VPC

Virtual Private Cloud

- red aislada
- puedes tener más de una por región (o en varias regiones)
- defines rangos, subredes, tablas de ruta y gateways
- ...
- seguridad:
  - NACL :
    - a nivel de subred
    - permite allow y deny
  - Security Groups:
    - solo allow
- subnet : recursos aislados
- internet gateway : acceso a internet (por defecto no hay definido)
- nat gateway : acceso a internet de salida
- hardware VPN connection
  - virtual private gateway : lado amazon
  - costumer gateway : lado cliente
  - Direct Connect para conexiones más potentes (por ver)
- Peering Connection: interconexión entre diferentes VPC
- VPC endpoints : tráfico interno
- GRAFICO AWS VPC COMPONETS
- al crearlo, el wizard nos permite:
  - VPC con 1 subnet
  - VPC con 2 subnets (público y privada)
  - ...
  - ...
- tamaño mínimo subnet: /28
- tamaño máximo: /16
- se puede añadir otro rango de IPs (nuevo, no examen)
- instancias sin IP pública se pueden conectar de 2 maneras:
  - NAT
  - hardware VPN connection o Direct connect : la salida a internet es a través del cliente (con sus recursos: conexión, firewall, etc)
- que puedo hacer:
  - lanzar instancias en una subnet
  - asignar rangos de IPs en las subnets
  - enrutado entre las subnets
  - crear internet gateway
  - más seguridad
  - Instance Security Groups - Stateful
  - NACL - Statefuless
- Default VPC VS Custom VPC
  - permite lanzar instancias inmediatamente
  - todas las subredes tiene acceso a internet
- VPC Peering
  - conexión de 2 VPC
  - permite entre-regiones
  - permite diferentes cuentas
  - han de tener rangos de IPs que no se solapen
  - no transitivas

Laboratorio

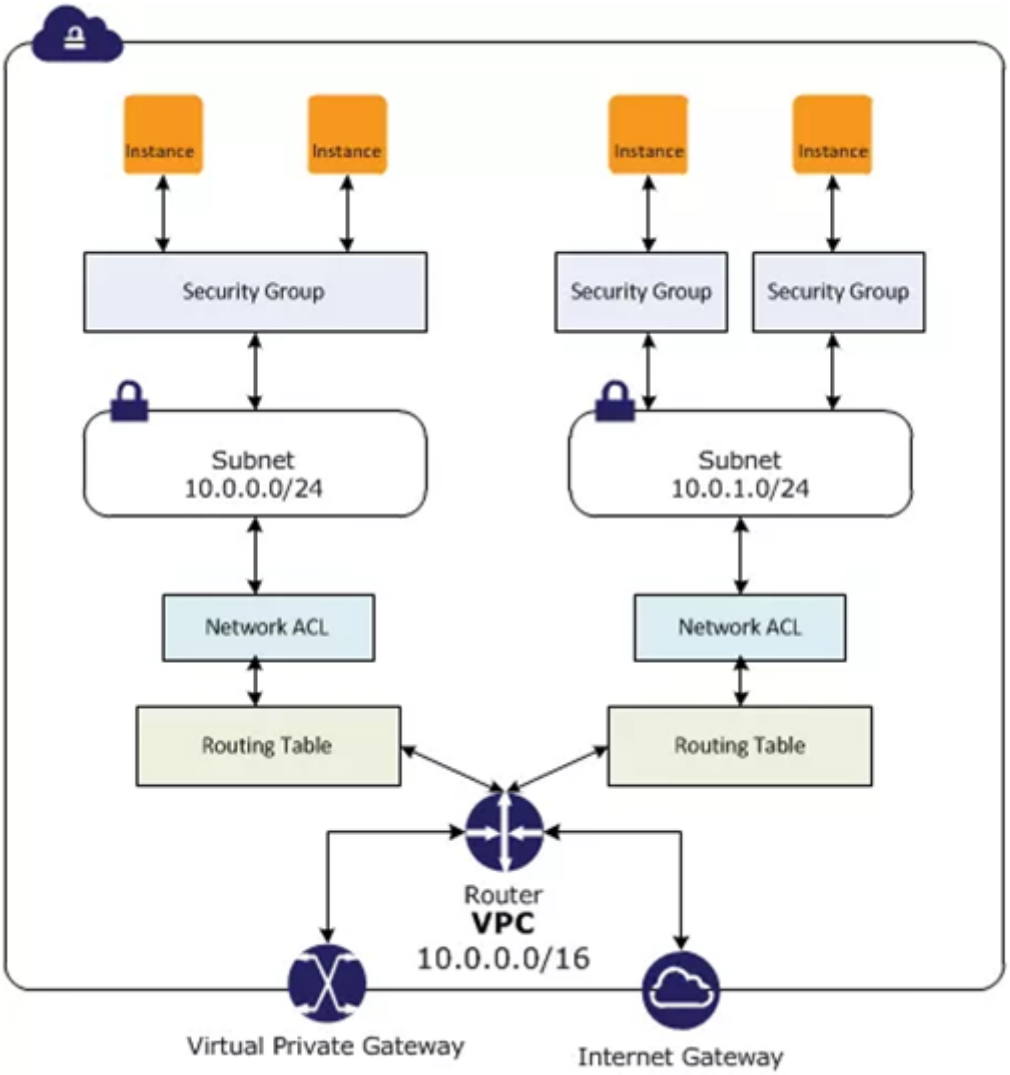
- crear VPC propia (rango 10.0.0.0)
- crear 2 subnets
    - solo disponible en una AZ
    - nombre: rango IP = 10.0.1.0-private
    - aunque tenga una IP pública, será innacesible hasta que no haya un internet gateway
- crear internet gateway
    - solo 1 por VPC
- atacharlo a la VPC
    - siguen sin tener acceso a internet
    - hay que modificar la Main Route Table
- crear una Route Table en la VPC
    - añadir una ruta de salida 0.0.0.0 al gateway que hemos creado anteriormente
- al crear un nuevo SG, el inbound está deshabilitado (o no tiene ninguna regla)

NAT Gateway

- salida de máquinas que no tienen un internet gateway asignado
- dos opciones:
    - ami nat instance server (en decadencia) :
        - hay que crearla en la subnet pública
        - modificar la instanacia → Networking → Change Source/Dest. Check
        - añadir en la subnet privada he de modificar la tabla de rutas y añadir un **0.0.0.0/0** y asignarle la NAT INSTANCE
    - NAT gateway
        - totalmente gestionado por Amazon
        - crear el NAT en la subnet pública
        - modificar la tabla de rutas de la subnet privada y añadir un **0.0.0.0/0** y asignarle el NAT

ACLs

esquema



más información de todo el curso: [[http://jayendrapatil.com/category/aws/vpc/acl/

VPC Flow logs

- a nivel de VPC, subnet o interfaz
- tráfico aceptado, rechazado o todo
- almacenamiento en CloudWatch Logs o S3 Bucket
- No se pueden hacer flow logs de VPCs «peered» que no estén en tu cuenta
- no se pueden tagear
- no se captura:
  - el tráfico a los DNS
  - activación de licencia de windows
  - tráfico a 169.254.169.254 (metadatos)
  - DHCP
  - ...

VPC Gateway Endpoint

- examen: solo los Gateway
- endpoints privados para S3 y DinamoDB, de manera que las conexiones a estos servicios se realice internamente (y no salga a internet, ya que estos servicios «publican» directamente con IP pública)
- el tráfico dentro del VPC no se cobra