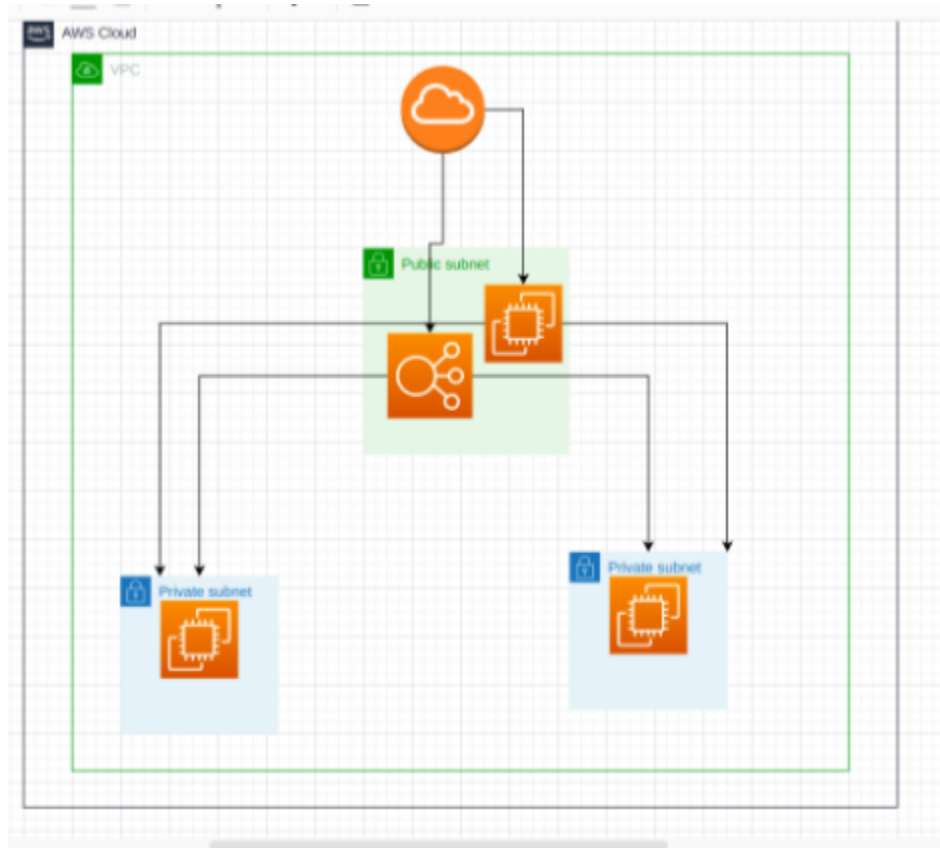


DevOps: Final Project AWS

Para el proyecto final nos daban una serie de restricciones que tenía que cumplir nuestra arquitectura para que esté acorde a los requisitos del cliente.

La arquitectura planteada en el ejercicio estaba mal por lo que tuvimos que corregir y hacer de la forma que consideramos apropiada con lo aprendido.

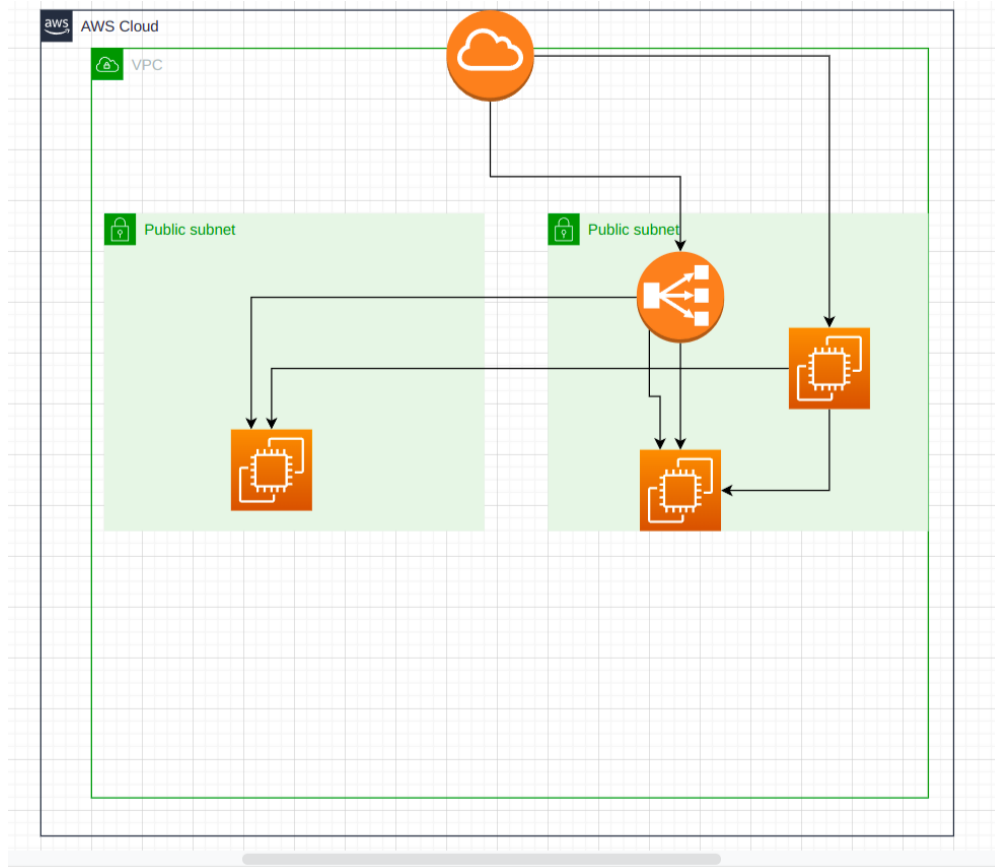
Primero planteamos una arquitectura de esta forma:



Donde en las subredes privadas colocamos los servidores y gestionamos las peticiones http mediante el load balancer, que este estaba alojado en la subred pública junto con el bastión.

Por mala suerte, luego de intentos, nos dimos cuenta que las app no podían estar en una subnet privada para recibir el tráfico proveniente del Load Balancer, además que este tenía que ser internet facing para recibir tráfico proveniente de la internet gateway

Al notar el problema mencionado, replanteamos la arquitectura de la siguiente manera:

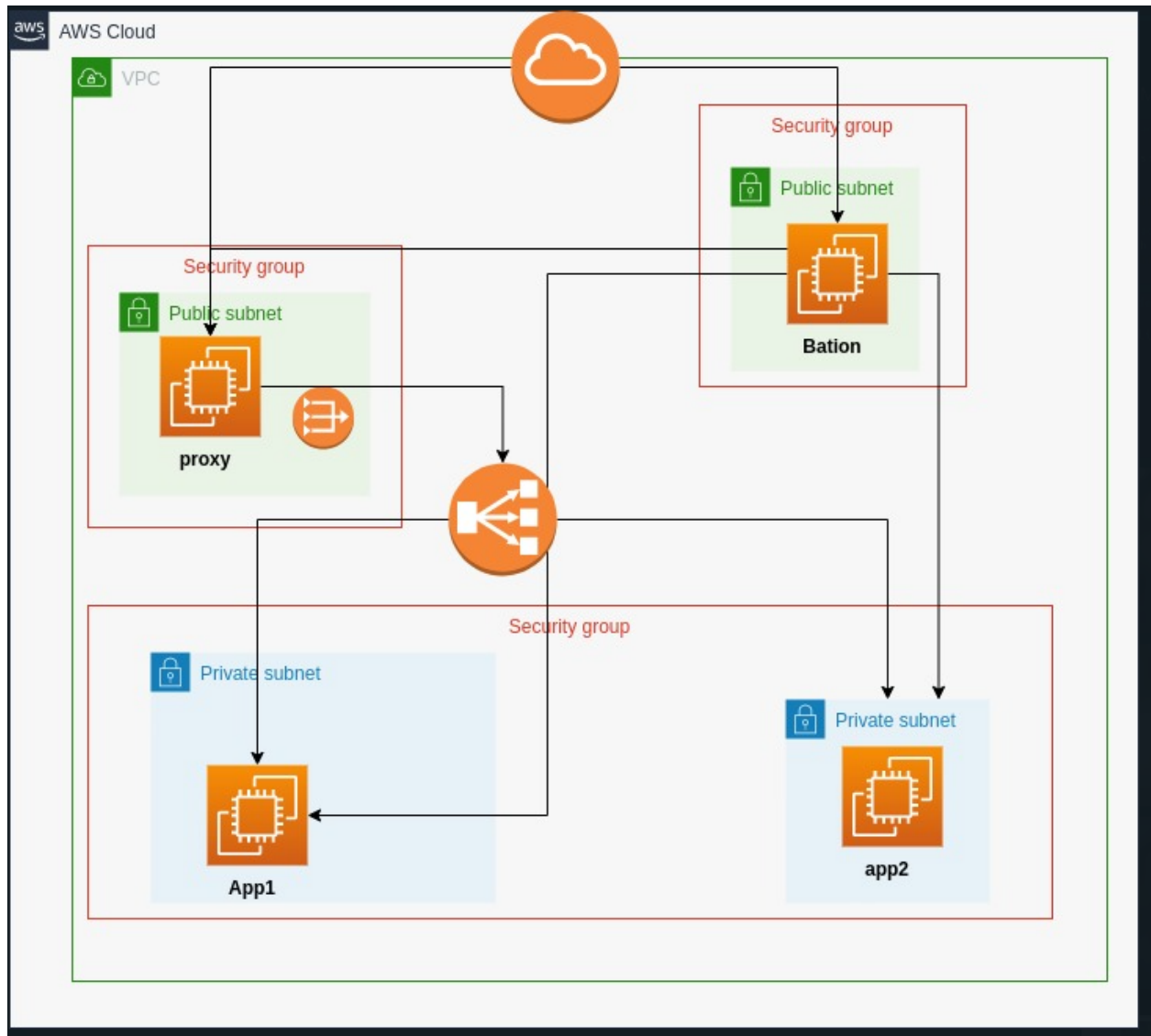


Esta solución no satisface los requerimientos de seguridad de la consigna pero podíamos hacer la conexión de los servidores con el load balancer y este repartir el tráfico proveniente de la internet gateway.

Donde contábamos con los dos servidores en subredes públicas y ambos conectados a un load balancer, esté alojado en una subred pública. Luego al bastion lo colocamos en una subred pública. Donde el bastion y el Load Balancer estaban conectados al internet gateway para la conexión a internet.

Pero surgió el problema de que las instancias de app tendrían que tener ip pública para que ambas tengan acceso a internet, por lo que no era nada seguro.

Entonces el profesor nos propuso colocar un proxy para que esta redirige el tráfico de la internet gateway al load balancer, así este balanceaba el tráfico a ambas instancias que estarán en subredes privadas para mayor seguridad, donde nos quedo el gráfico de esta forma:



Para esto creamos cuatro subredes dentro de la vpc, donde dos eran públicas y dos privadas, en distintas regiones. Además creamos cuatro instancias, dos en subredes públicas, siendo una el proxy que gestionará el tráfico que se dirige al load balancer y otra el bastión que sería el que administra todas las instancias, ambas conectadas a la internet gateway para el acceso a internet. Luego contamos con dos instancias privadas que ambas tienen una nat para tener acceso a internet y ambas conectadas al load balancer.

Para los security groups, creamos cuatro. Uno de ellos era para el bastión que permitía el ingreso de cualquier puerto por http y https. Luego el del proxy que solo permite acceso desde el bastión. En el tercero, que vendría a ser el del load balancer, donde permitimos acceso por todos los puertos, todo lo proveniente solamente del proxy. Y

por último el de las apps donde solo permitimos ingreso por el puerto 22 al security group del load balancer