Philippe, I heard about the **Azure Front Door (AFD)** service, could you tell us a little more?

Of course Lea. **AFD** is a global load balancing service which acts on the network layer **(L7)** via the **HTTP/S** protocol, it applies on the application layer. By global I mean that it is not deployed in a region.

One of its advantages is the use of Microsoft **Points of Presence (POP)**, which are the same as those used for the **Content Delivery Network (CDN)**. These **POPs** allow users to reduce latency when consuming services/applications.

I see. As I live in France, I connect to the **POP** closest to my home and it serves me the content.

In addition, **AFD** offers **SSL offloading**, so the decryption phase is managed directly on **AFD** side, which allows the backend servers to be less stressed!

It's true. Basically, **AFD** offers a URL with an **SSL certificate** provided by Azure. Of course, you can create a custom URL with your own **SSL certificate**.

By coupling **AFD** with an **Application Gateway** as a backend, **end-to-end encryption** is assured for the user. It means that there is no **SSL termination** between the client and the server that hosting its application.

Another interesting thing is the possibility of creating **several URLs** within **AFD**.

But then, how do you redirect traffic based on your application's URL to the correct server?
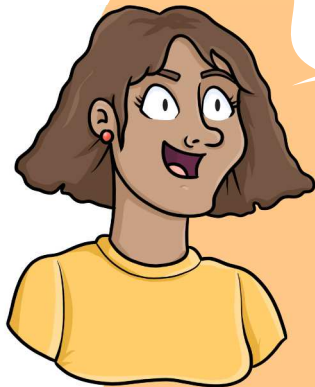
Everything happens at the configuration level within **AFD**, which is divided down into 3 steps:

The 1st, you enter the URL that will be used by your users and your **SSL certificate**. This is called the **frontend configuration**.

The 2nd, you configure the target on which the traffic is sent. The Azure server or service that hosts your application is called the **backend**. You can of course have multiple servers/services in your backend for **high availability** concerns.

And finally the last step concerns the **rules**. This is where you will associate your **frontend**, i.e. the URL called by your users, to your **backend**, i.e., the servers / services that host your application.

In addition, you can choose among the different routing methods: **Latency**, it's the backend that responds the fastest. **Priority** is when sending traffic to one backend rather than another. **Weight**, which allows you to distribute traffic evenly or use a predefined weight.

And we also have session affinity to redirect a user's requests to the same backend.

But that's not all, **AFD** also supports **caching** option!

What is caching?

Caching is the act of storing part of the content of your application in another place from where it is deployed, **to serve it faster**.

Typically what gets cached is **static content**, like images, HTML, CSS that rarely changes. That content is stored at the **POP level**. This is the principle of the **CDN**, which we quickly mentioned earlier.

I guess that this cached content is updated at certain frequencies, in case there are any changes?

Yes, and if necessary it can be purged to be updated automatically.

Regarding security, we have seen support for **SSL certificates** to encrypt traffic in transit. **AFD** also natively offers a **Web Application Firewall (WAF)** fully managed by Azure.

A WAF is an application-level firewall to protect against attacks, like SQL injections or other threats.

It comes with basic rules provided by Microsoft, but of course you can create your own rules.

https://