[Publish] - 1. Proteger las etapas API Gateway con una Web ACL de WAF

El hallazgo de seguridad **"Proteger las etapas (stages) de API Gateway con una Web ACL de WAF"** resalta la necesidad de una capa de defensa proactiva para tus APIs públicas. Mientras que API Gateway maneja la autenticación y autorización, **AWS WAF (Web Application Firewall)** actúa como un escudo en el perímetro, inspeccionando el tráfico HTTP/S entrante *antes* de que llegue a tu API.

Asociar una Web ACL (Lista de Control de Acceso Web) de WAF a tu API te permite bloquear automáticamente ataques web comunes, tales como:

- **Inyección de SQL (SQLi):** Intentos de manipular las consultas a tu base de datos.
- **Cross-Site Scripting (XSS):** Intentos de inyectar scripts maliciosos en las respuestas de tu API.
- **Ataques de Bots y Scrapers:** Bloqueo de tráfico automatizado no deseado.
- **Denegación de Servicio (DoS):** Mitigación de ataques volumétricos mediante reglas de limitación de velocidad (rate limiting).
- **Restricciones Geográficas:** Bloqueo de tráfico proveniente de países específicos.

Dejar una API pública sin la protección de WAF es como dejar la puerta principal de tu aplicación sin un guardia de seguridad.

Análisis de las Etapas de API Reportadas

Las siguientes etapas (stages) de API Gateway han sido identificadas por no estar asociadas a una Web ACL de WAF, dejándolas expuestas a amenazas web.

Tipo	Nombre del Recurso (API/Stage)	Número de Cuenta
APIGatewayStage	/restapis/5e8sc9cf66/stages/v1	002670977573
APIGatewayStage	/restapis/5xkI47jynp0/stages/dev	174771279728
APIGatewayStage	/restapis/zuriq0ckj8/stages/dev	174771279728

Preguntas para tu Equipo (Acción Requerida)

La implementación de WAF es una decisión de seguridad fundamental. Por favor, revisa lo siguiente con tus equipos de seguridad y desarrollo:

1. **¿Existe ya una Web ACL de WAF corporativa o estándar que se deba utilizar?** Muchas organizaciones definen una Web ACL base con reglas comunes para todas sus aplicaciones.
2. **¿Se necesitan reglas personalizadas?** Además de las reglas administradas por AWS, ¿necesita esta API reglas específicas, como limitar la velocidad de peticiones a un endpoint particular o bloquear un rango de IPs conocido por ser malicioso?
3. **Modo de Operación:** ¿Se puede empezar implementando la Web ACL en modo **"Conteo" (Count)**? Este modo no bloquea el tráfico, pero registra las solicitudes que coincidirían con las reglas. Es una excelente manera de probar el impacto de la WAF sin riesgo de bloquear tráfico legítimo.

Consideraciones de Costo

Implementar AWS WAF tiene un costo asociado que se compone de tres partes:

1. **Costo por Web ACL:** Un costo fijo mensual por cada Web ACL que creas (aproximadamente **$5 USD al mes**).
2. **Costo por Regla:** Un costo fijo mensual por cada regla que agregas a tu Web ACL (aproximadamente **$1 USD al mes por regla**).
3. **Costo por Solicitud:** Un costo variable basado en el número de solicitudes que WAF procesa (aproximadamente **$0.60 USD por cada millón de solicitudes**).

Conclusión sobre Costos:

El costo de WAF es relativamente bajo en comparación con el costo potencial de un incidente de seguridad. Para una API con tráfico moderado, el costo mensual suele ser muy razonable y proporciona una capa de seguridad de nivel empresarial.

Cómo Solucionarlo: Asociar una Web ACL de WAF

El proceso para remediar este hallazgo implica crear una Web ACL y luego asociarla a la etapa de la API.

1. **Crear una Web ACL en AWS WAF:**
   - Navega a la consola de **WAF & Shield**.
   - Haz clic en **Crear Web ACL**.
   - Dale un nombre descriptivo (ej. `api-gateway-proteccion-general`).
   - Como tipo de recurso, selecciona **API Gateway (REST)**.

- **Agregar Reglas:** Este es el paso más importante. Se recomienda empezar agregando los grupos de reglas administradas por AWS (**AWS managed rule groups**), como:
  - **Core rule set:** Protege contra las vulnerabilidades más comunes del top 10 de OWASP.
  - **Amazon IP reputation list:** Bloquea IPs conocidas por estar asociadas con bots o actividades maliciosas.
  - **Known bad inputs:** Bloquea patrones de solicitud que se sabe que son maliciosos.
- **Acción Predeterminada:** Configura la acción predeterminada como **Permitir (Allow)**. Esto significa que solo el tráfico que coincida con una regla de bloqueo será denegado.
- Revisa y crea la Web ACL.

2. **Asociar la Web ACL a la Etapa de la API:**
   - Navega a la consola de **API Gateway**.
   - Selecciona la API correspondiente.
   - En el panel de navegación izquierdo, ve a **Etapas (Stages)** y selecciona la etapa que deseas proteger (ej. `v1` o `dev`).
   - Ve a la pestaña **Configuración de la etapa (Stage settings)**.
   - En la sección **Firewall de aplicaciones web (WAF)**, haz clic en **Editar**.
   - En el menú desplegable, selecciona la Web ACL que creaste en el paso anterior.
   - Haz clic en **Guardar cambios**.

Recomendación

Se recomienda que se cree una Web ACL de WAF con, como mínimo, los grupos de reglas administradas por AWS (Core rule set y Amazon IP reputation list) y se asocie a todas las etapas de API públicas listadas. Esta acción proporciona una defensa esencial y automatizada contra una amplia gama de ataques web, fortaleciendo significativamente la seguridad de tus APIs.

Referencias

Use AWS WAF to protect your REST APIs in API Gateway - Amazon API Gateway