www.eazytraining.fr

Services réseau d’AWS

Par Lahda Biassou Alphonsine

Lahda Biassou Alphonsine

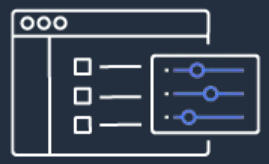
Ingénieure cloud et formatrice

Plan

- **Amazon VPC**
- **VPC peering**
- **VPC Endpoint**
- **Transit gateway**
- **AWS PrivateLink**
- **VPC Flow Logs**
- **Labs: VPC, VPC Peering, VPC Flow Logs & AWS Transit Gateway**

Amazon VPC

Provisionnez une section logiquement isolée du cloud AWS où vous pouvez lancer des ressources AWS dans un réseau virtuel que vous définissez.



adresse IP

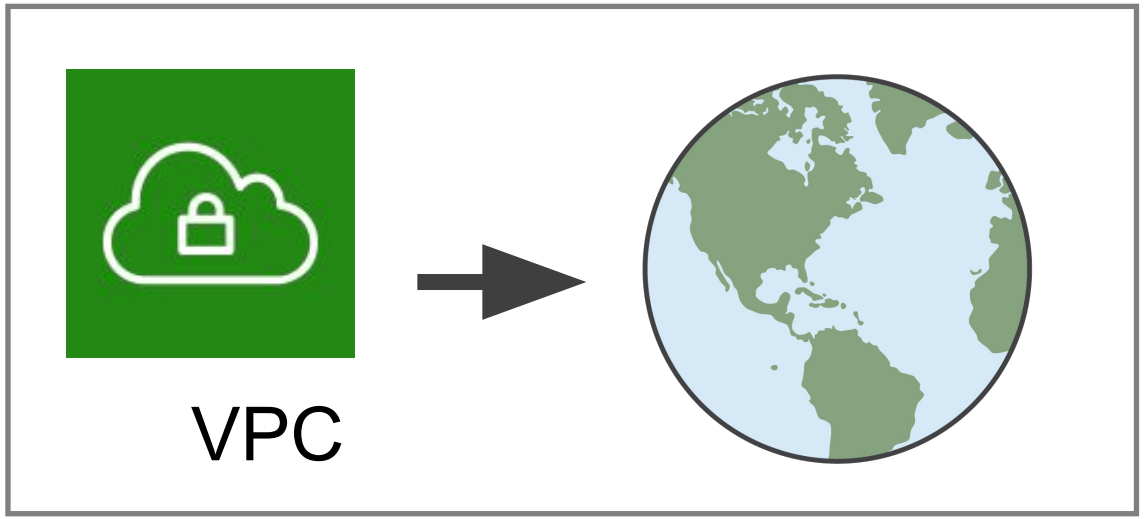
Sous-réseau

Tables de routage

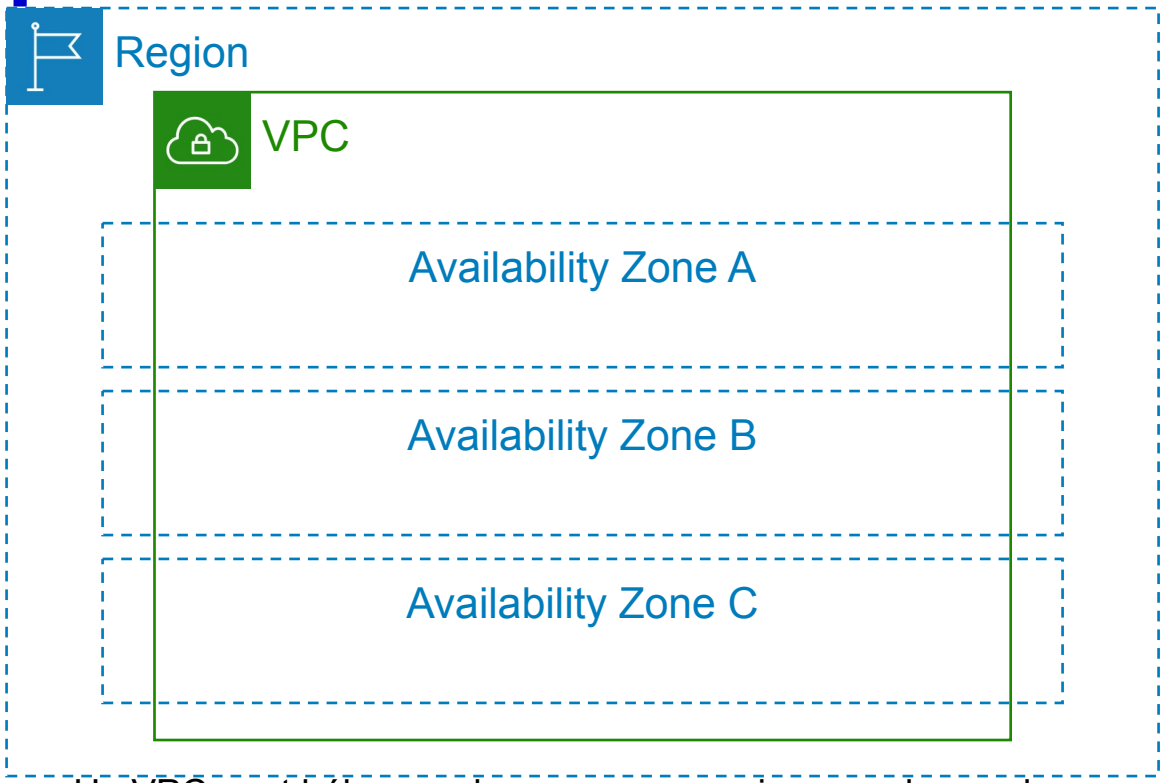
Configuration réseau

Regles de securite

VPC -déploiement



Vous pouvez déployer des VPCs dans toutes les régions.



Un VPC peut héberger des ressources prises en charge dans n'importe quelle zone de disponibilité de sa région.

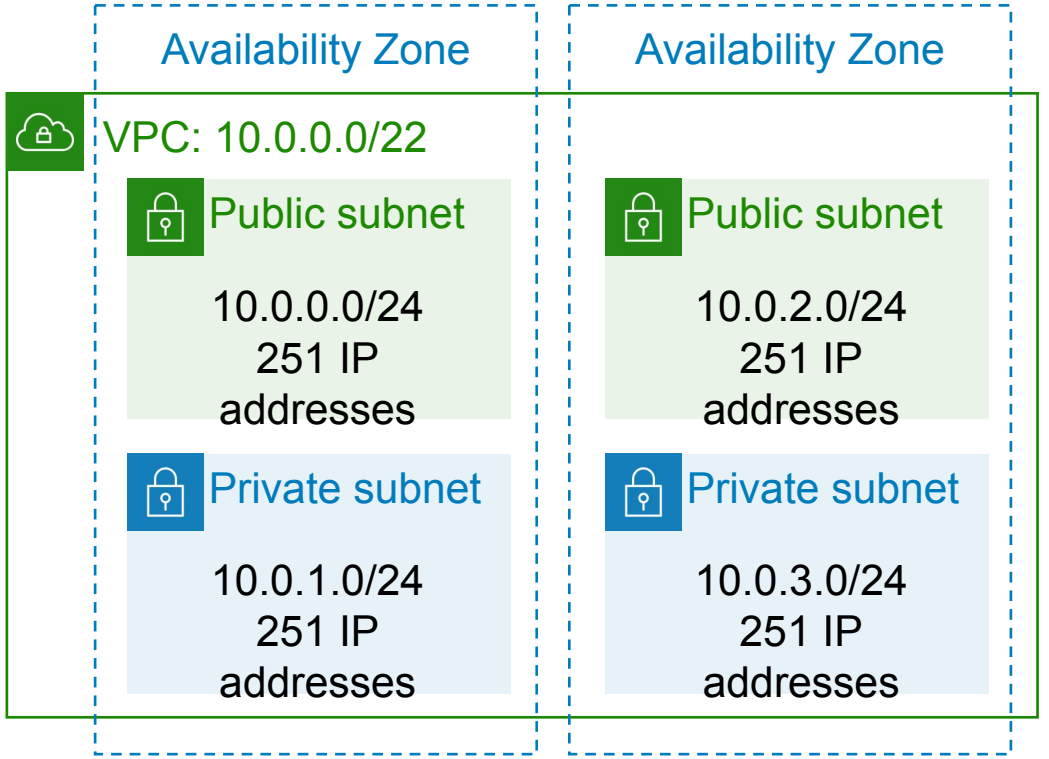
Classless Inter-Domain Routing (CIDR)

0.0.0.0/0	= All IP addresses
10.22.33.44/32	= 10.22.33.44
10.22.33.0/24	= 10.22.33.*
10.22.0.0/16	= 10.22.*.*

CIDR	Total IP addresses
/28	16
…	…
/20	4,096
/19	8,192
/18	16,384
/17	32,768
/16	65,536

VPC -les sous-réseaux

- Un sous-réseau est un segment ou une partition de la plage d'adresses IP d'un VPC où vous pouvez allouer un groupe de ressources.
- Les sous-réseaux ne sont pas des frontières d'isolation
- Les sous-réseaux sont un sous-ensemble du bloc CIDR du VPC
- Les blocs CIDR des sous-réseaux ne peuvent pas se chevaucher
- Chaque sous-réseau réside entièrement dans une zone de disponibilité.
- Vous pouvez ajouter un ou plusieurs sous-réseaux dans chaque zone de disponibilité ou dans une zone locale.
- AWS réserve cinq adresses IP dans chaque sous-réseau.



Exemple : Un VPC avec CIDR /22 comprend 1 024 adresses IP au total.

VPC -les bonnes pratiques

- Créez un sous-réseau par zone de disponibilité disponible pour chaque groupe d'hôtes ayant des exigences de routage uniques.
- Répartissez l'étendue de votre réseau VPC de manière égale sur toutes les zones de disponibilité disponibles dans une région.
- N'attribuez pas toutes les adresses réseau en une seule fois. Veillez plutôt à réserver une partie de l'espace d'adressage pour une utilisation future.
- Dimensionnez le CIDR et les sous-réseaux de votre VPC pour supporter une croissance significative des charges de travail prévues.
- Veillez à ce que votre plage de réseau VPC (bloc CIDR) n'empiète pas sur les autres plages de réseau privé de votre organisation.

VPC -un seul déploiement

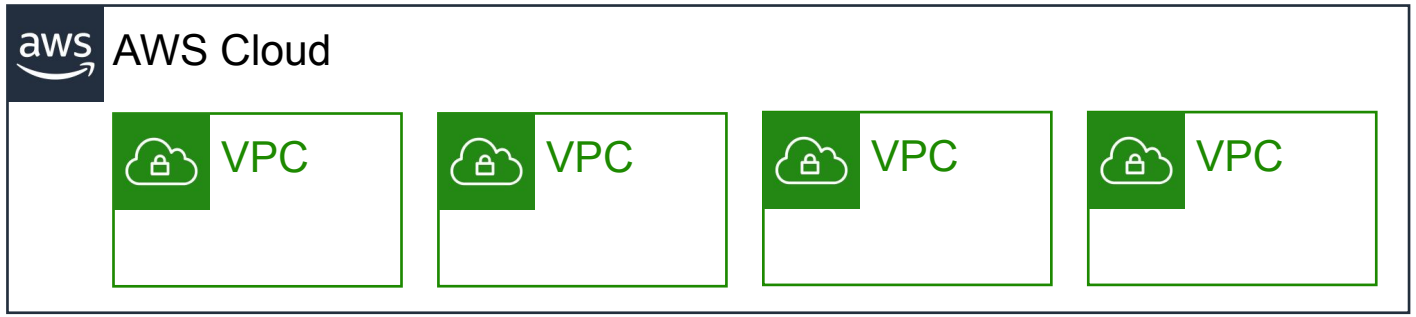
Il existe des cas d'utilisation limités où le déploiement d'un seul VPC peut s'avérer approprié :

- Petites applications uniques gérées par une petite équipe
- Calcul haute performance (HPC)
- Gestion des identités

Pour la plupart des cas d'utilisation, il existe deux modèles principaux pour organiser votre infrastructure : multi-VPC et multi-compte.

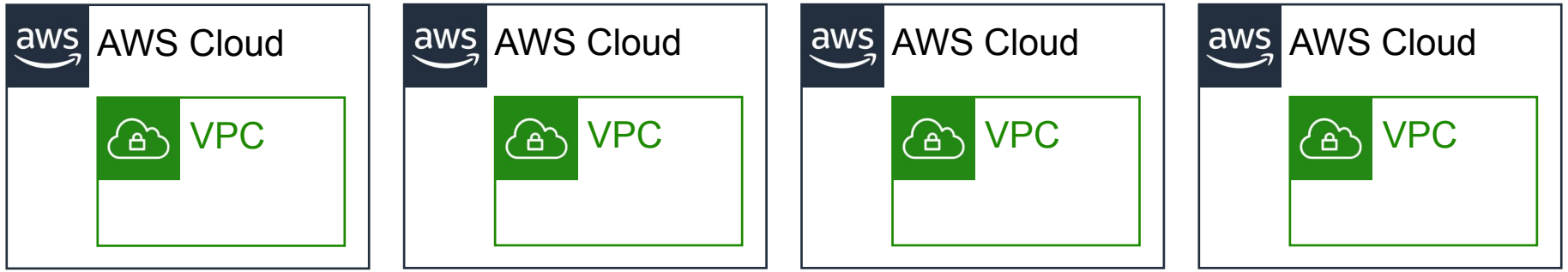
VPC multiple

- Mieux adapté à :
  - Une seule équipe ou une seule organisation, comme les fournisseurs de services gérés
  - Des équipes restreintes, ce qui facilite le maintien des normes et la gestion des accès.
- Exception :
  - Les normes de gouvernance et de conformité peuvent nécessiter une plus grande isolation de la charge de travail, quelle que soit la complexité de l'organisation.

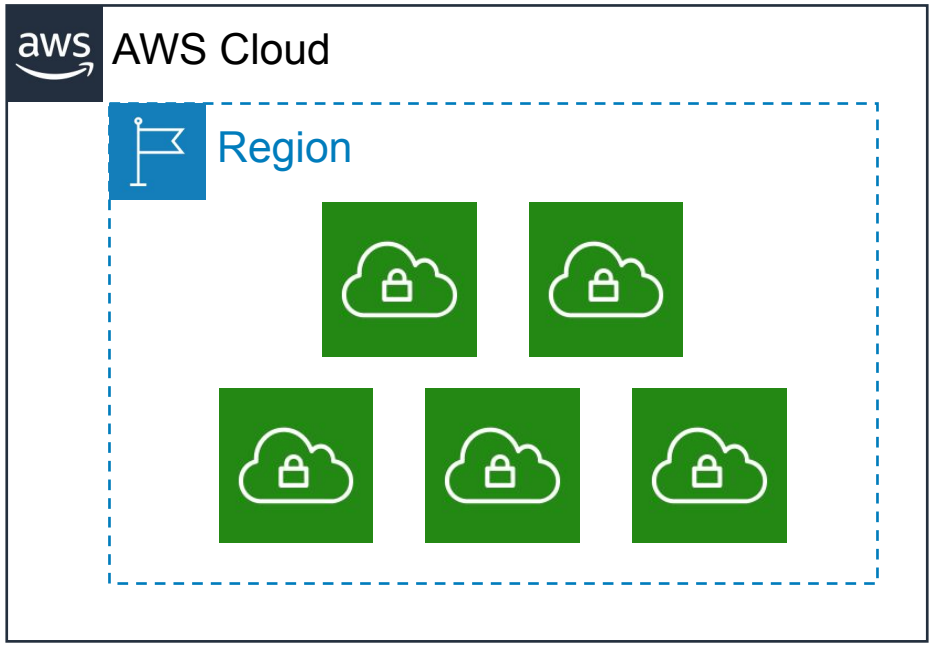


VPC multi comptes

- Mieux adapté à -
  - Les grandes organisations et les organisations disposant de plusieurs équipes informatiques
  - Les organisations de taille moyenne qui prévoient une croissance rapide
- Pourquoi ?
  - Il peut être plus difficile de gérer l'accès et les normes dans les organisations plus complexes.



VPC : limites de 5 VPCs par région



VPC : points clés

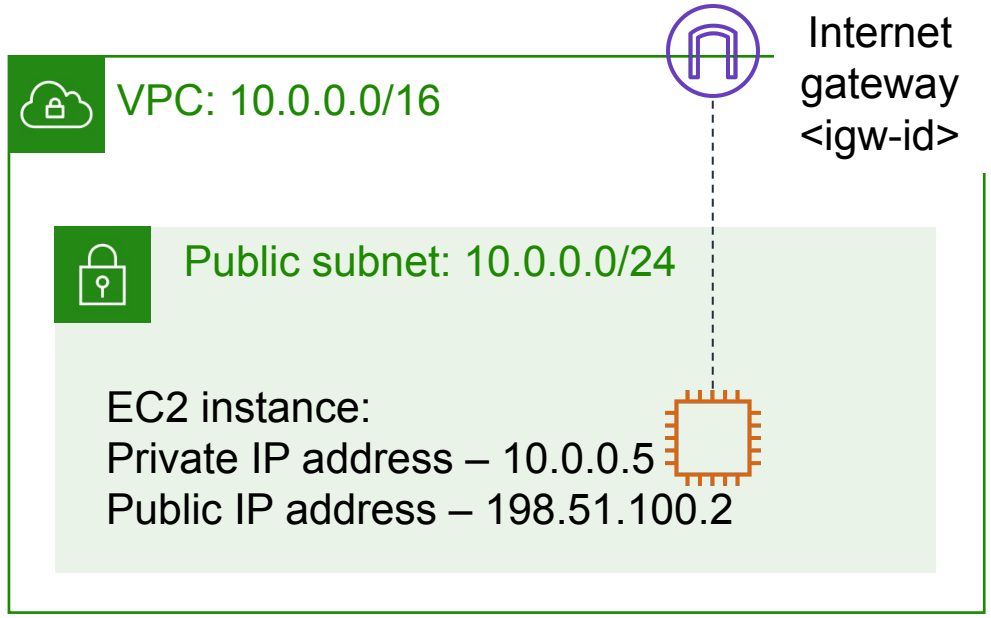
- Amazon VPC vous permet de provisionner des VPC, qui sont des sections logiquement isolées du cloud AWS où vous pouvez lancer vos ressources AWS.
- Un VPC appartient à une seule région et est divisé en sous-réseaux.
- Un sous-réseau appartient à une zone de disponibilité ou à une zone locale. Il s'agit d'un sous-ensemble du bloc CIDR du VPC.
- Vous pouvez créer plusieurs VPC dans la même région ou dans des régions différentes, et dans le même compte ou dans des comptes différents.
- Suivez les meilleures pratiques lorsque vous concevez votre VPC

VPC - connecter son réseau AWS a internet avec la passerelle internet

- Permettent la communication entre les ressources de votre VPC et l'internet
- sont dimensionnés horizontalement, redondants et hautement disponibles par défaut
- Fournissent une cible dans les tables de routage de votre sous-réseau pour le trafic routable sur l'internet

Direction des trafic entre les ressources VPCs

- Les **tables de routage** sont nécessaires pour diriger le trafic entre les ressources des VPC.
- Chaque VPC possède une table de **routage principale (par défaut)**.
- Tous les sous-réseaux **doivent être associés** à une table de routage.
- Vous pouvez créer des tables de routage **personnalisées.**
- **Meilleure pratique :** Utilisez des tables de routage personnalisées pour chaque sous-réseau.



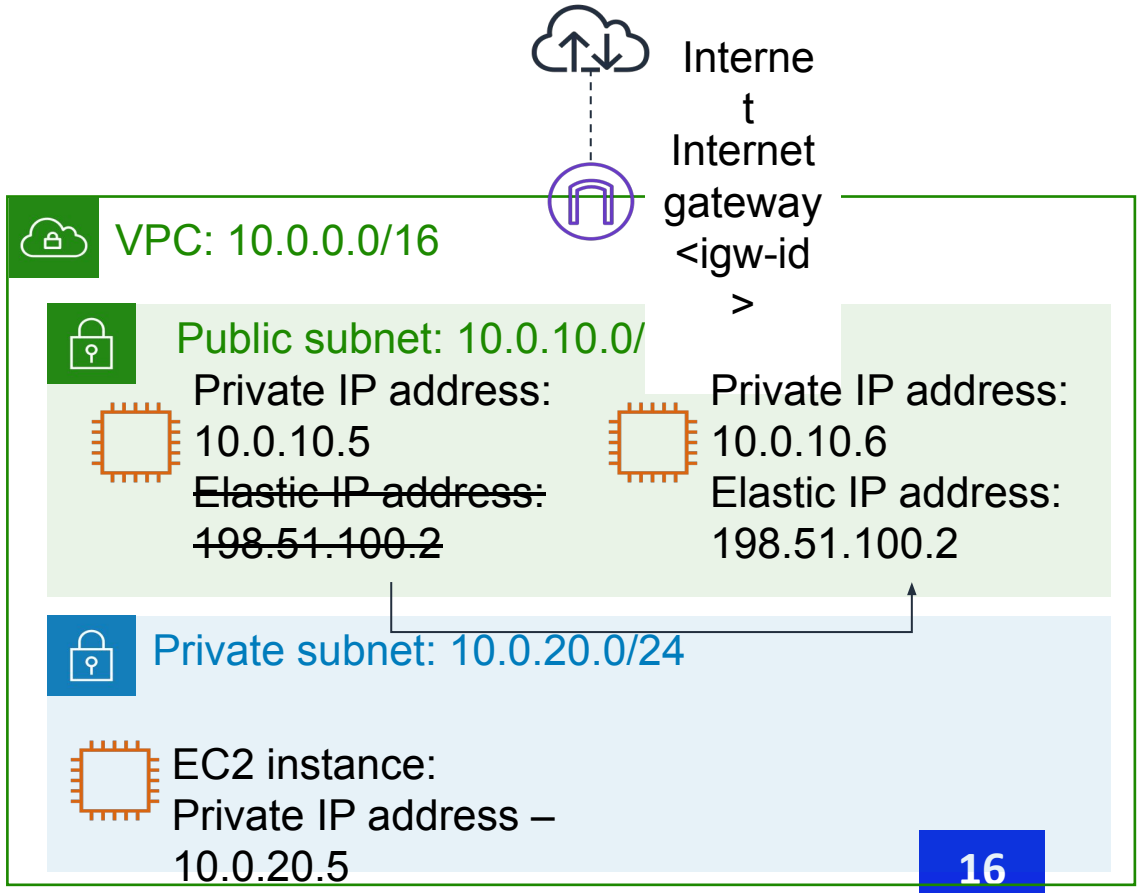
Public route table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	<igw-id>

Remapper une adresse IP d'une instance à une autre

Adresse IP Elastic

- sont des adresses IPv4 statiques et publiques associées à votre compte AWS
- Elles peuvent être associées à une instance ou à une interface de réseau élastique.
- Peuvent être réaffectées à une autre instance de votre compte.
- Sont utiles pour la redondance lorsque les équilibreurs de charge ne sont pas une option.



Connexion des réseaux privés à internet

Nat Gateway

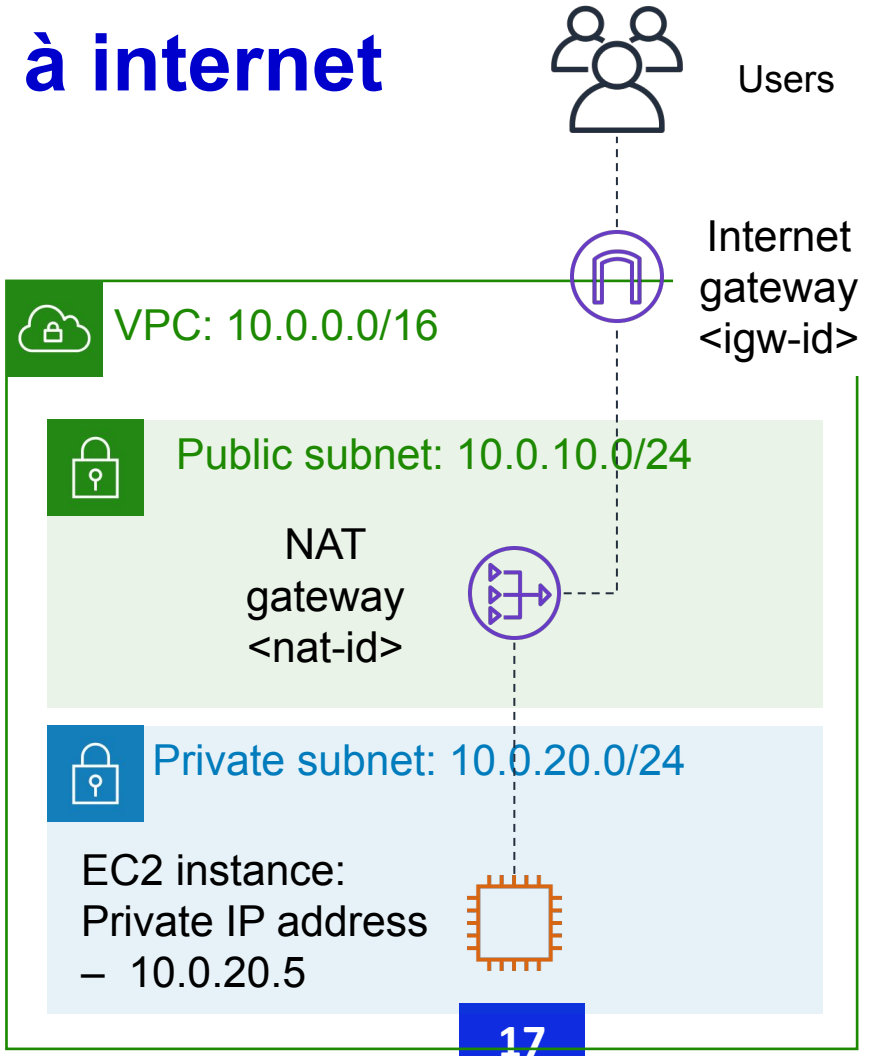
- Permettre aux instances d'un sous-réseau privé d'initier un trafic sortant vers l'internet ou d'autres services AWS
- Empêcher les instances privées de recevoir des demandes de connexion entrantes en provenance de l'internet
- Pas de résilience aux pannes, bande passante limitée basée sur le type d'instance, bon marché
- **Vous devez gérer vous-même le basculement - Vous devez désactiver la vérification de la source/destination (paramètre EC2). (paramètre EC2)**

Table de routage public

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	<igw-id>

Table de routage privée

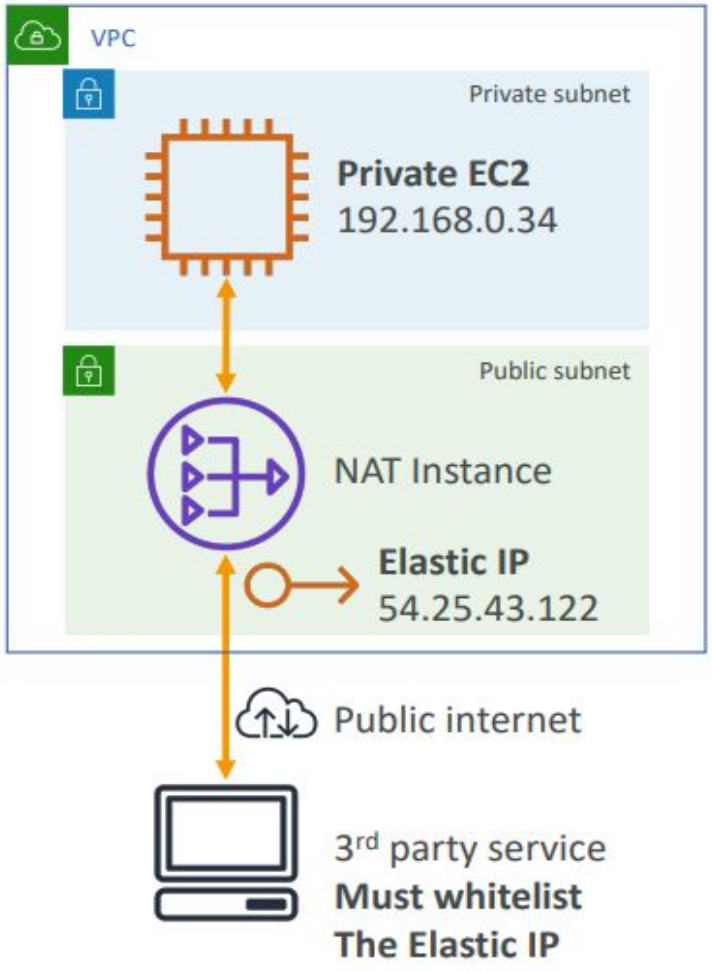
Destination	Target
10.0.0.0/16	local
0.0.0.0/0	<nat-id>

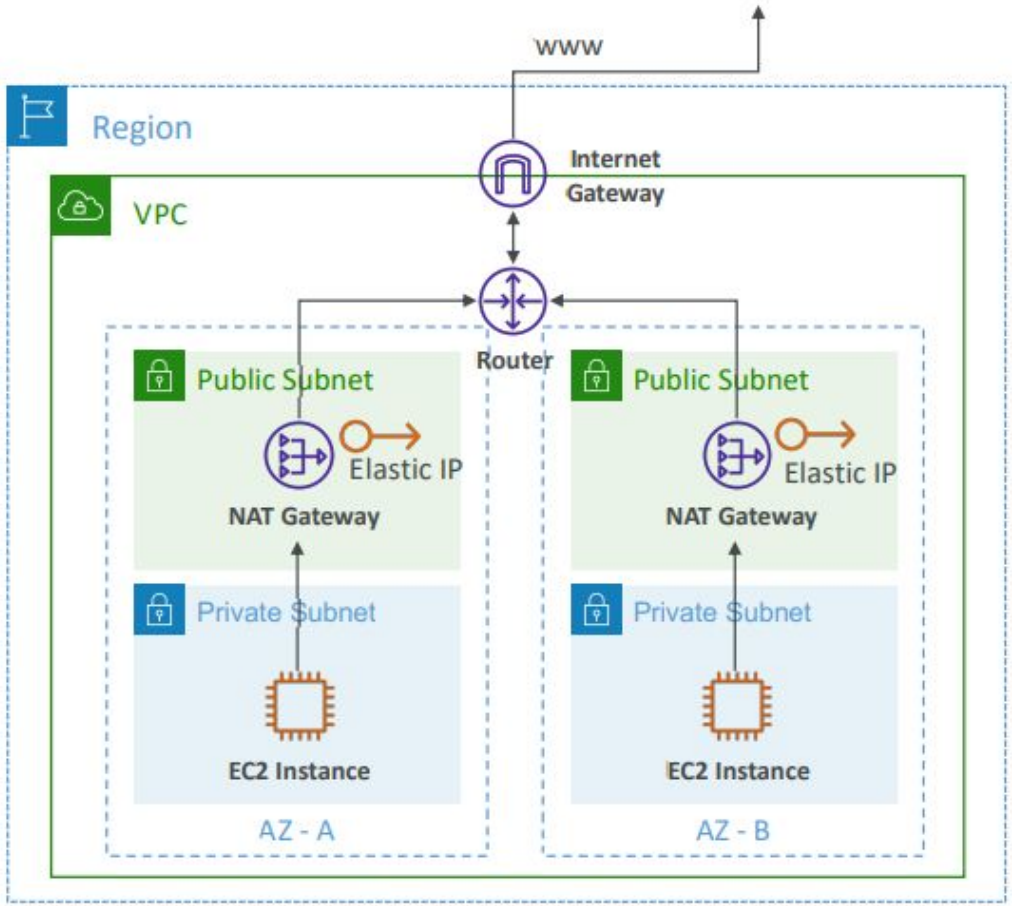


Connexion des réseaux privés à internet

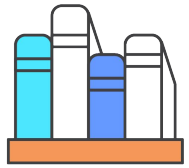
Nat Gateway

- Résilience aux pannes au sein d'une seule AZ
- Il faut déployer plusieurs passerelles NAT dans plusieurs AZ pour HA
- Possède une IP élastique, les services externes voient l'IP de la passerelle NAT comme la source





Exemples de cas d'utilisation de sous-réseaux



Instance de stockage des données → Sous-réseau privé

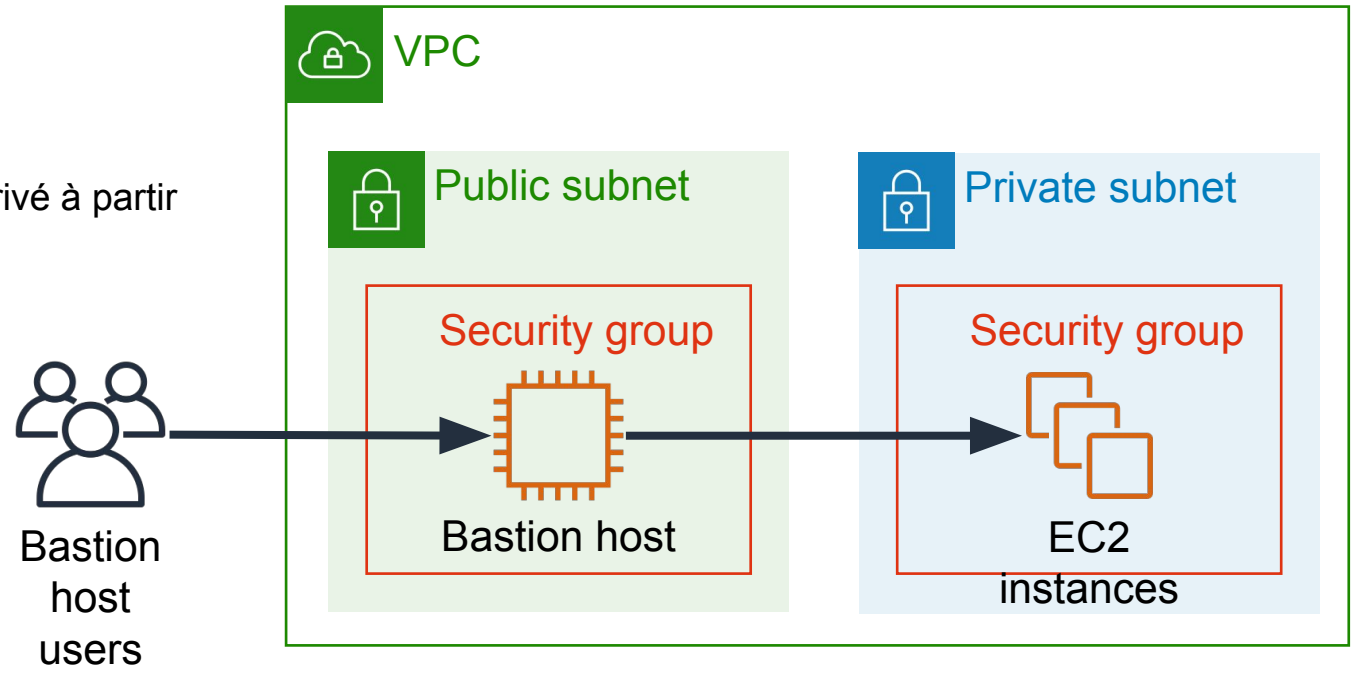
Instances de traitement par lots → Sous réseau privé

Instances en backend → Sous réseau privé

Instances d'application web → Sous réseau public ou privé

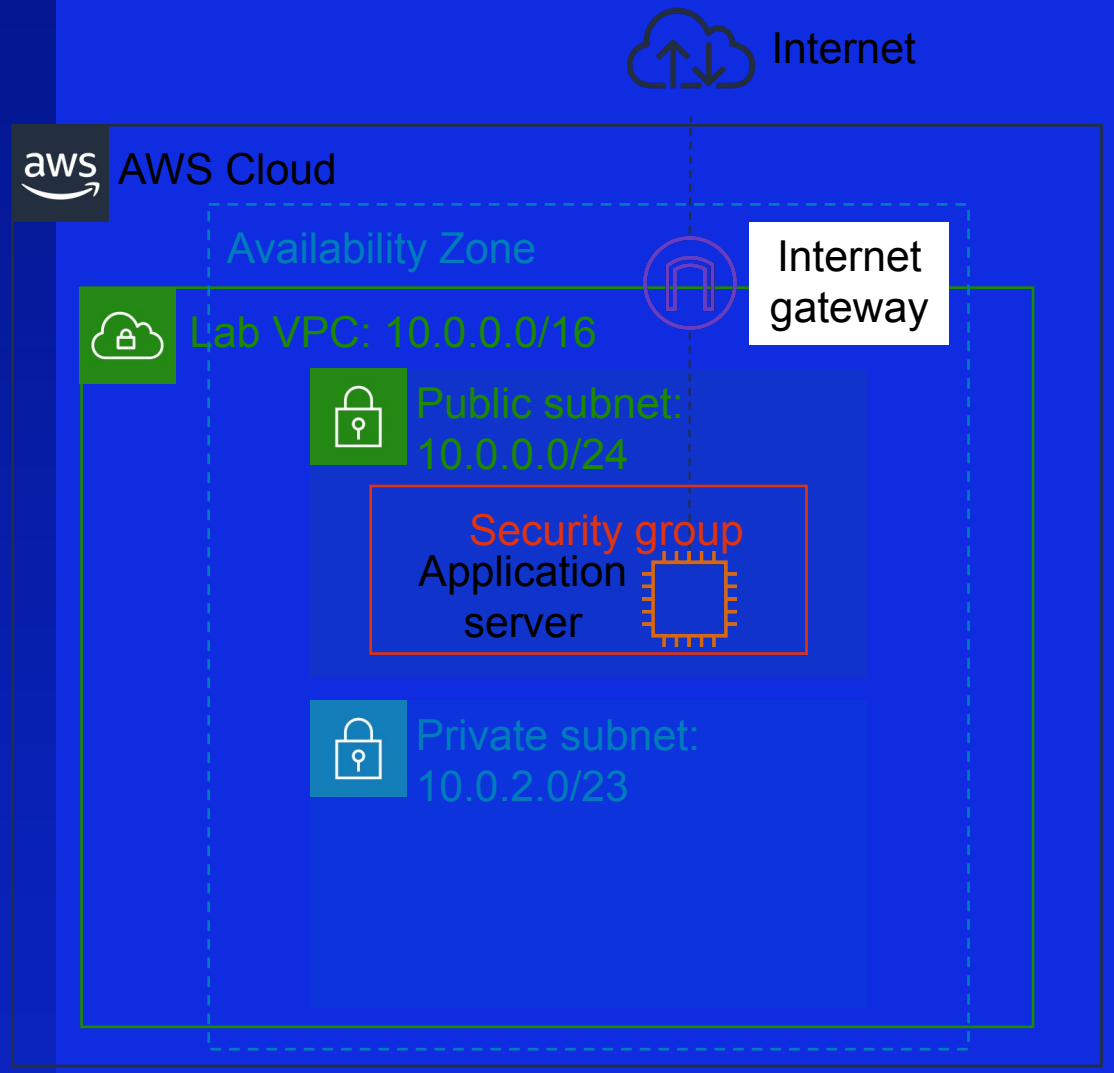
Bastion Host

- Serveur dont l'objectif est de fournir un accès à un réseau privé à partir d'un réseau externe.
- Doit minimiser les risques de pénétration



www.eazytraining.fr

Lab: Création d'un VPC et ses composants

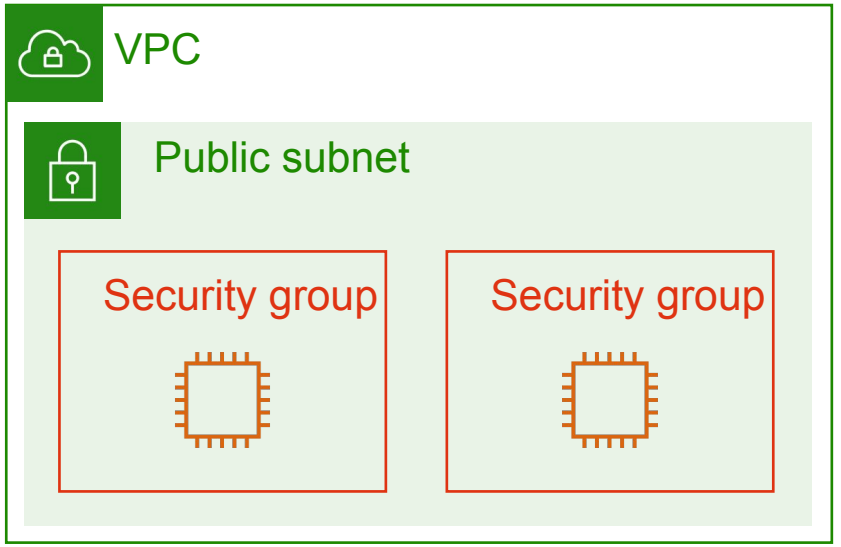


Points clés

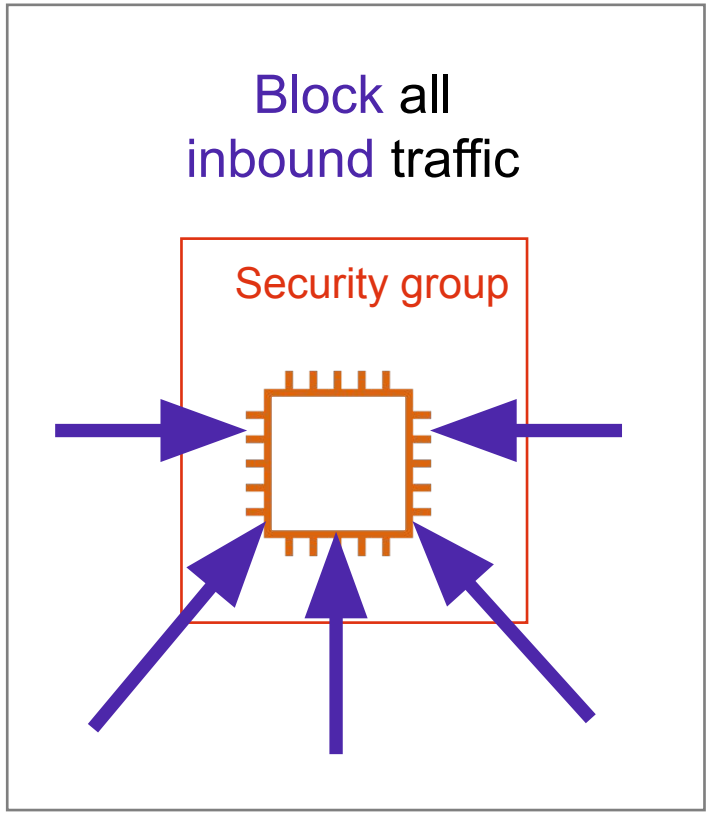
- Une passerelle internet permet la communication entre les instances de votre VPC et l'internet.
- Les tables de routage contrôlent le trafic à partir de votre sous-réseau ou de votre passerelle.
- Les adresses IP élastiques sont des adresses IPv4 statiques et publiques qui peuvent être associées à une instance ou à une interface réseau élastique. Elles peuvent être réaffectées à une autre instance de votre compte.
- Les passerelles NAT permettent aux instances du sous-réseau privé d'initier un trafic sortant vers Internet ou d'autres services AWS.
- Un hôte bastion est un serveur dont l'objectif est de fournir un accès à un réseau privé à partir d'un réseau externe, tel qu'Internet.

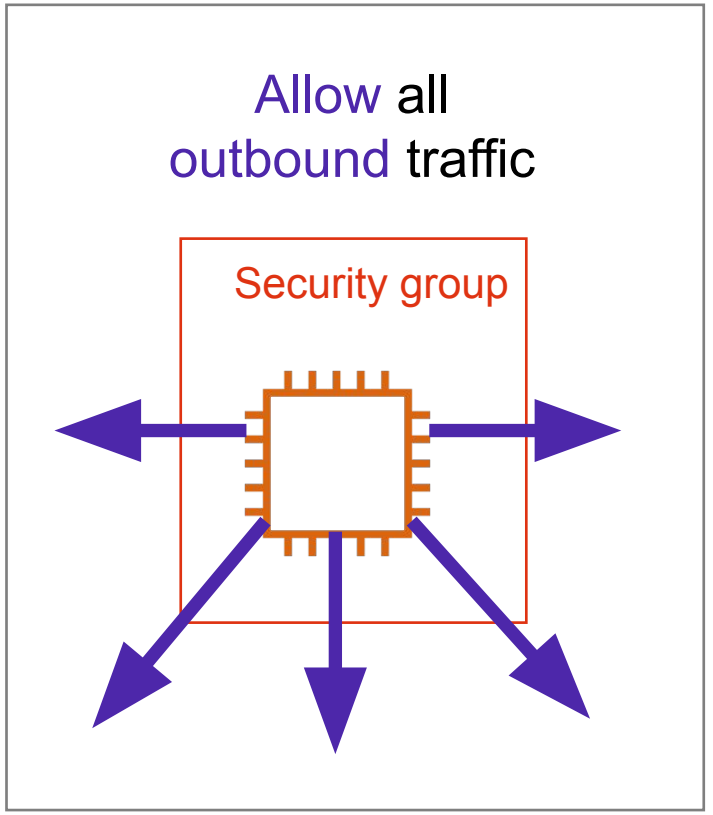
Groupe de sécurité

- Les groupes de sécurité sont des pare-feu dynamiques qui contrôlent le trafic entrant et sortant vers les ressources AWS.
- Agissent au niveau de l'instance ou de l'interface réseau

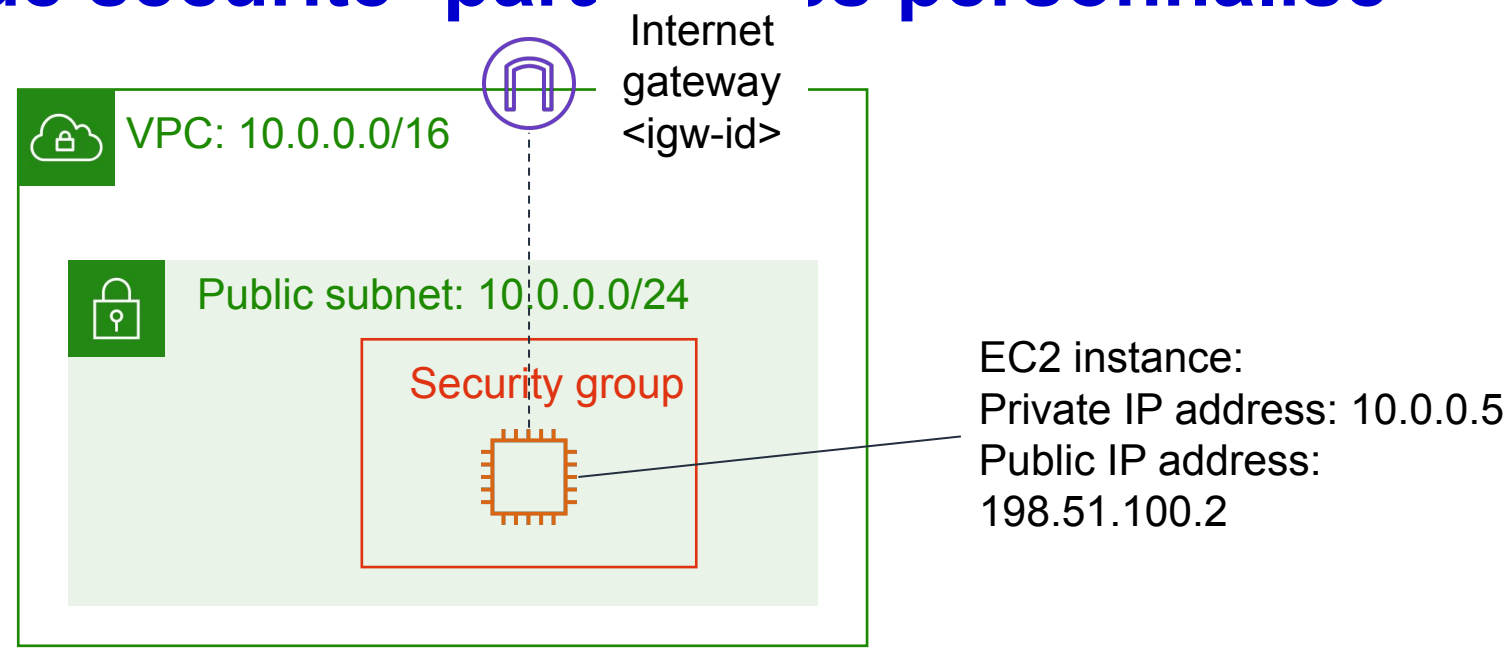


Groupe de sécurité -paramètres par défaut



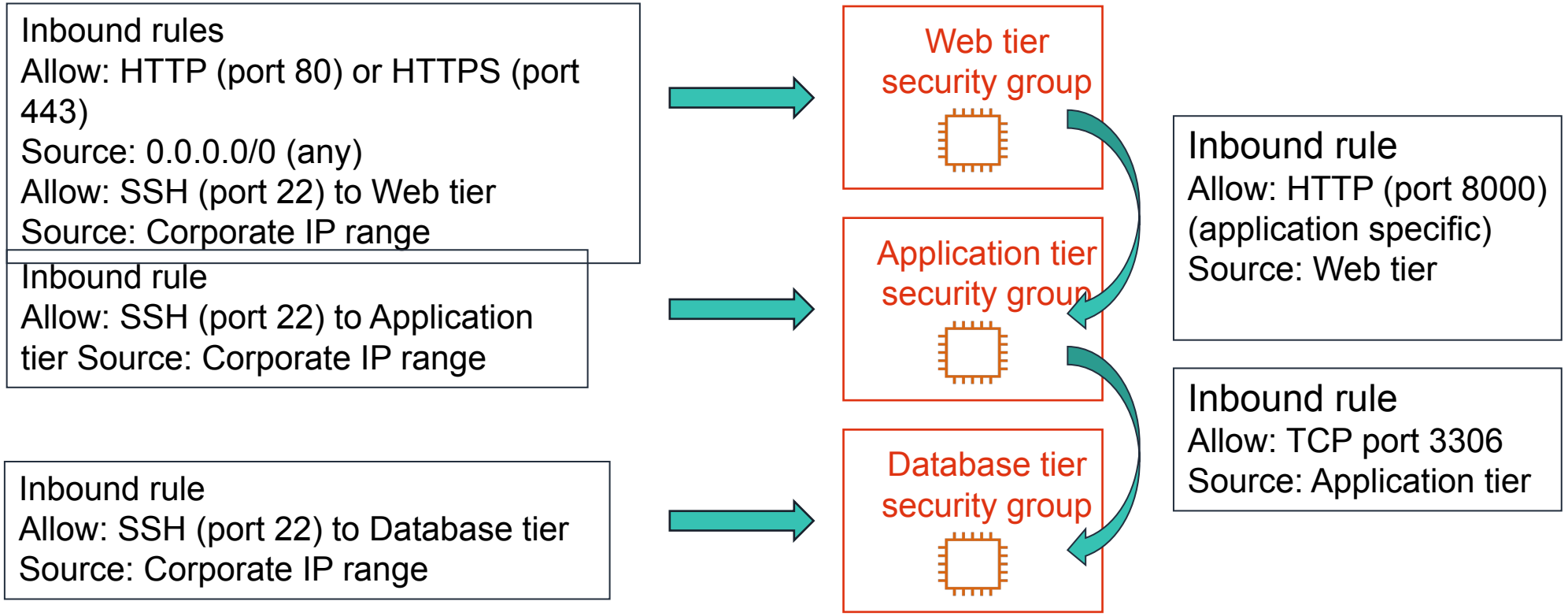


Groupe de sécurité -paramètres personnalise



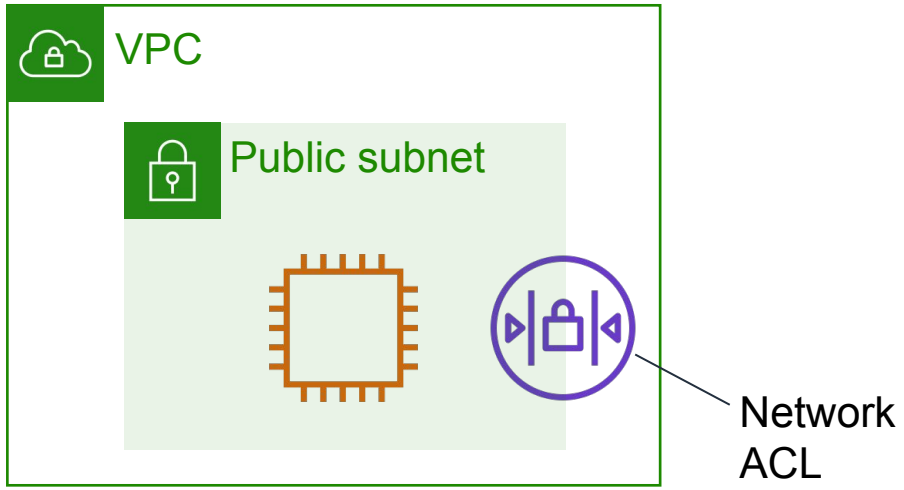
Inbound				
Type	Protocol	Port Range	Source	Destination
HTTP	TCP	80	Anywhere	Allow web access

Chaînage des groupes de sécurité



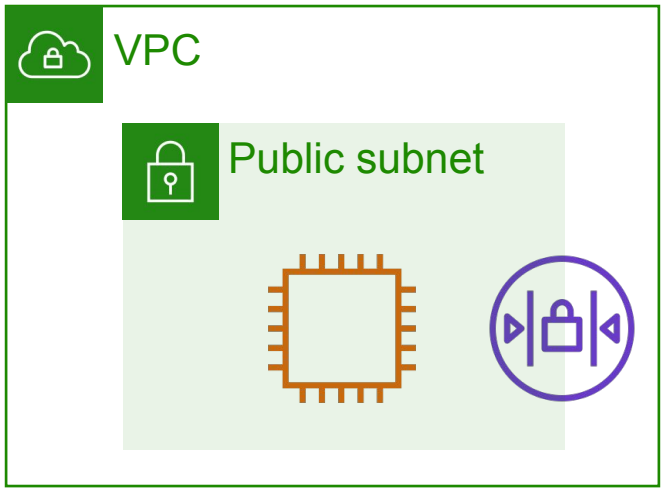
Network Access Control List (NACL)

- Agir au niveau du sous-réseau.
- autorisent par défaut tout le trafic entrant et sortant.
- sont des pare-feu sans état qui nécessitent des règles explicites pour le trafic entrant et sortant.



NACL personnalise

Recommandé pour
uniquement pour des exigences spécifiques en matière de sécurité des réseaux

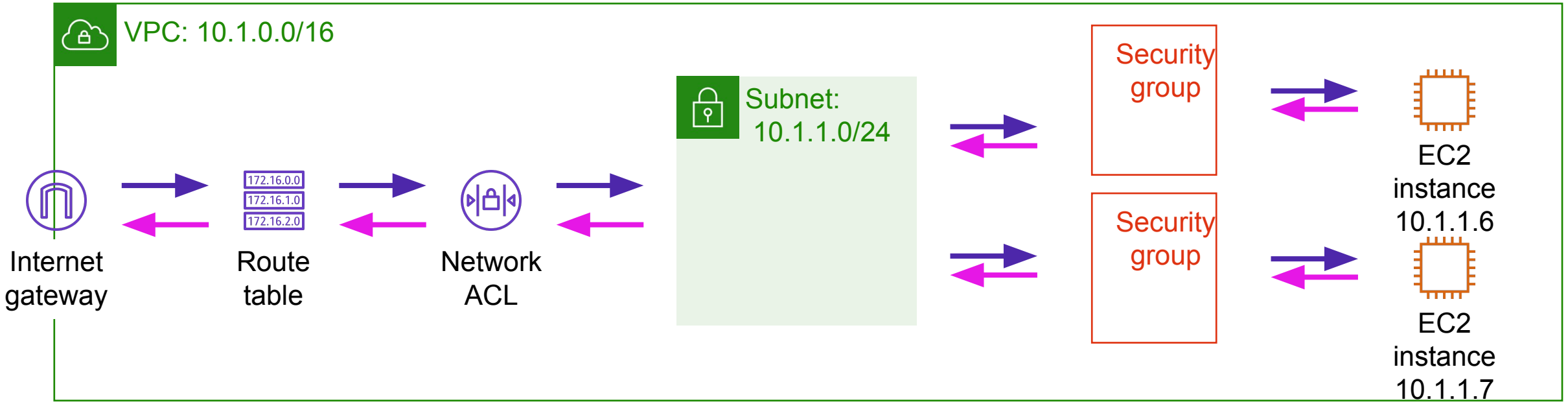


Nacl-11223344

Inbound:
Rules # 100: SSH 172.31.1.2/32 ALLOW
Rules # *: ALL traffic 0.0.0.0/0 DENY

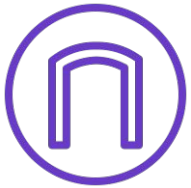
Outbound:
Rules # 100: Custom TCP 172.31.1.2/31 ALLOW
Rules # *: All traffic 0.0.0.0/0 DENY

Structurez votre infrastructure avec plusieurs couches de défense



Révision : Comment créer un sous-réseau public

Pour créer un sous-réseau public permettant la communication entre les instances de votre VPC et l'internet, vous devez :



Attacher
une passerelle internet
a votre VPC

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	<igw-id>

Pointez la table de **routage** de votre sous-réseau d'instance table de routage vers la passerelle internet.

Assurez-vous que vos instances ont des adresses **IP publiques ou des adresses IP** élastiques.

Security group

Assurez-vous que vos groupes de **sécurité et les ACL du réseau** autorisent la circulation du trafic concerné.

points clés

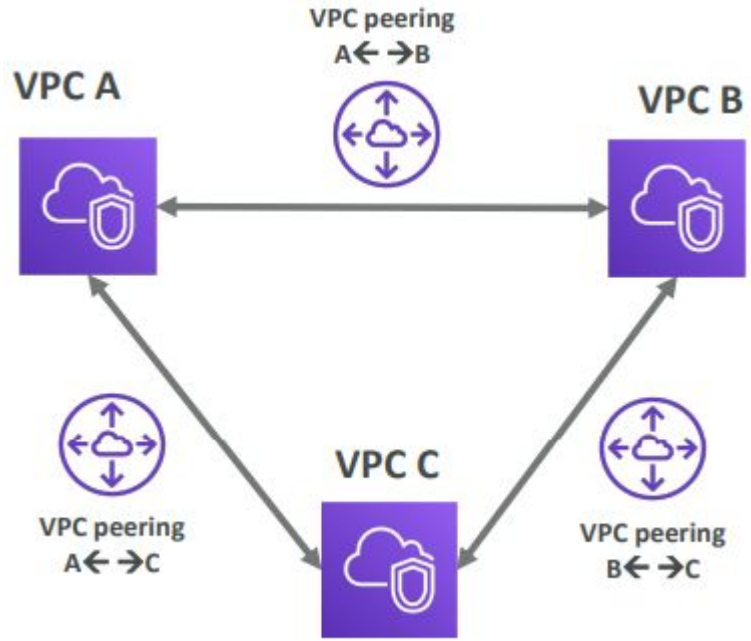
- Les groupes de sécurité sont des **pare-feux avec état ou stateful** qui agissent au niveau de l'instance.
- Les ACL réseau sont des **pare-feu sans état ou stateless** qui agissent au niveau du sous-réseau.
- Lorsque vous définissez des règles d'entrée et de sortie pour permettre au trafic de circuler du niveau supérieur au niveau inférieur de votre architecture, vous pouvez **enchaîner les groupes de sécurité** afin d'isoler une faille de sécurité.
- Vous devez structurer votre infrastructure avec **plusieurs couches de défense.**

Plan

- Amazon VPC
- VPC peering
- VPC Endpoint
- Transit gateway
- AWS PrivateLink
- VPC Flow Logs
- Labs: VPC, VPC Peering, VPC Flow Logs & AWS Transit Gateway

VPC peering

- Connecte deux VPC privé en utilisant le réseau AWS
- Faire en sorte qu'ils se comporte comme s'ils étaient dans un même réseau
- Ne doivent pas avoir les CIDR qui chevauche
- La connexion VPC Peering **n'est pas transitive** (doit être établie pour chaque VPC qui a besoin de communiquer avec d'autres)
- Vous pouvez faire Un VPC Peering avec un autre compte AWS
- **Vous devez mettre à jour la table de routage dans chaque sous-réseau du VPC pour s'assurer que les instances puissent communiquer**



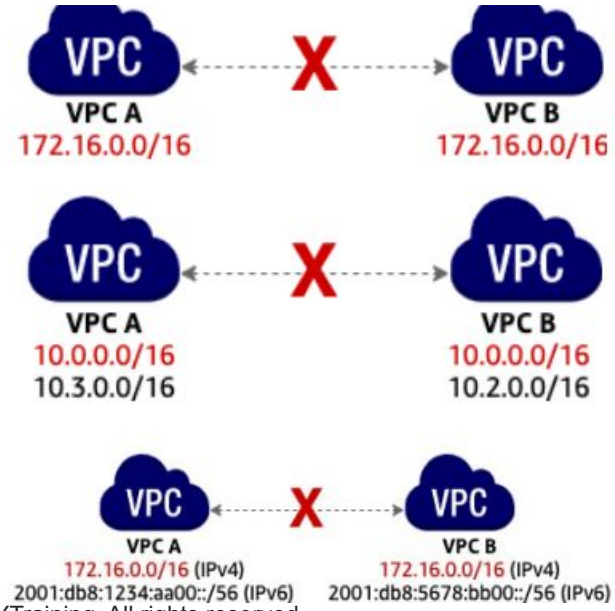
VPC Peering –Bon à savoir

- VPC Peering peut travailler **inter-region, cross-account**
- Vous pouvez référencer un groupe de sécurité d'un VPC peeré (travail entre les comptes)

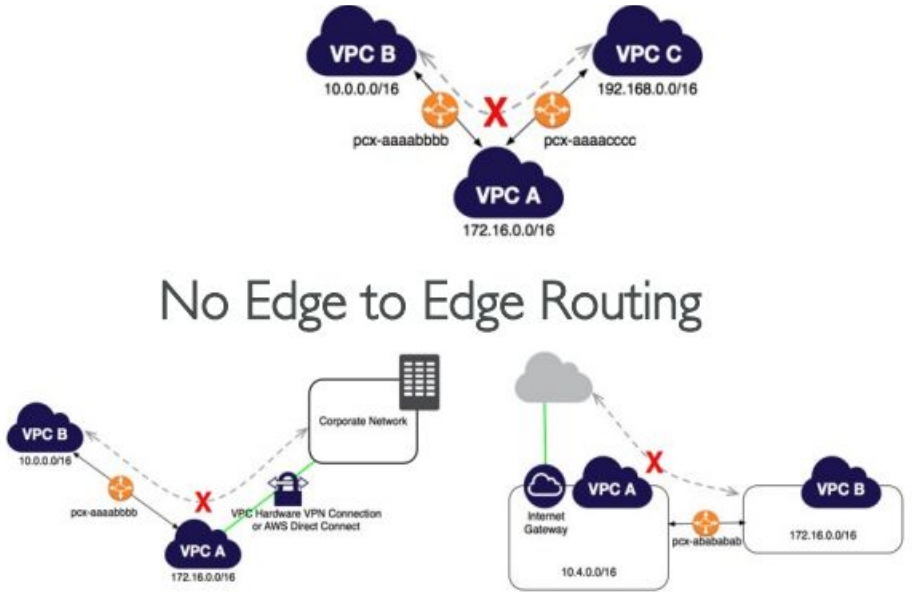
Type ⓘ	Protocol ⓘ	Port Range ⓘ	Source ⓘ
HTTP	TCP	80	sg-00d2b0f5fd6de757e
HTTP	TCP	80	sg-013347765f7a63aae/12356788

VPC Peering –les configurations invalides

Overlapping CIDR pour IPv4

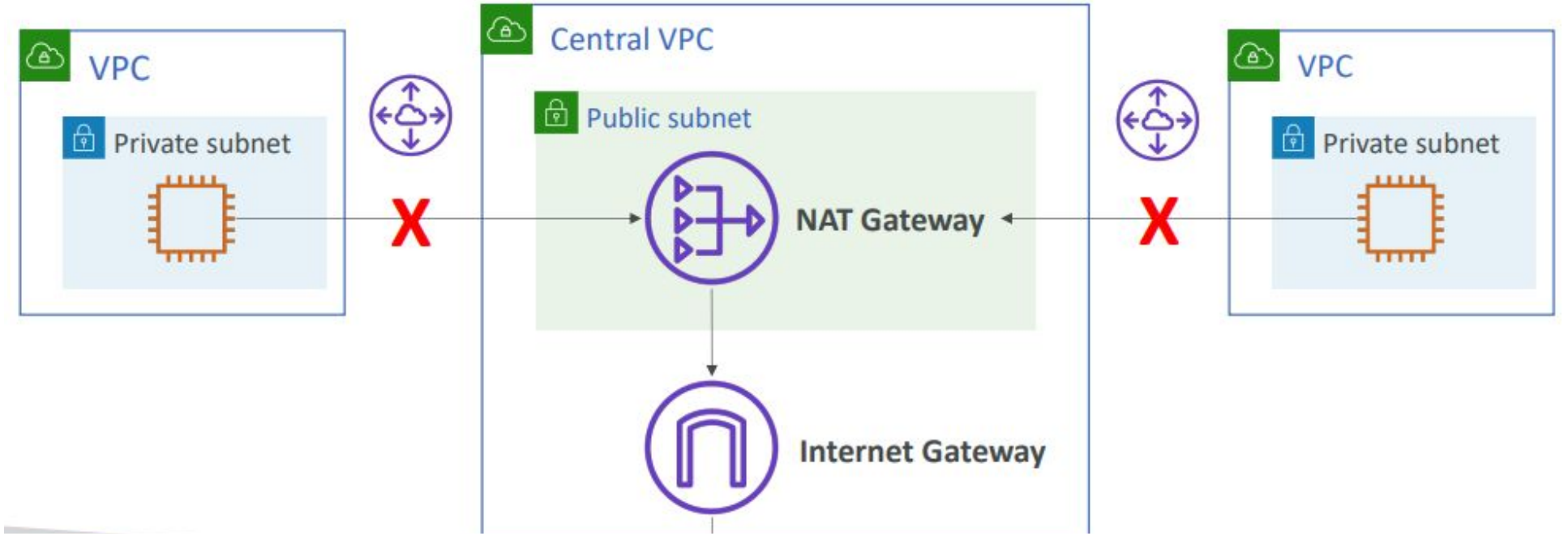


No transitive VPC Peering



VPC Peering – Invalid Configuration
No edge to edge routing

- Ceci est une configuration Invalide
- VPC Peering ne supporte pas le routage edge à edge pour le matériel NAT

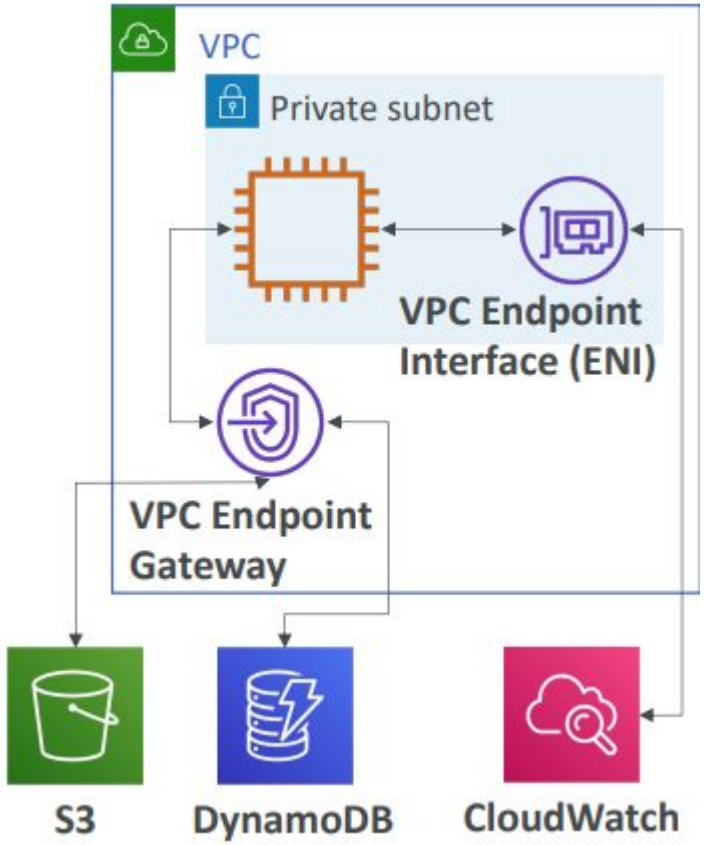


Plan

- Amazon VPC
- VPC peering
- VPC Endpoint
- Transit gateway
- AWS PrivateLink
- VPC Flow Logs
- Labs: VPC, VPC Peering, VPC Flow Logs & AWS Transit Gateway

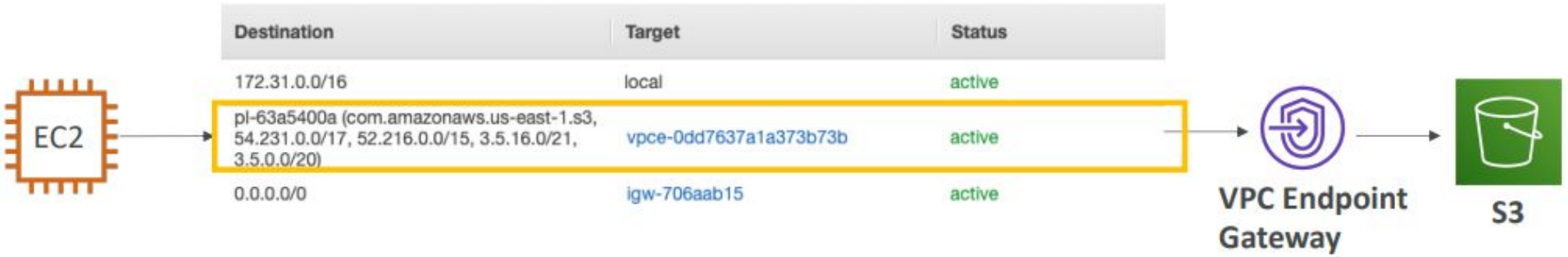
VPC Endpoint

- Les points de terminaison vous permettent de vous connecter aux services AWS en utilisant un réseau privé au lieu du réseau réseau **public www**
- Ils évoluent horizontalement et sont redondants
- Plus de IGW, NAT, etc... pour accéder aux services AWS. Services
- Passerelle VPC Endpoint (S3 & DynamoDB)
- Interface VPC Endpoint (tout sauf DynamoDB)
- En cas de problèmes :
  - Vérifiez la résolution des paramètres DNS dans votre VPC
  - Vérifiez les tables de routage



VPC Endpoint Gateway

- Ne fonctionne que pour S3 et DynamoDB, doit créer une passerelle par VPC
- Doit mettre à jour les entrées des tables de route
- La passerelle est définie au niveau du VPC



- La résolution DNS doit être activée dans le VPC.
- Le même nom d'hôte public peut être utilisé pour S3.
- Le point d'extrémité de la passerelle ne peut pas être étendu hors d'un VPC (VPN, DX, TGW, peering).

VPC Endpoint Interface

- Provisionner un ENI qui aura un nom d'hôte d'interface de point de terminaison privé.
- Utiliser les groupes de sécurité pour la sécurité
- DNS privé (paramètre lors de la création de l'endpoint)

  - Le nom d'hôte public d'un service sera résolu par le nom d'hôte privé de l'interface du point de terminaison.
  - Paramètre VPC : "Activer les noms d'hôtes DNS" et "Activer le support DNS" doivent être "true".
  - Exemple pour Athena :
    - Les vignettes-0b7d2995e9dfe5418-mwrths3x.athena.us-east-1.speeds.amazonaws.com
    - Avertissements-0b7d2995e9dfe5418-mwrths3x-us-east-1a.athena.us-east-1.vpce.amazonaws.com
    - Les deux premières années de fonctionnement de l'entreprise ont été marquées par des changements dans la structure de l'entreprise.
    - athena.us-east-1.amazonaws.com (nom DNS privé)
- L'interface est accessible depuis Direct Connect et Site-to-Site VPN.

VPC Endpoint policies

- Les politiques de points de terminaison sont des documents JSON permettant de contrôler l'accès aux services.
- Ne remplace pas les politiques d'utilisation IAM ni les politiques spécifiques aux spécifiques aux services (comme les politiques de seau S3).

```
{
   "Statement": [{
      "Action": ["sqs:SendMessage"],
      "Effect": "Allow",
      "Resource": "arn:aws:sqs:us-east-2:123456789012:MyQueue",
      "Principal": {
        "AWS": "arn:aws:iam:123456789012:user/MyUser"
      }
   }]
}
```

- **Remarque :** l'utilisateur IAM peut toujours utiliser les autres API de SQS depuis l'extérieur du point de terminaison VPC.
- Vous pouvez ajouter une politique de file d'attente SQS pour refuser toute action non effectuée par le biais du VPC Endpoint

VPC Endpoint exemples de policies

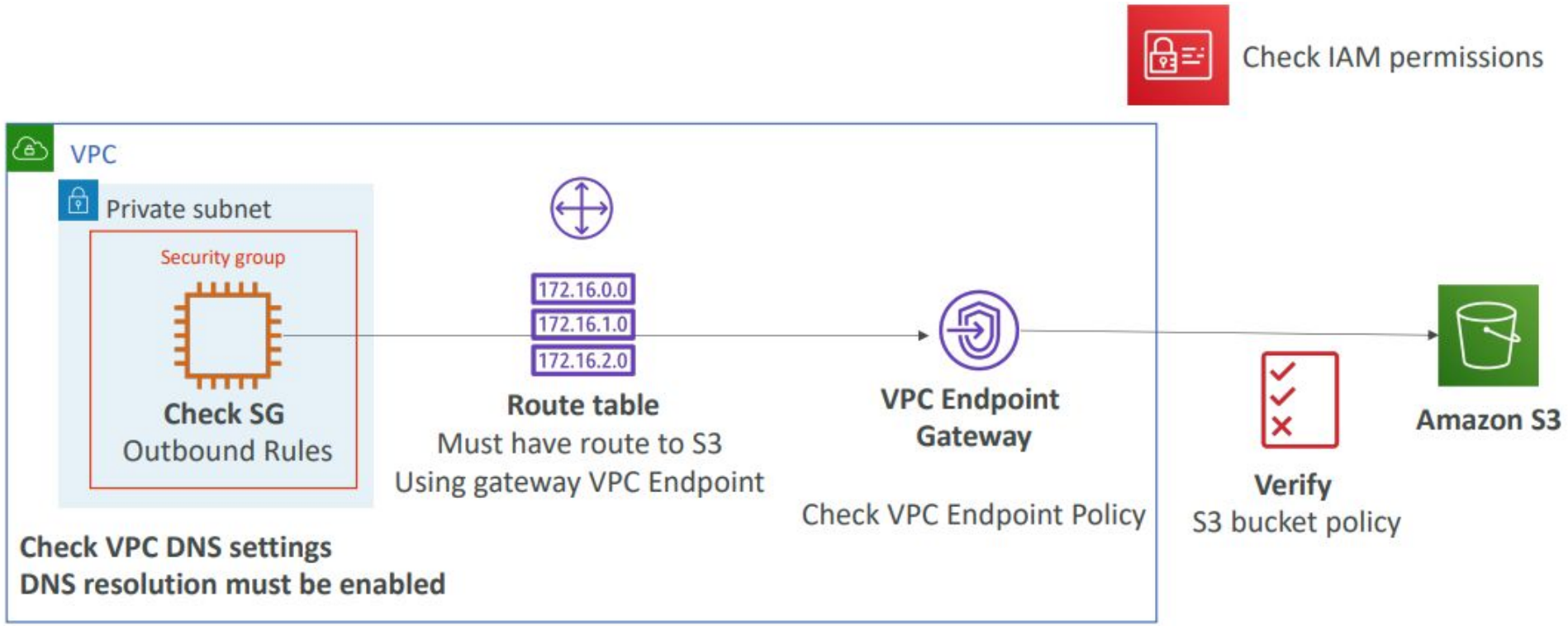
- **politique de seau S3 pour restreindre à un point d'extrémité VPC spécifique**

```
{
  "Version": "2012-10-17",
  "Id": "Policy1415115909152",
  "Statement": [
    {
      "Sid": "Access-to-specific-VPCE-only",
      "Principal": "*",
      "Action": "s3:*",
      "Effect": "Deny",
      "Resource": ["arn:aws:s3:::my_secure_bucket",
                   "arn:aws:s3:::my_secure_bucket/*"],
      "Condition": {
        "StringNotEquals": {
          "aws:sourceVpce": "vpce-1a2b3c4d"
        }
      }
    }
  ]
}
```

- **politique de seau S3 pour restreindre à un VPC entier (plusieurs points d'extrémité de VPC)**

```
{
  "Version": "2012-10-17",
  "Id": "Policy1415115909152",
  "Statement": [
    {
      "Sid": "Access-to-specific-VPC-only",
      "Principal": "*",
      "Action": "s3:*",
      "Effect": "Deny",
      "Resource": ["arn:aws:s3:::my_secure_bucket",
                   "arn:aws:s3:::my_secure_bucket/*"],
      "Condition": {
        "StringNotEquals": {
          "aws:sourceVpc": "vpc-111bbb22"
        }
      }
    }
  ]
}
```

VPC Endpoint Policies for S3 Troubleshooting

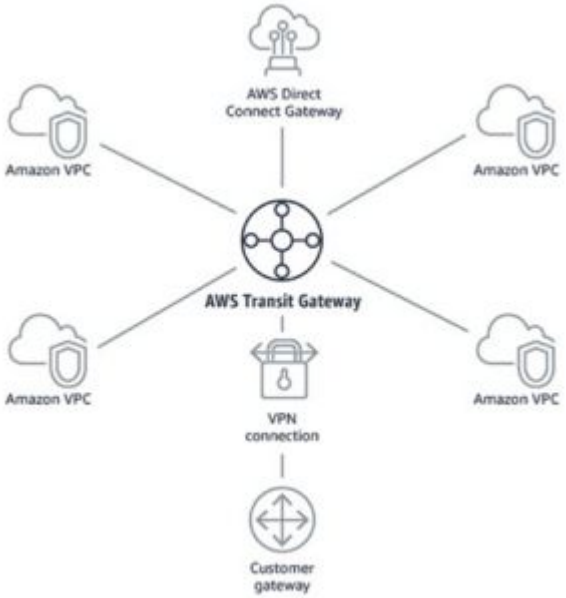


Plan

- Amazon VPC
- VPC peering
- VPC Endpoint
- Transit gateway
- AWS PrivateLink
- VPC Flow Logs
- Labs: VPC, VPC Peering, VPC Flow Logs & AWS Transit Gateway

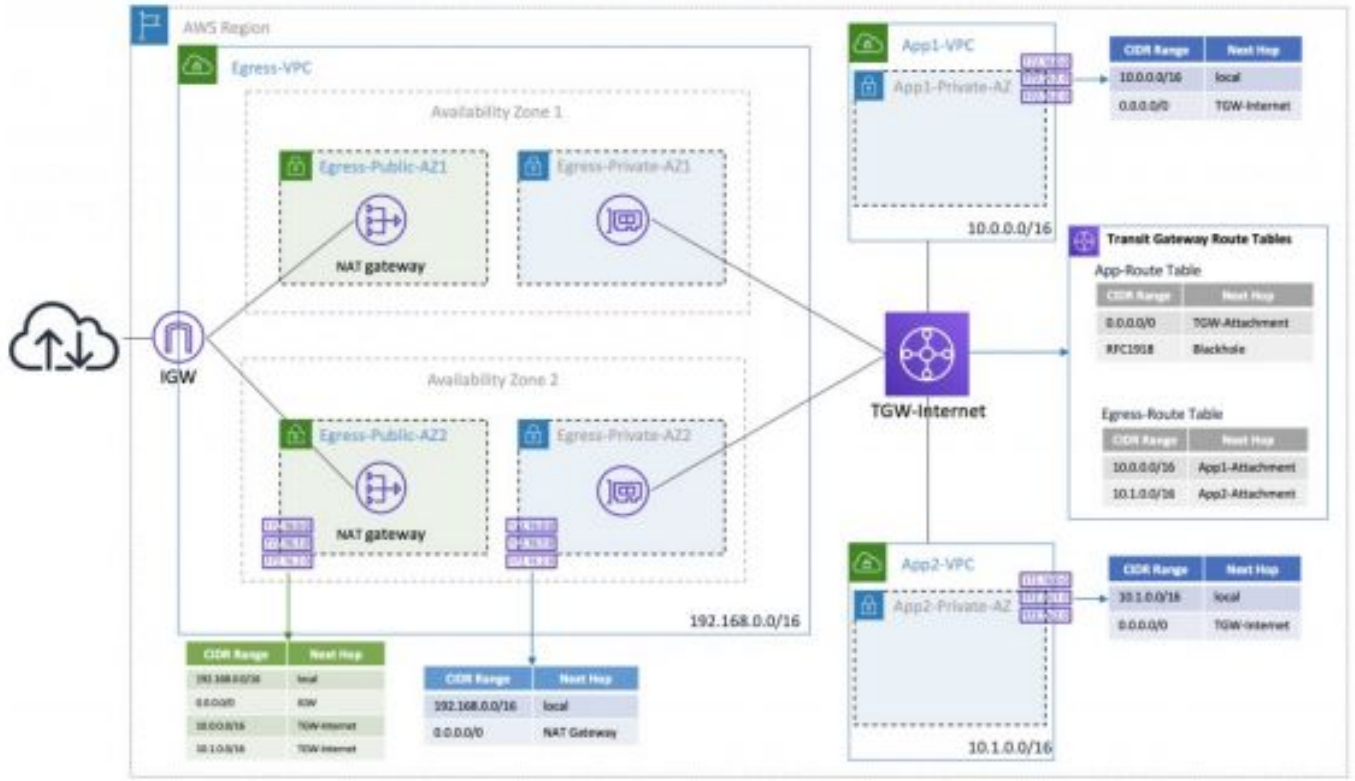
AWS Transit gateway

- Pour avoir un peering transitif entre des milliers de VPC et de sur premises, hub et en étoile
- Ressource régionale, peut fonctionner de manière trans-région
- Partage de comptes croisés
- Les tables de route limitent les VPC qui peuvent communiquer avec d'autres VPC.
- Vous pouvez partager des passerelles de transit entre régions - Tables de routage : limitent les VPC qui peuvent communiquer avec d'autres VPC - Fonctionne avec Direct Connect Gateway, connexions VPN - Supporte la multidiffusion IP (non supporté par d'autres services AWS)
- Les instances d'un VPC peuvent accéder à une passerelle NAT, NLB, PrivateLink et EFS dans d'autres VPC rattachés à la passerelle de transit AWS. Passerelle de transit



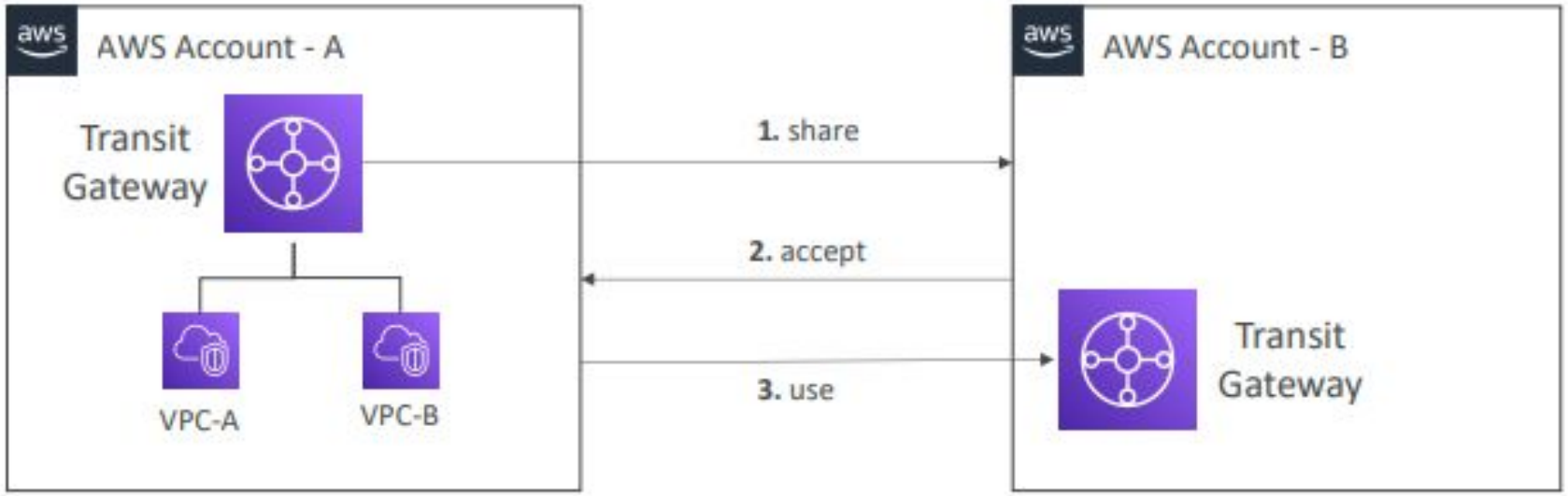
AWS Transit gateway

- La passerelle NAT est partagée dans l'EgressVPC
- Le VPC privé App peut accéder à Internet via le TGW
- Dans cet exemple, les App VPCs ne peuvent pas communiquer avec entre eux en se basant sur la table de route du TGW

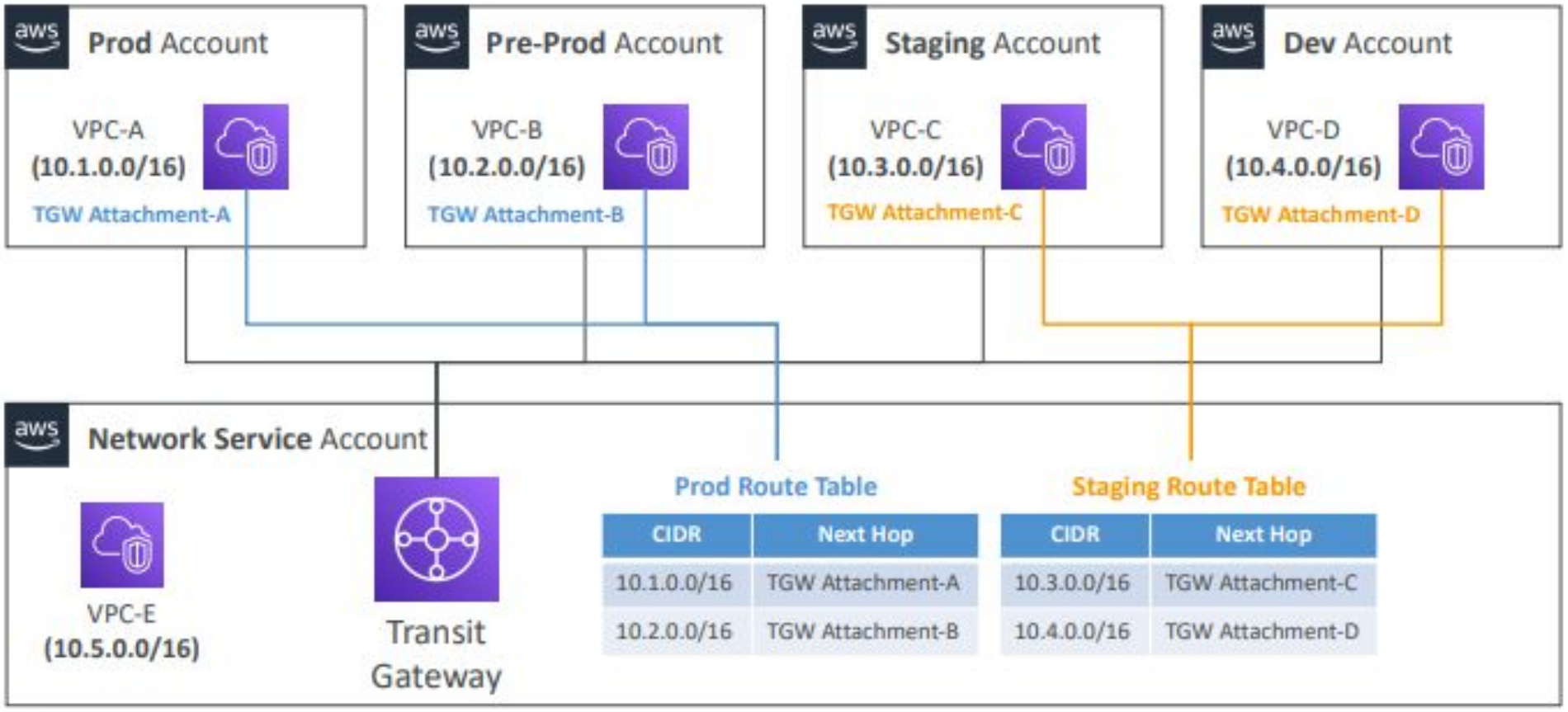


AWS Transit gateway - partage des ressources via RAM

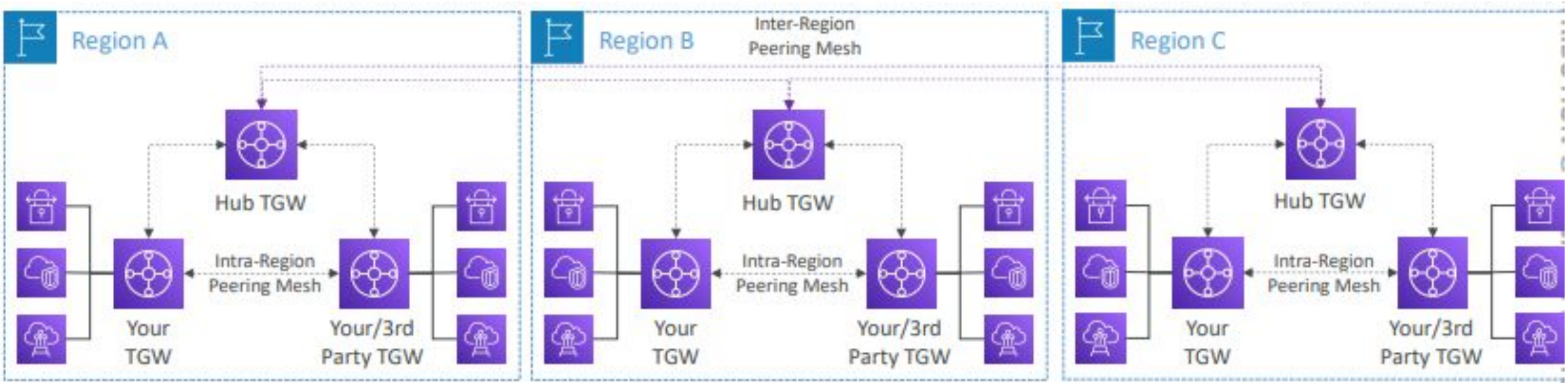
- Vous pouvez utiliser **AWS RAM (Resource Access Manager)** pour partager une passerelle de transit pour les pièces jointes VPC entre comptes ou entre organisations AWS



Transit Gateway - Utiliser des tables de routage différentes pour empêcher les VPC de communiquer



Transit Gateway - inter & intra region peering



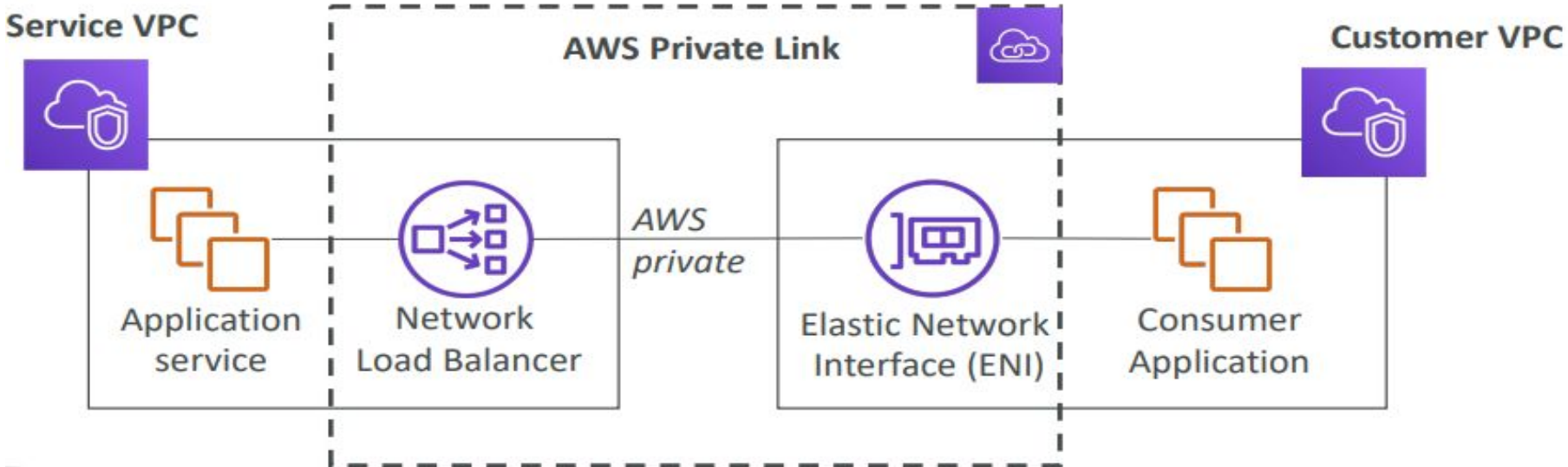
- Facturation horaire pour chaque attachement de peering, pas de frais de traitement de données
- Si les données traversent la région par le biais de l'attachement, les frais standard sont facturés.
- Spécifiez l'ID de la passerelle de transit

Plan

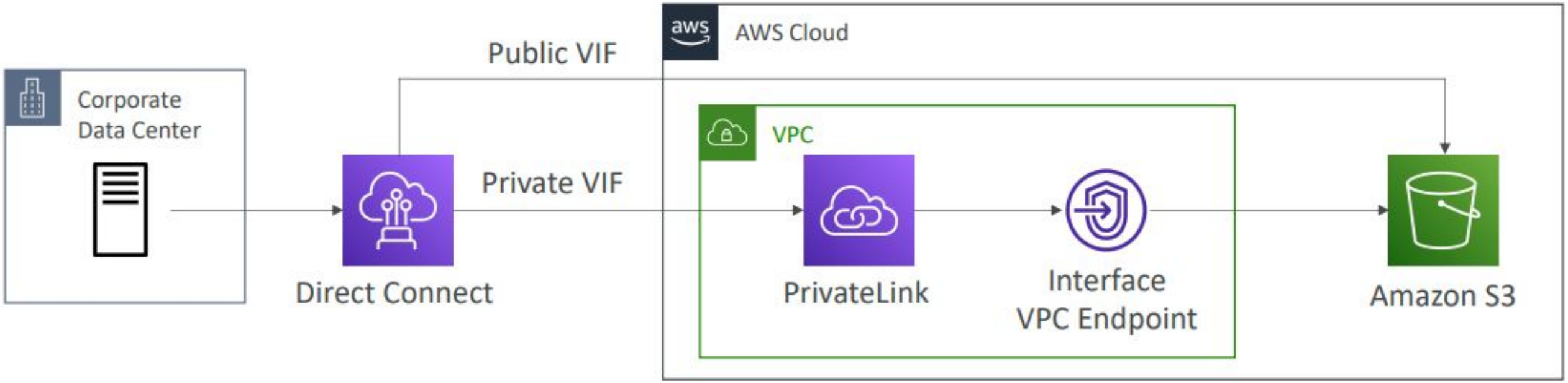
- Amazon VPC
- VPC peering
- VPC Endpoint
- Transit gateway
- AWS PrivateLink
- VPC Flow Logs
- Labs: VPC, VPC Peering, VPC Flow Logs & AWS Transit Gateway

AWS Privatelink

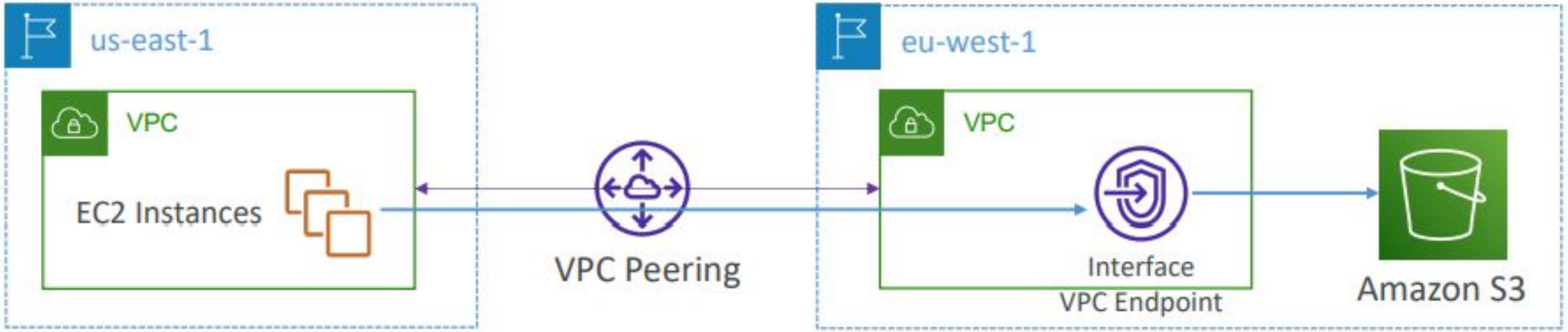
- Le moyen le plus sûr et le plus évolutif d'exposer un service à des milliers de VPC (comptes propres ou autres).
- Ne nécessite pas de peering VPC, de passerelle Internet, de NAT, de tables de routage...
- Nécessite un équilibreur de charge réseau (VPC de service) et un ENI (VPC de client).
- Si le NLB est dans plusieurs AZ, et l'ENI dans plusieurs AZ, la solution est tolérante aux pannes !



AWS PrivateLink pour Amazon S3 avec Direct connect



VPC Endpoints / PrivateLink et VPC Peering



Plan

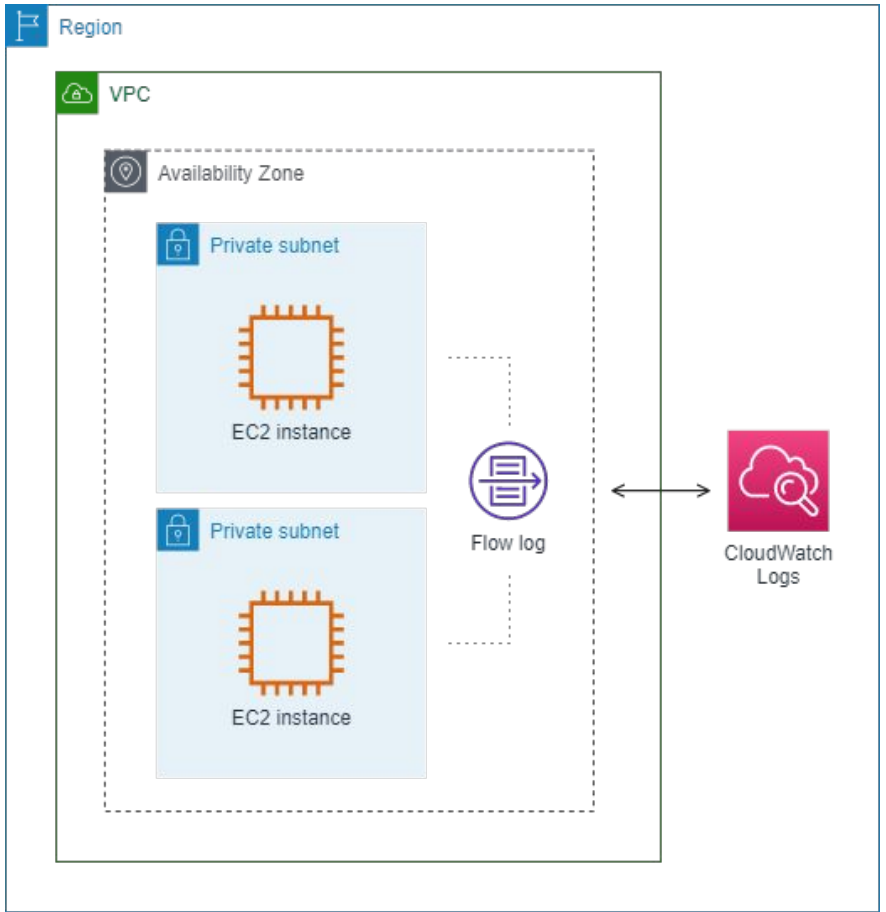
- Amazon VPC
- VPC peering
- VPC Endpoint
- Transit gateway
- AWS PrivateLink
- VPC Flow Logs
- Labs: VPC, VPC Peering, VPC Flow Logs & AWS Transit Gateway

VPC Flow Logs

- Capturez des informations sur le trafic IP entrant dans vos interfaces :
  - Journaux de flux VPC
  - Journaux de flux de sous-réseau
  - Journaux de flux de l'interface réseau élastique (ENI)
- Aide à surveiller et à résoudre les problèmes de connectivité.
- Les données des journaux de flux peuvent être envoyées vers S3 / CloudWatch Logs.
- Capture également les informations réseau des interfaces gérées par AWS : ELB, RDS, ElastiCache, Redshift, WorkSpaces, NATGW, Transit Gateway.

VPC Flow Logs -exemple

Dans l'exemple suivant, un journal de flux capture tout le trafic d'un sous-réseau et publie les enregistrements du journal de flux sur Amazon CloudWatch Logs. Le journal de flux capture le trafic de toutes les interfaces réseau du sous-réseau.



VPC Flow Logs -exemple

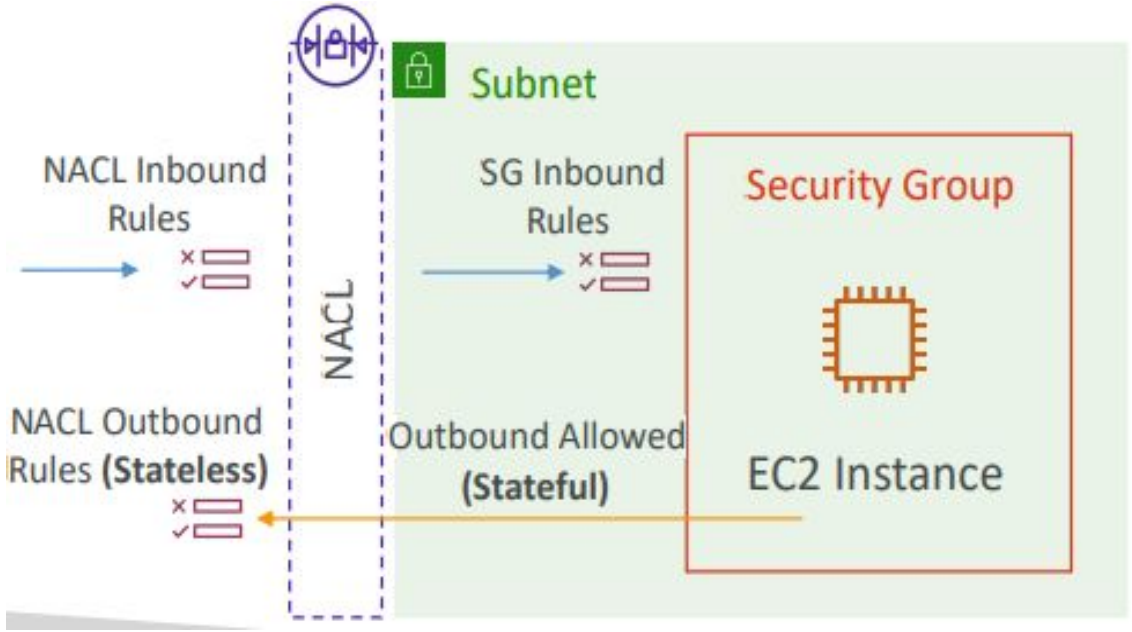
- **srcaddr & dstaddr** - aident à identifier les IP problématiques
- **srcport & dstport** - aide à l'identification des ports problématiques
- **Action -** succès ou échec de la demande en raison du groupe de sécurité / NACL
- Peut être utilisé pour l'analyse des modèles d'utilisation ou des comportements malveillants.
- **Interrogez les journaux de flux VPC à l'aide d'Athena sur S3 ou de CloudWatch Logs Insights**
- Exemples de journaux: https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs-records-examples.html/

VPC Flow Logs –Maintenance des problèmes de SG & NACL

Look at the "ACTION" field

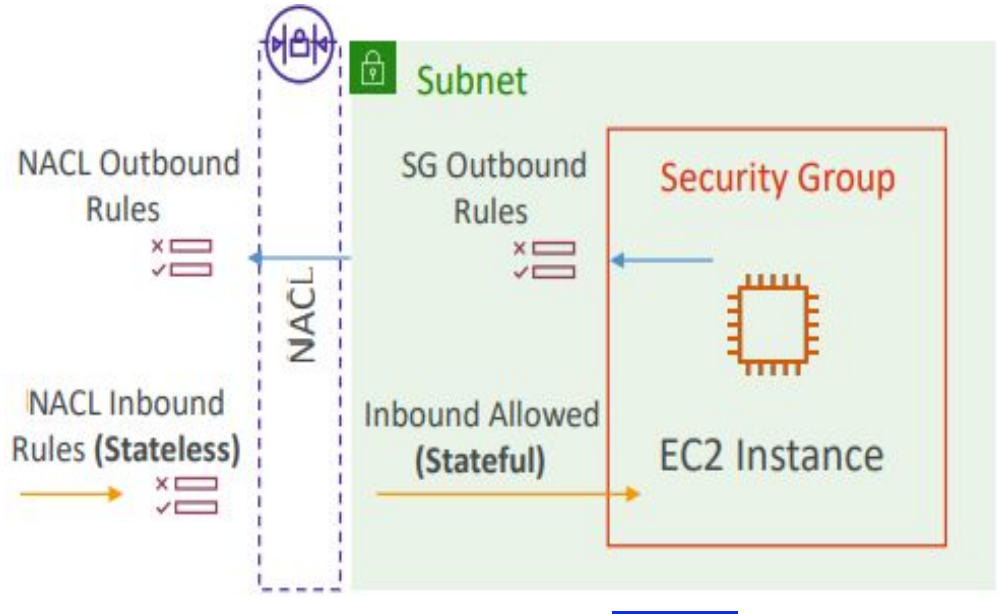
Requêtes entrants

- Inbound REJECT => NACL or SG
- Inbound ACCEPT, Outbound REJECT => NAC



Requêtes sortants

- Outbound REJECT => NACL or SG
- Outbound ACCEPT, Inbound REJECT => NACL



VPC Flow Logs -avec NAT Gateway

- *Votre flux de logs VPC montre Action = ACCEPT pour le trafic entrant venant des adresses publiques. Néanmoins, votre compréhension du NAT gateway est qu'il n'accepte pas le trafic de l'internet. Est-ce que votre NAT gateway accepte le trafic de l'internet?*

- **Inbound Traffic est permis par le groupe de sécurité ou NACLs**
  - Trafic n'est pas permise par le NAT Gateway, c'est annulé
  - Pour confirmer exécuter la requête suivante dans le CloudWatch Log Group

```
filter (dstAddr like 'xxx.xxx' and srcAddr like 'public IP')
| stats sum(bytes) as bytesTransferred by srcAddr, dstAddr
| limit 10
```

- Faire xxx.xxx les premiers octets pour votre VPC CIDR

- Remplacer l'adresse IP public avec l'adresse IP du NAT Gateway, mais nulle part autre: trafic a été sollicité et annulé

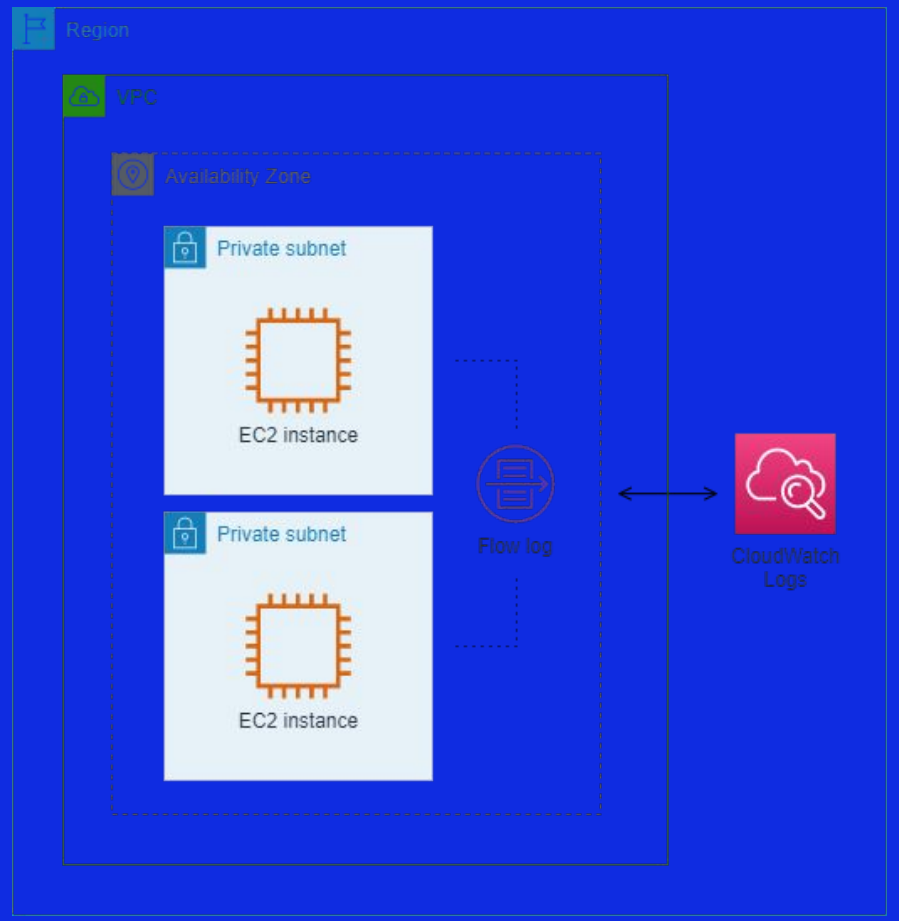
Plan

- Amazon VPC
- VPC peering
- VPC Endpoint
- Transit gateway
- AWS PrivateLink
- VPC Flow Logs
- Labs: VPC, VPC Peering, VPC Flow Logs & AWS Transit Gateway

www.eazytraining.fr

Lab-1 : création d’un VPC Flow logs.

Pour cette séance de laboratoire, nous allons créer et configurer la fonctionnalité de surveillance et de sécurité réseau VPC Flow Logs.



www.eazytraining.fr

Lab-2: configuration d’un VPC Peering

www.eazytraining.fr

Lab-3: configuration d’un Transit Gateway

MERCI POUR VOTRE AIMABLE ATTENTION!

EAZYTraining

Alphonsine Lahda

Lahda Biassou Alphonsine

Ingénieure cloud et Formatrice