[Publish] - 10. Asegurar que el tipo de Endpoint en API Gateway sea Privado y no esté expuesto a la internet pública

El hallazgo de seguridad **"Asegurar que el tipo de Endpoint de API en API Gateway sea Privado y no esté expuesto a la internet pública"** aborda un aspecto crítico de la seguridad de red. Por defecto, los endpoints de API Gateway de tipo Regional o Edge-optimized son públicos, lo que significa que pueden ser accedidos desde cualquier lugar en internet. Si bien esto es necesario para servicios de cara al público, expone la API a una gama más amplia de amenazas potenciales, como ataques de denegación de servicio, escaneo de vulnerabilidades e intentos de fuerza bruta.

Un **endpoint de API Gateway Privado** restringe el acceso para que solo sea posible desde dentro de tu Virtual Private Cloud (VPC). Esta es la configuración más segura para APIs internas, como las utilizadas para la comunicación entre microservicios, ya que las aísla completamente de la internet pública, reduciendo drásticamente su superficie de ataque.

Análisis de las APIs Públicas Reportadas

Las siguientes etapas (stages) de API Gateway han sido identificadas por tener endpoints públicos. Es necesario determinar su propósito de negocio para aplicar la configuración de seguridad correcta.

Tipo	Nombre (ID del API/Stage)	Número de Cuenta
APIGatewayStage	5e8sc9cf66	002670977573
APIGatewayStage	5xkI47jynp0	174771279728
APIGatewayStage	zuriq0ckj8	174771279728

Preguntas para tu Equipo (Acción Requerida)

Para determinar si estas APIs pueden convertirse en privadas, por favor trabaja con los dueños de las aplicaciones para responder las siguientes preguntas fundamentales:

1. **¿Cuál es el propósito de negocio de estas tres APIs?** ¿A qué aplicaciones o servicios dan soporte?
2. **¿Quiénes son los clientes previstos para estas APIs?**
   - **Aplicaciones Internas:** ¿Son consumidas únicamente por otras aplicaciones (ej. instancias EC2, funciones Lambda, contenedores) que se ejecutan dentro de tus VPCs de AWS?

- **Usuarios/Socios Internos:** ¿Son accedidas por empleados internos o socios de confianza a través de una VPN?
- **Usuarios Públicos:** ¿Están destinadas a ser utilizadas por clientes externos, aplicaciones móviles o sitios web públicos a través de internet?

Las respuestas a estas preguntas son cruciales. **Si los clientes son exclusivamente internos (dentro de una VPC, o conectados vía VPN, la API debe hacerse privada.**

Consideraciones de Costo: API Pública vs. Privada

Cambiar un endpoint de API de público a privado introduce un nuevo componente de infraestructura: un **Endpoint de VPC de tipo Interfaz (impulsado por AWS PrivateLink)**. Este componente incurre en costos que una API pública no tiene.

Comparemos los costos para una API hipotética que maneja 5 millones de llamadas y 15 GB de datos al mes en la región `us-east-1`.

Componente de Costo	API Pública (Costo Mensual)	API Privada (Costo Mensual)	Explicación de la Diferencia
Llamadas a API Gateway	~$17.50 USD (a $3.50/millón)	~$17.50 USD (a $3.50/millón)	Sin cambios. Pagas por las llamadas a la API sin importar el tipo de endpoint.
Tarifa por Hora del Endpoint de VPC	$0.00 USD	~$14.60 USD (para 2 Zonas de Disponibilidad)	**Este es el principal costo nuevo.** Un endpoint de VPC se factura por hora por cada Zona de Disponibilidad en la que se despliega (~$0.01/hr/AZ).
Procesamiento de Datos del	$0.00 USD	~$0.15 USD (a $0.01/GB)	**Este es un costo nuevo.** Se te factura por los

Endpoint de VPC			datos procesados a través del endpoint.
Total Estimado	**~$17.50 USD**	**~$32.25 USD**	El costo aproximadamente se duplica, y el aumento es directamente atribuible a la conectividad privada y segura que proporciona el Endpoint de VPC.

Conclusión sobre Costos:

Hacer una API privada introduce un costo fijo por hora para el Endpoint de VPC y una tarifa variable por procesamiento de datos. Si bien esto aumenta el costo en comparación con un endpoint público, se obtiene un aumento significativo en la seguridad al aislar tus APIs internas de la internet pública.

Cómo Solucionarlo: Haciendo una API Privada

Si has confirmado que una API debe ser privada, los pasos de alto nivel para la remediación son los siguientes:

1. **Crear un Endpoint de VPC de tipo Interfaz:** En tu VPC, crea un nuevo Endpoint de Interfaz para el servicio `execute-api`. Este es el componente que permite a los recursos dentro de tu VPC comunicarse de forma privada con API Gateway.
2. **Actualizar el Tipo de Endpoint de la API:**
   - Navega a la consola de **API Gateway** y selecciona la API específica.
   - Ve a **Configuración (Settings)**.
   - Cambia el **Tipo de endpoint (Endpoint Type)** de `Regional` o `Edge-Optimized` a `Privado (Private)`.
3. **Crear una Política de Recurso:** Adjunta una política de recurso a la API que permita explícitamente el acceso solo desde tu VPC o el Endpoint de VPC específico que creaste.

Este es un paso crítico para bloquear el acceso.

4. **Desplegar la API:** Vuelve a desplegar la etapa (stage) de la API para que los cambios surtan efecto.
5. **Actualizar Clientes:** Tus aplicaciones internas ahora necesitarán usar el nuevo nombre DNS privado proporcionado por el Endpoint de VPC para acceder a la API.

Recomendación

Se recomienda que se investigue el propósito y los clientes de las APIs reportadas. **La postura de seguridad por defecto debe ser hacerlas privadas.** Solo si encuentran un requisito de negocio claro y documentado para el acceso público a internet, deberían permanecer públicas. Para cualquier API que deba permanecer pública, asegúrense de que otros controles de seguridad como AWS WAF, limitación de velocidad (throttling) y mecanismos de autorización robustos estén implementados.

Referencias

Change a public or private API endpoint type in API Gateway - Amazon API Gateway