Laboratorio #4

Amazon EC2 y Seguridad de Red

Proyecto:
Laboratorios Virtuales de Redes en AWS para el
Fortalecimiento de Competencias en Redes de Nueva Generación

Estudiantes:
Nicolás Carreño Tascón
Juan Manuel Canchala Jiménez

Director:
Carlos Olarte

Asignatura:
Redes de Nueva Generación

Duración Estimada: 120 minutos
Costo: \$0.00 (100 % Gratuito - Free Tier)

Diciembre 2025

Índice

Resumen

En este laboratorio se introducen de forma práctica los conceptos fundamentales de **Amazon EC2 (Elastic Compute Cloud)** y su integración con los mecanismos de **seguridad de red** de AWS. El objetivo es que el estudiante sea capaz de lanzar una instancia EC2 `t2.micro` o `t3.micro` dentro del Free Tier, configurar correctamente los **Security Groups** (grupos de seguridad) y las **Network ACLs** (Listas de Control de Acceso a la Red), comprender la diferencia entre mecanismos *stateful* y *stateless*, aplicar mejores prácticas de seguridad y conectarse de forma segura vía SSH.

El laboratorio se desarrolla sobre la VPC creada en laboratorios anteriores, utilizando subredes públicas para exponer un servidor y aplicando controles de seguridad en varias capas. Se enfatiza el uso responsable del Free Tier, las 750 horas/mes disponibles para instancias de tipo `t2.micro/t3.micro`, y la importancia de diseñar reglas de acceso mínimas y específicas. Al finalizar, el estudiante habrá implementado una arquitectura básica pero realista de cómputo en la nube, protegida mediante políticas de red adecuadas.

Palabras clave: Amazon EC2, Security Groups, Network ACLs, Stateful, Stateless, SSH, Free Tier, Seguridad en la Nube.

1 Objetivos

1.1 Objetivo General

Proporcionar al estudiante una comprensión práctica y detallada de Amazon EC2 y de los mecanismos de seguridad de red asociados (Security Groups y Network ACLs), permitiéndole lanzar instancias de cómputo en la nube de forma segura, controlada y alineada con las mejores prácticas de la industria.

1.2 Objetivos Específicos

- Lanzar una instancia EC2 `t2.micro` o `t3.micro` aprovechando el Free Tier de AWS.
- Configurar **Security Groups** para controlar tráfico inbound y outbound hacia la instancia.
- Comprender las diferencias entre **Security Groups** y **Network ACLs** y cuándo usar cada uno.
- Explicar y ejemplificar la diferencia entre **mecanismos stateful y stateless** en la seguridad de red.
- Aplicar **mejores prácticas de seguridad**: principio de mínimo privilegio, bastion hosts, restricciones por IP, cierre de puertos innecesarios.
- Conectarse a la instancia EC2 vía **SSH** desde un equipo local siguiendo un flujo seguro.
- Verificar el correcto funcionamiento de las configuraciones de red y seguridad mediante pruebas de conectividad.

1.3 Competencias a Desarrollar

- **Administración de Cómputo en la Nube:** Capacidad para desplegar y gestionar instancias EC2.
- **Diseño de Políticas de Seguridad de Red:** Definición y aplicación de reglas de acceso con Security Groups y NACLs.
- **Diagnóstico de Conectividad:** Habilidad para identificar y resolver problemas de acceso causados por reglas de red.
- **Seguridad Operacional:** Uso de claves SSH, restricciones por IP y prácticas seguras para administración remota.

2 Marco Teórico

2.1 Introducción a Amazon EC2

Amazon EC2 (*Elastic Compute Cloud*) es el servicio de cómputo bajo demanda de AWS que permite lanzar instancias (máquinas virtuales) con diferentes capacidades de CPU, memoria, almacenamiento y red. EC2 es un componente central en la mayoría de arquitecturas en la nube, ya que ofrece flexibilidad, escalabilidad y un modelo de pago por uso.

2.1.1. Componentes Clave de EC2

- **Instancias:** máquinas virtuales que ejecutan un sistema operativo (Linux, Windows, etc.).
- **Amazon Machine Image (AMI):** plantilla que contiene el sistema operativo y, opcionalmente, software preinstalado.
- **Tipos de instancia:** combinaciones de CPU, memoria y red (por ejemplo: `t2.micro`, `t3.micro`, `m5.large`, etc.).
- **Almacenamiento:** típicamente volúmenes EBS (Elastic Block Store) asociados a las instancias.
- **Key pairs:** par de claves (pública/privada) utilizados para autenticación vía SSH en instancias Linux.
- **Regiones y Zonas de Disponibilidad (AZs):** ubicación física de los recursos.

2.1.2. Tipos de Instancia y Free Tier

Las instancias `t2.micro` o `t3.micro` son tipos de instancia de uso general que pueden ser elegibles para el nivel gratuito de AWS (Free Tier). El Free Tier incluye típicamente:

- **750 horas/mes** de uso combinado de instancias `t2.micro` o `t3.micro`.
- Si se usan varias instancias, la suma de sus horas no debe superar las 750 horas mensuales para mantener el costo en $0.00.

2.2 Security Groups

Los **Security Groups (SG)** son firewalls virtuales *stateful* que operan a nivel de instancia. Cada instancia EC2 asociada a un SG solo permite el tráfico que concuerda con las reglas del grupo de seguridad.

2.2.1. Características de los Security Groups

- Operan a nivel de **instancia**, no de subred.
- Son **stateful**: si se permite tráfico entrante, las respuestas se permiten automáticamente, aunque no haya reglas explícitas para el tráfico saliente y viceversa.
- Las reglas se definen en términos de:
  - Protocolo (TCP, UDP, ICMP).
  - Puerto o rango de puertos.
  - Origen/Destino (CIDR, otra SG, etc.).
- Las reglas son por defecto **permisivas**: se definen *permitir* (Allow), no existe un *deny* explícito. Todo lo que no está permitido se bloquea implícitamente.

2.2.2. Ejemplos Comunes de Reglas en SG

- Permitir SSH (puerto 22) únicamente desde la IP pública del administrador.
- Permitir HTTP (80) y HTTPS (443) desde `0.0.0.0/0` para servidores web públicos (solo en entornos de prueba y con cuidado).
- Permitir acceso a base de datos (por ejemplo, puerto 3306) solo desde un SG de aplicación, nunca desde internet.

2.3 Network ACLs (NACLs)

Las **Network ACLs** son listas de control de acceso que operan a nivel de subred dentro de una VPC. Proporcionan una capa adicional de seguridad y pueden permitir o denegar tráfico explícitamente.

2.3.1. Características de las NACLs

- Operan a nivel de **subred**.
- Son **stateless**: las reglas de entrada y salida son independientes; se deben configurar explícitamente ambas direcciones.
- Las reglas se evalúan en orden según un número (rule number) y se detiene en la primera coincidencia.
- Permiten reglas **Allow** y **Deny**.
- Cada subred debe estar asociada a una única NACL.

2.4 Stateful vs Stateless

- **Stateful (Security Groups):**
  - El sistema **recuerda** el estado de la conexión.
  - Si un paquete entrante está permitido, la respuesta saliente se permite automáticamente.
  - Simplifica la configuración de reglas de retorno.
- **Stateless (NACLs):**
  - El sistema **no recuerda** el estado.
  - Se deben definir reglas para tráfico entrante y saliente de forma separada.
  - Requiere mayor cuidado para no bloquear respuestas legítimas.

2.5 Mejores Prácticas de Seguridad para EC2

- **Principio de mínimo privilegio:** abrir solo los puertos estrictamente necesarios, hacia las direcciones mínimas posibles.
- **SSH restringido:** no permitir SSH desde `0.0.0.0/0`. Limitar por dirección IP pública o utilizar un bastion host.
- **Uso de claves SSH:** evitar contraseñas débiles; preferir autenticación por clave pública/privada.
- **Separación de capas:** colocar servidores públicos en subredes públicas y servidores internos (aplicaciones, bases de datos) en subredes privadas.
- **Monitoreo:** habilitar logs y métricas para detectar intentos de acceso no autorizados.
- **Parcheo y actualización:** mantener el sistema operativo y servicios actualizados.

3 Requisitos Previos

3.1 Conocimientos Necesarios

- Haber completado los laboratorios 1–3 (cuenta, IAM, VPC, subredes, IGW).
- Conocimientos básicos de:
  - Sistemas operativos Linux.
  - Uso de terminal y comandos básicos.
  - Conceptos de red (IP, puertos, protocolos).

3.2 Recursos Técnicos Requeridos

- Cuenta AWS activa con Free Tier.
- Usuario IAM con permisos suficientes sobre EC2 y VPC.
- Navegador web moderno (Chrome, Firefox, etc.).
- Cliente SSH:
  - Linux/macOS: OpenSSH.
  - Windows: PuTTY o cliente SSH integrado de Windows 10+.

3.3 Costos Estimados

Concepto	**Costo Estimado**
Instancia EC2 t2.micro/t3.micro (¡= 120 min)	$0.00 (dentro de 750 horas/mes)
VPC, Subredes, IGW, Tablas de Rutas	$0.00
Security Groups y NACLs	$0.00
Almacenamiento EBS (8 GB estándar)	$0.00 (dentro del Free Tier)
TOTAL (Laboratorio)	**$0.00**

Cuadro 1: Costos del Laboratorio 4 en modo práctico

3.4 Tiempo Estimado

- Revisión de marco teórico: 20–25 minutos.
- Lanzar y configurar instancia EC2: 40–45 minutos.
- Configurar Security Groups y NACLs: 25–30 minutos.
- Pruebas de conectividad y limpieza: 20–25 minutos.
- **TOTAL ESTIMADO:** 120 minutos.

4 Procedimiento Paso a Paso

4.1 Paso 1: Seleccionar Región y Preparar Entorno

Objetivo: Asegurar que los recursos se creen en la región adecuada y sobre la VPC existente de laboratorios previos.

1. Iniciar sesión en la consola de AWS con un usuario IAM administrativo.
2. Verificar la región seleccionada en la esquina superior derecha (por ejemplo, `us-east-1` o `sa-east-1`).
3. Verificar que la VPC creada en el Lab 2 está disponible y que existe al menos una subred pública con acceso a internet mediante IGW (Lab 3).

4.2 Paso 2: Crear o Verificar un Key Pair

Objetivo: Disponer de un par de claves para acceso SSH a la instancia EC2.

1. En la consola AWS, ir a **EC2** → **Key pairs**.
2. Si ya existe un key pair adecuado para esta región y laboratorio, tomar nota de su nombre y ubicación del archivo `.pem` (o `.ppk` en PuTTY).
3. Si no existe:
   - 3.1. Hacer clic en **Create key pair**.
   - 3.2. Name: `lab4-ec2-key`.
   - 3.3. Key pair type: `RSA`.
   - 3.4. Private key file format:
     - `.pem` si se usará OpenSSH.
     - `.ppk` si se usará PuTTY (o convertir posteriormente).
   - 3.5. Hacer clic en **Create key pair**.
   - 3.6. Guardar el archivo de clave privada en un lugar seguro en el equipo local.

4.3 Paso 3: Lanzar una Instancia EC2 (Free Tier)

Objetivo: Lanzar una instancia `t2.micro` o `t3.micro` en una subred pública.

1. En el servicio **EC2**, hacer clic en **Instances** → **Launch instances**.
2. **Nombre de la instancia:** `lab4-web-server`.
3. **AMI (Amazon Machine Image):**
   - Seleccionar `Amazon Linux 2` (Free Tier eligible).
4. **Tipo de instancia:**

- Seleccionar `t2.micro` o `t3.micro` (indicadas como Free Tier eligible).

5. **Key pair:**
   - En **Key pair (login)**, seleccionar `lab4-ec2-key` (u otro par existente).
6. **Configuración de red:**
   - VPC: seleccionar la VPC creada en el Lab 2 (por ejemplo, `MiVPC-Lab2`).
   - Subnet: elegir una **subred pública** (por ejemplo, `Public-Subnet-AZ1`).
   - Auto-assign public IP: **Enable** (necesario para acceso SSH desde internet).
7. **Firewall (Security Group):**
   - Seleccionar **Create security group**.
   - Security group name: `SG-Lab4-Web`.
   - Description: `SG para servidor web del Lab 4`.
   - Inbound rules (inicialmente):
     - Tipo: `SSH`, Puerto: 22, Origen: `My IP` (IP pública del estudiante).
     - Opcional: Tipo: `HTTP`, Puerto: 80, Origen: `0.0.0.0/0` (solo si se desea probar un servidor web SIMPLE).
   - Outbound rules:
     - Dejar el valor por defecto (`All traffic` hacia `0.0.0.0/0`) para facilitar el laboratorio.
8. **Almacenamiento:**
   - Volume type: `gp2` o `gp3`, tamaño 8 GB (dentro del Free Tier).
9. Revisar la configuración y hacer clic en **Launch instance**.
10. Esperar a que el estado de la instancia cambie a **running** y los *status checks* estén en **2/2 checks passed**.

4.4 Paso 4: Configuración de Security Groups (Inbound/Outbound)

Objetivo: Ajustar las reglas del Security Group según mejores prácticas.

1. En EC2, hacer clic en **Instances**, seleccionar `lab4-web-server`.
2. En la pestaña **Security**, identificar el `SG-Lab4-Web` y hacer clic en su ID.
3. **Inbound rules:**
   - Mantener:
     - SSH (22) con origen `My IP` (no `0.0.0.0/0`).

- Opcional: HTTP (80) desde `0.0.0.0/0` solo para pruebas temporales de un servidor web, dejando claro que en producción se debe restringir según sea necesario.

4. **Outbound rules:**
   - Permitir `All traffic` hacia `0.0.0.0/0` para que la instancia pueda actualizar paquetes, descargar software, etc.
   - En entornos más estrictos, estas reglas podrían limitarse a puertos específicos (por ejemplo, 80/443).

4.5 Paso 5: Configuración de Network ACLs

Objetivo: Revisar y, opcionalmente, ajustar las NACLs asociadas a la subred pública.

1. Ir a **VPC** → **Subnets**, seleccionar la subred pública donde se lanzó la instancia.
2. Revisar la **Network ACL** asociada:
   - Por defecto, la NACL `default` suele permitir todo el tráfico inbound y outbound.
3. Opcionalmente, crear una NACL más restrictiva:
   3.1. **Network ACLs** → **Create network ACL**.
   3.2. Name: `NACL-Public-Lab4`.
   3.3. VPC: VPC del laboratorio.
   3.4. Crear la NACL.
4. Definir reglas de ejemplo:
   - Inbound:
     - Permitir SSH (22) desde la IP del estudiante.
     - Permitir HTTP (80) desde `0.0.0.0/0` (si se usa).
     - Permitir puertos efímeros de retorno (por ejemplo, 1024–65535) desde `0.0.0.0/0`.
   - Outbound:
     - Permitir todo el tráfico hacia `0.0.0.0/0` (para el laboratorio).
5. Asociar la NACL a la subred pública utilizada por la instancia.

4.6 Paso 6: Conexión a la Instancia vía SSH

Objetivo: Verificar que la instancia es accesible de forma segura mediante SSH.

Desde Linux/macOS (OpenSSH)

1. En la consola de EC2, copiar la **IPv4 Public IP** de `lab4-web-server`.
2. En el equipo local:
   2.1. Abrir una terminal.
   2.2. Ubicarse en el directorio donde está el archivo de clave privada `lab4-ec2-key.pem`.
   2.3. Asegurar permisos correctos del archivo:

```
chmod 400 lab4-ec2-key.pem
```

Listing 1: Comando para asegurar permisos de la clave privada

   2.4. Conectarse vía SSH:

```
ssh -i lab4-ec2-key.pem ec2-user@IP_PUBLICA
```

Listing 2: Conexión SSH desde Linux/macOS

   2.5. Aceptar la huella (fingerprint) del servidor cuando se pregunte.

Desde Windows con cliente SSH integrado (Windows 10+)

1. Abrir **PowerShell** o **CMD**.
2. Navegar al directorio donde está `lab4-ec2-key.pem`.
3. Ejecutar:

```
ssh -i .\lab4-ec2-key.pem ec2-user@IP_PUBLICA
```

Listing 3: Conexión SSH desde Windows 10+

4. Aceptar la huella del servidor.

Prueba de conectividad dentro de la instancia

Una vez conectado:

1. Verificar la conectividad a internet:

```
ping -c 3 www.google.com
```

Listing 4: Prueba de conectividad desde la instancia

2. Actualizar paquetes (ejemplo en Amazon Linux 2):

```
sudo yum update -y
```

Listing 5: Actualizar paquetes del sistema

4.7 Paso 7: Pruebas de Seguridad (Stateful vs Stateless)

Objetivo: Observar efectos de reglas en SG y NACLs.

1. **Prueba con SG:**
   - Eliminar temporalmente la regla SSH en `SG-Lab4-Web`.
   - Intentar conectar nuevamente por SSH desde el equipo local (debe fallar).
   - Volver a agregar la regla SSH y verificar que la conexión vuelve a funcionar.
2. **Prueba con NACL:**
   - En la NACL asociada a la subred, añadir una regla **Deny** para tráfico entrante en puerto 22 desde cualquier origen.
   - Intentar conectarse por SSH (fallará aunque el SG lo permita, demostrando que las NACLs también influyen).
   - Eliminar la regla Deny para restaurar el acceso.

4.8 Paso 8: Reflexión sobre Mejores Prácticas

- Identificar qué puertos quedaron abiertos y justificar su necesidad.
- Evaluar si se usó la IP pública correcta para restringir SSH.
- Considerar la introducción de un bastion host en un diseño más avanzado (acceso indirecto a instancias privadas).

5 Tablas de Configuración

5.1 Configuración de la Instancia EC2

Parámetro	Valor
Nombre	lab4-web-server
AMI	Amazon Linux 2 (Free Tier eligible)
Tipo de instancia	t2.micro o t3.micro
VPC	VPC del laboratorio (Lab 2)
Subred	Subred pública (Lab 3)
IP pública	Asignada automáticamente
Key pair	lab4-ec2-key
Security Group	SG-Lab4-Web
Almacenamiento	8 GB gp2/gp3

Cuadro 2: Configuración de la instancia EC2 del Laboratorio 4

5.2 Reglas del Security Group SG-Lab4-Web

Dirección	Protocolo	Puerto	Origen/Destino
Inbound	TCP	22 (SSH)	IP pública del estudiante
Inbound (opcional)	TCP	80 (HTTP)	0.0.0.0/0
Outbound	All	All	0.0.0.0/0

Cuadro 3: Reglas de ejemplo para el Security Group SG-Lab4-Web

5.3 Ejemplo de Reglas en NACL Pública

# Regla	Dirección	Protocolo	Puerto	Acción / Origen/Destino
100	Inbound	TCP	22	Allow desde IP del estudiante
110	Inbound	TCP	80	Allow desde 0.0.0.0/0
120	Inbound	TCP	1024-65535	Allow desde 0.0.0.0/0
100	Outbound	All	All	Allow hacia 0.0.0.0/0

Cuadro 4: Ejemplo de reglas en NACL para la subred pública

6 Verificación

6.1 Verificación de la Instancia EC2

1. En **EC2** → **Instances** verificar que `lab4-web-server` está en estado **running**.
2. Asegurarse de que los *status checks* están en **2/2 checks passed**.

6.2 Verificación de Conectividad SSH

1. Conectarse vía SSH usando el comando correspondiente (Linux/macOS/Windows).
2. Confirmar que el prompt muestra `ec2-user@ip-...`.
3. Ejecutar comandos básicos:

```
whoami
hostname
ip addr
```

Listing 6: Comandos básicos de verificación

6.3 Verificación de Reglas de Seguridad

1. **Acceso permitido:**
   - Desde la IP configurada en SG y NACL, la conexión SSH funciona.
2. **Acceso denegado:**
   - Cambiar temporalmente de red o IP y verificar que el acceso se bloquea.
   - Introducir una regla **Deny** en NACL y observar su efecto.

7 Limpieza de Recursos

Objetivo: Evitar costos innecesarios después del laboratorio.

1. **Instancia EC2:**
   - En **EC2** → **Instances**, seleccionar `lab4-web-server`.
   - Hacer clic en **Instance state** → **Terminate instance**.
   - Confirmar la terminación.
2. **Volúmenes EBS:**
   - Verificar en **EC2** → **Volumes** que el volumen asociado a la instancia se eliminó (según la política por defecto).
3. **Security Groups y NACLs:**
   - Si se crearon exclusivamente para el laboratorio y no se utilizarán más, eliminarlos una vez que no estén asociados a recursos.
4. **Key pair:**
   - Mantener el key pair si se usará en laboratorios posteriores.
   - En caso de no necesitarlo, puede eliminarse desde **EC2** → **Key pairs**.

8 Cuestionario de Evaluación

8.1 Preguntas de Selección Múltiple

1. **¿Cuál es la función principal de Amazon EC2?**

   a) Proveer almacenamiento de objetos.

   b) Proveer máquinas virtuales bajo demanda para ejecutar aplicaciones.

   c) Administrar bases de datos relacionales.

   d) Gestionar usuarios e identidades en AWS.

2. **¿Qué tipo de instancia es elegible para el Free Tier en este laboratorio?**

   a) `m5.large`

   b) `r5.xlarge`

   c) `t2.micro` o `t3.micro`

   d) `p3.2xlarge`

3. **¿Cuántas horas al mes de uso de instancias `t2.micro/t3.micro` típicamente permite el Free Tier?**

   a) 100 horas/mes

   b) 750 horas/mes

   c) 1000 horas/mes

   d) 24 horas/mes

4. **Los Security Groups en AWS son:**

   a) Firewalls *stateless* aplicados a nivel de subred.

   b) Firewalls *stateful* aplicados a nivel de instancia.

   c) Listas de control de acceso para S3.

   d) Herramientas para cifrar volúmenes EBS.

5. **Las Network ACLs (NACLs) se caracterizan por:**

   a) Ser *stateful* y aplicarse a instancias.

   b) Ser *stateless* y aplicarse a subredes.

   c) Solo permitir reglas de tipo Allow.

   d) No afectar el tráfico dentro de una VPC.

6. **En un mecanismo de seguridad *stateful*:**

   a) Se deben configurar reglas de respuesta explícitas para cada conexión.

   b) El sistema recuerda el estado de la conexión y permite las respuestas automáticamente.

c) No se permite el tráfico de retorno.

d) Solo se evalúan las reglas outbound.

7. **¿Cuál es la mejor práctica para permitir acceso SSH a una instancia EC2?**

   a) Permitir SSH (22) desde `0.0.0.0/0`.

   b) Permitir SSH solo desde la IP pública del administrador o desde un bastion host.

   c) Deshabilitar SSH completamente.

   d) Permitir SSH desde cualquier red privada.

8. **Si un Security Group permite tráfico SSH desde la IP del estudiante, pero la NACL asociada a la subred deniega puerto 22, el resultado será:**

   a) El tráfico se permite porque el Security Group tiene prioridad.

   b) El tráfico se deniega porque la NACL bloquea el puerto 22.

   c) El tráfico se permite solo la primera vez.

   d) El tráfico no se ve afectado por la NACL.

9. **¿Qué componente es necesario para que una instancia en subred pública tenga acceso a internet?**

   a) NAT Gateway

   b) Internet Gateway (IGW) asociado a la VPC y ruta por defecto

   c) VPC Peering

   d) Transit Gateway

10. **La clave privada de un key pair de EC2 debe:**

    a) Compartirse con todos los miembros del equipo para facilitar acceso.

    b) Subirse como archivo público a un repositorio git.

    c) Mantenerse segura en el equipo local y no compartirse.

    d) Guardarse dentro de la instancia EC2 para facilitar el login.

8.2 Preguntas Verdadero/Falso

VF1. Un Security Group puede contener tanto reglas inbound como outbound, y todo tráfico no permitido explícitamente es bloqueado por defecto.

VF2. Las Network ACLs solo se aplican al tráfico que va hacia internet, no al tráfico dentro de la VPC.

VF3. En el Free Tier, si se lanzan dos instancias `t2.micro` de forma simultánea durante todo el mes, se corre el riesgo de superar las 750 horas gratuitas.

8.3 Escenarios Prácticos

E1. Escenario 1: Conexión SSH bloqueada

Has lanzado una instancia EC2 y configurado un Security Group permitiendo SSH (22) desde tu IP. Sin embargo, no puedes conectarte via SSH. Lista al menos tres posibles causas relacionadas con Security Groups, NACLs o configuración de red, y cómo las verificarías/corregirías.

E2. Escenario 2: Servidor web accesible desde cualquier lugar

Has configurado un servidor web en la instancia EC2 con HTTP (80) abierto a `0.0.0.0/0` en el Security Group. La empresa ahora exige restringir el acceso solo a un conjunto de direcciones IP corporativas. Describe los cambios que realizarías en el Security Group y cómo probarías que la restricción funciona correctamente.

8.4 Respuestas del Cuestionario

Selección Múltiple

1. **b)** Proveer máquinas virtuales bajo demanda para ejecutar aplicaciones.
2. **c)** `t2.micro` o `t3.micro`.
3. **b)** 750 horas/mes.
4. **b)** Firewalls *stateful* aplicados a nivel de instancia.
5. **b)** Ser *stateless* y aplicarse a subredes.
6. **b)** El sistema recuerda el estado de la conexión y permite las respuestas automáticamente.
7. **b)** Permitir SSH solo desde la IP pública del administrador o desde un bastion host.
8. **b)** El tráfico se deniega porque la NACL bloquea el puerto 22.
9. **b)** Internet Gateway (IGW) asociado a la VPC y ruta por defecto.
10. **c)** Mantenerse segura en el equipo local y no compartirse.

Verdadero/Falso

1. **Verdadero.** Los Security Groups permiten solo el tráfico definido; no hay reglas de Deny explícitas, pero todo lo no permitido se bloquea.
2. **Falso.** Las NACLs se aplican al tráfico que entra y sale de las subredes, incluyendo tráfico interno dentro de la VPC.
3. **Verdadero.** Dos instancias ejecutadas simultáneamente 24/7 sumarían 2 x 720 horas aprox., superando las 750 horas/mes.

Guía para Escenarios

Escenario 1: Conexión SSH bloqueada
Posibles causas y soluciones:

- **Security Group sin regla SSH correcta:**
  - Verificar que el SG asociado a la instancia tiene una regla inbound:
    - Protocolo: TCP, Puerto: 22.
    - Origen: IP pública actual del estudiante.
  - Corregir la regla si el origen es incorrecto (por ejemplo, estaba `My IP` anterior).
- **NACL denegando puerto 22:**
  - Revisar la NACL asociada a la subred.

- Verificar si existe alguna regla **Deny** para puerto 22 inbound o outbound.
- Ajustar las reglas para permitir el tráfico SSH.

- **IP o DNS incorrectos:**
  - Confirmar que se está usando la IP pública actual de la instancia (no una anterior).
  - Verificar que la instancia tiene estado **running** y **status checks** en 2/2.

Escenario 2: Servidor web accesible desde cualquier lugar
Pasos para restringir:

- Identificar el rango de IPs corporativas (por ejemplo, `200.10.20.0/24` y `201.30.40.0/24`).
- Editar las reglas inbound del SG que controla el servidor web:
  - Eliminar la regla HTTP (80) con origen `0.0.0.0/0`.
  - Agregar reglas HTTP (80) con origen:
    - `200.10.20.0/24`.
    - `201.30.40.0/24`.
- Pruebas:
  - Desde una IP corporativa, verificar que la aplicación web sigue siendo accesible.
  - Desde otra red (por ejemplo, datos móviles personales), verificar que el acceso HTTP es bloqueado.

9 Conclusiones

En este laboratorio, el estudiante ha dado un paso clave en la transición desde el diseño puramente lógico de redes en AWS hacia la operación práctica de **cómputo en la nube** con Amazon EC2. La experiencia de lanzar una instancia, protegerla con **Security Groups**, reforzar la seguridad con **Network ACLs** y conectarse vía SSH, permite cerrar el ciclo de conceptos trabajados en los laboratorios anteriores de VPC e Internet Gateway.

Entre los principales logros se destacan:

- La comprensión del rol de EC2 como servicio de máquinas virtuales bajo demanda y su relación con la VPC y las subredes.
- La diferenciación clara entre **Security Groups (stateful)** y **NACLs (stateless)**, entendiendo cómo se complementan en una estrategia de defensa en profundidad.
- La aplicación de **mejores prácticas de seguridad**, restringiendo el acceso SSH a direcciones IP específicas y evitando aperturas indiscriminadas de puertos.
- La construcción de habilidades prácticas para diagnosticar problemas de conectividad y aislar si el bloqueo ocurre a nivel de SG, NACL o configuración de red.

Finalmente, el laboratorio refuerza la idea de que el uso correcto de EC2 va mucho más allá de "encender una máquina virtual": implica **diseñar cuidadosamente la superficie de exposición de red**, controlar quién puede conectarse y desde dónde, y mantener una disciplina de cierre y limpieza de recursos para respetar límites de Free Tier y evitar costos inesperados. Estas competencias serán esenciales para los laboratorios posteriores, donde EC2 se integrará con otros servicios en arquitecturas cada vez más complejas y cercanas a escenarios de producción.

10 Referencias

10.1 Documentación Oficial de AWS

1. Amazon EC2 User Guide for Linux Instances
   https://docs.aws.amazon.com/ec2/

2. Amazon VPC User Guide
   https://docs.aws.amazon.com/vpc/latest/userguide/

3. Security Groups for Your VPC
   https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html

4. Network ACLs
   https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html

5. AWS Free Tier
   https://aws.amazon.com/free/

6. Best practices for securing Amazon EC2 instances
   https://docs.aws.amazon.com/whitepapers/latest/aws-overview/security-and-compliance
   html

10.2 Recursos de Aprendizaje

1. AWS Training and Certification - Introducción a EC2
   https://www.aws.training/

2. AWS Skill Builder - Cursos introductorios de EC2 y VPC
   https://skillbuilder.aws/

Nota: Las URLs anteriores fueron verificadas al momento de elaboración de este laboratorio. La documentación de AWS se actualiza frecuentemente, por lo que se recomienda consultar siempre la versión más reciente desde el portal oficial.