Laboratorio #5

Seguridad Avanzada en Redes en AWS

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: 90 minutos
Costo: \$0.00 (100 % Gratuito - Free Tier)

Diciembre 2025

Índice

Resumen

Este laboratorio está orientado a la **seguridad avanzada en redes sobre AWS**, utilizando como base la infraestructura construida en laboratorios anteriores (VPC, subredes, instancias EC2 y grupos de seguridad básicos). El objetivo principal es diseñar y aplicar una arquitectura de **defensa en profundidad** que combine **Security Groups multicapa**, **VPC Flow Logs** y **CloudWatch Logs Insights** para mejorar la visibilidad, detectar tráfico anómalo y aplicar el **principio de mínimo privilegio** de forma práctica.

A lo largo del laboratorio, el estudiante configurará múltiples grupos de seguridad para las diferentes capas (bastion, capa web y capa privada), habilitará y analizará VPC Flow Logs, ejecutará consultas básicas con CloudWatch Logs Insights para inspeccionar tráfico permitido/denegado y ajustará las reglas para reducir la superficie de ataque. Finalmente, se valida el correcto funcionamiento de la arquitectura y se realiza la limpieza de recursos usados.

Palabras clave: Security Groups, VPC Flow Logs, CloudWatch Logs Insights, Defense in Depth, Mínimo Privilegio, Seguridad en Redes, AWS, Tráfico Anómalo.

1 Objetivos

1.1 Objetivo General

Diseñar y aplicar una arquitectura de **seguridad avanzada en redes sobre AWS** basada en **defensa en profundidad**, utilizando **Security Groups multicapa**, **VPC Flow Logs** y **CloudWatch Logs Insights** para monitorear, analizar y proteger el tráfico de red conforme al principio de mínimo privilegio.

1.2 Objetivos Específicos

- Comprender el papel de los Security Groups dentro de la arquitectura de red de AWS y su relación con NACLs.
- Implementar **Security Groups multicapa** para separar y proteger las distintas zonas (bastion, capa web, capa privada).
- Habilitar y configurar **VPC Flow Logs** para registrar el tráfico de red a nivel de VPC/subred/ENI.
- Utilizar **CloudWatch Logs Insights** para ejecutar consultas básicas que permitan identificar patrones de tráfico, intentos de acceso no autorizados y tráfico anómalo.
- Aplicar de forma práctica el **principio de mínimo privilegio** en las reglas de seguridad.
- Diseñar una arquitectura coherente con el enfoque de **defense in depth**, combinando capas de protección y monitoreo.

1.3 Competencias a Desarrollar

- **Seguridad en Redes de Nueva Generación:** Diseño de arquitecturas segmentadas y protegidas mediante controles de red y monitoreo continuo.
- **Gestión de Seguridad en la Nube:** Configuración de reglas de acceso, logging de tráfico y análisis de eventos de red en AWS.
- **Análisis de Tráfico:** Capacidad para interpretar registros de VPC Flow Logs e identificar tráfico legítimo, sospechoso y potencialmente malicioso.
- **Aplicación de Principios de Seguridad:** Implementación práctica de mínimo privilegio y defensa en profundidad.
- **Uso de Herramientas de Observabilidad:** Manejo de CloudWatch Logs e Insights para consultar y visualizar información relevante de seguridad.

2 Marco Teórico

2.1 Seguridad en Redes en AWS y Defense in Depth

La **defensa en profundidad** (defense in depth) es una estrategia de seguridad que consiste en implementar **múltiples capas de protección** alrededor de los activos críticos. En lugar de depender de un solo control (por ejemplo, un firewall perimetral), se combinan controles de red, controles de identidad, monitoreo, registro de eventos, segmentación y endurecimiento de sistemas.

En AWS, la defensa en profundidad se materializa a través de:

- **Controles de red:** VPC, subredes públicas y privadas, *Security Groups*, *Network ACLs*.
- **Controles de identidad:** IAM, roles, políticas y autenticación multifactor.
- **Controles de monitoreo:** CloudWatch, CloudTrail, *VPC Flow Logs*, AWS Config.
- **Controles de aplicación:** WAF, validación de entradas, cifrado de datos en tránsito y en reposo.

El objetivo es que, aun si una capa es vulnerada, las demás sigan ofreciendo protección.

2.2 Security Groups

Los **Security Groups (SG)** son **firewalls virtuales a nivel de instancia** que controlan el tráfico entrante (ingress) y saliente (egress). Cada instancia EC2 debe estar asociada al menos a un Security Group, y este grupo define qué tráfico está permitido según:

- **Protocolo:** TCP, UDP, ICMP, etc.
- **Puerto o rango de puertos:** por ejemplo, 22 (SSH), 80 (HTTP), 443 (HTTPS).
- **Origen/Destino:** rangos CIDR (ej: 0.0.0.0/0, 10.0.1.0/24) o *otros Security Groups*.

2.2.1. Características Clave

- Son **stateful**: si se permite tráfico de entrada, la respuesta de salida se permite automáticamente (y viceversa).
- Se aplican a nivel de interfaz de red (ENI) de la instancia.
- Pueden referenciar otros Security Groups como origen/destino, permitiendo diseños multicapa.
- Soportan múltiples reglas y múltiples SG por instancia.

2.2.2. Security Groups Multicapa

En una arquitectura de aplicación típica de tres capas (bastion, web, aplicación/base de datos) se recomienda usar **SGs separados por función**, por ejemplo:

- **SG_Bastion:** Permite SSH (22) solo desde una IP pública confiable.
- **SG_Web:** Permite HTTP/HTTPS desde internet (0.0.0.0/0) y SSH únicamente desde SG_Bastion.
- **SG_Privado:** Permite tráfico de base de datos (ej. 3306) únicamente desde SG_Web.

De esta forma, ningún cliente externo puede conectarse directamente a la capa privada, y el acceso administrativo pasa únicamente por el bastion.

2.3 Network ACLs (NACLs) vs Security Groups

Los **Network ACLs** son listas de control de acceso a nivel de subred, mientras que los Security Groups se aplican a nivel de instancia. Algunas diferencias importantes:

- Los NACLs son **stateless**: se deben crear reglas para tráfico entrante y saliente.
- Los Security Groups son **stateful**: la respuesta es automáticamente permitida.
- Un NACL se asocia a una subred; un SG se asocia a una interfaz de red/instancia.

En este laboratorio, el enfoque principal está en **Security Groups** y **VPC Flow Logs**, asumiendo que los NACLs mantienen una configuración por defecto o alineada con buenas prácticas.

2.4 VPC Flow Logs

VPC Flow Logs es una funcionalidad que permite capturar información sobre el tráfico IP que entra y sale de:

- Interfaces de red (ENI).
- Subredes.
- La VPC completa.

Cada registro de Flow Log incluye, entre otros:

- `srcaddr`, `dstaddr`: IP de origen y destino.
- `srcport`, `dstport`: puertos de origen y destino.
- `protocol`: protocolo (6=TCP, 17=UDP, etc.).
- `action`: `ACCEPT` o `REJECT`, según lo que determinen SGs y NACLs.
- `log-status`: estado del registro.

Los Flow Logs pueden enviarse a:

- **CloudWatch Logs**.
- **S3**.

En este laboratorio se usarán **CloudWatch Logs**, lo que permite consultas con **CloudWatch Logs Insights**.

2.5 CloudWatch Logs Insights

CloudWatch Logs Insights es un motor de consultas interactivo para analizar grandes volúmenes de logs en tiempo casi real. Permite:

- Ejecutar consultas con una sintaxis similar a SQL adaptada a logs.
- Filtrar por campos (por ejemplo, solo `action = REJECT"`).
- Agrupar por IP origen/destino, puerto o protocolo.
- Visualizar tendencias de tráfico.

2.5.1. Ejemplo de Consulta para VPC Flow Logs

```
fields srcAddr, dstAddr, srcPort, dstPort, action, protocol
| filter action = 'REJECT'
| stats count(*) as intentos_bloqueados by srcAddr, dstPort
| sort intentos_bloqueados desc
| limit 20
```

Listing 1: Ejemplo de consulta básica en CloudWatch Logs Insights

Esta consulta permite identificar las direcciones IP que más intentos de conexión bloqueados han generado y hacia qué puertos se dirigían.

2.6 Principio de Mínimo Privilegio

El **principio de mínimo privilegio** establece que cada entidad (usuario, servicio, instancia) debe tener únicamente los permisos (o puertos) indispensables para realizar su función, y nada más. Aplicado a redes:

- Abrir solo los puertos estrictamente necesarios.
- Limitar el origen a rangos específicos (por ejemplo, una IP fija o un SG específico).
- Evitar reglas amplias como `0.0.0.0/0` salvo que sean imprescindibles (ej: HTTP público).

2.7 Tráfico Anómalo

Se considera **tráfico anómalo** aquel que:

- No corresponde al uso esperado de la aplicación.
- Presenta volúmenes inusualmente altos.
- Intenta acceder a puertos no expuestos o no utilizados.
- Proviene de rangos geográficos inesperados.

VPC Flow Logs junto con CloudWatch Logs Insights permiten detectar este tipo de patrones para tomar acciones (ajustar SGs, bloquear rangos, endurecer la arquitectura, etc.).

3 Requisitos Previos

3.1 Conocimientos Necesarios

- Laboratorios previos completados (VPC, subredes, IGW, EC2 y Security Groups básicos).
- Conocimientos fundamentales de redes IP (subredes, puertos, protocolos).
- Familiaridad con la consola de AWS.
- Conocimiento básico de CloudWatch (dashboard y navegación).

3.2 Recursos Técnicos

- **Computadora:** PC, Mac o Linux con navegador actualizado.
- **Cuenta AWS:** Activa y configurada con Free Tier.
- **Usuario IAM:** Con permisos administrativos según mejores prácticas de los laboratorios anteriores.
- **Infraestructura base:**
  - VPC creada (por ejemplo, `10.0.0.0/16`).
  - Subred pública (ej: `10.0.1.0/24`) con acceso a internet.
  - Subred privada (ej: `10.0.2.0/24`).
  - Una instancia EC2 en subred pública (capa *web*).
  - Una instancia EC2 en subred privada (capa *app/bd*), opcional según diseño previo.

3.3 Costos Estimados

Concepto	**Costo Estimado**
Uso de Security Groups	$0.00
VPC Flow Logs (nivel de laboratorio, bajo volumen)	$0.00 (dentro de Free Tier)
CloudWatch Logs e Insights (bajo volumen)	$0.00 (dentro de Free Tier)
Instancias EC2 t2.micro/t3.micro	Incluidas en Free Tier si se respeta el límite d
TOTAL	**$0.00**

Cuadro 1: Costos del Laboratorio 5

NOTA: Este laboratorio está diseñado para ejecutarse dentro de los límites del Free Tier. Es fundamental seguir la sección de limpieza para evitar costos.

3.4 Tiempo Estimado

- Lectura del marco teórico: 20 minutos.
- Configuración de Security Groups multicapa: 20 minutos.
- Habilitación de VPC Flow Logs: 15 minutos.
- Consultas en CloudWatch Logs Insights: 20 minutos.
- Verificación y limpieza: 15 minutos.
- **TOTAL ESTIMADO:** 90 minutos.

4 Procedimiento Paso a Paso

En este laboratorio se asumirá que ya existe una VPC creada en laboratorios anteriores. Si tu arquitectura difiere, adapta los nombres de recursos manteniendo la lógica del ejercicio.

4.1 Paso 1: Definir el Escenario de Seguridad

Objetivo: Definir una arquitectura lógica de capas para aplicar Security Groups multicapa y registrar el tráfico con VPC Flow Logs.

Descripción

Se trabajará con una VPC que tenga:

- Una **subred pública** donde reside una instancia EC2 de la capa web.
- Una **subred privada** donde puede residir una instancia EC2 de aplicación o base de datos.
- Un **bastion host** opcional (en subred pública) desde el cual se administran las instancias por SSH.

Valores de Referencia a Utilizar

- Nombre VPC: `VPC-RNG-Lab5`
- CIDR VPC: `10.0.0.0/16`
- Subred pública: `10.0.1.0/24`
- Subred privada: `10.0.2.0/24`
- Instancia web: `WebServer-Lab5`
- Instancia privada (opcional): `AppServer-Lab5`

4.2 Paso 2: Crear Security Group para Bastion (SG_Bastion)

Objetivo: Crear un Security Group que limite el acceso SSH a una IP de administración específica, evitando SSH abierto a todo el mundo.

4.2.1. Instrucciones

1. Iniciar sesión en la consola de AWS con tu usuario IAM administrador.
2. En la barra de búsqueda, escribir `EC2` y seleccionar el servicio.
3. En el panel izquierdo, hacer clic en **Security Groups**.
4. Hacer clic en **Create security group**.

5. Completar el formulario:
   - **Security group name:** `SG_Bastion_Lab5`
   - **Description:** `Security Group para bastion host (SSH desde IP de administración).`
   - **VPC:** Seleccionar `VPC-RNG-Lab5` (o la VPC utilizada en tus labs).
6. En la sección **Inbound rules**, hacer clic en **Add rule**:
   - **Type:** SSH
   - **Port range:** 22
   - **Source:** `My IP` (la consola rellenará tu IP pública actual).
   - **Description:** `SSH solo desde IP de administración.`
7. En **Outbound rules**, dejar la regla por defecto:
   - **Type:** All traffic
   - **Destination:** `0.0.0.0/0`
8. Hacer clic en **Create security group**.

Qué esperar

- El SG `SG_Bastion_Lab5` aparecerá en la lista.
- Solo permitirá SSH desde tu IP pública actual.

4.3 Paso 3: Crear Security Group para Capa Web (SG_Web)

Objetivo: Proteger la instancia web permitiendo solo HTTP/HTTPS desde internet y SSH exclusivamente desde el bastion.

4.3.1. Instrucciones

1. Desde la misma sección de **Security Groups**, hacer clic en **Create security group**.
2. Completar:
   - **Security group name:** `SG_Web_Lab5`
   - **Description:** `Security Group para capa web con acceso HTTP/HTTPS y SSH desde bastion.`
   - **VPC:** `VPC-RNG-Lab5`
3. En **Inbound rules**:
   - Regla 1:
     - **Type:** HTTP
     - **Port range:** 80

- **Source:** `0.0.0.0/0`
- **Description:** `Tráfico web HTTP público.`

- Regla 2:
  - **Type:** HTTPS
  - **Port range:** 443
  - **Source:** `0.0.0.0/0`
  - **Description:** `Tráfico web HTTPS público.`
- Regla 3:
  - **Type:** SSH
  - **Port range:** 22
  - **Source:** Seleccionar la opción `Custom` y en el campo escribir el ID del SG `SG_Bastion_Lab5` (puedes buscarlo por nombre).
  - **Description:** `SSH solo desde bastion.`

4. En **Outbound rules**, dejar:
   - **Type:** All traffic
   - **Destination:** `0.0.0.0/0`
5. Crear el Security Group.

Qué esperar

- La instancia web sólo aceptará:
  - HTTP/HTTPS desde internet.
  - SSH únicamente desde instancias que tengan asignado `SG_Bastion_Lab5`.

4.4 Paso 4: Crear Security Group para Capa Privada (SG_Privado)

Objetivo: Crear un SG para la capa interna (aplicación o base de datos) permitiendo únicamente tráfico desde la capa web.

4.4.1. Instrucciones

1. Crear un nuevo Security Group:
   - **Security group name:** `SG_Privado_Lab5`
   - **Description:** `Security Group para capa privada (app/bd) accesible solo desde capa web.`
   - **VPC:** `VPC-RNG-Lab5`
2. En **Inbound rules**, según el tipo de servicio interno:
   - Ejemplo: base de datos MySQL:

- **Type:** MySQL/Aurora
- **Port range:** 3306
- **Source:** `SG_Web_Lab5` (seleccionarlo como origen).
- **Description:** `MySQL solo desde capa web.`

3. Opcionalmente, permitir ICMP desde la capa web para pruebas de `ping`:
   - **Type:** All ICMP - IPv4
   - **Source:** `SG_Web_Lab5`
   - **Description:** `Pruebas de conectividad desde web.`
4. En **Outbound rules**, dejar por defecto (All traffic a 0.0.0.0/0) o restringir según necesidades.

4.5 Paso 5: Asociar los Security Groups a las Instancias

Objetivo: Aplicar los SGs creados a las instancias correspondientes.

4.5.1. Instrucciones

1. En EC2, ir a **Instances**.
2. Seleccionar la instancia de bastion (si existe).
3. En el panel inferior, pestaña **Security**.
4. Hacer clic en el icono de edición de **Security groups**.
5. Asignar `SG_Bastion_Lab5` (manteniendo otros SGs necesarios).
6. Repetir el proceso para:
   - Instancia `WebServer-Lab5`: asignar `SG_Web_Lab5`.
   - Instancia `AppServer-Lab5` (si existe): asignar `SG_Privado_Lab5`.

4.6 Paso 6: Habilitar VPC Flow Logs

Objetivo: Registrar el tráfico de red de la VPC (o subred) en un grupo de logs de CloudWatch para su posterior análisis.

4.6.1. Instrucciones

1. En la barra de búsqueda, escribir `VPC` y abrir el servicio.
2. En el panel izquierdo, hacer clic en **Your VPCs**.
3. Seleccionar `VPC-RNG-Lab5`.
4. En el panel inferior, ir a la pestaña **Flow logs**.

5. Hacer clic en **Create flow log**.
6. Completar:
   - **Filter:** `ALL` (para registrar ACCEPT y REJECT).
   - **Maximum aggregation interval:** 1 minute.
   - **Destination:** `Send to CloudWatch Logs`.
   - **Destination log group:** `/aws/vpc/flowlogs/lab5` (si no existe, se creará).
   - **IAM role:** Crear un rol nuevo usando la opción `Set up permissions` automática.
7. Confirmar la creación del Flow Log.

Qué esperar

- Aparecerá un Flow Log con estado `ACTIVE` en la pestaña **Flow logs**.
- En pocos minutos se comenzarán a recibir registros en CloudWatch Logs.

4.7 Paso 7: Consultar VPC Flow Logs desde CloudWatch Logs Insights

Objetivo: Ejecutar consultas básicas en CloudWatch Logs Insights para analizar tráfico aceptado y rechazado.

4.7.1. Instrucciones

1. En la barra de búsqueda, escribir `CloudWatch` y abrir el servicio.
2. En el panel izquierdo, hacer clic en **Logs** → **Log groups**.
3. Localizar el grupo de logs `/aws/vpc/flowlogs/lab5`.
4. Hacer clic en el nombre del log group.
5. Hacer clic en el botón **Actions** y seleccionar **View in Logs Insights**.
6. Verificar que en la parte superior aparezca el log group correcto.

Consulta 1: Ver tráfico rechazado

```
fields @timestamp, srcAddr, dstAddr, srcPort, dstPort, protocol,
    action
| filter action = 'REJECT'
| sort @timestamp desc
| limit 20
```

Listing 2: Tráfico rechazado por reglas de seguridad

Consulta 2: Contar intentos bloqueados por IP de origen

```
fields srcAddr, dstPort, action
| filter action = 'REJECT'
| stats count(*) as intentos_bloqueados by srcAddr, dstPort
| sort intentos_bloqueados desc
| limit 10
```

Listing 3: Conteo de intentos bloqueados por IP

Qué esperar

- Verás registros donde `action` es `ACCEPT` o `REJECT`.
- Al ejecutar las consultas, deberías observar:
  - Intentos de acceso a puertos no permitidos (REJECT).
  - Tráfico legítimo hacia puertos HTTP/HTTPS (ACCEPT).

4.8 Paso 8: Simular Tráfico Anómalo y Ajustar Reglas

Objetivo: Generar tráfico hacia puertos no permitidos, observar cómo se registran en los Flow Logs y ajustar las reglas de SG para endurecer la arquitectura.

4.8.1. Simulación Básica (desde tu propia máquina)

1. Obtener la **IP pública** de la instancia web `WebServer-Lab5`.
2. Desde tu máquina, generar tráfico a un puerto no permitido, por ejemplo 23 (Telnet):

```
telnet IP_PUBLICA_WEB 23
```

Listing 4: Intento de conexión a puerto no permitido

3. El intento fallará (no se establecerá conexión).
4. Esperar 2-3 minutos e ir nuevamente a CloudWatch Logs Insights.
5. Ejecutar la Consulta 1 de tráfico rechazado.

Análisis

- Deberías ver registros con `dstPort = 23` y `action = REJECT`.
- Puedes identificar desde qué IP se generó el tráfico (tu IP pública).

4.8.2. Ajuste de Reglas (Endurecimiento)

Aunque el tráfico ya era rechazado, en arquitecturas más complejas se pueden:

- Cerrar aún más los puertos salientes desde la capa web.
- Restringir SSH sólo a bastion y no a otras fuentes.
- Identificar IPs que generen muchos `REJECT` y, si se considera necesario, bloquearlas mediante NACLs.

5 Tablas de Configuración

Recurso	Parámetro	Valor	Propósito
VPC	CIDR	10.0.0.0/16	Red lógica principal
Subred pública	CIDR	10.0.1.0/24	Alojar capa web y ba
Subred privada	CIDR	10.0.2.0/24	Alojar capa de aplica
SG_Bastion_Lab5	Inbound	SSH (22) desde IP de admin	Acceso administrativ
SG_Web_Lab5	Inbound	HTTP (80) y HTTPS (443) desde 0.0.0.0/0	Acceso web público
SG_Web_Lab5	Inbound	SSH (22) desde SG_Bastion_Lab5	Administración solo
SG_Privado_Lab5	Inbound	MySQL (3306) desde SG_Web_Lab5	Tráfico de app hacia
VPC Flow Logs	Filter	ALL	Registrar ACCEPT
VPC Flow Logs	Destino	/aws/vpc/flowlogs/lab5 (CloudWatch Logs)	Análisis con Logs Ins

Cuadro 2: Resumen de parámetros de configuración del Laboratorio 5

6 Verificación del Funcionamiento

6.1 Verificación de Security Groups

1. Desde la consola EC2, seleccionar `WebServer-Lab5`.
2. En la pestaña **Security**, verificar que:
   - El SG adjunto incluye `SG_Web_Lab5`.
   - Las reglas de entrada son exactamente las definidas (HTTP, HTTPS y SSH desde bastion).
3. Intentar conectarse por SSH desde tu máquina directamente a la IP pública de `WebServer-Lab5`:

```
ssh ec2-user@IP_PUBLICA_WEB
```

Listing 5: Intento de SSH directo (debería fallar)

4. El intento debería ser rechazado si tu IP no corresponde al bastion (según diseño).

6.2 Verificación de VPC Flow Logs

1. En el servicio VPC, ir a **Your VPCs**.
2. Seleccionar `VPC-RNG-Lab5`, pestaña **Flow logs**.
3. Verificar que el estado del Flow Log sea `ACTIVE`.
4. Ir a CloudWatch → **Log groups**.
5. Confirmar la existencia del grupo `/aws/vpc/flowlogs/lab5`.
6. Abrir Logs Insights y ejecutar la consulta de tráfico rechazado.

6.3 Verificación de Tráfico Anómalo

1. Generar algunos intentos de conexión a puertos no permitidos (por ejemplo, 21, 23, 3389).
2. Esperar unos minutos.
3. Ejecutar en Logs Insights una consulta filtrando por `action = 'REJECT'`.
4. Verificar que los puertos usados aparecen con acción `REJECT`.
5. Analizar qué IPs han generado más intentos y hacia qué puertos.

6.4 Troubleshooting Común

- **No aparecen registros en Flow Logs:**
  - Verificar que el Flow Log esté en estado `ACTIVE`.
  - Confirmar que hay tráfico real en la VPC (generar pings o curl a la instancia web).
  - Revisar el rol IAM asociado al Flow Log.
- **No se puede acceder por HTTP/HTTPS a la instancia web:**
  - Verificar que la instancia esté en ejecución.
  - Verificar que el SG asignado tenga reglas HTTP/HTTPS desde 0.0.0.0/0.
  - Revisar NACLs de la subred pública (que no bloqueen tráfico).

7 Limpieza de Recursos

Objetivo: Asegurar que los recursos creados específicamente para este laboratorio no generen costos posteriores.

7.1 Pasos de Limpieza

1. **Instancias EC2 de Prueba**
   - Si creaste instancias temporales para este lab, detenlas y **termina** aquellas que no se reutilizarán en otros laboratorios.
2. **Security Groups**
   - Verificar si `SG_Bastion_Lab5`, `SG_Web_Lab5` y `SG_Privado_Lab5` serán reutilizados.
   - Si NO se reutilizarán y ya no están asociados a ninguna instancia:
     a) Ir a EC2 → Security Groups.
     b) Seleccionar el SG.
     c) Hacer clic en **Actions** → **Delete security group**.
3. **VPC Flow Logs**
   - Si solo se usan para este laboratorio:
     a) Ir a VPC → Your VPCs.
     b) Seleccionar la VPC.
     c) Pestaña **Flow logs**.
     d) Seleccionar el Flow Log creado.
     e) Hacer clic en **Actions** → **Delete flow log**.
4. **CloudWatch Logs**
   - Ir a CloudWatch → **Log groups**.
   - Seleccionar `/aws/vpc/flowlogs/lab5`.
   - Hacer clic en **Actions** → **Delete log group**.
   - Confirmar la eliminación.

7.2 Comando de Verificación de Instancias (CLI Opcional)

```
aws ec2 describe-instances --query 'Reservations[*].Instances
    [*].[InstanceId,State.Name,Tags]' --output table
```

Listing 6: Verificar instancias EC2 en ejecución

8 Cuestionario de Evaluación

Instrucciones: Selecciona la respuesta correcta o marca Verdadero/Falso según corresponda. Al final se incluyen las respuestas sugeridas.

8.1 Preguntas de Selección Múltiple

1. **¿Qué afirma mejor el concepto de *defense in depth* en AWS?**

   a) Proteger solo la capa perimetral de la VPC.

   b) Usar un único firewall muy fuerte es suficiente.

   c) Implementar varias capas de controles de seguridad y monitoreo.

   d) Usar únicamente IAM para proteger recursos.

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

   a) Firewalls a nivel de subred, stateless.

   b) Firewalls a nivel de instancia, stateful.

   c) Firewalls físicos en los data centers.

   d) Únicamente listas de control de acceso globales.

3. **¿Cuál de las siguientes afirmaciones sobre Security Groups es correcta?**

   a) Pueden permitir tráfico de salida, pero no de entrada.

   b) No pueden referenciar otros Security Groups.

   c) Siempre se aplican a nivel de VPC, no de instancia.

   d) Pueden usar como origen/destino otros Security Groups.

4. **¿Qué campo de VPC Flow Logs indica si el tráfico fue permitido o bloqueado?**

   a) `log-status`

   b) `action`

   c) `srcport`

   d) `protocol`

5. **¿Cuál es el destino más usado en este laboratorio para VPC Flow Logs?**

   a) Amazon S3

   b) Amazon RDS

   c) CloudWatch Logs

   d) DynamoDB

6. **En una arquitectura de tres capas (bastion, web, bd), cuál es una buena práctica?**

a) Permitir SSH desde internet directamente a la base de datos.

b) Permitir HTTP desde internet a la base de datos.

c) Permitir acceso a base de datos solo desde la capa web.

d) Exponer la base de datos con una IP pública.

7. **¿Qué consulta en CloudWatch Logs Insights ayuda a encontrar IPs con más tráfico bloqueado?**

a) Filtrar solo por `action = 'ACCEPT'`.

b) Usar `stats count(*) by srcAddr` filtrando `action = 'REJECT'`.

c) Ordenar por `@timestamp` ascendente.

d) Limitar siempre a 1 resultado.

8. **El principio de mínimo privilegio aplicado a Security Groups implica:**

a) Abrir todos los puertos para evitar problemas de conectividad.

b) Abrir solo los puertos y orígenes estrictamente necesarios.

c) Usar siempre 0.0.0.0/0 en todas las reglas.

d) Nunca permitir tráfico saliente.

9. **¿Qué tipo de tráfico es más probable que se considere anómalo?**

a) HTTP a puerto 80 desde clientes esperados.

b) Muchas conexiones fallidas a puertos no abiertos desde una misma IP.

c) Respuestas HTTP 200 OK a clientes conocidos.

d) Consultas de base de datos desde la capa web.

10. **¿Qué ventaja ofrece enviar VPC Flow Logs a CloudWatch Logs en lugar de ignorarlos?**

a) Ninguna, solo consume espacio.

b) Permite analizar tráfico y detectar patrones sospechosos.

c) Desactiva automáticamente el tráfico malicioso.

d) Reemplaza la necesidad de Security Groups.

8.2 Preguntas Verdadero/Falso

VF1. Los Security Groups en AWS son stateless y requieren reglas separadas para tráfico entrante y saliente.

VF2. VPC Flow Logs permiten registrar tanto tráfico aceptado como trafico-rechazado según la configuración.

VF3. CloudWatch Logs Insights solo puede ejecutarse sobre logs de VPC Flow Logs y no sobre ningún otro tipo de log.

8.3 Escenarios Prácticos

E1. Escenario 1: SSH expuesto

Tienes una instancia EC2 en la subred pública con un Security Group que permite:

- SSH (22) desde 0.0.0.0/0.
- HTTP (80) desde 0.0.0.0/0.

En los VPC Flow Logs observas múltiples intentos de conexión SSH fallidos desde direcciones IP de diferentes países.

Pregunta: ¿Qué cambios harías en el Security Group y en la arquitectura para reducir la superficie de ataque, aplicando defensa en profundidad?

E2. Escenario 2: Detención de escaneo de puertos

Tu aplicación solo necesita HTTP/HTTPS. En VPC Flow Logs identificas que una IP externa intenta conectarse a muchos puertos (21, 23, 3389, 1433, etc.) hacia tu instancia web, todos con `action = 'REJECT'`.

Pregunta: ¿Cómo usarías la información de VPC Flow Logs y qué medidas adicionales podrías implementar (por ejemplo, con NACLs o WAF) para mitigar este tipo de comportamiento?

8.4 Respuestas del Cuestionario

Selección Múltiple

1. **c)** Implementar varias capas de controles de seguridad y monitoreo.
2. **b)** Firewalls a nivel de instancia, stateful.
3. **d)** Pueden usar como origen/destino otros Security Groups.
4. **b)** `action`.
5. **c)** CloudWatch Logs.
6. **c)** Permitir acceso a base de datos solo desde la capa web.
7. **b)** Usar `stats count(*) by srcAddr` filtrando `action = 'REJECT'`.
8. **b)** Abrir solo los puertos y orígenes estrictamente necesarios.
9. **b)** Muchas conexiones fallidas a puertos no abiertos desde una misma IP.
10. **b)** Permite analizar tráfico y detectar patrones sospechosos.

Verdadero/Falso

1. **Falso.** Los Security Groups son **stateful**, no stateless.
2. **Verdadero.** Pueden configurarse para registrar `ACCEPT`, `REJECT` o ambos (`ALL`).
3. **Falso.** CloudWatch Logs Insights también puede analizar otros tipos de logs (aplicación, Lambda, etc.).

Escenarios (Guía de Respuesta)

Escenario 1:

- Cerrar SSH desde 0.0.0.0/0.
- Crear un **bastion host** con SG que permita SSH solo desde IPs de administración.
- Configurar el SG de la instancia web para permitir SSH únicamente desde el SG del bastion.
- Seguir monitoreando VPC Flow Logs para verificar disminución de intentos.

Escenario 2:

- Usar VPC Flow Logs para identificar la IP y el patrón de escaneo.
- Considerar bloquear el rango de IP en un NACL (regla DENY explícita).
- Mantener Security Groups con mínimo privilegio (solo HTTP/HTTPS).
- Para tráfico a nivel de aplicación, integrar AWS WAF para detectar patrones maliciosos en HTTP.

9 Conclusiones

En este laboratorio se ha profundizado en el diseño de **seguridad avanzada en redes sobre AWS**, pasando de configuraciones básicas a una arquitectura más madura basada en **defensa en profundidad** y **mínimo privilegio**. El estudiante ha experimentado la importancia de segmentar la red en capas (bastion, web, privada) y de utilizar **Security Groups multicapa** para controlar de forma granular quién puede comunicarse con quién y a través de qué puertos.

La habilitación de **VPC Flow Logs** y su análisis mediante **CloudWatch Logs Insights** demuestran que la seguridad no solo se limita a bloquear o permitir tráfico, sino también a **observar, registrar y entender** los patrones de comunicación que se producen en la VPC. Esto permite detectar tráfico anómalo, posibles intentos de explotación y escaneos de puertos, proporcionando insumos para tomar decisiones informadas de endurecimiento (hardening).

Finalmente, la combinación de estos mecanismos refuerza la idea de que la nube no es intrínsecamente insegura ni segura, sino que depende del diseño y de las prácticas aplicadas. El uso consistente del principio de mínimo privilegio, junto con controles de monitoreo y registro, prepara al estudiante para diseñar y operar arquitecturas de red en AWS que sean robustas, observables y alineadas con las mejores prácticas de seguridad en la industria.

10 Referencias

10.1 Documentación Oficial de AWS

1. **Amazon VPC**
   - Amazon VPC Documentation
     https://docs.aws.amazon.com/vpc/
   - VPC Flow Logs
     https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html
2. **Amazon EC2 Security Groups**
   - Amazon EC2 Security Groups for Linux Instances
     https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-security-groups.html
   - Security Group Rules Reference
     https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/security-group-rules-referenc
     html
3. **Network ACLs**
   - Network ACLs
     https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html
4. **Amazon CloudWatch Logs e Insights**
   - Amazon CloudWatch Logs
     https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/WhatIsCloudWatchLogs.html
   - Analyzing Log Data with CloudWatch Logs Insights
     https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/AnalyzingLogData.html
5. **AWS Security Best Practices**
   - AWS Security Best Practices Whitepaper
     https://docs.aws.amazon.com/whitepapers/latest/aws-security-best-practices/
   - Security Pillar - AWS Well-Architected Framework
     https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/welcome.html

10.2 Recursos de Aprendizaje y Arquitectura

1. AWS Architecture Center
   https://aws.amazon.com/architecture/
2. AWS Prescriptive Guidance - Security Patterns
   https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/

10.3 Bibliografía General de Seguridad en Redes

1. Stallings, W. (2014). *Network Security Essentials: Applications and Standards*. Pearson.

2. Anderson, R. (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley.

Nota: Las URLs fueron verificadas al momento de elaboración de este laboratorio. Es posible que AWS actualice la ubicación de algunos documentos; en ese caso, se recomienda comenzar desde el portal principal de documentación: https://docs.aws.amazon.com/.