Nadia Arellano G.
Ingeniera en Informática

Actividad – Sesión 1: Protección de Redes e Infraestructura en la Nube

Eres el administrador de una infraestructura de nube en AWS para una empresa que planea desplegar varias aplicaciones críticas para el negocio. Estas aplicaciones deberán ser accesibles desde internet, pero también requieren comunicación segura entre diferentes servicios dentro de la red privada. La empresa está preocupada por la seguridad y quiere seguir las mejores prácticas recomendadas por AWS.

1. Desarrollo de la infraestructura de red

Parte 1: Creación y configuración de la red.

¿Cómo crearías una VPC (Virtual Private Cloud) para esta infraestructura?
(R). Para crear la VPC utilizaría el terminal de AWS CLI, ejecutando el siguiente comando que crea un entorno lógico aislado con un espacio de direcciones privadas de 10.0.0.0/16.

```
aws ec2 create-vpc --cidr-block 10.0.0.0/16 \--tag-specifications
'ResourceType=vpc,Tags=[{Key=Name,Value=MiVPC}]'
```

¿Cuántas subredes públicas y privadas necesitarías y cómo las distribuirías dentro de la VPC?
(R). Como se debe implementar varias aplicaciones críticas con acceso desde internet y además diferentes servicios internos, realizaría la siguiente estructura de subredes segmentadas por capas que permita aplicar el principio de menor privilegio, usando diferentes zonas para mejorar la resiliencia y 4 subredes como mínimo para balanceo de carga y mejor tolerancia a los fallos.

Subred	Tipo	CIDR	Zona
SubredPublicWeb	Pública	10.0.1.0/24	us-east-1a
SubredPublicWeb	Pública	10.0.2.0/24	us-east-1b
SubredPrivateApp	Privada	10.0.3.0/24	us-east-1c
SubredPrivateBD	Privada	10.0.4.0/24	us-east-1d

¿Cómo configurarías las tablas de enrutamiento para permitir la comunicación entre las subredes privadas y públicas?
(R). Es importante crear como mínimo 2 tablas de enrutamiento, una tabla pública que esté asociada a la subred pública y otra tabla privada que esté asociada a la subred privada. Se debe ejecutar el siguiente comando en la terminal de AWS CLI.

```
aws ec2 associate-route-table --route-table-id rtb-12345678 \
--subnet-id subnet-12345678
```

Nadia Arellano G.
Ingeniera en Informática

Parte 2: Gestión del Tráfico

¿Qué tipo de gateways utilizarías para asegurar que las subredes privadas tengan acceso a internet? Explica cómo usarías un Internet Gateway y un NAT Gateway en la infraestructura.
(R). Utilizaría dos tipos de gateways: Internet Gateway (IGW) asociado a la VPC y que permitirá el acceso directo a internet de las subredes públicas. Además, utilizaría un NAT Gateway que se ubicará en una subred pública con el objetivo de dar acceso a internet a las subredes privadas sin exponerlas directamente.

¿Qué configuraciones realizarías en los grupos de seguridad y ACLs para permitir uacceso controlado a los servicios?
(R). En los Grupos de Seguridad, configuraría que el servidor web permita tráfico HTTP/HTTPS desde 0.0.0.0/0. El servidor de aplicación sólo permitiría tráfico desde el grupo de seguridad del servidor web y la base de datos sólo desde el grupo de seguridad de la aplicación. En las ACLs definiría reglas específicas para IP, puerto y protocolo, bloqueando por defecto el tráfico no deseado.

¿Qué políticas de tráfico de entrada y salida definirías para las subredes públicas y privadas?
(R). Para asegurar que las subredes públicas puedan recibir tráfico web externo de usuarios y que las subredes privadas no queden expuestas, pero si puedan comunicarse internamente con los servicios necesarios, definiría la siguiente política de tráfico de entrada y salida:

Subred	Entrada	Salida
Pública	Permitir HTTP (80), HTTPS (443), SSH (22) solo desde IP confiables	Permitir todo tráfico saliente
Privada	Permitir tráfico sólo desde la subred pública (por puertos internos necesarios)	Permitir salidas a internet vía NAT Gateway

Parte 3: Buenas Prácticas de Seguridad

Menciona al menos tres buenas prácticas para la segmentación y la seguridad de las redes dentro de AWS.
(R). Principio de menor privilegio: Cada recurso debe tener sólo los permisos mínimos necesarios.
Uso de subredes separadas: Separa los recursos en subredes públicas y privadas según su exposición y función, por ejemplo, servidores web en subredes públicas y base de datos en subredes privadas.
Monitoreo y logging: Habilitar las herramientas de AWS llamadas: VPC Flow Logs para revisar y auditar el tráfico de red y AWS CloudTrail para registrar todas las acciones realizadas sobre la infraestructura.

Nadia Arellano G.
Ingeniera en Informática

¿Cómo garantizarías que los datos sensibles dentro de la red privada estén protegidos y no sean accesibles por servicios no autorizados?
(R). Para garantizar protección a los datos sensibles dentro de la red privada, aplicaría las siguientes medidas: alojarlos en subredes privadas, sin acceso directo a internet. Usaría grupos de seguridad específicos, que solo permitan el tráfico desde servicios autorizados y limitando el tráfico en las ACLs. Habilitaría cifrado en reposo y cifrado en tránsito para proteger la información durante la transmisión y gestionaría identidades y permisos IAM para asegurar que sólo los roles o usuarios con permisos mínimos puedan acceder a esos datos.

2. Entrega del diseño y justificación

(R). Como recién egresada de Ingeniería en Informática, estoy comenzando a interiorizarme en el mundo de la seguridad en la nube gracias a este bootcamp intensivo. Este diseño está pensado para ser seguro, funcional y ordenado, aunque es mi primer acercamiento al tema, la presentación entregada y la guía del módulo fueron mi base para aplicar estas buenas prácticas.

Las decisiones que tomé al diseñar la infraestructura solicitada en el estudio del caso son las siguientes:
Subredes, infraestructura: Opté por crear una VPC con tres subredes (Dos privadas para servicios internos y Base de Datos y una pública para aplicaciones accesibles desde internet). Esta segmentación se basa en el principio de separación por función, lo que permite mayor control y seguridad sobre cada capa de la aplicación.
Gateways: acceso a internet controlado: Implementé dos tipos de gateways (Internet Gateway y NAT Gateway), esto ayuda a mantener la privacidad de los servicios interno y evita riesgos innecesarios.
Tablas de enrutamiento: Asocié una tabla de enrutamiento diferente a cada tipo de subred (subred pública con Internet Gateway y subredes privadas con NAT Gateway). Así, cada subred tiene el nivel de acceso adecuado y se evita que servicios sensibles queden expuestos directamente.
Grupos de Seguridad y ACLs: En los Grupos de Seguridad, configuré reglas estrictas, por ejemplo: El servidor web acepta tráfico HTTP y HTTPS y la BD sólo acepta tráfico desde el servidor de aplicación. En las ACLs, reforcé estos controles a nivel de subred, permitiendo únicamente el tráfico esencial. Esto responde a la buena práctica del principio de menor privilegio: cada componente sólo puede hacer lo que necesita, nada más.