

[Publish] - 11. Los Grupos de Seguridad aceptan tráfico global solo de los puertos 80 y 443

El hallazgo de seguridad "**Los Grupos de Seguridad aceptan tráfico global solo de los puertos 80 y 443**" se enfoca en una de las reglas más importantes de la seguridad de red: **limitar la superficie de ataque**. Un Grupo de Seguridad (Security Group) actúa como un firewall virtual para tus recursos de AWS (como instancias EC2, bases de datos RDS, etc.), controlando el tráfico de entrada y salida.

Cuando una regla de entrada (`inbound rule`) permite el tráfico desde el origen `0.0.0.0/0` o `::/0`, significa que **cualquier persona en internet** puede intentar conectarse a tus recursos en el puerto especificado. Si bien esto es necesario para los puertos web estándar (**80 para HTTP** y **443 para HTTPS**), es extremadamente peligroso para otros puertos, especialmente los de administración como:

- **SSH (puerto 22):** Usado para la administración de servidores Linux.
- **RDP (puerto 3389):** Usado para la administración de servidores Windows.
- **Puertos de bases de datos (ej. 3306 para MySQL, 5432 para PostgreSQL):** Usados para la conexión a bases de datos.

Dejar estos puertos abiertos al mundo invita a ataques de fuerza bruta, escaneo de vulnerabilidades y otros intentos de acceso no autorizado.

Análisis de los Grupos de Seguridad Reportados

Los siguientes Grupos de Seguridad han sido identificados por tener reglas que permiten el acceso desde `0.0.0.0/0` en puertos no estándar (diferentes de 80 y 443).

Ver archivo adjunto 11. Los Grupos de Seguridad aceptan tráfico global solo de los puertos 80 y 443.csv

Preguntas para tu Equipo (Acción Requerida)

Para cada uno de los Grupos de Seguridad listados, es crucial identificar la necesidad de negocio de la regla abierta.

1. **¿Cuál es el propósito de la regla abierta?** Revisa las reglas de entrada (`inbound rules`) de cada grupo de seguridad para identificar qué puerto está abierto a `0.0.0.0/0`.

2. ¿Quién necesita realmente acceso a este puerto?

- **Si es para administración (SSH/RDP):** El acceso debe restringirse a las direcciones IP de las oficinas, a la red de la VPN corporativa o, idealmente, eliminarse por completo en favor de métodos de acceso más seguros como **AWS Systems Manager Session Manager**.
- **Si es para una base de datos:** El acceso solo debe permitirse desde los Grupos de Seguridad de las instancias EC2 de la aplicación que necesitan conectarse a ella, nunca desde internet.
- **Si es para una API o servicio específico:** El acceso debe limitarse a las direcciones IP de los clientes o sistemas que consumen ese servicio.

Consideraciones de Costo

No hay **ningún costo directo** asociado con la modificación de las reglas de un Grupo de Seguridad. Esta es una configuración de seguridad fundamental proporcionada por AWS sin cargo adicional. El costo de no remediar este hallazgo es el alto riesgo de un compromiso de seguridad.

Cómo Solucionarlo: Restringir las Reglas de Entrada

El proceso implica editar las reglas de entrada del grupo de seguridad para que sean más específicas.

1. Navegar al Grupo de Seguridad:

- Ve a la consola de **EC2**.
- En el panel de navegación izquierdo, en **Red y Seguridad**, elige **Grupos de Seguridad**.
- Selecciona uno de los grupos de seguridad de la lista.

2. Editar las Reglas de Entrada:

- Ve a la pestaña **Reglas de entrada (Inbound rules)**.
- Haz clic en **Editar reglas de entrada**.

3. Modificar o Eliminar la Regla Insegura:

- Localiza la regla que tiene como **Origen (Source)** `0.0.0.0/0` o `::/0` en un puerto que no sea 80 o 443.
- **Modifica el Origen:** Cambia `0.0.0.0/0` por una dirección IP específica (ej. `200.100.50.1/32`), un rango de IPs (ej. el rango de la VPN de tu oficina) o el ID de otro Grupo de Seguridad (ej. `sg-XXXXXXXX`).
- **Elimina la Regla:** Si el acceso ya no es necesario, simplemente elimina la regla.
- Haz clic en **Guardar reglas**.


4. Repetir: Realiza este proceso para todos los grupos de seguridad identificados.

Recomendación

Se recomienda que se revise y restrinja el acceso en todos los grupos de seguridad listados con la máxima prioridad. La exposición de puertos de administración o de bases de datos a internet es una de las configuraciones de mayor riesgo en cualquier entorno de nube.

Para el acceso administrativo, la mejor práctica es utilizar **AWS Systems Manager Session Manager**, que proporciona un acceso seguro a través de la consola de AWS o la CLI sin necesidad de abrir ningún puerto de entrada, eliminando por completo esta superficie de ataque.

Referencias

 [Control traffic to your AWS resources using security groups - Amazon Virtual Private Cloud](#)