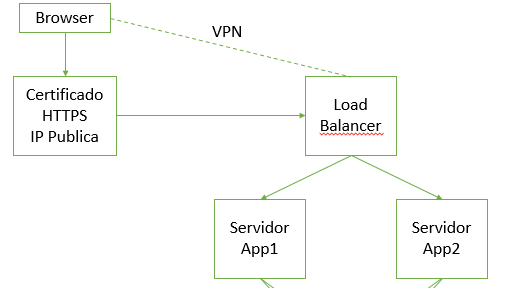
QA Disponibilidad

Arquitectura Base:



Certificado HTTPS LetsEncrypt:

* Se solicita el certificado a la CA con la herramienta letsencrypt, con los siguientes comandos

$sudo /root/certbot-auto certonly --cert-path /etc/letsencrypt/archive/st0263.dis.eafit.edu.co --expand -d proyecto26.dis.eafit.edu.co

$sudo /root/certbot-auto certonly -d st0263.dis.eafit.edu.co --expand -d proyecto19.dis.eafit.edu.co

Se deben concatenar 2 archivos:

$ sudo mkdir /etc/haproxy/certs

$ sudo cd /etc/haproxy/certs/

$ sudo cat /etc/letsencrypt/live/st0263.dis.eafit.edu.co/fullchain.pem /etc/letsencrypt/live/st0263.dis.eafit.edu.co/privkey.pem > /etc/haproxy/certs/st0263.pem

Para probar la conexión se ingresa <https://proyecto26.dis.eafit.edu.co> y <http://proyecto26.dis.eafit.edu.co>

* Se configura el HAProxy para que acepte peticiones por ambos protocolos, se agregan las siguientes líneas:

Frontend https

bind proyecto26.dis.eafit.edu.co:443 ssl crt /etc/haproxy/certs/proyecto26.pem

acl host\_proyecto26 hdr(host) -i proyecto26.dis.eafit.edu.co

use\_backend proyecto26\_cluster if host\_proyecto26

Frontend http \*:80

acl host\_proyecto26 hdr(host) -i proyecto26.dis.eafit.edu.co

use\_backend proyecto26\_cluster if host\_proyecto26

backend proyecto26\_cluster

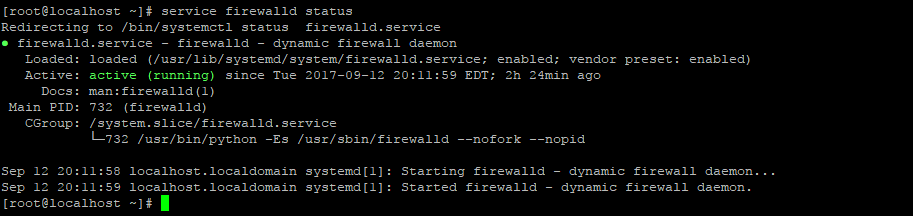
balance leastconn

option httpclose

cookie JSESSIONID prefix

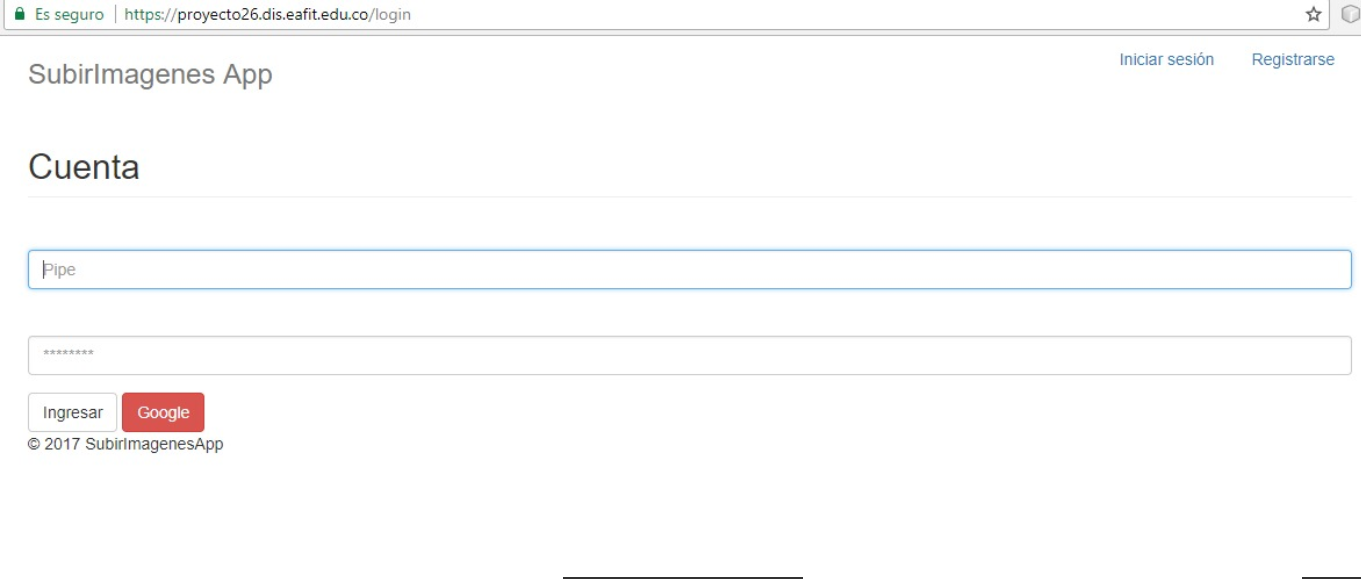
server node6 10.131.137.184:80

* Se valida que el firewall de los demas servidos este activo (corriendo), con el comando service firewall status.

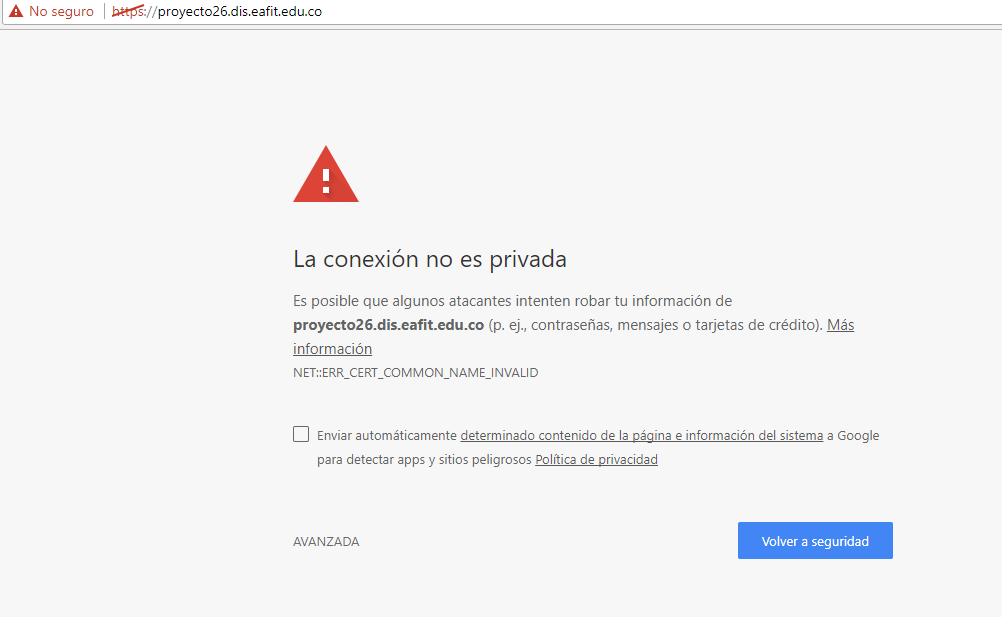


Caso de Estudio:

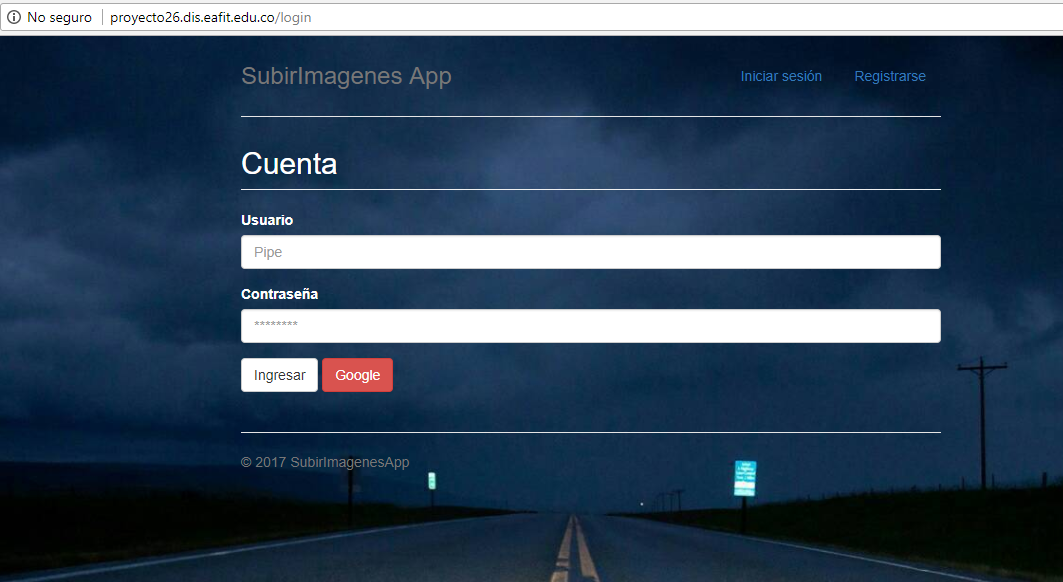
* Se ingresa por la dirección <https://proyecto26.dis.eafit.edu.co>



En este certificado se tienen varios inconvenientes, ya que desconfigura la aplicación y en la mayoría de las veces genera la alerta de certificado no seguro



Tambien se prueba la conexión por http:/proyecto26.dis.eafit.edu.co



Para la parte de la autenticación con Google se utilizó la estrategia de Google “passport-google-oauth”, en el que se debe configurar un clientID, clientSecret y callbackURL. Éstos se obtienen a través de Google Developers Console, es decir, para cada cuenta de google que se vaya a utilizar para autenticarse al sistema, se debe crear un proyecto y seguidamente crear una credencial que es la que me va a permitir que una aplicación externa utilice los datos de mi cuenta de Google. Además se debe configurar la url desde donde se realiza la petición a google y la url de re direccionamiento después de la autenticación.

