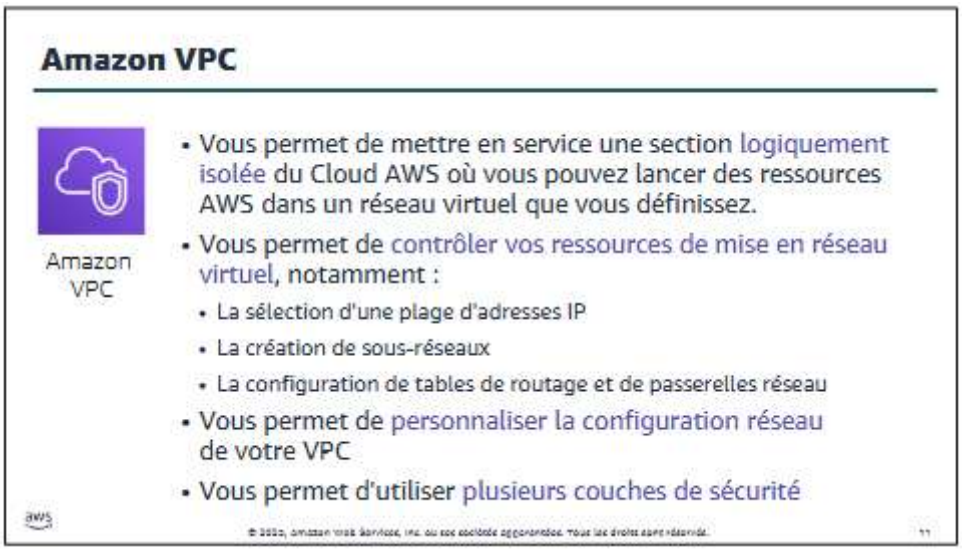
Mise en réseau et diffusion de contenu Amazon VPC

Amazon Virtual Private Cloud (Amazon VPC) est le service de mise en réseau AWS.

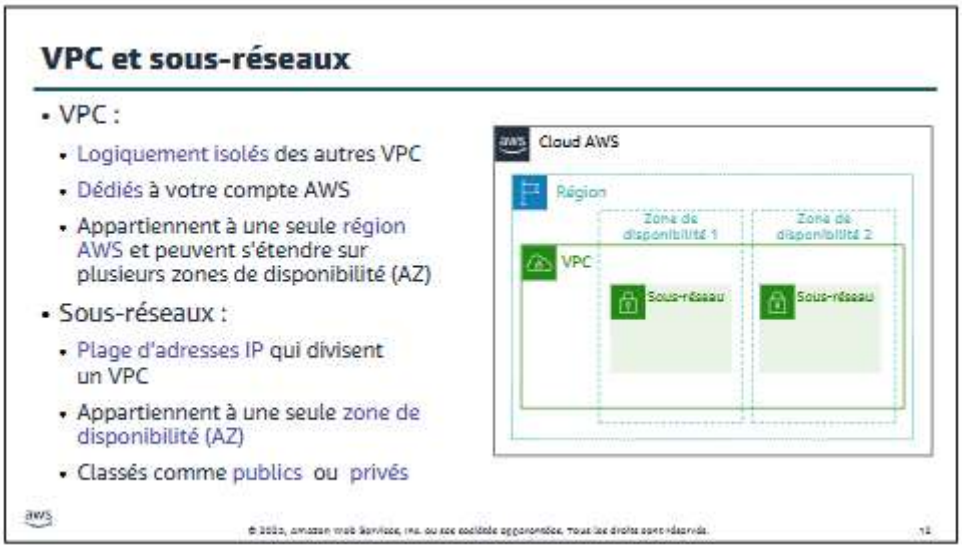
Un réseau informatique est constitué de deux machines clientes ou plus qui sont connectées les unes aux autres pour partager des ressources. Un réseau peut être divisé logiquement en sous-réseaux. Cette mise en réseau nécessite un périphérique réseau comme un routeur ou un commutateur pour connecter tous les clients entre eux et permettre la communication entre eux.



Amazon Virtual Private Cloud (Amazon VPC) est un service qui permet de mettre en service une section logiquement isolée du Cloud AWS, section dans laquelle on peut lancer ses ressources AWS.

Amazon VPC permet de contrôler les ressources de mise en réseau virtuel, y compris la sélection de sa propre plage d'adresses IP, la création de sous-réseaux et la configuration des tables de routage et des passerelles réseau. Dans le VPC il est possible d'utiliser les protocoles IPv4 et IPv6 pour un accès sécurisé aux ressources et aux applications.

Il est également possible de personnaliser la configuration du réseau pour son VPC. À titre d'exemple, vous pouvez créer un sous-réseau public pour vos serveurs web qui ont accès à Internet. Il est également possible de placer dans un sous-réseau privé sans accès Internet public vos systèmes backend comme les bases de données ou les serveurs d'applications. Enfin, vous pouvez exploiter plusieurs couches de sécurité, y compris les groupes de sécurité et les listes de contrôle d'accès au réseau (ACL réseau), afin de renforcer le contrôle des accès aux instances Amazon Elastic Compute Cloud (AmazonEC2) dans chaque sous-réseau.

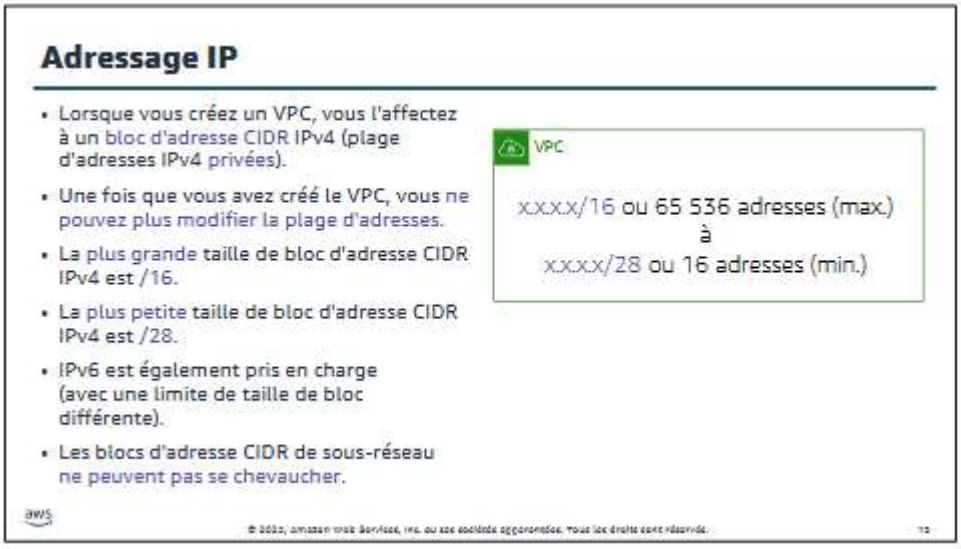


Amazon VPC permet de mettre en service des VPC, un réseau virtuel qui est logiquement isolé des autres réseaux virtuels dans le Cloud AWS, ils appartiennent à une seule région AWS et peuvent s'étendre sur plusieurs zones de disponibilité.

Après avoir créé un VPC, on peut le diviser en un ou plusieurs sous-réseaux.

Dans un VPC un sous-réseau est une plage d'adresses IP.

Ils sont généralement classés comme publics ou privés. Les sous-réseaux publics ont un accès direct à Internet, contrairement aux sous-réseaux privés.



Les adresses IP permettent aux ressources du VPC de communiquer entre elles et avec des ressources sur Internet. Lorsqu'un VPC est créer, il est affectez à un bloc d'adresse CIDR IPv4 (plage d'adresses IPv4 privées). Une fois que créé, modifier la plage d'adresses est impossible, il est donc important de la sélectionner avec soin.

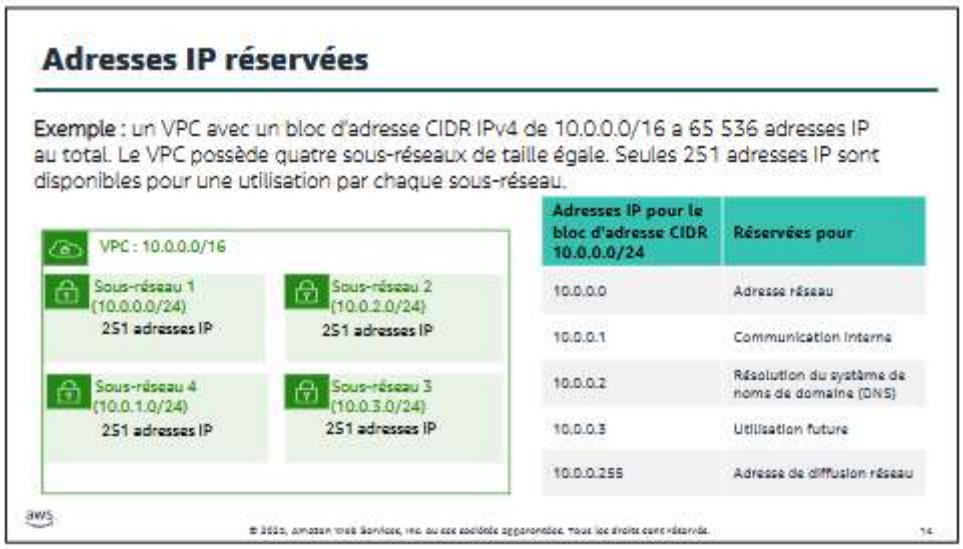
Le bloc d'adresse CIDR IPv4 peut être aussi grand que /16 (soit 65 536 adresses) ou aussi petit que /28 (soit 16 adresses).

Vous pouvez éventuellement associer un bloc d'adresse CIDR IPv6 à votre VPC et vos sous-réseaux et attribuer des adresses IPv6 à partir de ce bloc aux ressources de votre VPC. Les blocs d'adresse CIDR IPv6 ont une limite de taille de bloc différente.

Le bloc d'adresse CIDR d'un sous-réseau peut être le même que le bloc d'adresse CIDR d'un VPC.

Dans ce cas, le VPC et le sous-réseau ont la même taille (un seul sous-réseau dans le VPC).

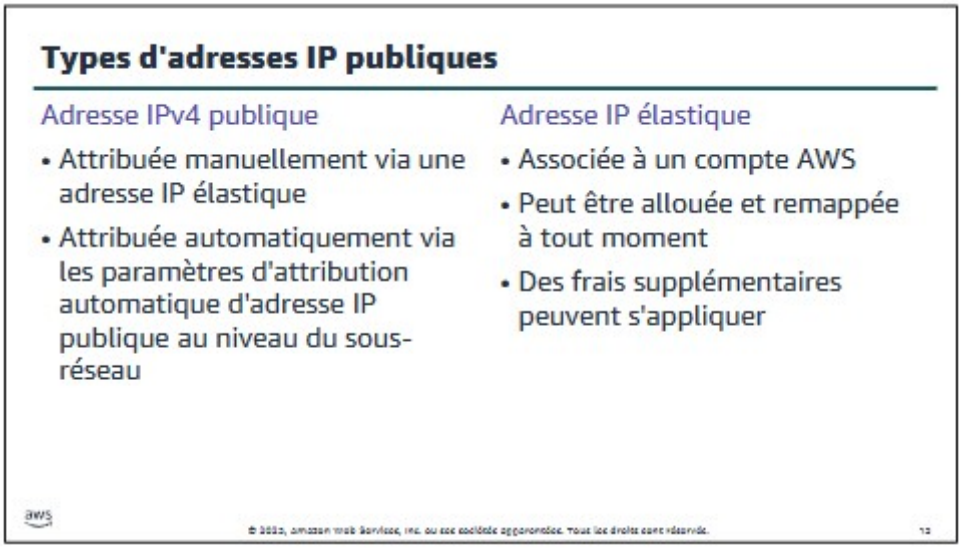
En outre, le bloc d'adresse CIDR d'un sous-réseau peut être un sous-ensemble du bloc d'adresse CIDR du VPC. Cette structure permet de définir plusieurs sous-réseaux. Si vous créez plus d'un sous-réseau dans un VPC, les blocs d'adresse CIDR de ces sous-réseaux ne peuvent pas se chevaucher. Vous ne pouvez pas avoir d'adresses IP en double dans le même VPC.



Lorsque vous créez un sous-réseau, il nécessite son propre bloc d'adresse CIDR. Pour chaque bloc d'adresse CIDR que vous spécifiez, AWS réserve cinq adresses IP dans ce bloc. Ces adresses ne peuvent pas être utilisées. AWS réserve ces adresses IP pour ces éléments :

- Adresse réseau
- Routeur local de VPC (communications internes)
- Résolution du système de noms de domaine (DNS)
- Utilisation future
- Adresse de diffusion réseau

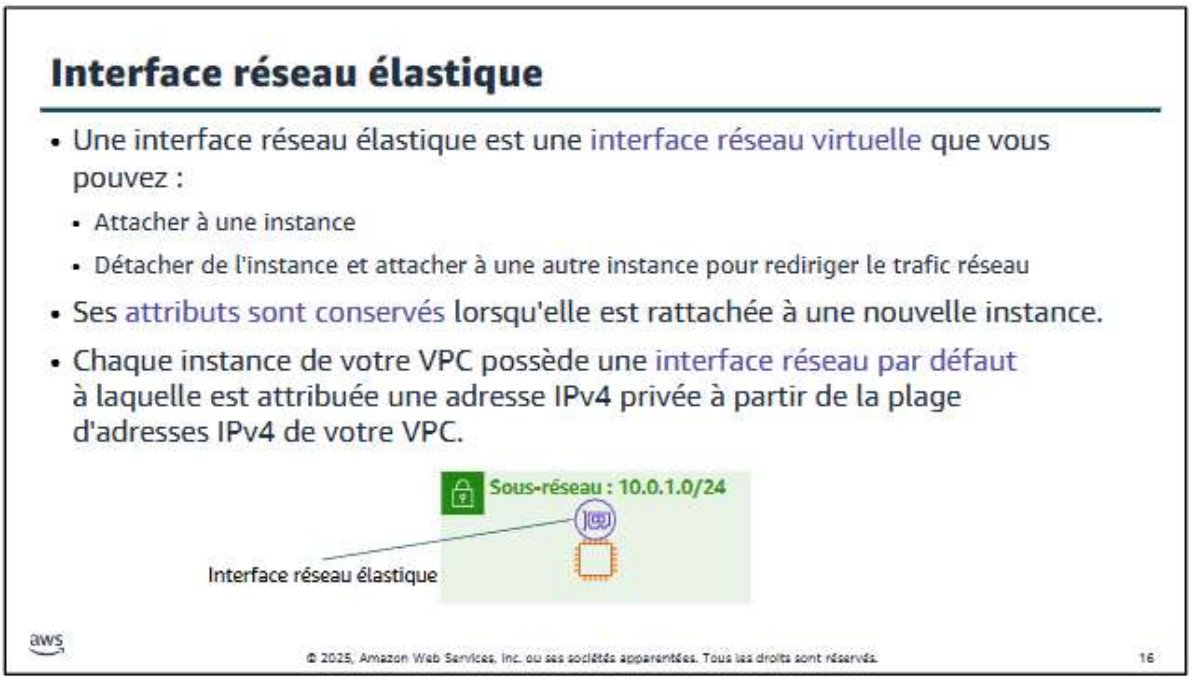
Par exemple, supposons que vous créez un sous-réseau avec le bloc d'adresse CIDR IPv4 10.0.0.0/24 (qui compte 256 adresses IP au total). Bien que le sous-réseau compte 256 adresses IP, seules 251 adresses sont disponibles, car cinq d'entre elles sont réservées.



Lorsque vous créez un VPC, chacune de ses instances reçoit automatiquement une adresse IP privée. Pour demander qu'une adresse IP publique soit attribuée lorsque vous créez l'instance, modifiez les propriétés d'attribution automatique de l'adresse IP publique du sous-réseau.

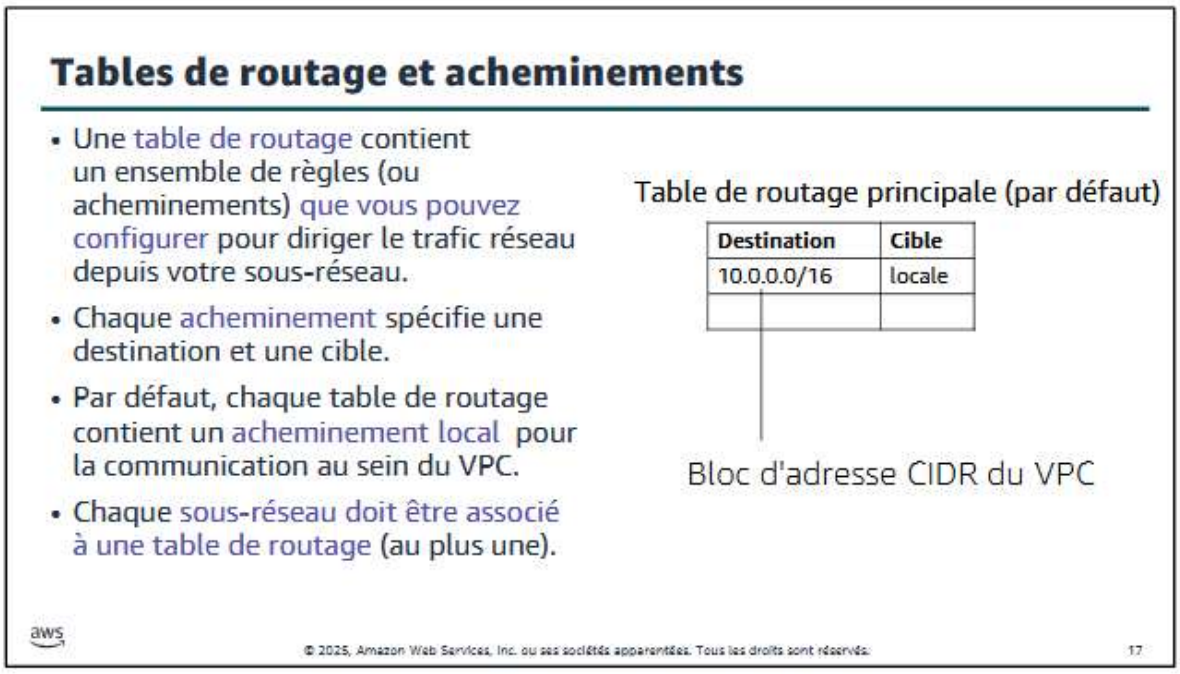
Une adresse IP élastique est une adresse IPv4 publique statique conçue pour le cloud computing dynamique permettant d'associer une adresse IP élastique à n'importe quelle instance ou interface réseau pour n'importe quel VPC dans votre compte.

Avec une adresse IP élastique, vous pouvez contourner un problème d'échec d'une instance en remappant rapidement l'adresse vers une autre instance de votre VPC. Associer l'adresse IP élastique à l'interface réseau présente un avantage par rapport à une association directe avec l'instance. Vous pouvez déplacer tous les attributs de l'interface réseau d'une instance vers une autre en une seule étape.



Une interface réseau élastique est une interface réseau virtuelle que vous pouvez attacher à une instance dans un VPC. Un attribut d'interface réseau la suit lorsqu'elle est rattachée à une autre instance. Lorsque vous déplacez une interface réseau d'une instance vers une autre, le trafic réseau est redirigé vers la nouvelle instance.

Chaque instance d'un VPC comporte une interface réseau par défaut (interface réseau principale) à laquelle est attribuée une adresseIPv4 privée à partir de la plage d'adressesIPv4 de votre VPC. Vous ne pouvez pas détacher une interface réseau principale d'une instance. Vous pouvez créer et attacher une interface réseau supplémentaire à toute instance de votre VPC. Le nombre d'interfaces réseau que vous pouvez attacher varie en fonction du type d'instance.



Une table de routage contient un ensemble de règles (appelées acheminements) qui dirigent le trafic réseau depuis votre sous-réseau. Chaque acheminement spécifie une destination et une cible.

La destination est le bloc d'adresse CIDR où vous voulez que le trafic de votre sous-réseau aille.

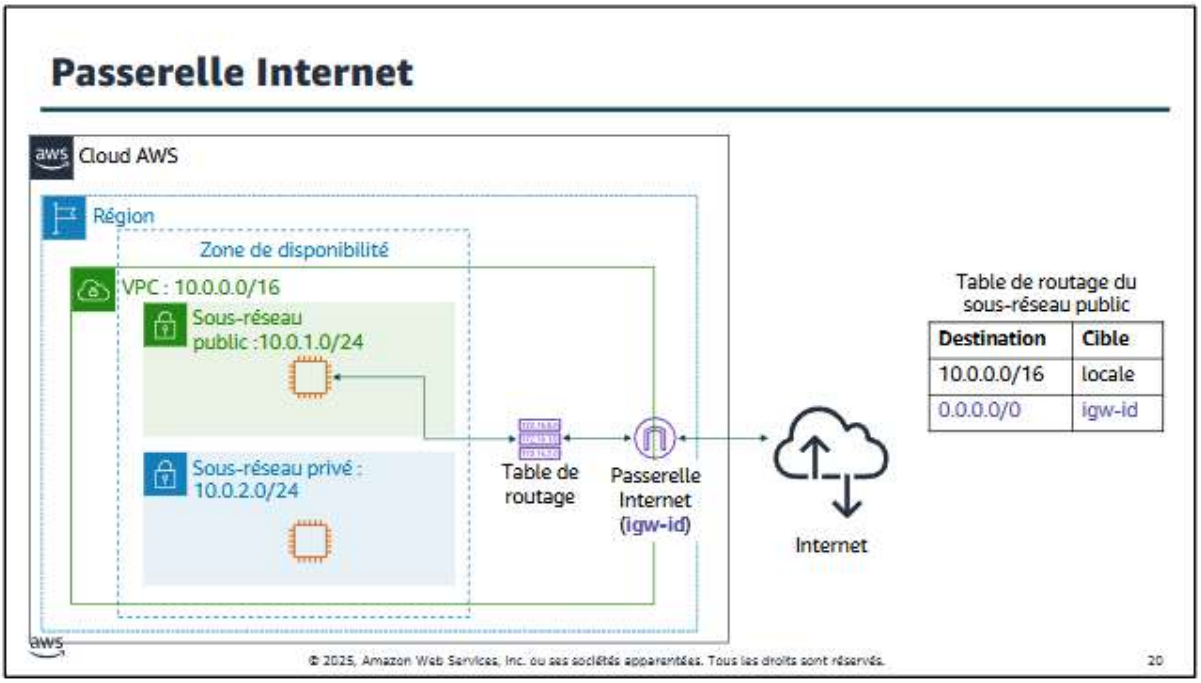
La cible est l'endroit via lequel le trafic de destination est envoyé.

En une phrase : Une table de routage dit “Si le trafic veut aller à CETTE adresse, envoie-le PAR CE chemin.”

Par défaut, chaque table de routage contient un acheminement local pour la communication au sein du VPC. Les tables de routage sont personnalisables en ajoutant des acheminements. L'entrée d'acheminement local utilisée pour les communications internes ne peut pas être supprimée.

Chaque sous-réseau de votre VPC doit être associé à une table de routage. La table de routage principale est la table qui est automatiquement attribuée à votre VPC. Elle contrôle le routage de tous les sous-réseaux qui ne sont pas explicitement associés à une autre table de routage. Un sous-réseau peut être associé à une seule table de routage à la fois, mais vous pouvez associer plusieurs sous-réseaux à une même table de routage.

Voyons maintenant la notion d'acheminement du trafic de manière intéressante.



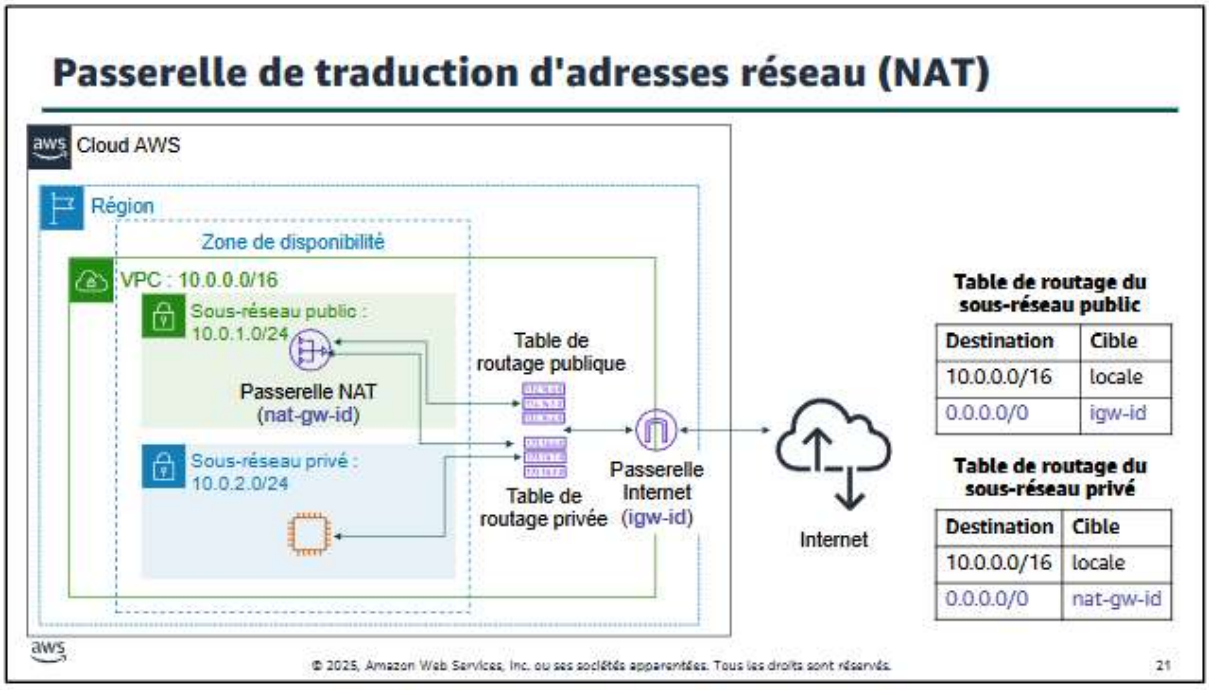
Une passerelle Internet est un composant VPC pouvant être mis à l'échelle, redondant et hautement disponible qui permet la communication entre les instances de votre VPC et Internet.

Une passerelle Internet a deux objectifs :

- Fournir une cible dans les tables de routage de votre VPC pour le trafic acheminé sur Internet
- Effectuer une traduction d'adresses réseau pour les instances auxquelles des adresses IPv4 publiques ont été attribuées.

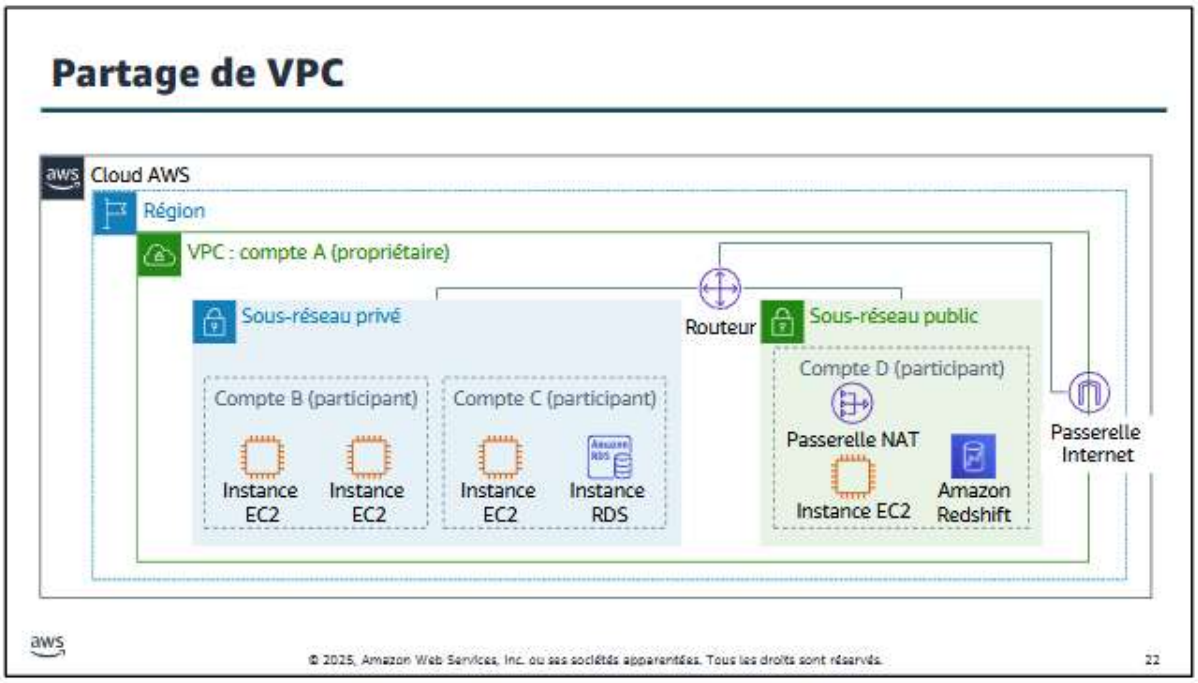
Pour rendre un sous-réseau public, vous devez attacher une passerelle Internet à votre VPC et ajouter un acheminement à la table de routage pour envoyer le trafic non local via cette passerelle vers Internet (0.0.0.0/0).

Si le trafic veut aller à CETTE adresse (0.0.0.0/0), envoie-le PAR CE chemin. (Igw-id)



Une passerelle de traduction d'adresses réseau (NAT) permet d'autoriser les instances d'un sous-réseau privé à se connecter à Internet ou à d'autres services AWS, mais empêche Internet d'initier une connexion avec ces instances.

Pour créer une passerelle NAT, vous devez spécifier le sous-réseau public que cette passerelle NAT devra occuper.
Vous devez également spécifier une adresse IP Elastic à associer à la passerelle NAT lorsque vous la créerez.
Une fois que vous avez créé une passerelle NAT, vous devez mettre à jour la table de routage qui est associée à un ou plusieurs de vos sous-réseaux privés pour diriger le trafic Internet vers cette passerelle.
De cette manière, les instances de vos sous-réseaux privés peuvent communiquer avec Internet.



Le partage de VPC permet aux clients de partager des sous-réseaux avec d'autres comptes AWS de la même organisation dans AWS Organizations.

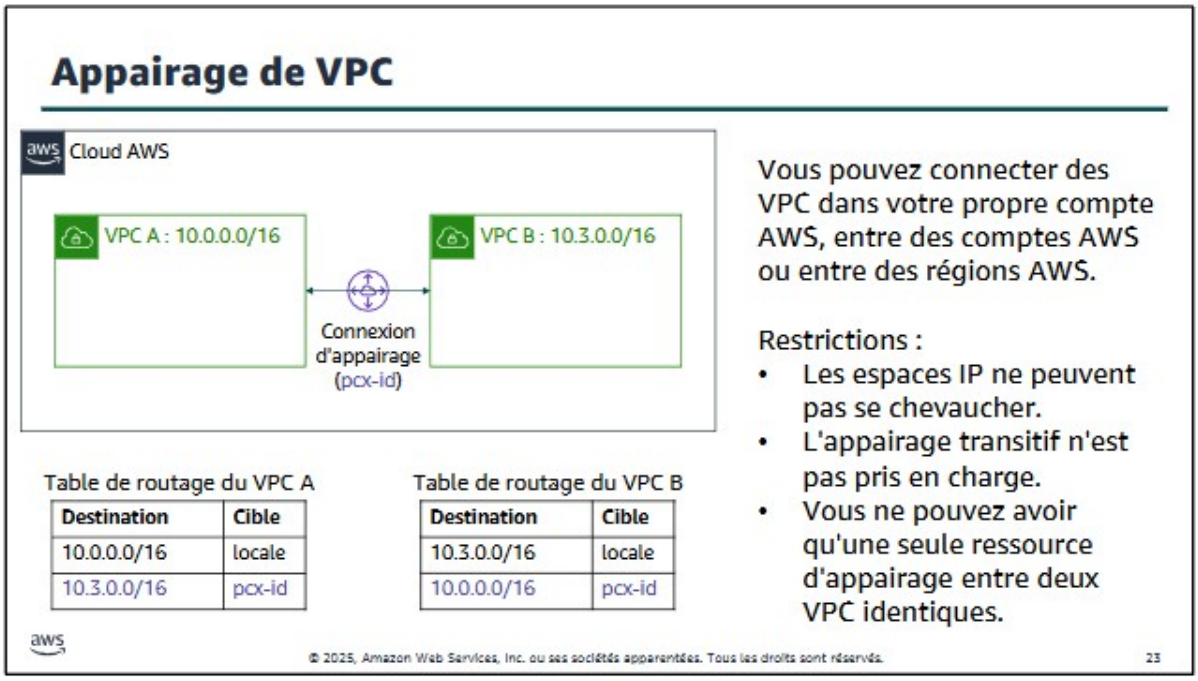
Le partage de VPC permet à plusieurs comptes AWS de créer leurs ressources d'application, telles que les instances Amazon EC2, les bases de données Amazon Relational Database Service (Amazon RDS), les clusters Amazon Redshift et les fonctions AWS Lambda, dans des VPC partagés et gérés de manière centralisée.

Dans ce modèle, le compte qui possède le VPC (propriétaire) partage un ou plusieurs sous-réseaux avec d'autres comptes (participants) qui appartiennent à la même organisation dans AWS Organizations.

Après le partage d'un sous-réseau, les participants peuvent visualiser, créer, modifier et supprimer leurs ressources d'application dans les sous-réseaux qui sont partagés avec eux. Ils ne peuvent pas afficher, modifier ou supprimer des ressources appartenant à d'autres participants ou au propriétaire du VPC.

Le partage de VPC offre plusieurs avantages :

- Séparation des tâches : structure du VPC contrôlée de manière centralisée, routage, attribution d'adresses IP.
- Responsabilité : les propriétaires d'applications continuent d'être responsables de leurs propres ressources, comptes et groupes de sécurité.
- Groupes de sécurité : les participants au partage de VPC peuvent référencer les ID de groupe de sécurité les uns des autres.
- Efficacité : densité plus élevée dans les sous-réseaux, utilisation efficace des VPN et d'AWS Direct Connect.
- Aucune limite stricte: les limites strictes peuvent être évitées (par exemple, 50 interfaces virtuelles par connexion AWS Direct Connect via une architecture réseau simplifiée).
- Optimisation des coûts: les coûts peuvent être optimisés grâce à la réutilisation des passerelles NAT, des points de terminaison d'interface VPC et le trafic intra-zone de disponibilité.

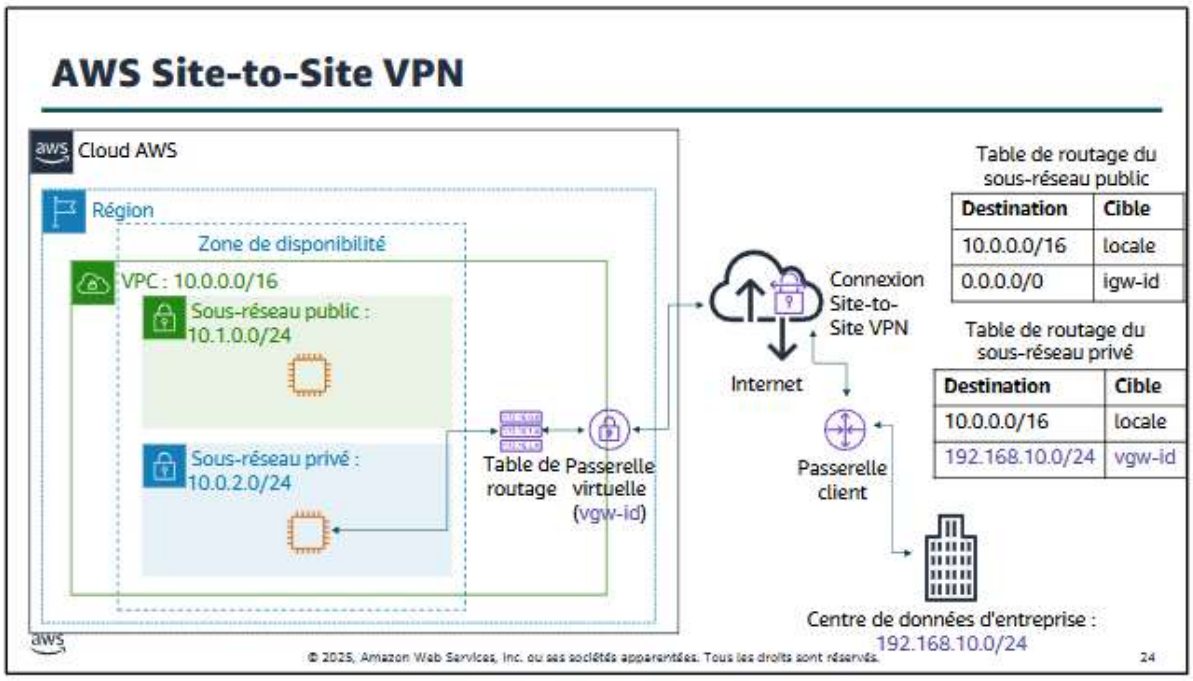


Une connexion d'appairage de VPC est une connexion de mise en réseau entre deux VPC. Elle permet d'acheminer le trafic entre ces derniers de manière privée. Les instances dans les deux VPC peuvent communiquer entre elles comme si elles font partie du même réseau.

Vous pouvez créer une connexion d'appairage de VPC entre vos propres VPC, avec un VPC situé dans un autre compte AWS ou avec un VPC au sein d'une autre région AWS.

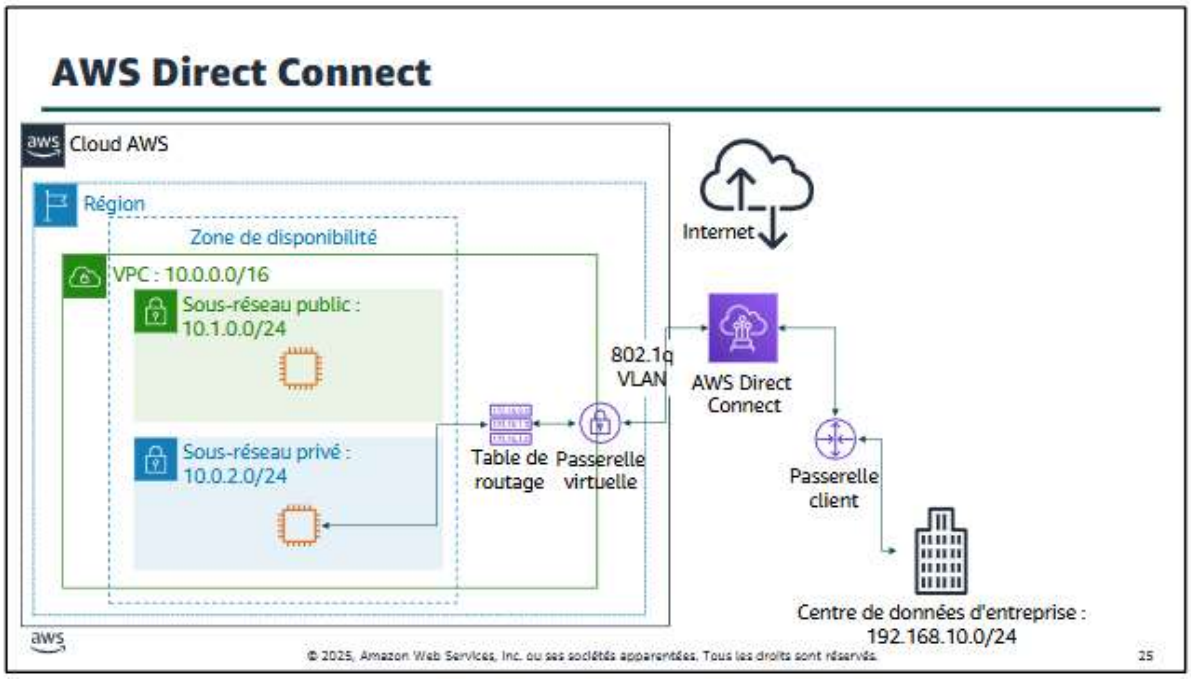
Lorsque vous configurez la connexion d'appairage, vous créez des règles dans votre table de routage pour permettre aux VPC de communiquer entre eux via la ressource d'appairage.

Par exemple, supposons que vous ayez deux VPC. Dans la table de routage du VPCA, vous définissez la destination comme étant l'adresse IP du VPC B et la cible comme étant l'ID de la ressource d'appairage.
Dans la table de routage du VPC B, vous définissez la destination comme étant l'adresse IP du VPC A et la cible comme étant l'ID de la ressource d'appairage.

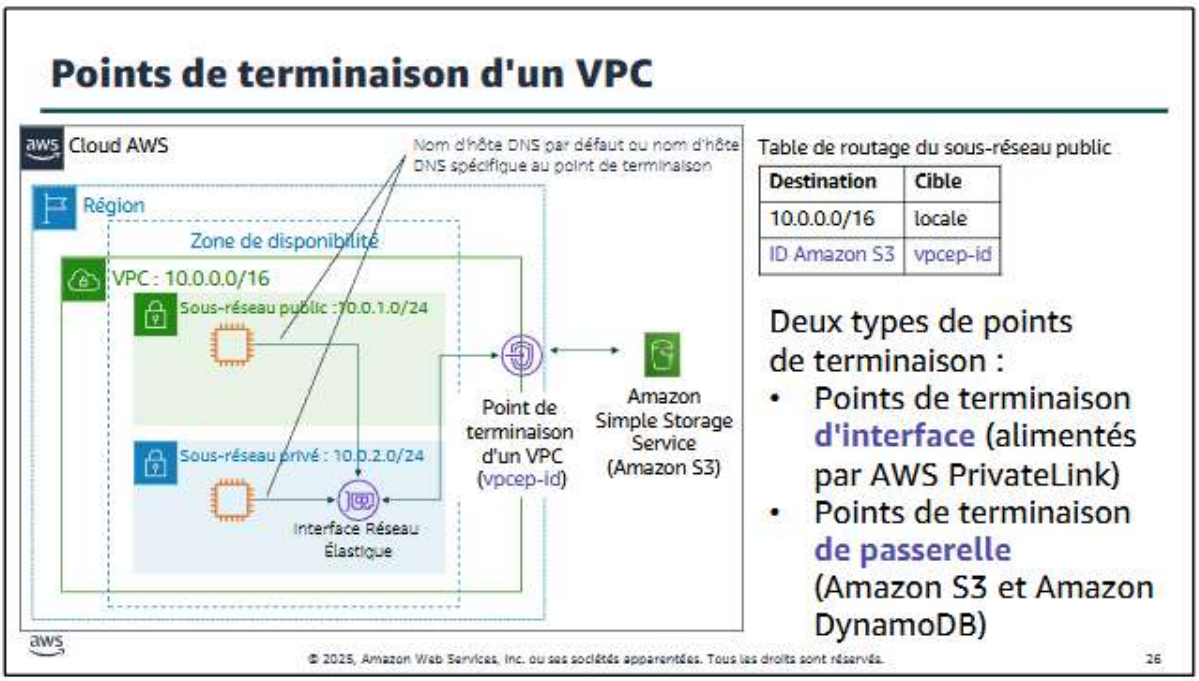


Par défaut, les instances que vous lancez dans un VPC ne peuvent pas communiquer avec un réseau distant. Pour connecter votre VPC à votre réseau distant (c'est-à-dire créer un réseau privé virtuel ou une connexion VPN), procédez comme suit :

1. Créez un périphérique de passerelle virtuelle (appelé passerelle de réseau privé virtuel (VPN)) et attachez-le à votre VPC.
2. Définissez la configuration du périphérique VPN ou de la passerelle client. La passerelle client n'est pas un périphérique, mais une ressource AWS qui fournit des informations à AWS sur votre périphérique VPN.
3. Créez une table de routage personnalisée pour diriger le trafic lié au centre de données d'entreprise vers la passerelle VPN. Vous devez également mettre à jour les règles du groupe de sécurité. (Vous découvrirez les groupes de sécurité dans la section suivante.)
4. Établissez une connexion AWS Site-to-Site VPN (Site-to-Site VPN) pour relier les deux systèmes.
5. Configurez le routage pour faire passer le trafic via la connexion.



L'un des défis de la communication en réseau est la performance du réseau. Les performances peuvent être dégradées si le centre de données est éloigné de la région AWS.
Pour de telles situations, AWS propose AWS Direct Connect (DX) qui permet d'établir une connexion réseau privée dédiée entre votre réseau et celui des emplacements DX.
Cette connexion privée peut réduire les coûts réseau, augmenter le débit de la bande passante et fournir une expérience réseau plus constante que les connexions basées sur Internet.
DX utilise des réseaux locaux virtuels (VLAN) conformes à la norme ouverte 802.1q.



Un point de terminaison d'un VPC est un périphérique virtuel qui vous permet de connecter en privé votre VPC aux services AWS pris en charge et aux services de point de terminaison d'un VPC basés sur la technologie AWS PrivateLink.

La connexion à ces services ne nécessite pas de passerelle Internet, de périphérique NAT, de connexion VPN ni de connexion AWS Direct Connect. Les instances de votre VPC ne requièrent pas d'adresses IP publiques pour communiquer avec les ressources du service. Le trafic entre votre VPC et les autres services ne quitte pas le réseau Amazon.

Il existe deux types de points de terminaison d'un VPC:

- Le point de terminaison d'un VPC d'interface (ou point de terminaison d'interface) vous permet de vous connecter à des services basés sur la technologie AWS PrivateLink. Parmi ces services citons certains services AWS, des services qui sont hébergés par d'autres clients AWS et des membres du réseau de partenaires AWS (APN) dans leurs propres VPC (appelés services de point de terminaison) et les services APN AWS Marketplace pris en charge.
  Le propriétaire du service est le fournisseur du service et vous, en tant que mandataire qui crée le point de terminaison d'interface, êtes l'utilisateur du service. Vous êtes facturé pour la création et l'utilisation d'un point de terminaison d'interface avec un service. Des tarifs d'utilisation horaires et de traitement des données s'appliquent.

- Points de terminaison de passerelle : l'utilisation de points de terminaison de passerelle n'entraîne aucun frais supplémentaire. Des frais standard pour le transfert de données et l'utilisation des ressources s'appliquent.

Voici quelques points clés à retenir :
Il existe plusieurs options de mise en réseau de VPC, notamment :

- Passerelle Internet: connecte votre VPC à Internet
- Passerelle NAT: permet aux instances d'un sous-réseau privé de se connecter à Internet.
- Point de terminaison d'un VPC: connecte votre VPC aux services AWS pris en charge.
- Appairage de VPC: connecte votre VPC à d'autres VPC.
- Partage de VPC: permet à plusieurs comptes AWS de créer leurs ressources d'application dans des VPC Amazon partagés et gérés de manière centralisée.
- AWS Site-to-Site VPN: connecte votre VPC à des réseaux distants.
- AWS Direct Connect: connecte votre VPC à un réseau distant à l'aide d'une connexion réseau dédiée.
- AWS Transit Gateway: alternative de connexion en étoile à l'appairage de VPC.