[GCP] Cloud Run with Secure External Access

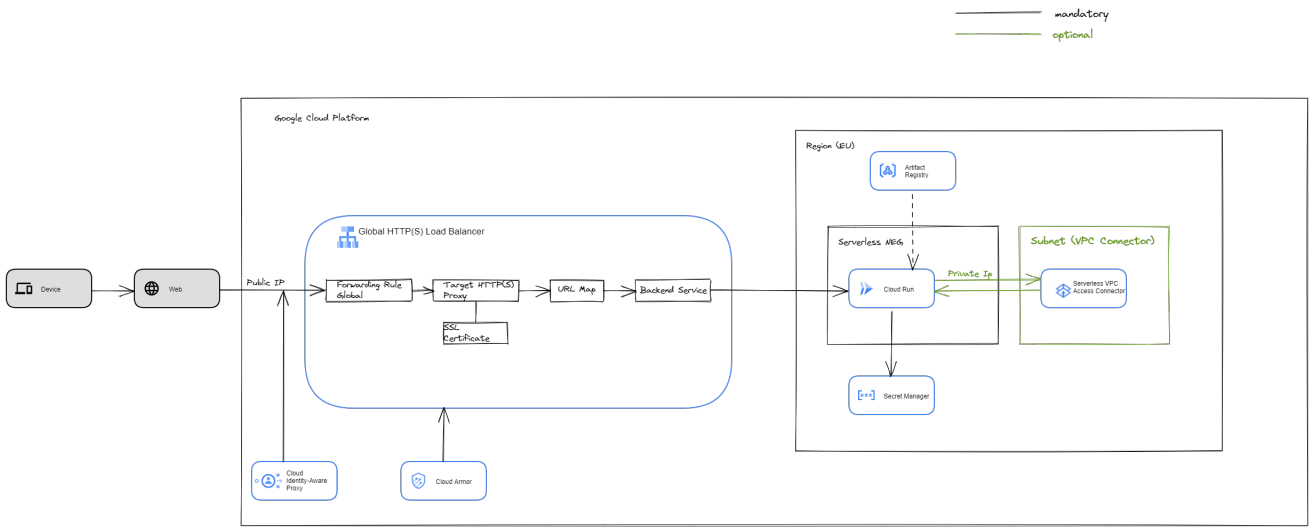
Cloud Run with Secure External Access

Cloud Run is a managed compute platform that lets you run containers directly on top of Google's scalable infrastructure.
The following post provides a quick overview of GCP's compute option and use-cases.

Architecture

The following architecture deploys the Cloud Run service with Secured external access.
user audience must be known the google orange.com, and Not all user has access to Google Orange.com

The diagram of the deployment is presented below:



Objective

The scope of the use-case is to aid the projects be compliant with Orange GCP Security requirements, have a good Security posture, as well as manage the infrastructure in a standardized and trackable manner with Terraform.

Cloud Run is a managed service provided by GCP that allows us to deploy containerised applications. The services (the container images deployed on Cloud Run) have an URL associated with them that is used to access our application. We can lock access to the Cloud Run service using IAM, however this provides limited security.

With this example, we are having addtional security benefits by using external ingress controls, **WAF rules** and **authentication only for authorized internal users**.

- Ingress controls are implemented with the help of an **External HTTPS Load Balancer** that has **Cloud Armor security policies** attached to it, ensuring that only trusted sources can access the load balancer.

- For authenticating only the authorized internal users making requests to the Cloud Run service we are using **Identity Aware Proxy(IAP)**.

Features

The example deploys the following services:

- **Cloud Run Service** with the following configuration:
  - Restricted network access with Internal and Cloud Load Balancing - Accepts requests from an external HTTP(S) load balancer but not directly from the internet.
  - Environment variables fetched from Secret Manager
  - Container images stored in Artifact Registry

- **External HTTPS Load Balancer with Serveless NEG** to route external traffic to the Cloud Run service
  - uses Orange GCP Security compliant SSL Policy
  - uses a Google-managed certificate

- **Internal Identity Aware Proxy** to restrict access only to authenticated internal users

- **Cloud Armor Security Policy** to protect the Cloud Run service against common web attacks and provide layer 7 filtering
  - (Optional) Allow region specific access
  - Preconfigured OWASP Top 10 rules
  - Mitigate Log4J vulnerability

-
  - According to language used to develop your application, the cloud Armor rules may need to be tuned by activating the load balancer logs. otherwise, it may block your users' application.

- **Secret Manager** to store sensitive information needed by the Cloud Run service (i.e API keys, passwords, accounts etc.)

- **Artifact Registry** to store the repo with the Cloud Run docker image

- (Optional) **Serverless VPC Access** to allow the Cloud Run service to connect to a private VPC Network or Google APIs

Gitlab repository

The Terraform code can be found in the following Gitlab repository.

Please refer to the README file for a detailed description of all the deployed resources, as well as the prerequisites and limitations.