[Publish] - 4. Asegurar que los balanceadores de carga elásticos (ELB) usen listeners seguros

El hallazgo de seguridad **"Asegurar que los balanceadores de carga elásticos (ELB) usen listeners seguros"** se enfoca en una práctica de seguridad esencial: el cifrado de datos en tránsito. Un "listener" es un proceso que verifica las solicitudes de conexión que llegan al balanceador. Si un listener está configurado para usar un protocolo no seguro como **HTTP**, todo el tráfico entre el cliente (usuario) y el balanceador de carga viaja en texto plano.

Esto crea un riesgo de seguridad significativo:

- **Interceptación de Datos (Man-in-the-Middle):** Un atacante en la misma red puede interceptar el tráfico y leer información sensible, como nombres de usuario, contraseñas, números de tarjetas de crédito y datos personales.
- **Manipulación de Datos:** Un atacante podría modificar los datos en tránsito sin que el usuario o la aplicación se den cuenta.
- **Pérdida de Confianza:** Los navegadores modernos marcan activamente los sitios HTTP como "No Seguros", lo que daña la confianza del usuario en tu aplicación.

Para mitigar estos riesgos, es imperativo usar un listener seguro que utilice el protocolo **HTTPS (HTTP sobre TLS)**, el cual cifra toda la comunicación entre el cliente y el balanceador de carga.

Análisis de los Listeners Reportados

Los siguientes listeners de balanceadores de carga han sido identificados por no utilizar un protocolo seguro (HTTPS).

Tipo	Nombre del Recurso (Listener)	Número de Cuenta
LoadBalancer	listener/app/Colabora/1d5feb4717929008/3384be1888b63b9e	398984081329
LoadBalancer	listener/app/django-lb/30a6513ddc6c110e/78ca2c282d701320	002670977573
LoadBalancer	listener/app/gs-services/844a3cc33b5	002670977573

	de0c7/bbd83a43c7a18843	
LoadBalancer	listener/app/ServDigitales/392f0dbef015d8d1/811fa4d7af3f9169	890342916428

Preguntas para tu Equipo (Acción Requerida)

Para asegurar una transición sin problemas a HTTPS, por favor coordina con los dueños de las aplicaciones correspondientes para responder lo siguiente:

1. **Soporte de Aplicación:** ¿Las aplicaciones detrás de estos balanceadores de carga están configuradas para manejar tráfico HTTPS? (Generalmente, la terminación SSL/TLS se hace en el balanceador, por lo que la aplicación no necesita cambios mayores, pero es crucial confirmarlo).
2. **Certificados SSL/TLS:** ¿Tenemos un certificado SSL/TLS válido para los dominios asociados a estas aplicaciones, disponible en AWS Certificate Manager (ACM)? Si no, necesitamos solicitar o importar uno.
3. **Redirección HTTP a HTTPS:** Una vez que el listener HTTPS esté activo, ¿queremos forzar todo el tráfico para que use la conexión segura? La mejor práctica es configurar una redirección permanente (HTTP 301) del listener HTTP al listener HTTPS.

Consideraciones de Costo

Implementar listeners seguros es muy rentable en AWS.

- **Listeners en ELB:** No hay un costo adicional por usar un listener HTTPS en lugar de uno HTTP en tu balanceador de carga.
- **Certificados SSL/TLS:** Si utilizas **AWS Certificate Manager (ACM)** para aprovisionar tus certificados, los certificados públicos que uses con tu balanceador de carga son **gratuitos**.
- **Tráfico de Red:** No hay diferencia en el costo del procesamiento de datos entre HTTP y HTTPS.

Conclusión sobre Costos:

No hay un aumento significativo en los costos por migrar a listeners seguros, y los beneficios en seguridad son inmensos.

Cómo Solucionarlo: Configurar un Listener Seguro (HTTPS)

El proceso para remediar este hallazgo implica agregar un nuevo listener para el puerto 443 y asociarle un certificado.

1. **Verificar/Solicitar Certificado en ACM:**
   - Navega a la consola de **AWS Certificate Manager (ACM)**.
   - Verifica que tengas un certificado emitido y válido para el dominio de tu aplicación (ej. `colabora.sanchezgrupo.com`).
   - Si no tienes uno, solicita un nuevo certificado público.
2. **Agregar un Listener HTTPS al Balanceador:**
   - Navega a la consola de **EC2**.
   - En el panel de navegación izquierdo, ve a **Balanceadores de Carga**.
   - Selecciona el balanceador de carga correspondiente.
   - Ve a la pestaña **Listeners**.
   - Haz clic en **Agregar listener**.
   - Para el protocolo, elige **HTTPS** y el puerto **443**.
   - En la sección **Acción predeterminada**, configura el reenvío al grupo de destino (target group) correcto.
   - En la sección **Política de seguridad**, se recomienda dejar la política predeterminada (`ELBSecurityPolicy-2016-08`) a menos que tengas requisitos de cumplimiento específicos.
   - En **Certificado SSL/TLS predeterminado**, elige **Desde ACM** y selecciona el certificado que verificaste en el paso 1.
   - Haz clic en **Agregar**.
3. **(Recomendado) Configurar Redirección:**
   - Edita el listener existente de **HTTP en el puerto 80**.
   - Elimina la acción actual de reenvío al grupo de destino.
   - Agrega una nueva acción que sea **Redirigir a...**.
   - Configura la redirección a **HTTPS** en el puerto **443** con un código de respuesta **301 - Movido permanentemente**.
   - Guarda los cambios.

Recomendación

Se recomienda que se actualicen todos los balanceadores de carga listados para que utilicen listeners HTTPS (puerto 443) y que se configure una redirección de todo el tráfico HTTP a HTTPS. Esta acción es fundamental para proteger la integridad y confidencialidad de los datos que se transmiten hacia tus aplicaciones, además de fortalecer la confianza de tus usuarios.

Referencias

Ensure AWS load balancers use secure listener protocols (HTTPS, SSL/TLS) - AWS Prescriptive Guidance