Networking

VPC

Architecture

VPC

- CIDR de /16 à /28

Subnets

- private (par défaut) ou public (si on assigne une IGW Internet Gateway)
- 5 adresses réservées

Première	Network
Deuxième	AWS routing
Troisième	AWS DNS
Quatrième	AWS réservé
Dernière	Broadcast

Securité

NACL

- Règles de firewalling s'appliquant à un ou des subnets
- Par défaut le NACL autorise tous les trafics
- On peut ajouter des règles allow et deny
- Stateless : si on autorise un flux entrant il faut autoriser le flux pour la réponse

Security Group

- Règles de firewalling s'appliquant à une ou des instances
- Ce que l'on ajoute est allow
- Par défaut ce qui n'apparait pas est deny
- La règle par défaut interdit le trafic entrant, autorise le trafic sortant et le trafic avec les ressources du même security group par défaut
- Statefull : quand on autorise un flux entrant, la réponse sera autorisé

NAT gateway

- Permet l'accès internet sortant à un réseau privé (pour mise à jour OS par exemple)

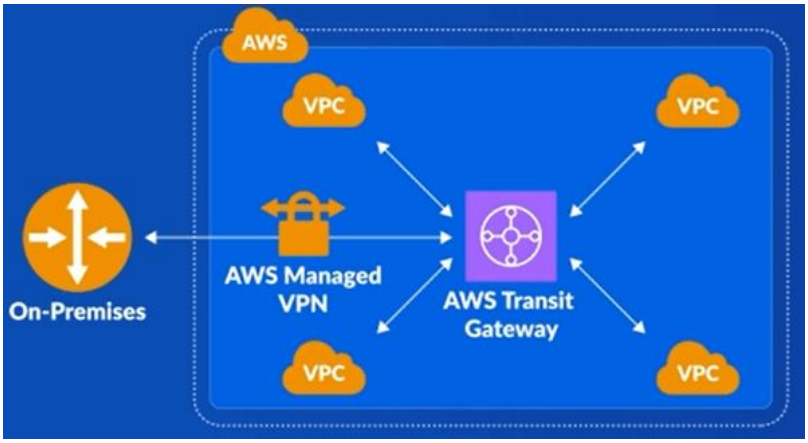
Bastion

- Instance de rebond dans un réseau public pour accéder à des instances dans un réseau privé
- Doit être particulièrement sécurisé
- Autoriser SSH entrant depuis une @IP externe, autoriser SSH entrant sur instance dans le réseau privé depuis @IP du bastion et utiliser SSH Agent Forwarding.

Connectivité

VPN

- Virtual Gateway (VGW) côté AWS (comme IGW géré par AWS)
- Customer Gateway (CGW) côté client
- Le tunnel est initialisé par le client, il faut introduire un monitoring ping pour éviter une déconnexion du tunnel au bout de 10s
- Ajouter une route côté réseau privé pour accéder au réseau client via la VGW

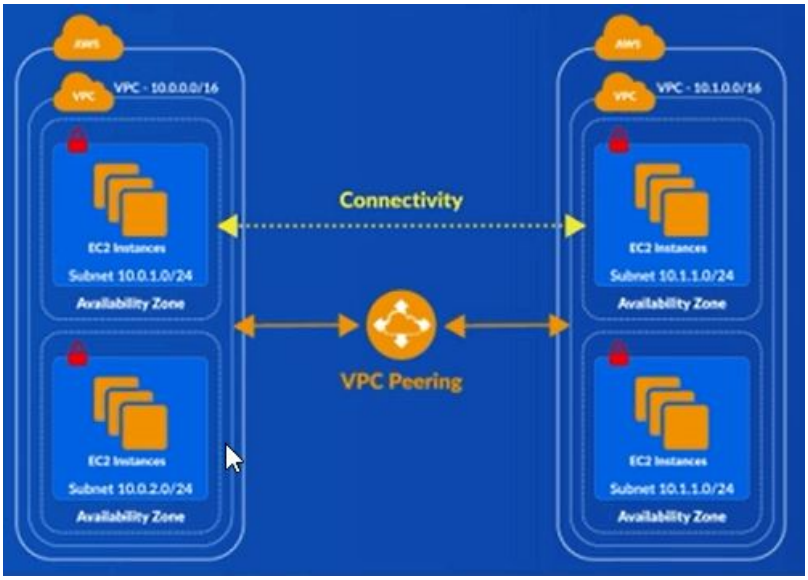


Direct Connect

- Accès direct sans passer par internet
- Un batiment avec des équipements AWS et client

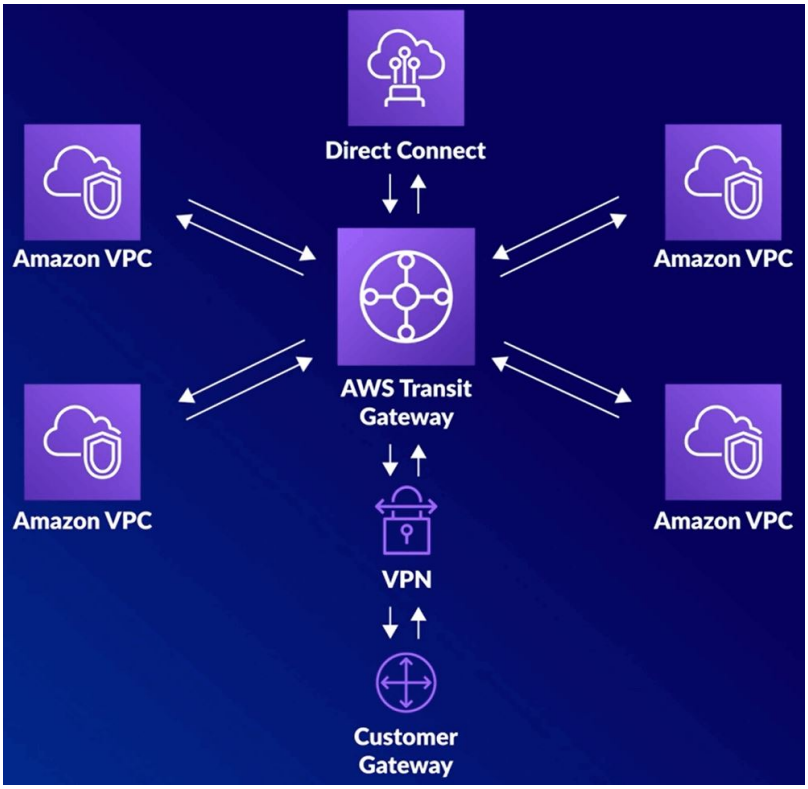
VPC peering

- Possible d'un VPC à un autre en one to one y compris entre différentes régions
- Attention pas possible si recouvrement d'adresse entre les 2 VPCs
- Requestor / Acceptor



Transit Gateway

- Sorte de routeur régional pour interconnecter plusieurs réseaux
- Comme pour le VPC peering impossible de relier des VPCs ayant un recouvrement d'adresse
- Fonctionne en créant des attachment (VPC, VPN, ...)
- 5 TGW max par région et par compte
- 5 TGW attachments max par VPC
- 5000 TGW attachments max



Divers

Composants

Elastic IP Adress

- Permet d'avoir une @IP publique qui ne change pas

Elastic Network Interface

- Permet d'ajouter des interfaces réseaux pour adresser différents subnets

Performances

Elastic Network Adaptor

- Pour de meilleures performances réseaux jusqu'à 100 Gbps pour instances Linux (kernel 2.6.32 et 3.2 et supérieures)
- Il faut installer le module ENA et activer l'attribut enaSupport

VPC Endpoints

AWS Global Accelerator

- Permet d'envoyer les requêtes TCP et UDP plus rapidement aux ressources au sein du réseau AWS

DNS Route 53

Zones

- Public hosted zone : routage du trafic sur internet
- Private hosted zone : routage au sein des VPC

Route 53 routing policy

- failover routing policy : routage en fonction de l'état des ressources
- weighted routing policy : routage en fonction d'un pourcentage que l'on a déterminé
- latency routing policy : routage selon le temps de réponse le plus rapide au sein de plusieurs régions

Amazon Cloud Front

- Service qui utilise les Edge Locations pour servir de cache aux applications

---

From:
https://wiki.iot-acs.fr/ - **Wiki**

Permanent link:
https://wiki.iot-acs.fr/doku.php?id=all:bibles:aws:presentation:4-networking

Last update: **2026/07/23 13:29**