Construisez un réseau sécurisé sur AWS

Par Pierre-François HOUESSOU

Qui suis-je?

Architecte Cloud à COFOMO Québec avec 9 ans d’exp

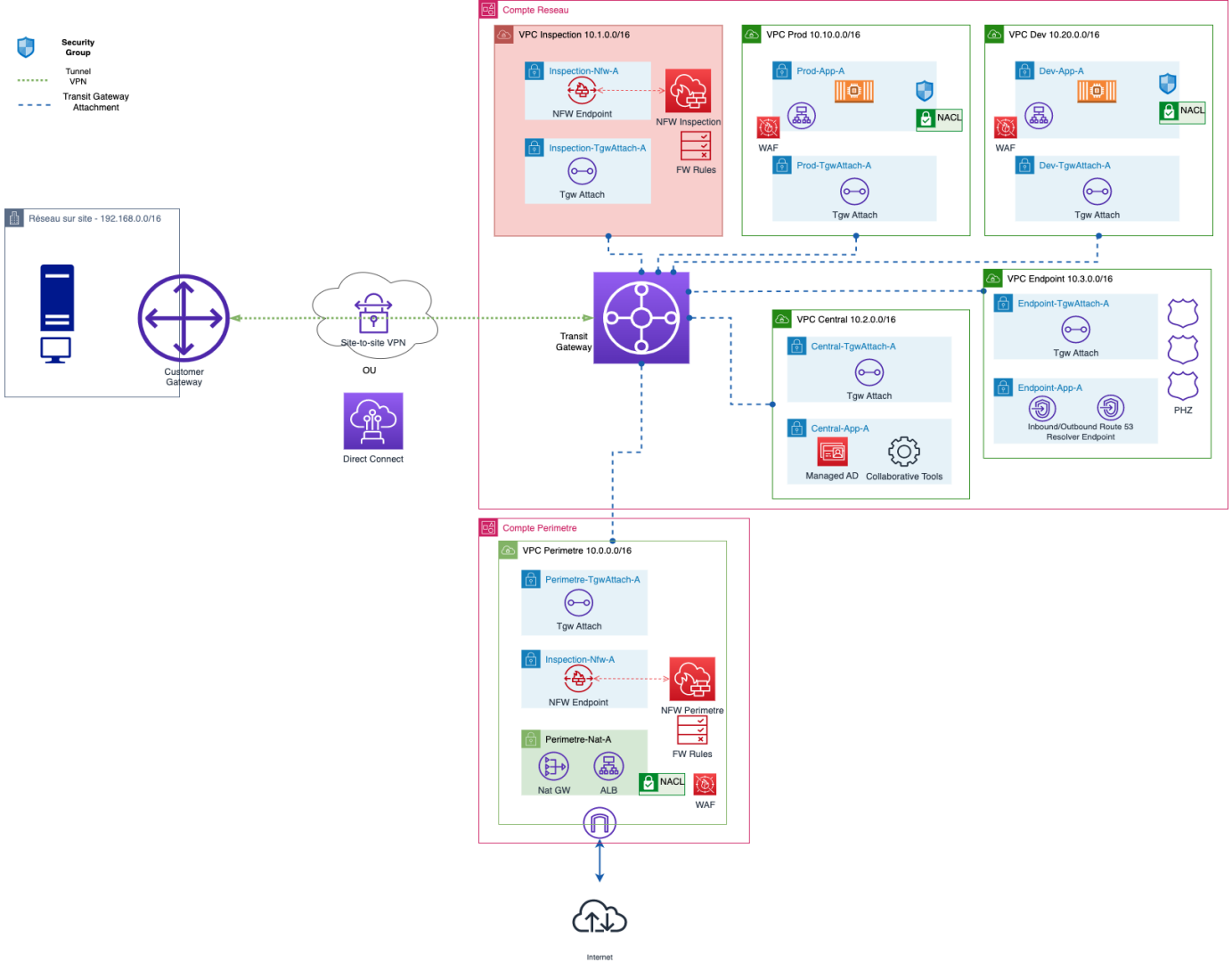
Introduction

Agenda

Sommaire

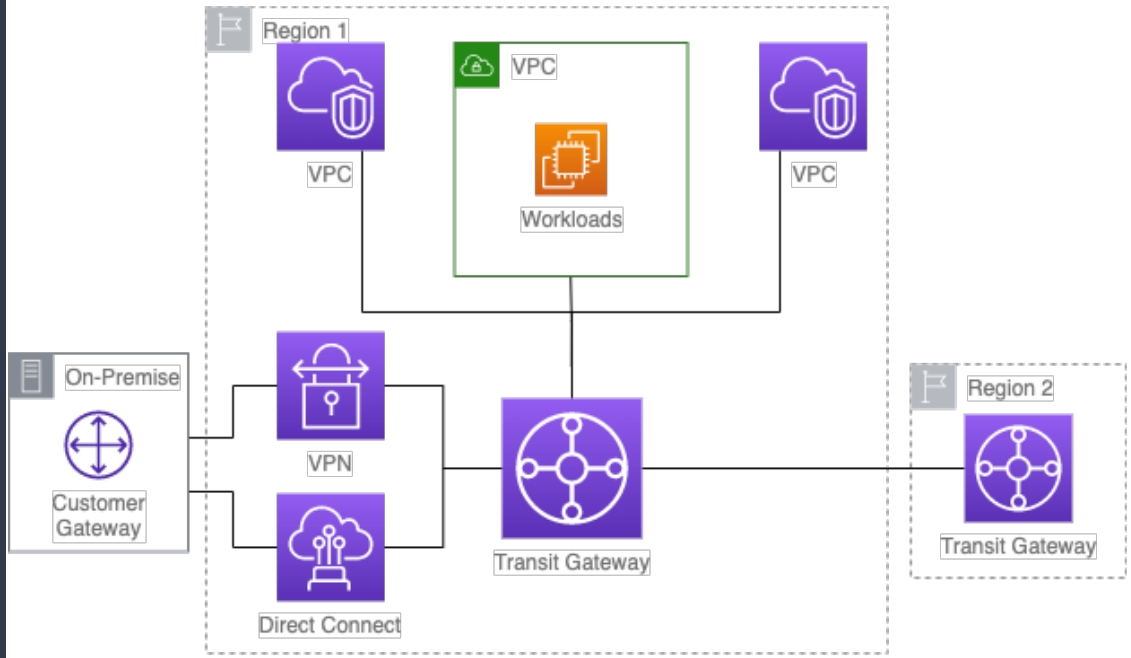
- Présentation de l’architecture cible
- Démo
- Questions - Réponses
- Conclusion

Architecture cible


Security Group
Tunnel VPN
Transit Gateway Attachment
Compte Reseau
VPC Inspection 10.1.0.0/16
Inspection-Nfw-A
NFW Endpoint
NFW Inspection
Inspection-TgwAttach-A
Tgw Attach
FW Rules
VPC Prod 10.10.0.0/16
Prod-App-A
NACL
WAF
Prod-TgwAttach-A
Tgw Attach
VPC Dev 10.20.0.0/16
Dev-App-A
NACL
WAF
Dev-TgwAttach-A
Tgw Attach
Réseau sur site - 192.168.0.0/16
Customer Gateway
Site-to-site VPN
OU
Direct Connect
Transit Gateway
VPC Endpoint 10.3.0.0/16
Endpoint-TgwAttach-A
Tgw Attach
Endpoint-App-A
Inbound/Outbound Route 53 Resolver Endpoint
PHZ
VPC Central 10.2.0.0/16
Central-TgwAttach-A
Tgw Attach
Central-App-A
Managed AD
Collaborative Tools
Compte Perimetre
VPC Perimetre 10.0.0.0/16
Perimetre-TgwAttach-A
Tgw Attach
Inspection-Nfw-A
NFW Endpoint
NFW Perimetre
FW Rules
Perimetre-Nat-A
Nat GW
ALB
NACL
WAF
Internet

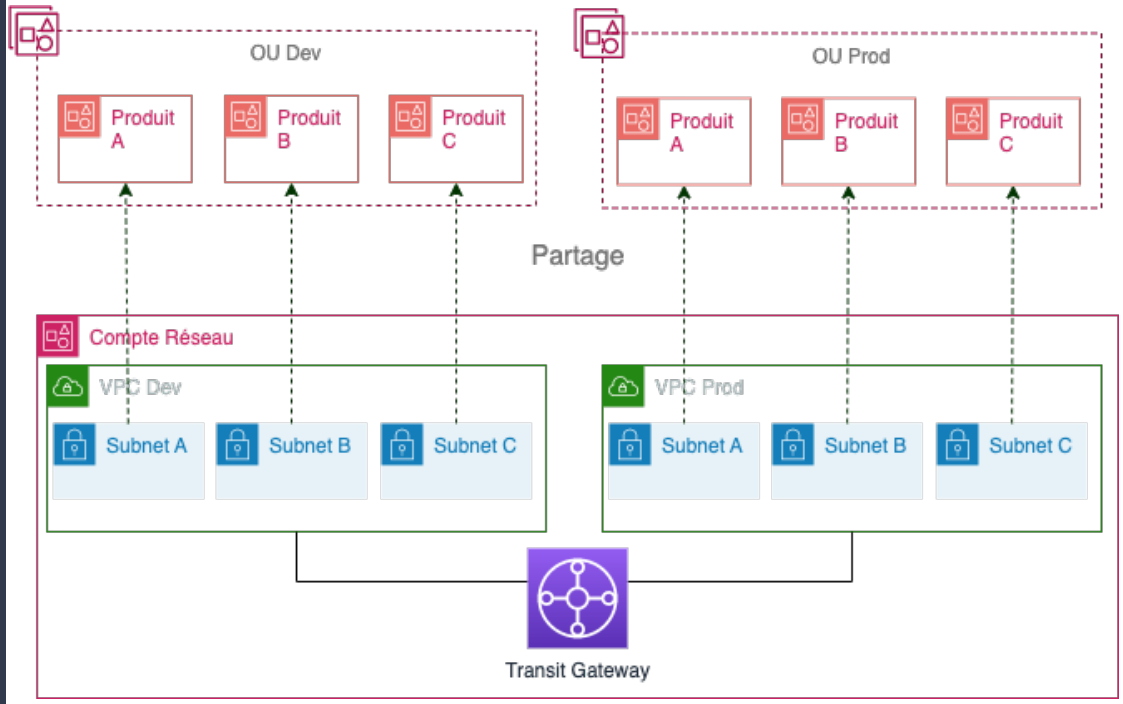
Transit Gateway

- **Architecture Hub-and-Spoke**
  - Connecte VPCs et réseaux locaux.
  - Routage centralisé et dynamique.
  - Jusqu'à 20 Gbps par connexion.
- **Interconnexion Efficace**
  - Peering régional et inter-régional.
  - Se connecte aux VPC, VPN, TGW, DX Gateway…
- **Gestion Centralisée**
  - Déploiement dans un compte dédié et partage via RAM



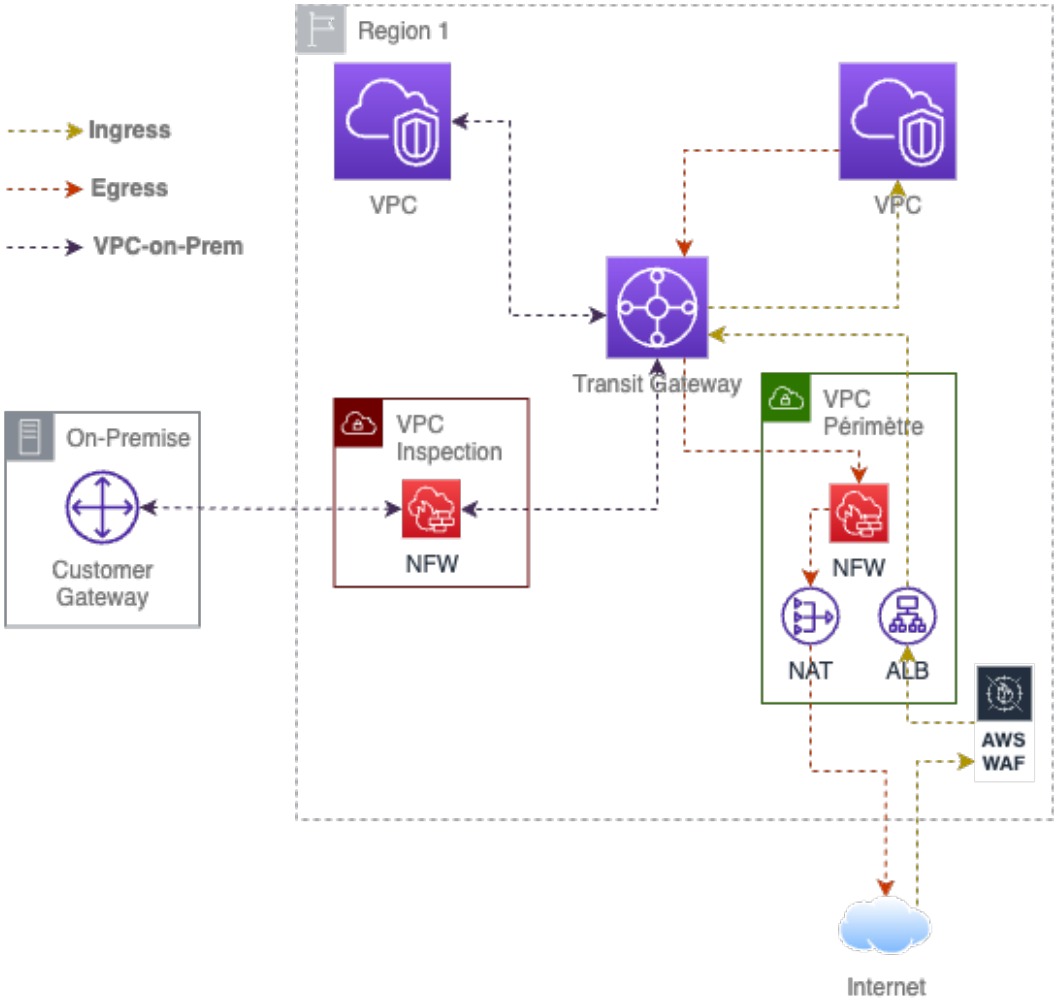
Partage de VPC

- Ressources (Sous-réseaux) partagés entre comptes AWS.
- Gestion centralisée des ressources réseaux.
- Micro segmentation assurée par les groupes de sécurité et les NACLs.
- Au total, moins de VPCs et économie sur les frais de transfert inter-VPCs.



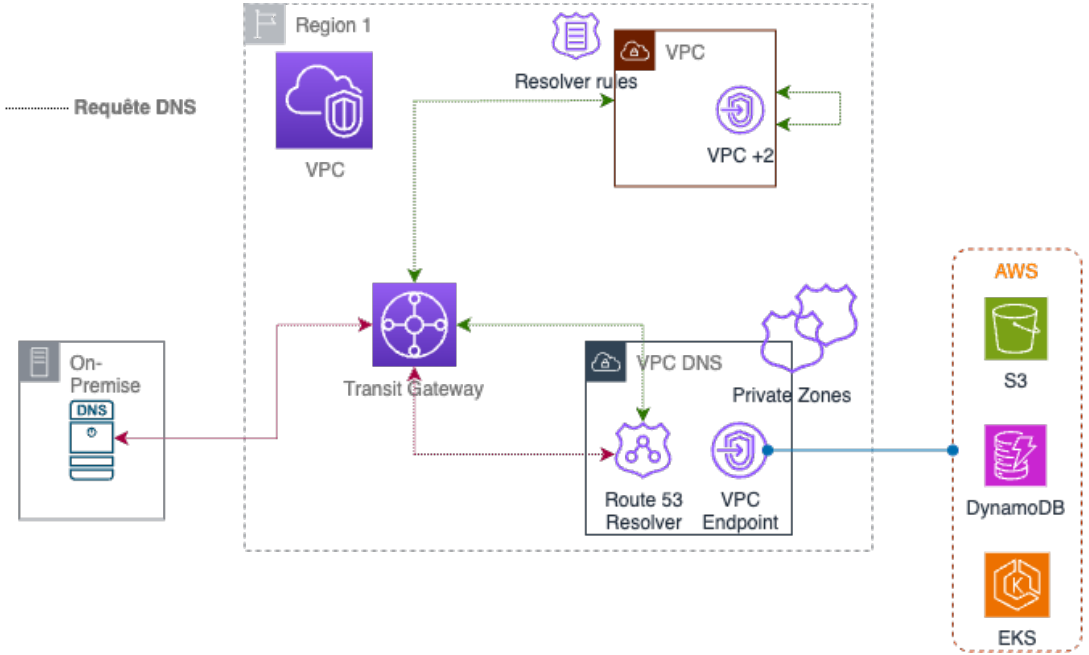
Ingress/Egress centralisé et Inspection

- **Egress Centralisé avec NAT Gateway + NFW**
  - VPC Périmètre pour le trafic face à Internet.
  - Flux sortant acheminé via un NAT gateway centralisé.
  - AWS Network Firewall inspecte le trafic avant d'atteindre le NAT gateway.
- **Ingress centralisé avec ALB + WAF**
  - Sécurité des applications exposées à Internet
  - AWS WAF ou IDS/IPS avec AWS Gateway Load Balancer/AWS Network Firewall pour protège contre les exploits web et les bots
- **Inspection Centralisée avec AWS Network Firewall**
  - VPC-à-VPC et inspection du trafic VPC-on-premises.
  - Renforce la segmentation du réseau



DNS Hybride

- **Résolution DNS dans le VPC:**
  - Résolution des dns internes dans le VPC avec le VPC+2.
  - Association des zones Route 53 privées au VPC dédié.
  - Résolution interne par Route 53 Resolver.
- **DNS Hybride:**
  - Résolution des zones privées AWS et VPC via Route 53 Endpoints
  - Utilise des règles de forwarding DNS
- **Centralisation des Endpoints Resolver:**
  - Centralisation des endpoint Route 53 dans un VPC dédié
  - Centralisation des VPC endpoints dans un VPC dédié



Démo

Q-R

Conclusion