Nadia Arellano G.
Ingeniera en Informática

Actividad – Sesión 2: Redes Públicas y Privadas en la Nube

Eres el encargado de configurar la infraestructura de red para una pequeña empresa de tecnología que necesita garantizar la conectividad segura y eficiente de sus servicios internos y externos. La empresa cuenta con una aplicación web que debe ser accesible desde Internet y un sistema interno de gestión que solo puede ser accedido desde la red privada.

Requerimientos técnicos:

1. **Diseño de la Red**
   (R). Configuraré dos subredes públicas para la aplicación web, con el fin de que sea accesible desde internet para los usuarios externos. Sus principales características serán:
   - Se asociarán a una tabla de enrutamiento con acceso al Internet Gateway (IGW).
   - Las instancias dentro de estas subredes pueden tener IP pública o una Elastic IP.
   - Permitirán publicar API externas.

   Configuraré también dos subredes privadas para el sistema interno de gestión, el que no debe estar expuesto a Internet. Sus principales características serán:
   - No tendrán acceso directo a Internet.
   - Cuando requieran conexión a internet por ejemplo para alguna actualización, se habilitará el acceso a través de un NAT Gateway.
   - Tendrán accesibilidad sólo desde la red interna o a través de una conexión segura desde la subred pública.

2. **Asignación de Direcciones IP**
   (R). Para las subredes públicas, se asignarán IP públicas o Elastic IPs a las instancias que deben ser accesibles desde Internet.
   Para las subredes privadas, se asignarán sólo direcciones IP privadas, las cuales no son accesibles directamente desde Internet. Estas IPs se asignan automáticamente desde el rango CIDR definido para las subredes.

3. **Configuración de Conectividad**
   (R). En las subredes públicas se configurará un NAT Gateway con el fin de permitir que los recursos en las subredes privadas puedan acceder a internet sin quedar expuestos. Se asignará también una Elastic IP al NAT Gateway para su funcionamiento, esto garantizará una salida estable a internet. Además, los recursos en las subredes públicas utilizarán Elastic IPs si requieren disponibilidad constante desde el exterior.

4. **Políticas de Acceso y Control**
   (R). La aplicación web se encontrará en dos subredes públicas con un grupo de seguridad que permitirá tráfico HTTP/HTTPS desde internet, aplicando el principio de menor privilegio para limitar accesos sólo a los puertos necesarios. El sistema interno

estará en unas subredes privadas con reglas que restringirán el acceso únicamente a conexiones internas autorizadas, impidiendo cualquier entrada directa desde internet.

5. **Configuración de Grupos de Seguridad y ACLs**
   (R). Se configurarán grupos de seguridad específicos para cada tipo de recurso:
   - La aplicación web permite únicamente tráfico HTTP/HTTPS desde internet.
   - El sistema interno aceptará conexiones sólo desde la subred pública o direcciones internas autorizadas.

   Además, se definirán Listas de Control de Acceso (ACLs) a nivel de subredes para reforzar el aislamiento y controlar el tráfico de entrada y salida, sin interferir con la operación de los servicios.

6. **Balance entre Seguridad y Rendimiento**
   (R). Se optimizarán las reglas de acceso para que sean específicas, pero no excesivas, para evitar cuellos de botella. También, se aplicarán medidas de seguridad como grupos de seguridad, ACLs y segmentación de red sin sobrecargar la infraestructura. Esto permitirá mantener el rendimiento de la red fluido, garantizando también un entorno protegido.

Diagrama de la Arquitectura Propuesta

(R). El siguiente esquema (**Imagen_1**), muestra la infraestructura de red propuesta en AWS. Se identifican los componentes principales que serán utilizados para segmentar y proteger los servicios de la aplicación web pública y del sistema interno privado. Se muestra también, los mecanismos de seguridad que se aplicarán para garantizar una operación segura y eficiente.

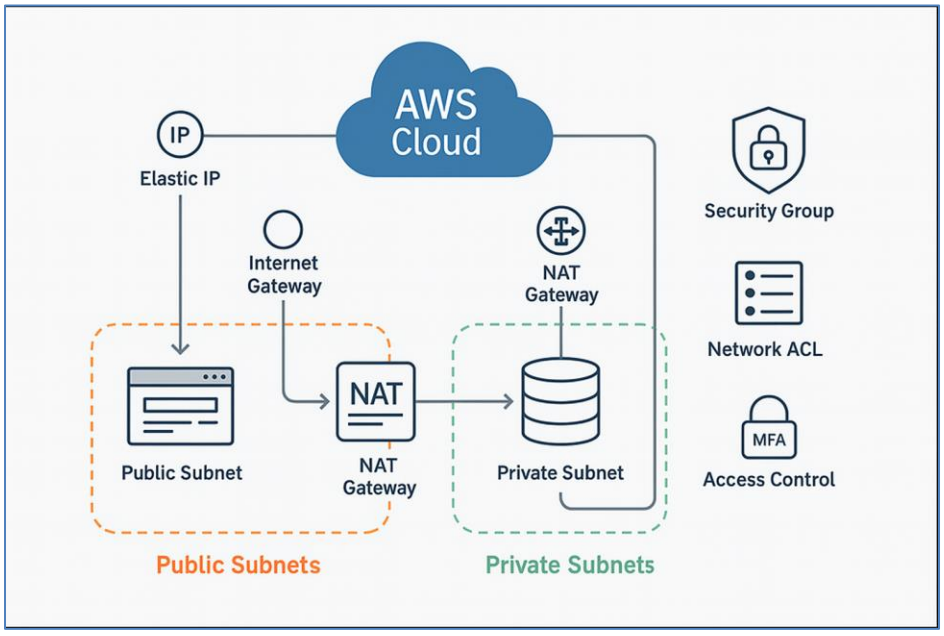

Imagen_1: Diagrama de la red que muestra la estructura propuesta.

Nadia Arellano G.
Ingeniera en Informática