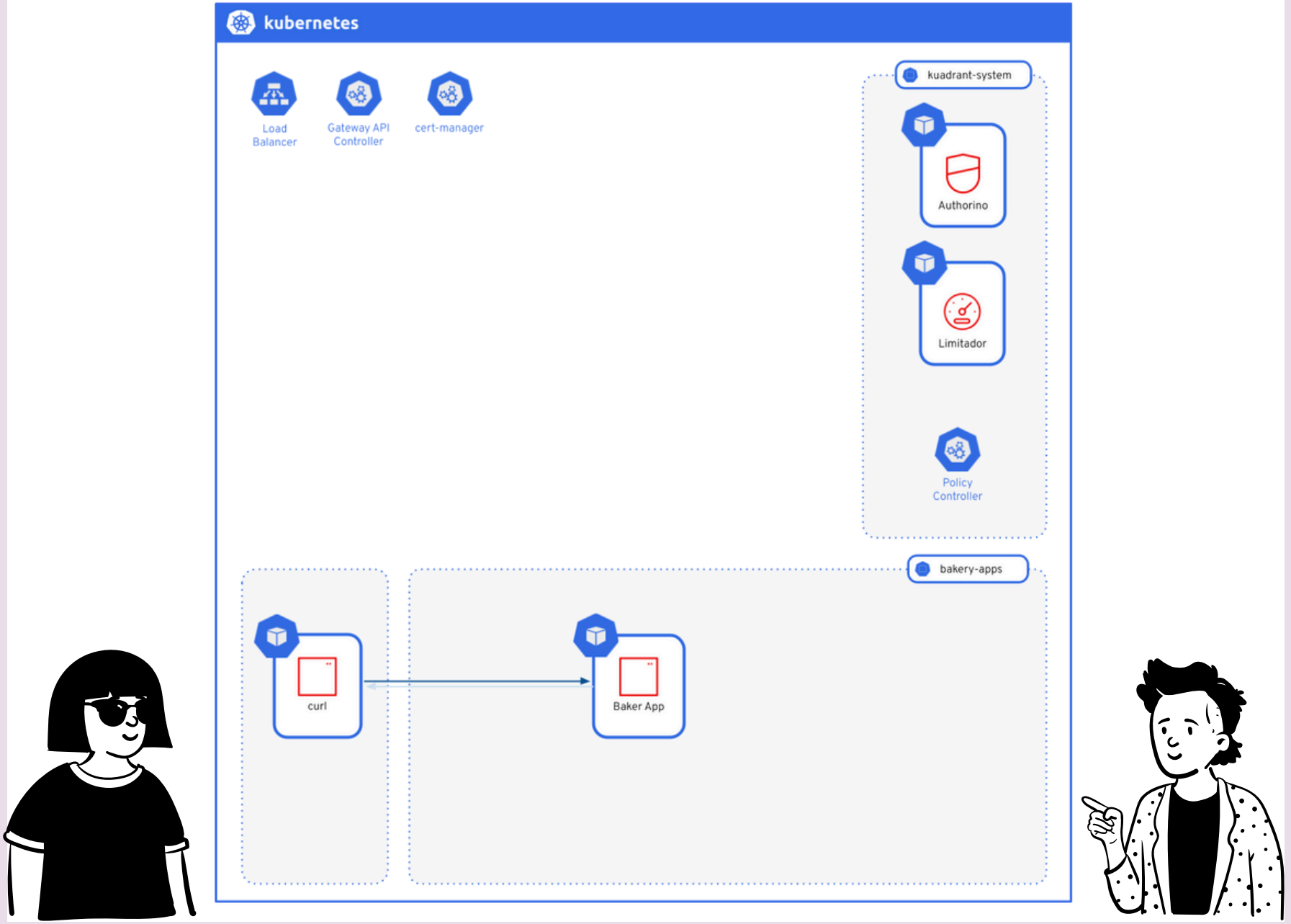
My work depends on Chiriro's a little, because the **gateways must be there**, but once they are, we're very **autonomous** regarding how we **deploy** the apps and **roll out new versions**.

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.

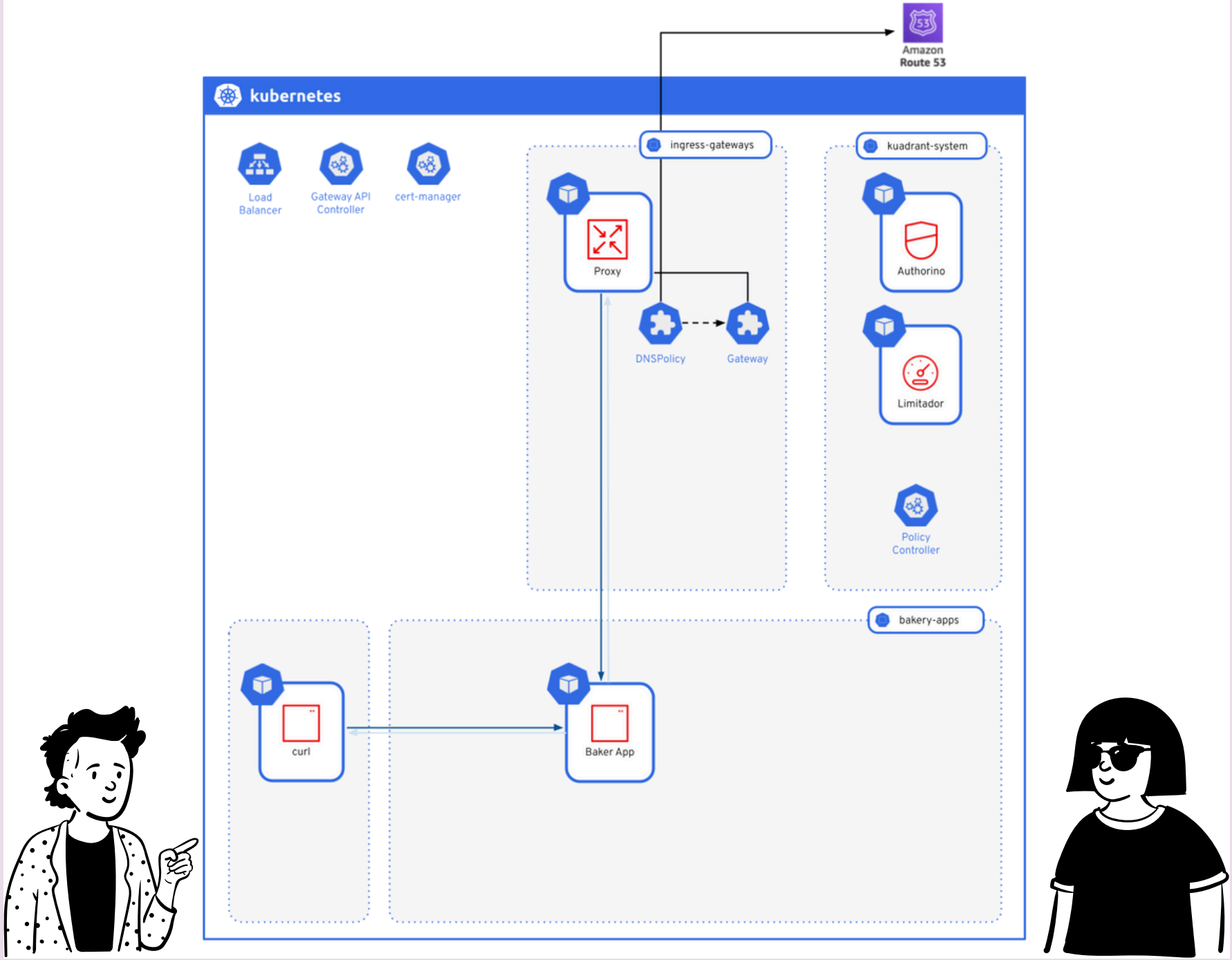



kubernetes
Load Balancer
Gateway API Controller
cert-manager
kuadrant-system
Authorino
Limitador
Policy Controller
bakery-apps
curl
Baker App

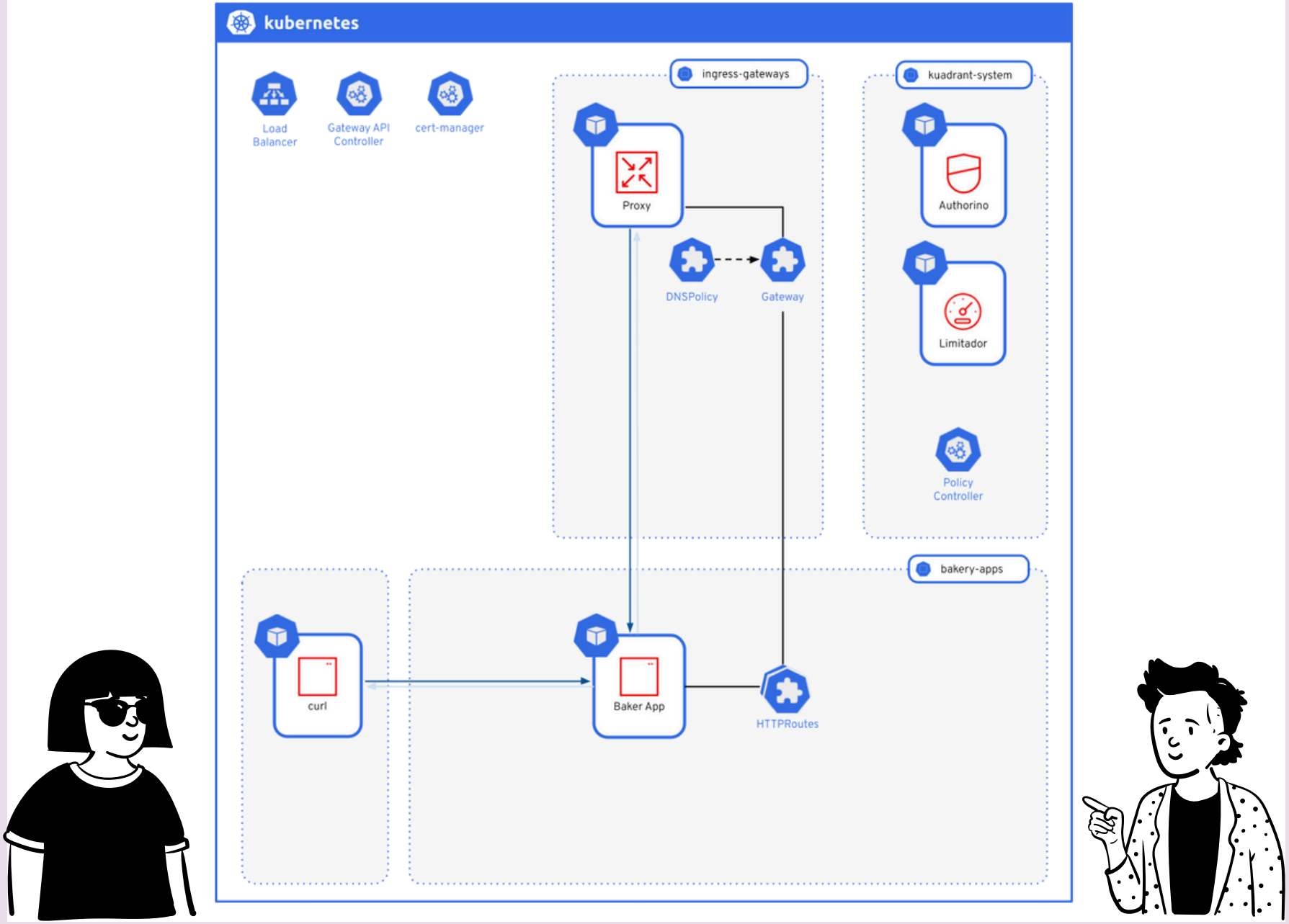
Configure Ingress Gateway

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.

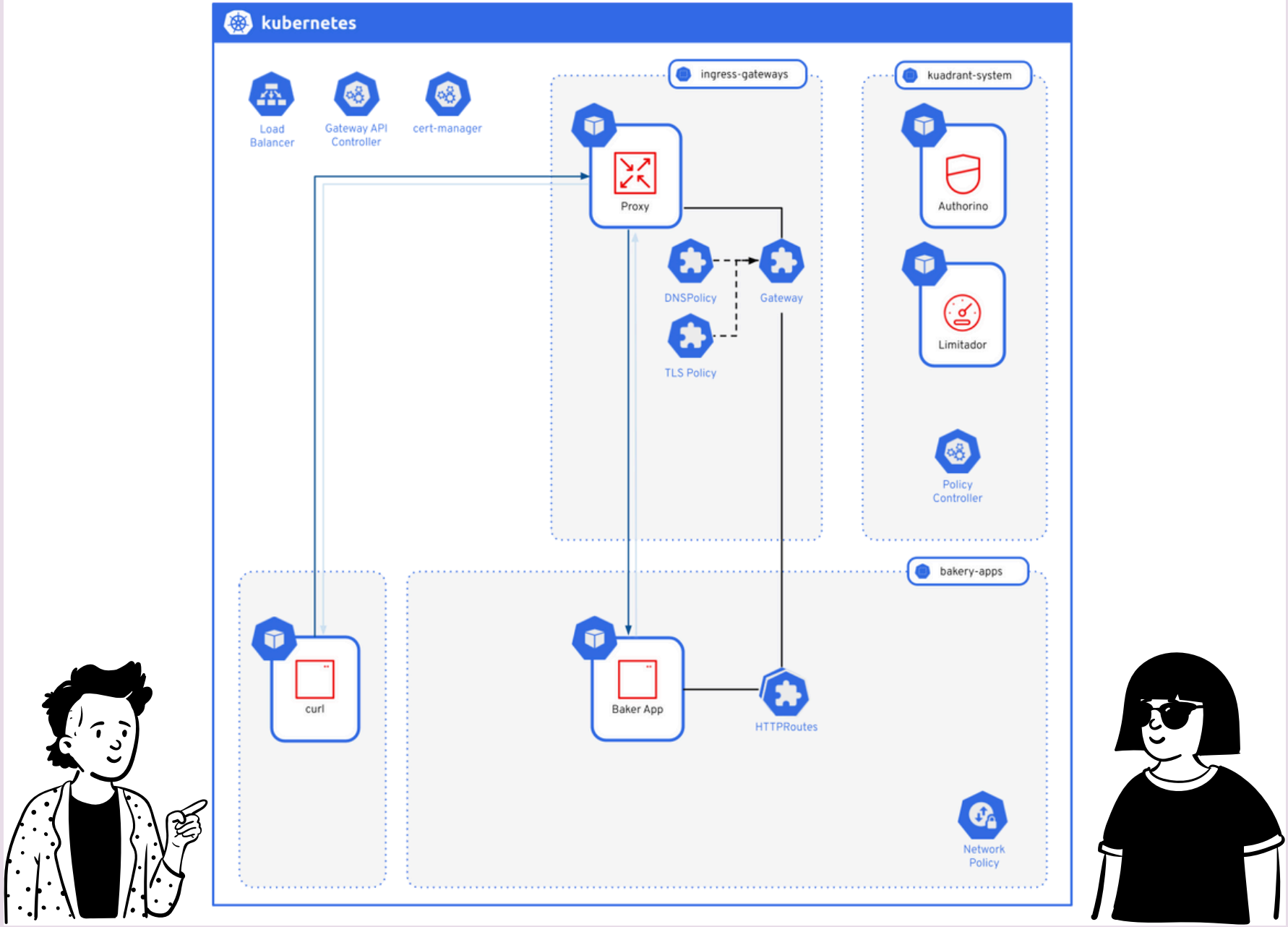

Amazon
Route 53
kubernetes
Load
Balancer
Gateway API
Controller
cert-manager
ingress-gateways
Proxy
DNSPolicy
Gateway
kuadrant-system
Authorino
Limitador
Policy
Controller
bakery-apps
curl
Baker App

Connecting to the Gateway

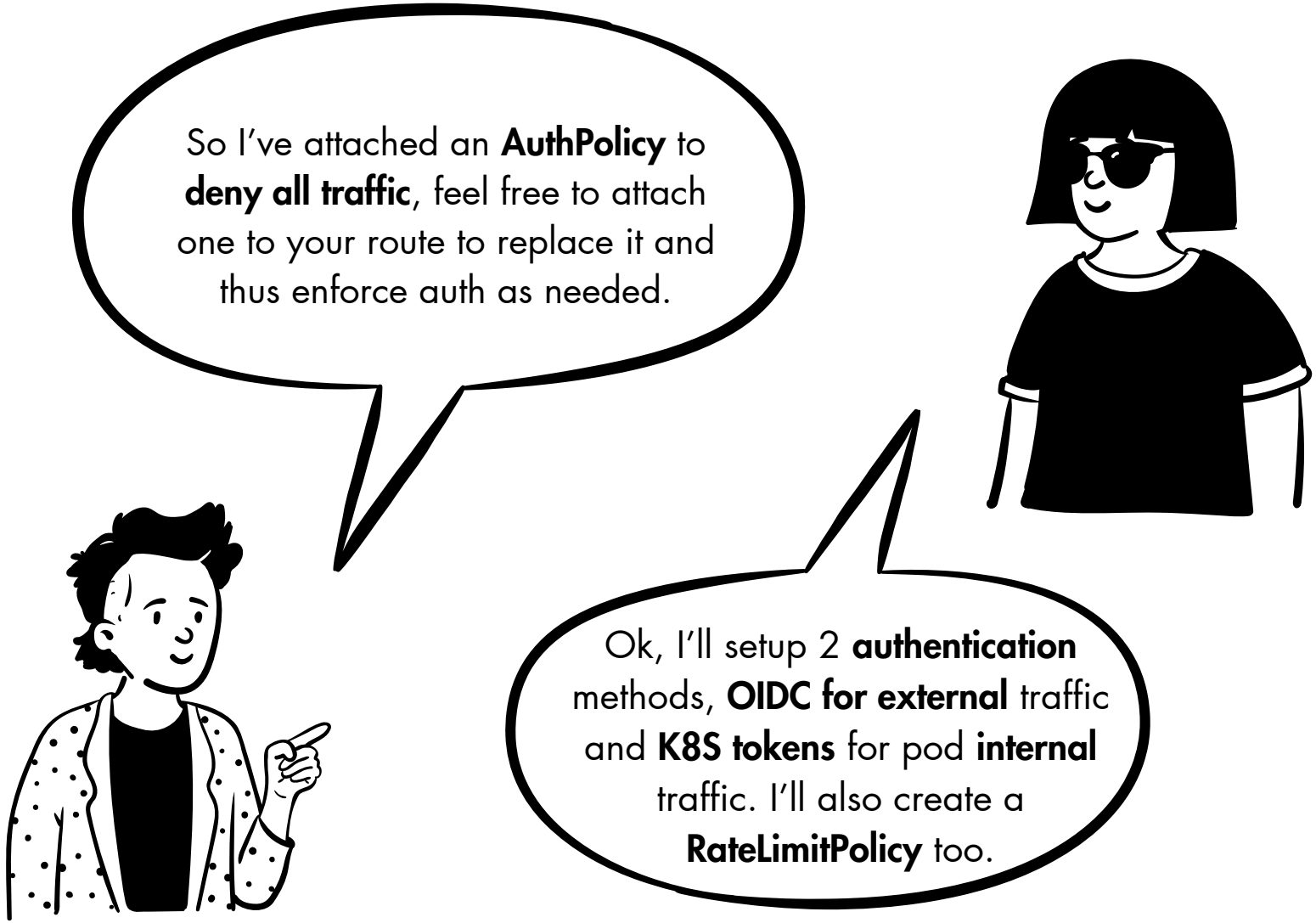

kubernetes
Load Balancer
Gateway API Controller
cert-manager
ingress-gateways
Proxy
DNSPolicy
Gateway
kuadrant-system
Authorino
Limitador
Policy Controller
bakery-apps
curl
Baker App
HTTPRoutes

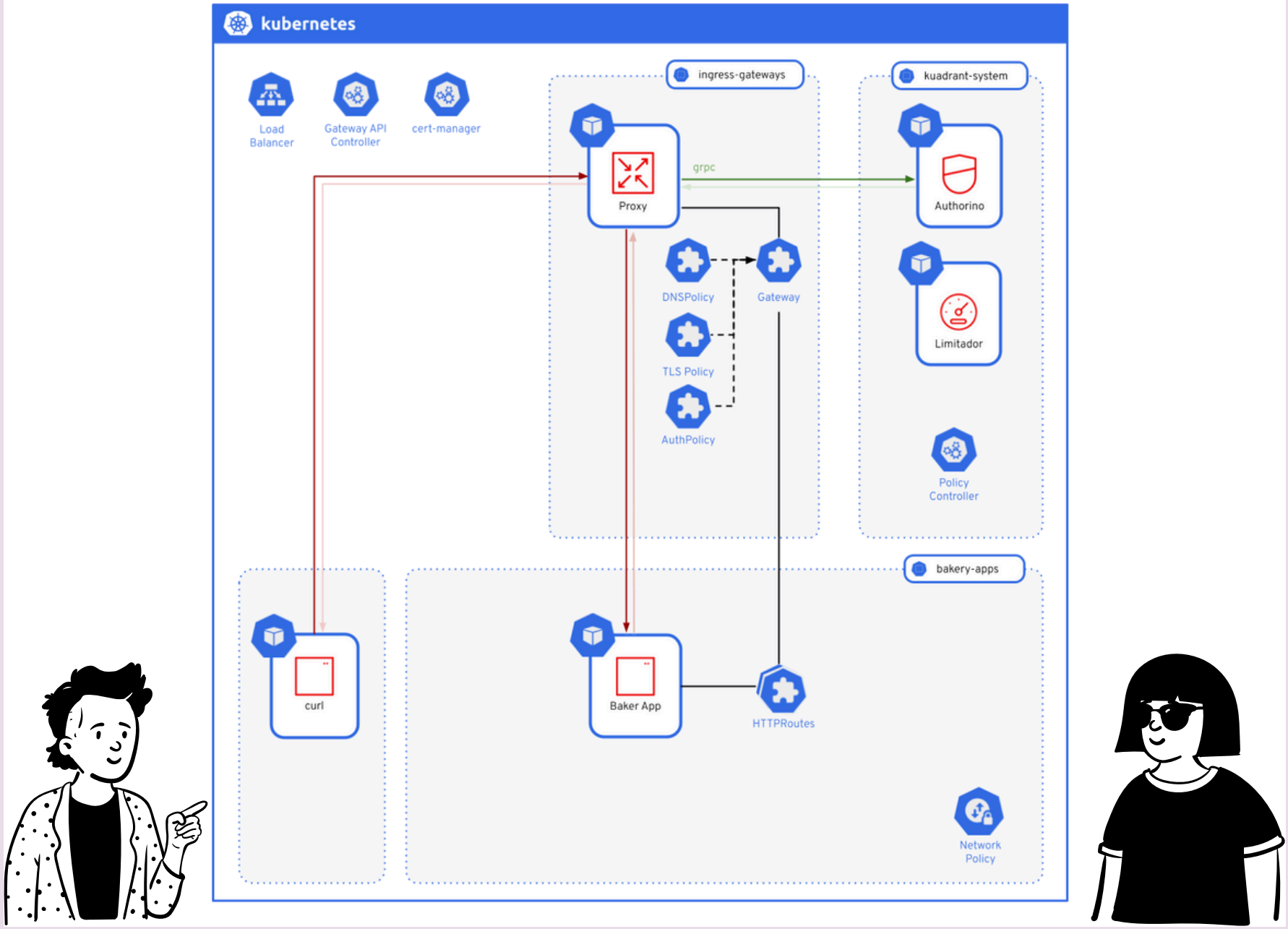
Securing the Gateway

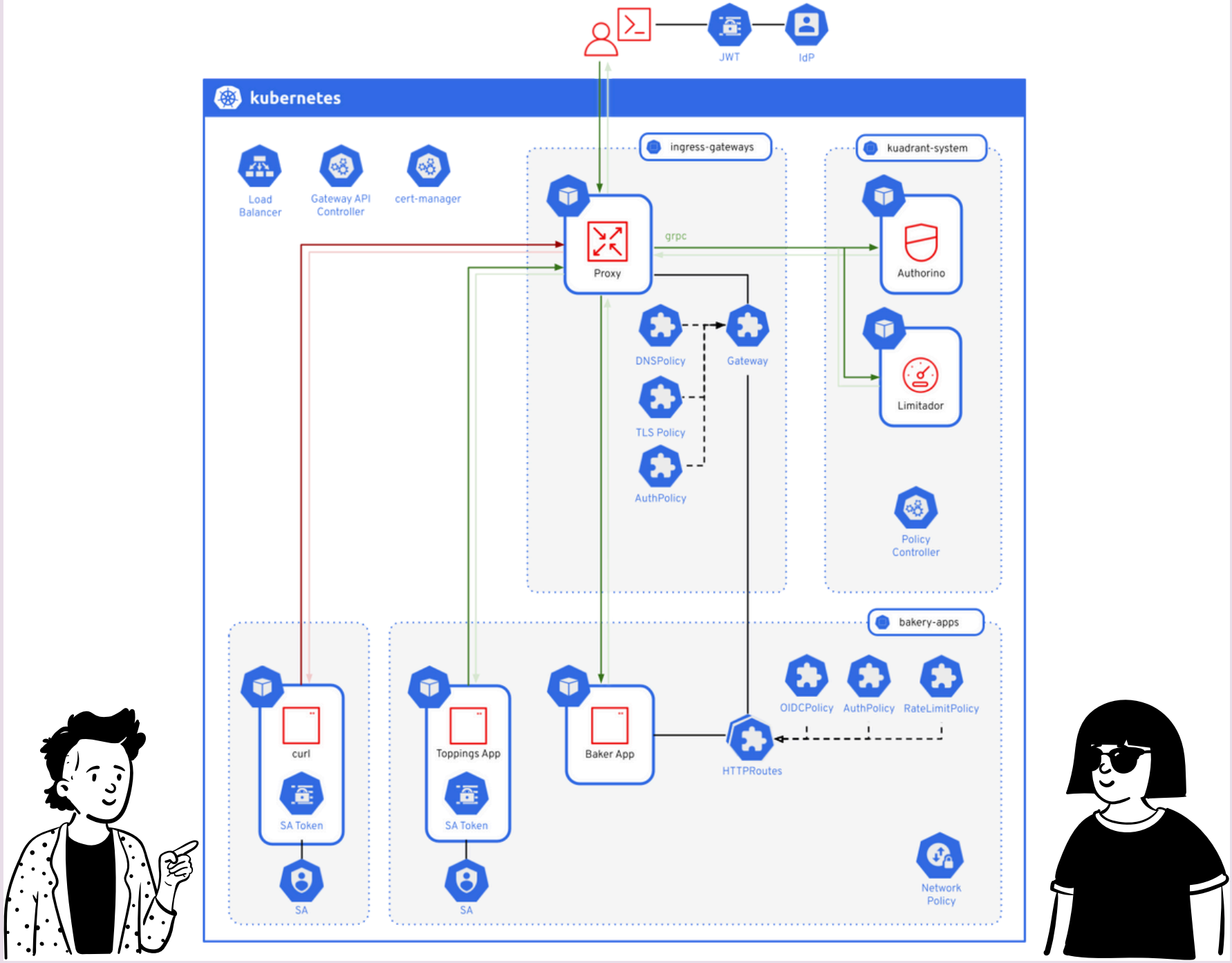
I've realised we might have traffic within the cluster hitting your apps directly. We need a **NetworkPolicy** so all the traffic goes through the ingress gateway.


kubernetes
Load Balancer
Gateway API Controller
cert-manager
ingress-gateways
Proxy
DNSPolicy
Gateway
TLS Policy
kuadrant-system
Authorino
Limitador
Policy Controller
bakery-apps
curl
Baker App
HTTPRoutes
Network Policy

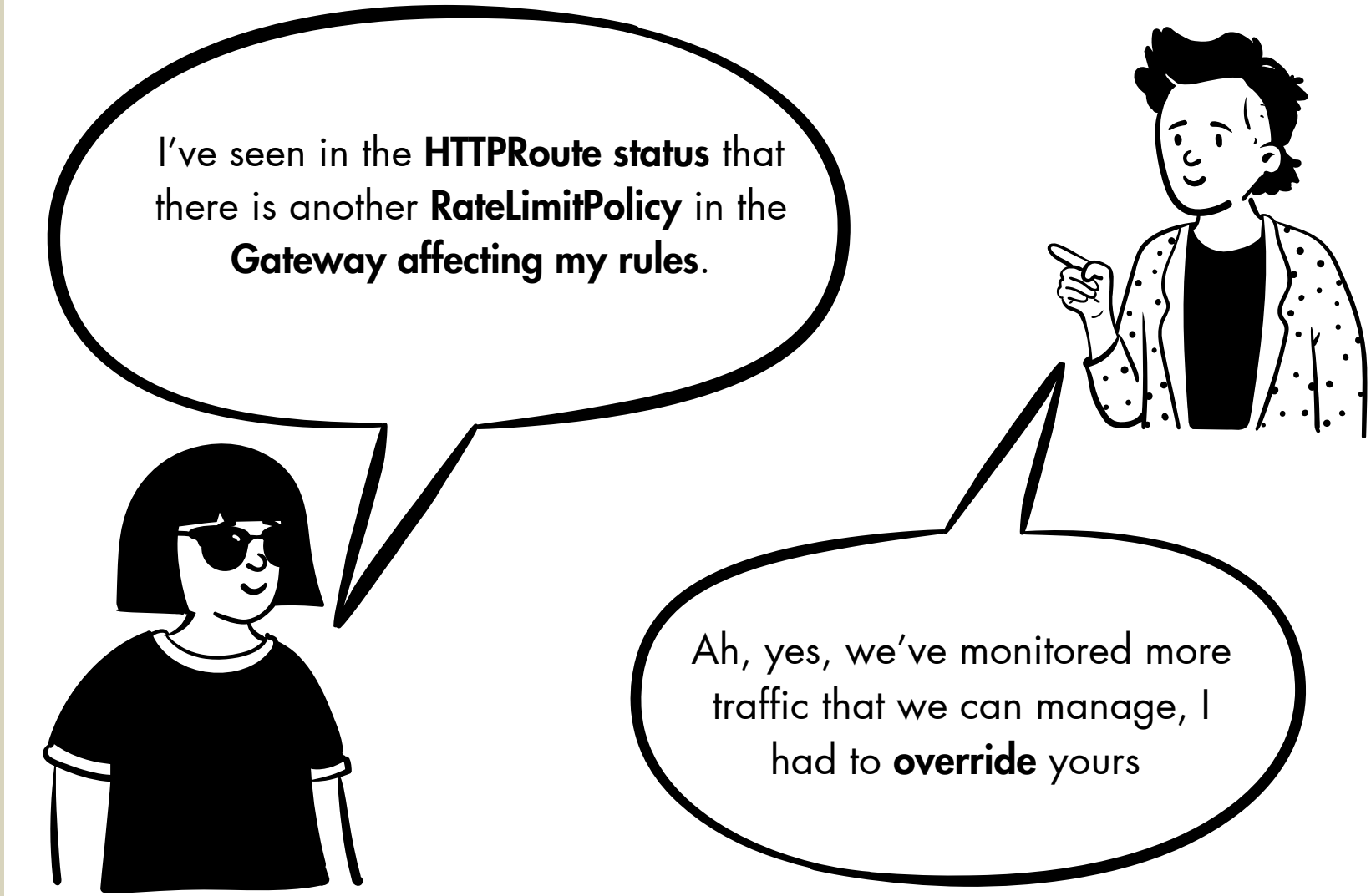
Authenticated Traffic

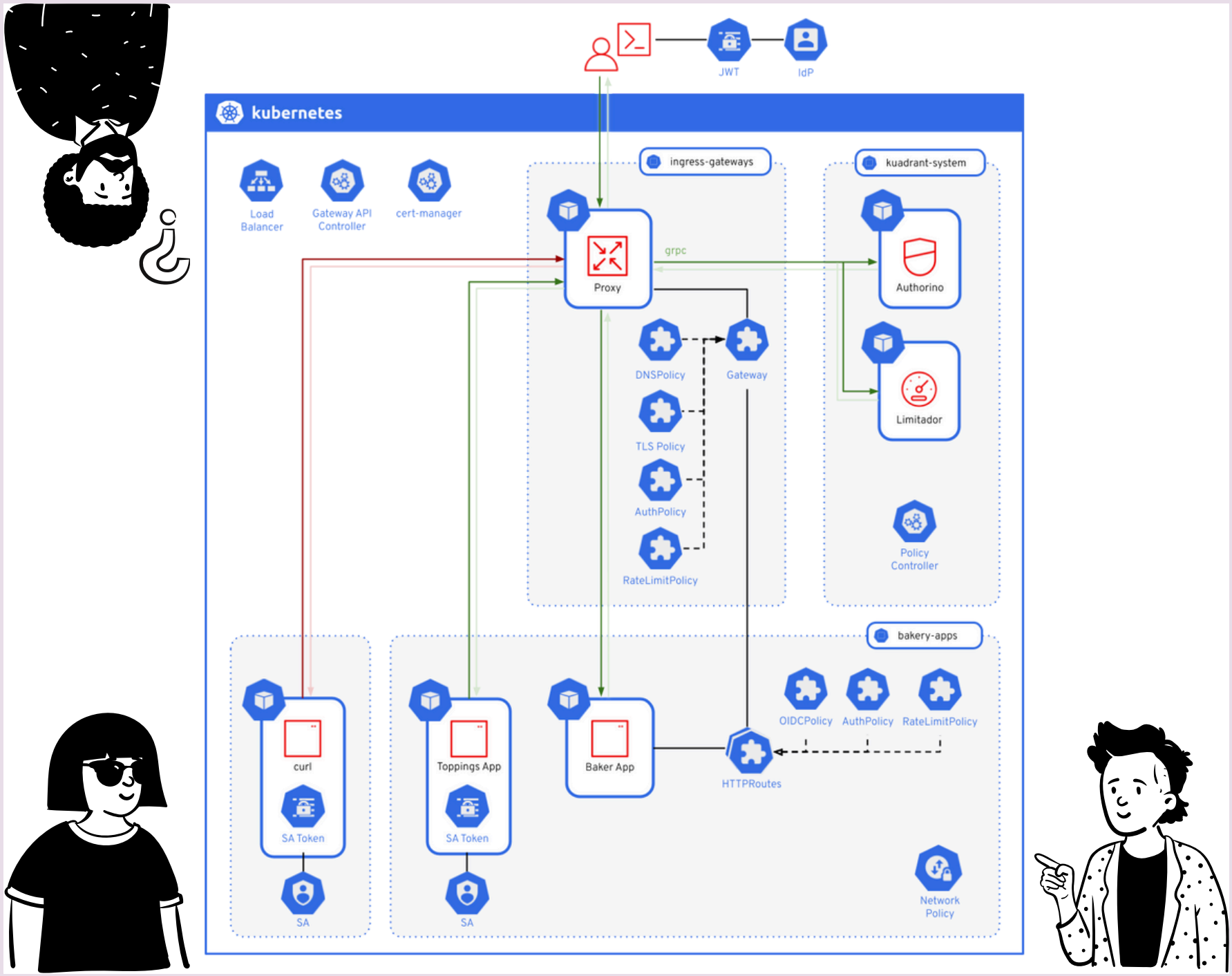



kubernetes
Load Balancer
Gateway API Controller
cert-manager
ingress-gateways
Proxy
grpc
DNSPolicy
Gateway
TLS Policy
AuthPolicy
kuadrant-system
Authorino
Limitador
Policy Controller
bakery-apps
curl
Baker App
HTTPRoutes
Network Policy


JWT
IdP
kubernetes
Load Balancer
Gateway API Controller
cert-manager
ingress-gateways
kuadrant-system
Proxy
grpc
Authorino
Limitador
DNSPolicy
Gateway
TLS Policy
AuthPolicy
Policy Controller
bakery-apps
curl
SA Token
SA
Toppings App
SA Token
SA
Baker App
HTTPRoutes
OIDCPolicy
AuthPolicy
RateLimitPolicy
Network Policy

Rate limiting




JWT
IdP
kubernetes
Load Balancer
Gateway API Controller
cert-manager
ingress-gateways
kuadrant-system
Proxy
grpc
Authorino
Limitador
DNSPolicy
Gateway
TLS Policy
AuthPolicy
RateLimitPolicy
Policy Controller
bakery-apps
curl
SA Token
SA
Toppings App
SA Token
SA
Baker App
HTTPRoutes
OIDCPolicy
AuthPolicy
RateLimitPolicy
Network Policy

Questions ?

@ddicesare

@didierofrivia

@mastodon.online/@didierofrivia

@guilherme-cassolato

@guicassolato