

Secure App

AREM-1

April 21, 2020

1 Introducción

En este laboratorio se desarrolló una aplicación web cuyos servicios pueden ser consumidos únicamente por usuarios autorizados a través de tokens. De la misma manera, esta aplicación se comunica con otra y accede a los servicios ofrecidos por la misma, utilizando certificados SSL.

2 Descripción

El cliente accede a la aplicación utilizando el protocolo HTTPS, de modo que primero debe tener en su navegador el certificado que dice que el sitio es confiable. Como el usuario debe loggearse para que se pueda identificar si es un usuario válido (se utiliza una base de datos PostgreSQL), se garantiza la autenticación. Si el usuario es válido, se le asigna un token con el cual podrá acceder a los servicios ofrecidos en la app (servidor), el cual desencripta el token y comprueba si el cliente tiene permisos para acceder al recurso solicitado. De este modo se garantiza la autorización, y la integridad ya que el servidor tiene que verificar que el token no fue alterado y es legítimo. Al acceder a la app principal, esta se comunica a través de certificados SSL con otra aplicación, de este manera se garantiza autenticación porque el certificado SSL asegura la identidad, y se asegura la integridad, ya el protocolo SSL asegura que el intercambio de información en la red no es alterado y por tanto se dice que es fiable.

A continuación se presenta la arquitectura:

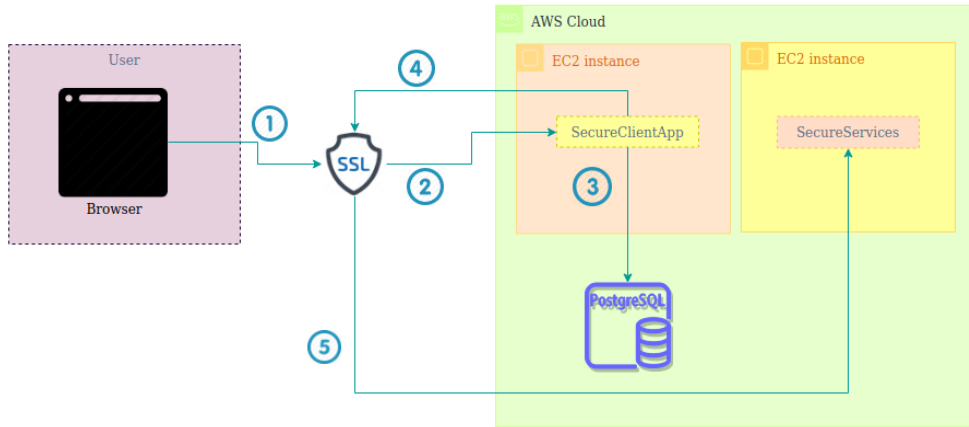


Figure 1: Diagrama-Estructura

3 Escalabilidad

- Por parte de los servicios, si se desea adicionar más de ellos, simplemente se agregan sus respectivas funcionalidades en la aplicación correspondiente, ya sea creando una nueva interfaz de servicios y incluyéndolos en la que se encuentra actualmente.

- Por el lado de los servidores web, si se quiere añadir más de ellos, estos pueden comunicarse con los ya existentes generando certificados SSL que confíen en ellos y que los ya existentes confíen en los nuevos.

4 Conclusiones

En este laboratorio se pudo crear una aplicación web segura en todos frentes, cuyo funcionamiento además, puede ser probado en servidores del mundo real, ya sea utilizando AWS, GPC, Azure, entre otros, para tener una idea más práctica del comportamiento de la aplicación.