

# Construisez un réseau sécurisé sur AWS

Par Pierre-François HOUESSOU



# Qui suis-je?

Architecte Cloud à COFOMO Québec avec 9 ans d'exp



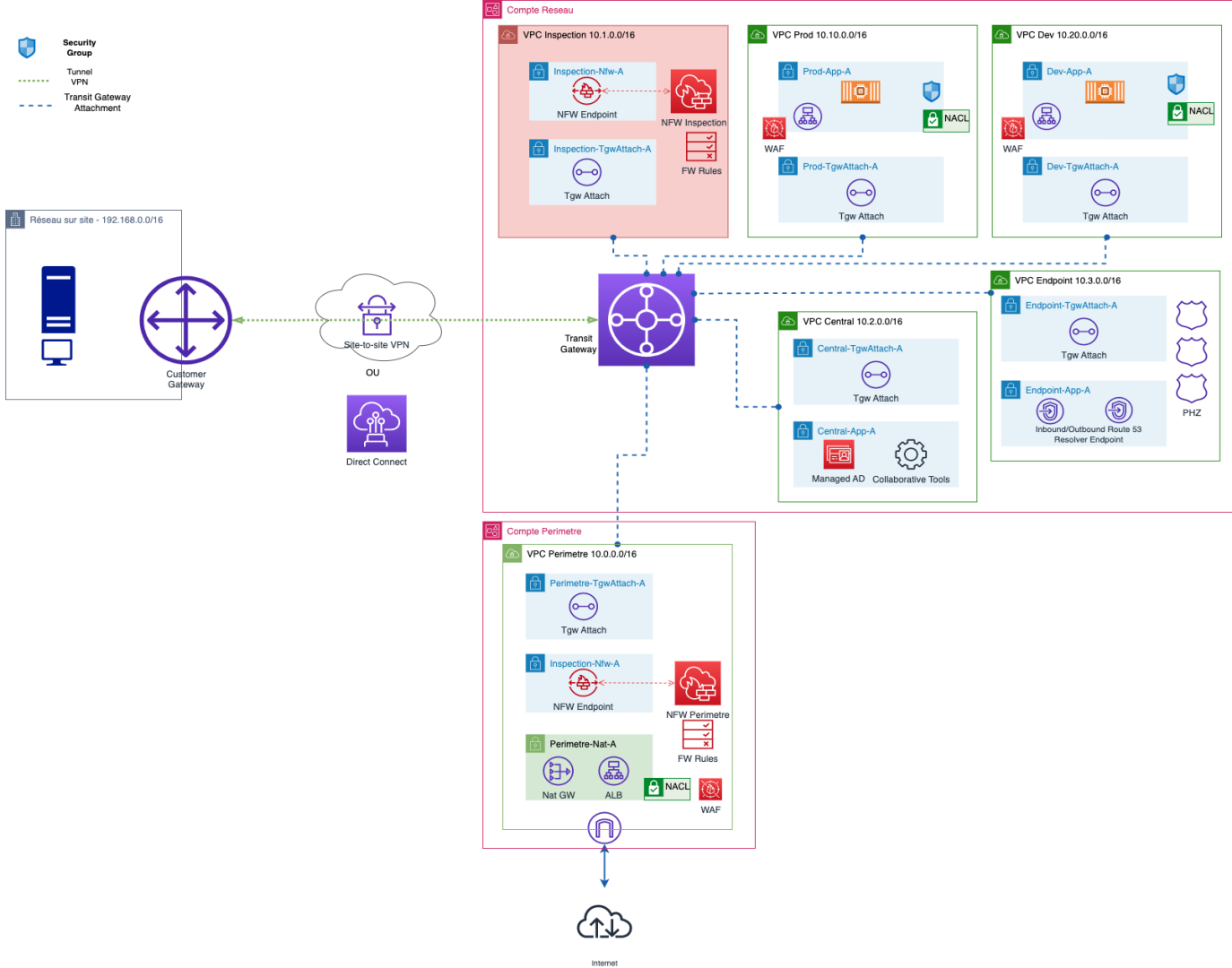
# Introduction

# Agenda

## Sommaire

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

Architecture cible



# Transit Gateway

## Architecture Hub-and-Spoke

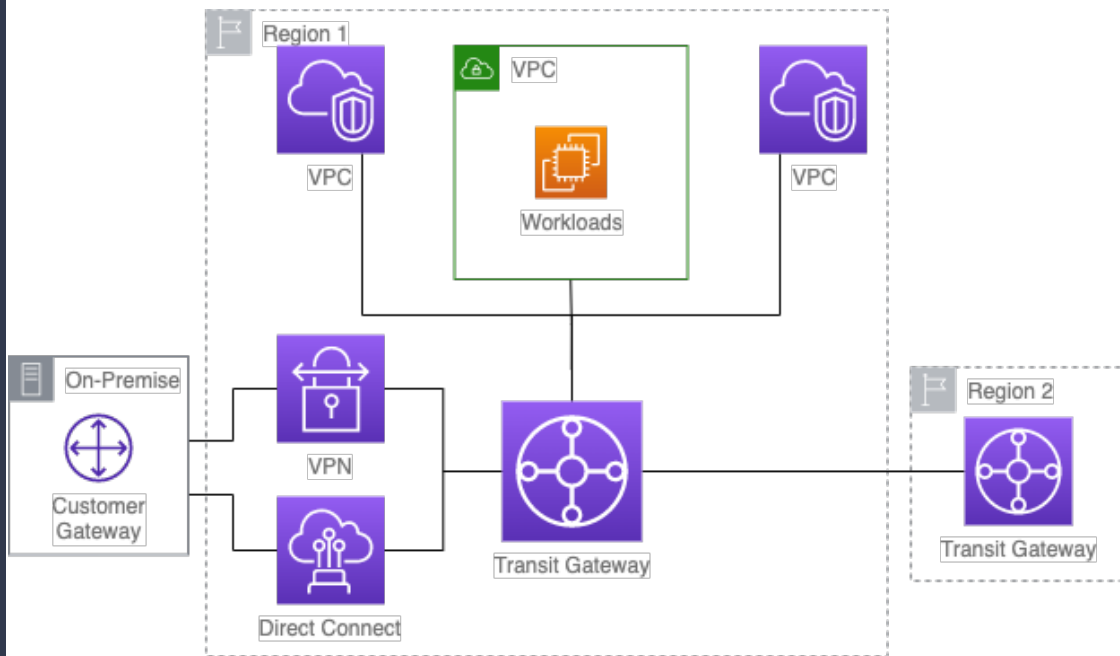
- Connecte VPCs et réseaux locaux.
- Routage centralisé et dynamique.
- Jusqu'à 20 Gbps par connexion.

## Interconnexion Efficace

- Peering régional et inter-régional.
- Se connecte aux VPC, VPN, TGW, DX Gateway...

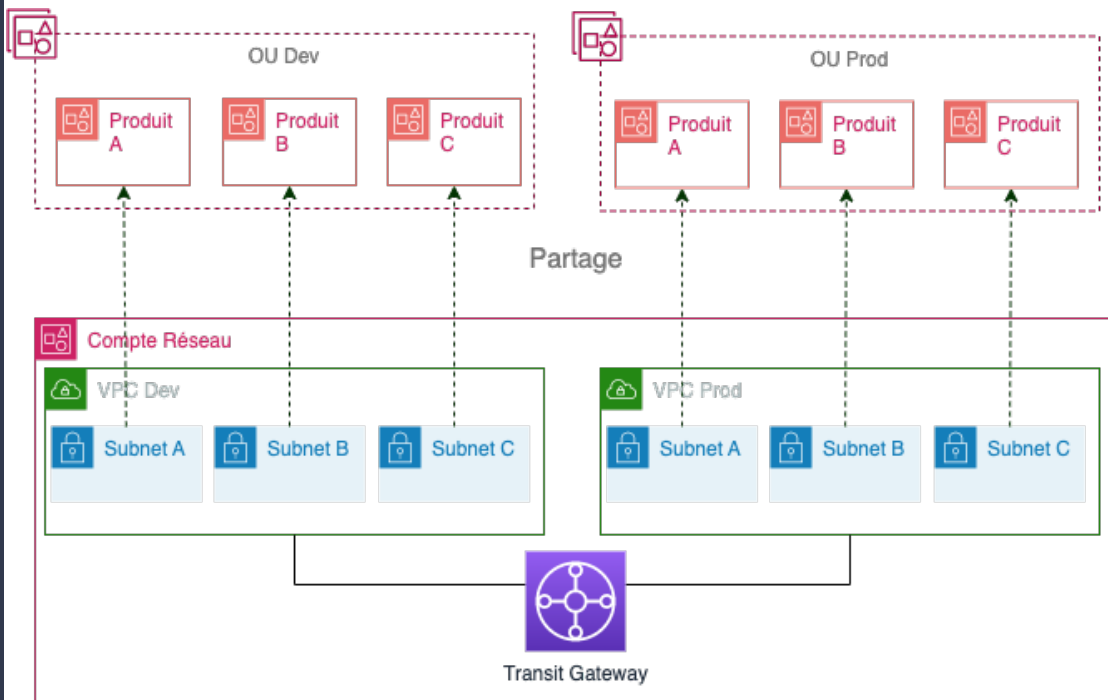
## Gestion Centralisée

- 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 protéger contre les exploits web et les bots

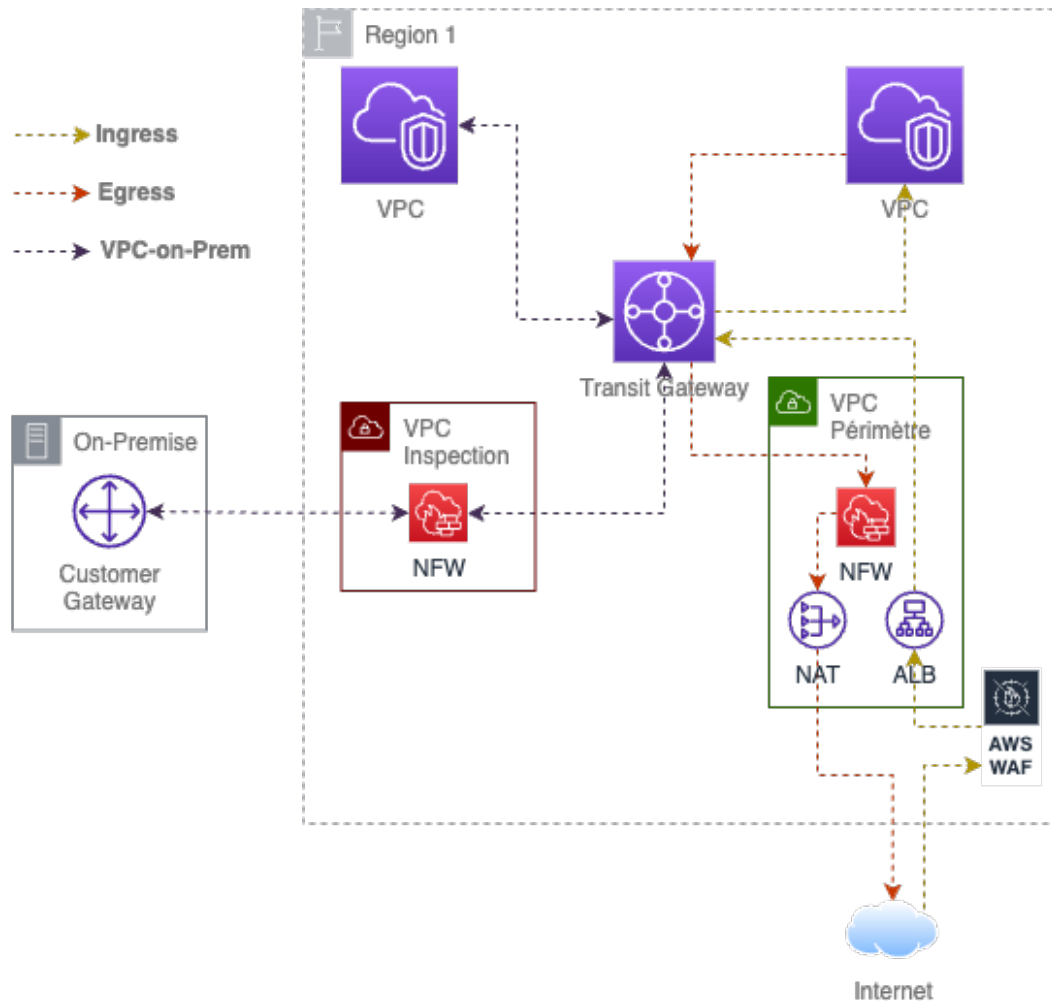
## Inspection Centralisée avec AWS

### 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

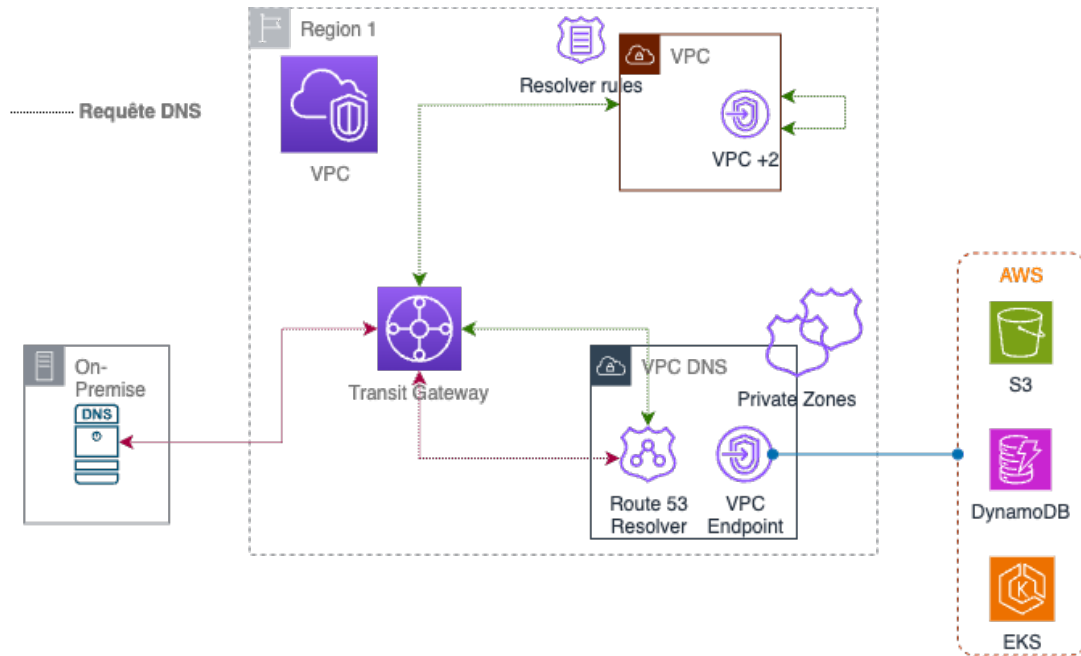
Utilise des règles de forwarding DNS

## 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