networking

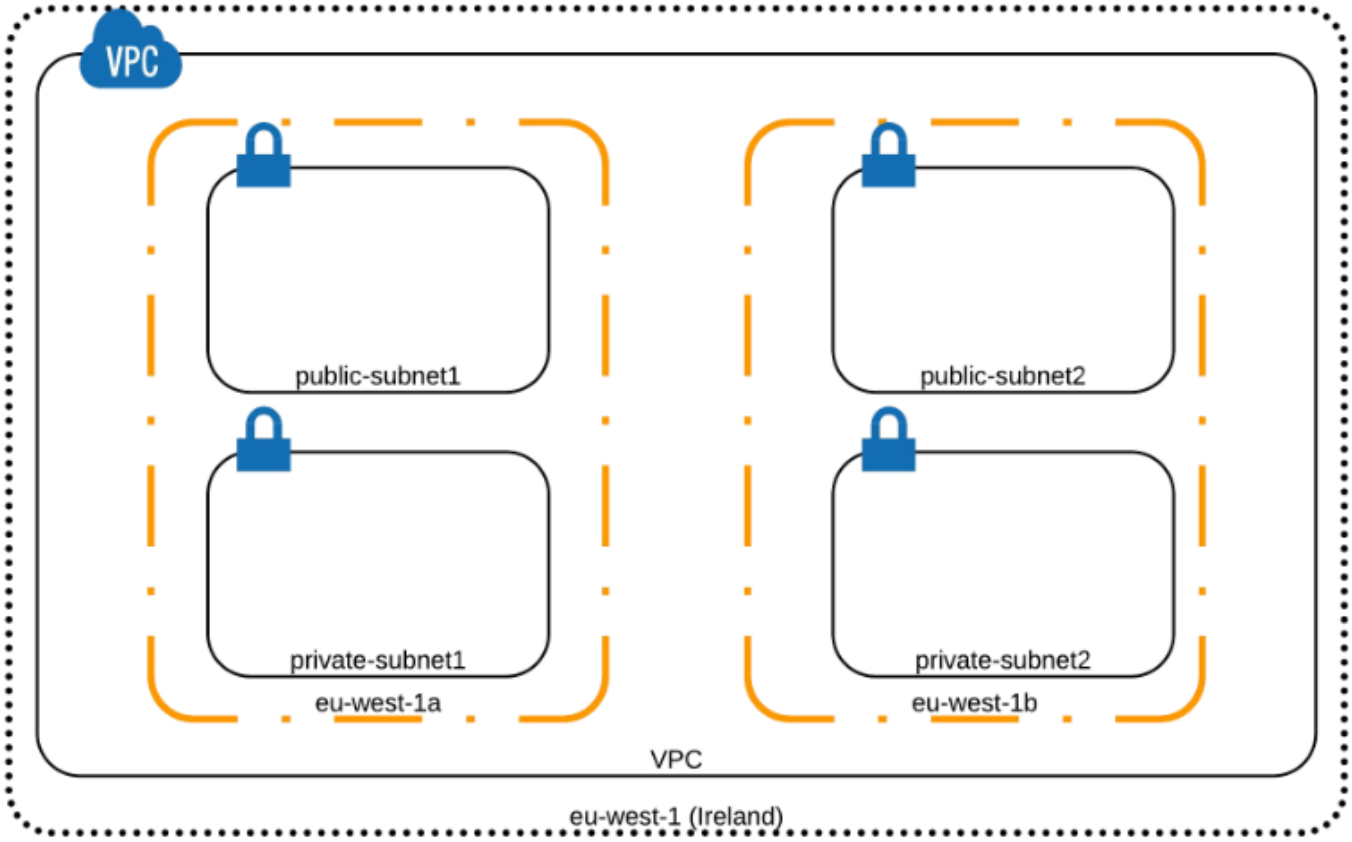
VPC y subnets

VPC (Virtual Private Cloud)

- Segmento de red completamente aislado
- Utiliza direccionamiento privado
- Permite segmentar la arquitectura en redes distintas y gestionar las visibilidades según os convenga
- Pueden tener acceso directo a Internet o no
- Permite comunicar recursos de AWS sin necesidad de utilizar direcciones IP públicas
- Es de alcance regional

Subnets

- Pequeños segmentos de red dentro de nuestra VPC
- Se pueden crear todas las subnets que necesitemos siempre y cuando os queden bloques CIDR disponibles dentro de la VPC
- Pueden estar comunicadas entre ellas o no
- Son de alcance zonal (AZ)
- No son modificables luego de creadas



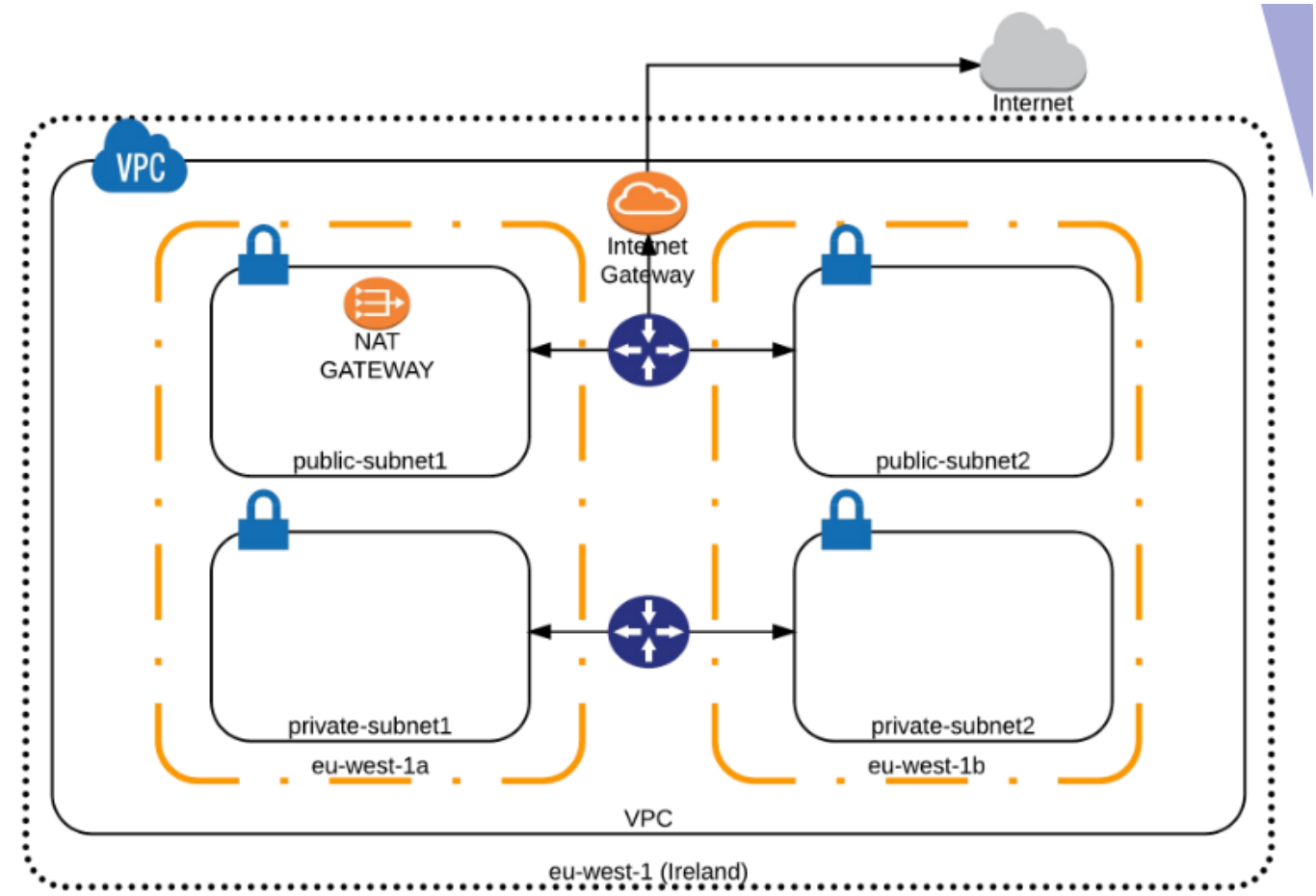
Práctica con subnets públicas y privadas

- Networking → VPC
  - espacio direccionamiento más amplio (10.0.0.0/16)
  - se crea para cada VPC el DHCP y la tabla de enrutado

- dentro creamos subnets
- al crear subnets en zonas de disponibilidad diferentes podemos hacer nuestro sistema más resistente a una caída (de 1 zona)
- subnet actions:
  - modificar autoasignación ip pública

Routing table

interconexión entre la VPC



Routing tables

- Son utilizadas para enrutar el tráfico dentro de las VPCs
- Se crea una default en el momento de creación de VPC
- Se pueden crear varias y asociar subnets de manera independiente
- Deberíamos tener al menos una tabla de rutas para subnets públicas y otra para subnets privadas

IGW (Internet Gateway)

- Es el punto de conexión de la VPC con Internet
- Se referencia en la tabla de rutas
- Solo pueden llegar a Internet los recursos que tenga IP pública
- Es gestionado y escalado por AWS
- No requiere configuración

- solo puede haber un IGW por VPC
- añadimos la ruta por defecto (0.0.0.0) al IGW creado

NAT Gateway

- Es el Gateway de acceso a Internet para las subnets privadas
- Tiene que estar creado en una subnet pública con una tabla de rutas que tenga como ruta por defecto el IGW
- Tiene una IP pública y estática (elastic IP)
- Es muy útil para consultar APIs o servicios de terceros que requieren que las peticiones vengan de IP fija
- Es escalado y gestionado por AWS
- en las subnets privadas indicamos una ruta por defecto al NAT creado

NACL (Network Access Control List)

- Son listas de control de acceso a nivel de red y transporte que aplican a las subnets de VPC
- La configuración por defecto es de tipo ALLOW ALL
- Es muy útil cuando detectamos que de una IP o un bloque en particular estamos recibiendo un ataque
- Podemos crear varias NACL y asociarlas de manera independiente a las subnets de la VPC

Internet Gateway

NAT Gateway

Network Access Control List