UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE INGENIERÍA
ESCUELA DE CIENCIAS Y SISTEMAS
REDES DE COMPUTADORAS 2
ING. MANUEL FERNANDO LÓPEZ
AUXILIARES: EDGAR CIL / RANDY CAN

Proyecto Fase 2

Objetivos

- Conocer las herramientas provistas por los sistemas en la nube para la creación y manejo de Virtual Networks.
- Comprender el funcionamiento de las redes virtuales y como estas permiten la comunicación entre host virtuales.
- Comprender el funcionamiento de las redes privadas y públicas dentro de un ambiente en la nube.
- Utilizar balanceo de carga por software para distribuir el tráfico entre instancias.
- Familiarizarse con Amazon Web Services.
- Conocer e implementar el protocolo de red https.
- Conocer qué es un certificado SSL y su relación con https.
- Conocer e implementar nombres de dominio.
- Crear ACLs para controlar el tráfico en las subredes.
- Configurar Security Group para controlar el tráfico en las instancias.
- Configurar NAT Gateway para permitir el acceso a internet de las instancias de manera segura.

Definición del problema

El país de Ucron ahora cuenta con una página para darse a conocer al mundo; sin embargo, aún no cuentan con la seguridad para prevenir futuros ataques

cibernéticos y el servicio no cumple con la disponibilidad adecuada para cubrir la demanda de peticiones realizadas.

Por ello le solicita nuevamente que realice la configuración necesaria dentro de la nube para salvaguardar la información con la que cuentan dentro de su gobierno y restringir el acceso a la misma utilizando los servicios que proporciona AWS.

Requerimientos

Según lo anterior mencionado se le pide a usted que muestre las páginas web realizadas previamente mediante el uso de EC2 y balanceadores de carga dentro de subredes creadas en AWS. Debe de instalar un servidor HTTP (Ejemplo: Apache2) y reemplazar la vista por default por una página de su diseño personal.

Arquitectura

Para implementar la seguridad requerida se propone la siguiente arquitectura

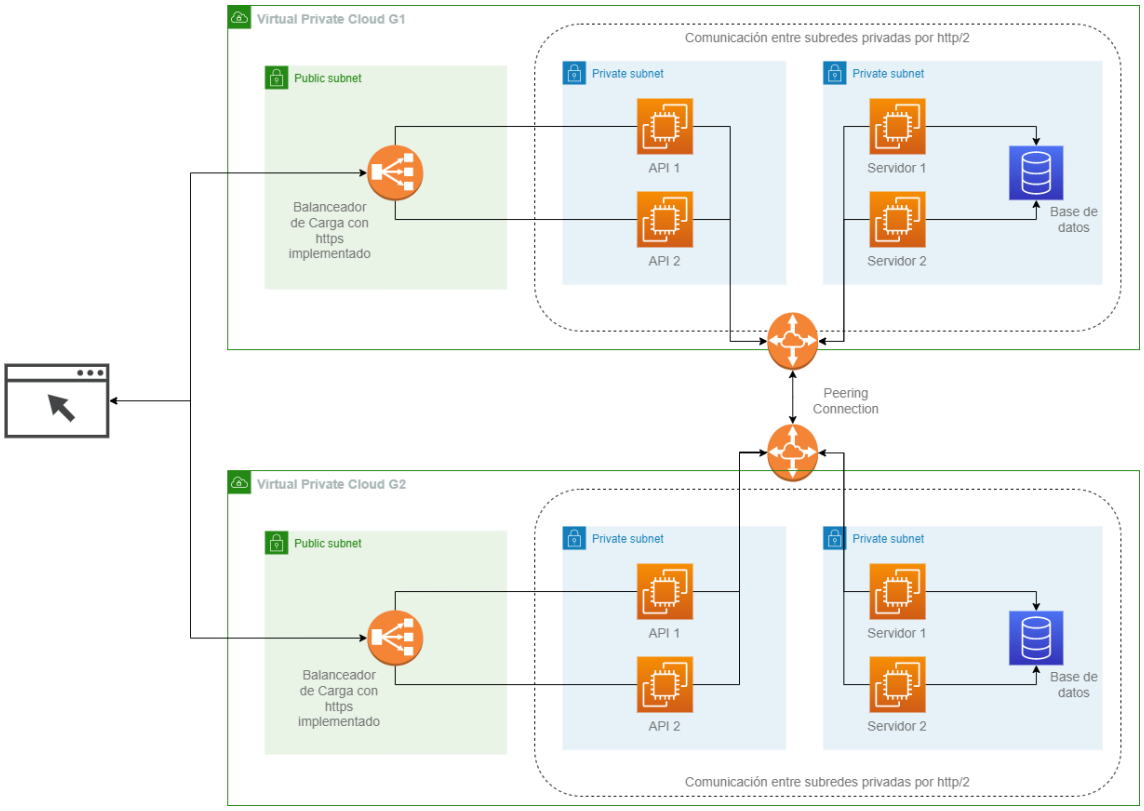

Diagrama de Arquitectura

HTTPS

Para la implementación de https se le recomienda utilizar un certificado gratuito. Puede elegir entre utilizar un certificado de AWS CM o un certificado de Let´s Encrypt.

Seguridad

Se le solicita que proponga y cree las políticas de seguridad para el tráfico a través de la creación de ACLs y/o Security Groups. Este paso es de vital importancia para agregar capas extra de seguridad dentro de la VPC. Debe documentar y justificar las reglas creadas en la documentación (documentar reglas de las ACL utilizadas y puertos expuestos de las instancias EC2 o LoadBalancer).

Nombres de Dominio

También se le solicita crear nombres de dominio, que permitan acceder a la API. Se le socilita un nombre de dominio principal y un nombre de dominio secundario que funcione como un alias para los dominios principales.

- grupo#-fp-api.tk (principal)
- grupo#-de-api.tk (principal)
- grupo#-fp-api.ml (secundario)
- grupo#-de-api.ml (secundario)

La página debe poder ser accedida desde cualquiera de los dos dominios definidos para cada departamento. Debe agregar a la documentación la información relacionada a los registros utilizados para llevar a cabo lo solicitado.

Acceso a internet para las instancias dentro de las subredes privadas

Debido a que las instancias se encuentran en una subred privada, estas no poseen acceso a internet. Esto imposibilita la capacidad de actualizar o instalar paquete en las instancias. Es por ello que se le solicita que agregue un NAT

Gateway, y realice las configuraciones necesarias para garantizar el acceso a internet de manera segura para las instancias.

Restricciones

- El proyecto se realizará en grupos de máximo 4 personas.
- Todos los integrantes del grupo deben tener conocimiento del desarrollo de la práctica.
- Se debe utilizar AWS como proveedor de servicios en la nube.
- Para la calificación se debe de presentar la práctica en una computadora de los integrantes del grupo.
- En el repositorio creado debe crearse una carpeta con nombre PF2 en la cual se irá actualizando el desarrollo del proyecto. Debe de contener como mínimo 2 commits por semana por parte de cada uno de los integrantes del grupo.
- Durante la calificación se preguntará información relevante de la práctica para comprobar la autoría de este.
- El manual técnico debe ser un archivo README del repositorio con el nombre **PF2_Manual_#grupo.md**

Penalizaciones

- Falta de seguimiento de desarrollo continuo por medio de Gitlab o GitHub tendrá una penalización del 10%.
- Falta de seguimiento de instrucciones conforme al método de entrega (nombre del repositorio) tendrá una penalización del 5%.
- Falta de puntualidad conforme a la entrega tendrá una penalización de la siguiente manera:
    - 1 – 10 minutos: 10%
    - 11 – 59 minutos: 30%
    - Pasados 60 minutos tendrá una nota de 0 y no se calificará.

Observaciones

- Proveedor de servicios en la nube: **Amazon Web Services**
- La entrega se realizará por medio de UEDI, cada grupo deberá utilizar el repositorio creado para la práctica 1. Se debe crear una carpeta con el nombre **PF2**.
- Se debe agregar a los auxiliares como colaboradores de este, para poder analizar su progreso.
    - 201503600 (Gitlab y Github)
    - RandyCan2000 (Gitlab y Github)
- Fecha y hora de entrega: **viernes 04 de noviembre, antes de las 18:59 horas.**
- **Las copias serán penalizadas con una nota de 0 y serán sancionados según lo indique el reglamento.**

Entregables

- Enlace al repositorio.
- Manual Técnico.
- Archivos de configuración Nginx.