Caso Práctico Compute & Redes

Introducción

En este caso práctico, nos enfrentamos a un escenario crucial en la administración de entornos en la nube: la necesidad de proteger nuestro clúster privado de Google Kubernetes Engine (GKE) zonal de accesos no autorizados, al mismo tiempo que permitimos que ciertas aplicaciones sean accesibles desde Internet de forma segura y controlada.

Imagina que eres el responsable de la infraestructura en la nube de una empresa con información sensible. Tu misión es diseñar e implementar una solución que cumpla con los siguientes requisitos:

1. **Máxima Seguridad**: El acceso a nuestro clúster GKE privado debe estar restringido y solo permitido a personal autorizado.
2. **Acceso Controlado**: Se debe establecer un punto de acceso seguro y controlado para interactuar con el clúster privado.
3. **Exposición Selectiva**: Solo ciertas aplicaciones específicas deben ser accesibles desde Internet, y esta exposición debe ser gestionada de forma segura.
4. **Conectividad a Internet**: Las aplicaciones que se ejecutan en el clúster deben poder acceder a Internet para consumir APIs, servicios externos y recursos necesarios para su funcionamiento.

Para lograr estos objetivos, vamos a construir una solución robusta y segura que incluye los siguientes componentes:

- **Bastion Host**: Una máquina virtual (VM) que actuará como nuestro "bastión" de acceso al clúster privado. Esta VM tendrá una dirección IP pública para permitir el acceso SSH desde Internet. Solo se permitirá el acceso al clúster desde esta instancia.

- **Acceso Seguro al Clúster GKE**: El bastión host se configurará con las herramientas necesarias (gcloud y kubectl) para interactuar con el clúster de GKE zonal. El acceso al clúster se realizará de forma segura, utilizando las credenciales y configuraciones apropiadas, y se restringirá el acceso solo al rango de red de la subred del bastión host. No debe usarse autopilot, debe crearse un cluster standard.

- **Clúster GKE Privado**: El clúster se configurará para que tanto los nodos de Kubernetes como los nodos de la API de Kubernetes sean privados, lo que significa que no tendrán direcciones IP públicas.

- **Acceso a Internet desde el cluster**: Se configurará el clúster para que las aplicaciones que se ejecutan en él puedan acceder a Internet de forma segura.

- **Despliegue de Aplicaciones**: Se desplegará una aplicación de ejemplo en el clúster de GKE utilizando una imagen pública (por ejemplo, docker.io/istio/examples-helloworld-v1:1.0 | ficheros aqui https://github.com/istio/istio/blob/master/samples/helloworld/helloworld.yaml | se accede a la <IP>/hello) para verificar el acceso a Internet desde el clúster.

- **Exposición con Load Balancer**: Se configurará un servicio de tipo Load Balancer en el clúster de GKE para exponer la aplicación a Internet. El load balancer enrutará el tráfico al servicio de la aplicación.

Entregables

- Documento con la descripción detallada de los pasos seguidos para completar el ejercicio, incluyendo el direccionamiento IP utilizado para la VPC, las reglas de firewall y el razonamiento detrás de cada componente.
- Archivos de configuración utilizados para crear los recursos en GCP y GKE.
- Demostración del acceso a la aplicación desde Internet a través del load balancer.