Livre blanc AWS

Amazon Virtual Private Cloud Connectivity Options

Amazon Virtual Private Cloud Connectivity Options: Livre blanc AWS

Table of Contents

Amazon Virtual Private Cloud Connectivity Options

Date de publication : 5 avril 2023 (Révisions du document)

Résumé

Amazon Virtual Private Cloud (Amazon VPC) permet aux clients de fournir une section privée et isolée du cloud Amazon Web Services (AWS) où ils peuvent lancer des ressources AWS sur un réseau virtuel à l'aide de plages d'adresses IP définies par le client. Amazon VPC propose aux clients plusieurs options pour connecter leurs réseaux virtuels AWS à d'autres réseaux distants. Ce document décrit plusieurs options de connectivité réseau courantes disponibles pour nos clients. Il s'agit notamment d'options de connectivité permettant d'intégrer des réseaux clients distants à Amazon VPC et de connecter plusieurs Amazon VPC à un réseau virtuel contigu.

Ce livre blanc est destiné aux architectes et ingénieurs de réseaux d'entreprise ou aux administrateurs Amazon VPC qui souhaitent passer en revue les options de connectivité disponibles. Il fournit une vue d'ensemble des différentes options permettant de faciliter les discussions sur la connectivité réseau, ainsi que des indications vers de la documentation et des ressources supplémentaires avec des informations plus détaillées ou des exemples.

Introduction

Amazon VPC propose plusieurs options de connectivité réseau que vous pouvez utiliser, en fonction de la conception et des exigences actuelles de votre réseau. Ces options de connectivité incluent l'utilisation d'Internet ou d'une AWS Direct Connect connexion comme épine dorsale du réseau et la terminaison de la connexion à AWS ou à des points de terminaison réseau gérés par l'utilisateur. En outre, avec AWS, vous pouvez choisir la manière dont le routage réseau est fourni entre Amazon VPC et vos réseaux, en tirant parti des services AWS ou de l'équipement réseau et des itinéraires gérés par l'utilisateur. Ce livre blanc examine les options suivantes avec une vue d'ensemble et une comparaison détaillée de chacune d'entre elles :

- Options de connectivité entre le réseau et Amazon VPC
  - VPN AWS Site-to-site : décrit l'établissement d'une connexion VPN IPSec gérée entre votre équipement réseau sur un réseau distant et Amazon VPC.
  - AWS Transit Gateway + AWS Site-to-Site VPN — Décrit l'établissement d'une connexion VPN IPsec gérée entre votre équipement réseau sur un réseau distant et un hub réseau régional pour Amazon VPC, en utilisant. AWS Transit Gateway
  - AWS Direct Connect- Décrit l'établissement d'une connexion logique privée entre votre réseau distant et Amazon VPC, en utilisant. AWS Direct Connect
  - AWS Direct Connect + AWS Transit Gateway— Décrit l'établissement d'une connexion logique privée entre votre réseau distant et un hub réseau régional pour Amazon VPC, en utilisant AWS Direct Connect etAWS Transit Gateway.
  - AWS Direct Connect+ VPN AWS Site-to-Site : décrit l'établissement d'une connexion privée cryptée entre votre réseau distant et Amazon VPC, à l'aide d'un VPN AWS AWS Direct Connect Site-to-Site.
  - AWS Direct Connect + AWS Transit Gateway + VPN de site à site AWS— Décrit l'établissement d'une connexion privée cryptée entre votre réseau distant et un hub réseau régional pour Amazon VPC, en utilisant AWS Direct Connect etAWS Transit Gateway.
  - AWS VPN CloudHub— Décrit l'établissement d'un hub-and-spoke modèle pour connecter les succursales distantes.
  - Logiciel VPN— Décrit l'établissement d'une connexion VPN entre votre équipement sur un réseau distant et une appliance VPN logicielle gérée par l'utilisateur exécutée au sein d'un Amazon VPC.

  - AWS Transit Gateway + Solutions SD-WAN- Décrit l'intégration de solutions de réseau étendu défini par logiciel (SD-WAN) pour interconnecter plusieurs sites distants à un hub réseau régional pour Amazon VPC, en utilisant le AWS backbone ou Internet comme réseau de transit.
- Options de connectivité entre Amazon VPC et Amazon VPC
  - Appairage de VPC— Décrit la connexion d'Amazon VPC au sein des régions et entre celles-ci à l'aide de la fonction de peering Amazon VPC.
  - AWS Transit Gateway— Décrit la connexion des Amazon VPC au sein et entre les régions AWS Transit Gateway à l'aide d'un hub-and-spoke modèle.
  - AWS PrivateLink— Décrit la connexion des Amazon VPC aux points de terminaison d'interface VPC et aux services de point de terminaison VPC.
  - Logiciel VPN— Décrit la connexion d'Amazon VPC à l'aide de connexions VPN établies entre des appliances VPN logicielles gérées par l'utilisateur exécutées au sein de chaque Amazon VPC.
  - Logiciel VPN vers AWS Site-to-Site VPN— Décrit la connexion d'Amazon VPC à une connexion VPN établie entre une appliance VPN logicielle gérée par l'utilisateur dans un Amazon VPC et un VPN AWS Site-to-site connecté à l'autre Amazon VPC.
- Options d'accès à distance logicielle à Amazon VPC
  - AWS Client VPN— Décrit la connexion de l'accès à distance du logiciel à Amazon VPC, en utilisant le VPN Client AWS.
  - Logiciel client VPN— Décrit la connexion de l'accès à distance du logiciel à Amazon VPC, en tirant parti des appliances VPN logicielles gérées par l'utilisateur.
- VPC de transit- Décrit la mise en place d'un réseau de transit mondial sur AWS à l'aide d'un VPN logiciel associé à un VPN géré par AWS.
- Réseau étendu dans le cloud AWS- Décrit la mise en place d'un réseau étendu (WAN) géré pour créer, gérer et surveiller facilement les interconnexions mondiales entre les ressources des VPC Amazon, des centres de données et des succursales distantes.

Options de connectivité entre le réseau et Amazon VPC

Cette section fournit des modèles de conception pour connecter des réseaux distants à votre environnement Amazon VPC. Ces options sont utiles pour intégrer les ressources AWS à vos services sur site existants (par exemple, surveillance, authentification, sécurité, données ou autres systèmes) en étendant vos réseaux internes dans le cloud AWS. Cette extension réseau permet également à vos utilisateurs internes de se connecter facilement aux ressources hébergées sur AWS, comme toute autre ressource interne.

La connectivité VPC aux réseaux clients distants est optimale lorsque des plages IP ne se chevauchent pas pour chaque réseau connecté. Par exemple, si vous souhaitez connecter un ou plusieurs VPC à votre réseau d'entreprise, assurez-vous qu'ils sont configurés avec des plages CIDR (Classless Inter-Domain Routing) uniques. Nous recommandons d'allouer un bloc CIDR unique, contigu et ne se chevauchant pas, à utiliser par chaque VPC. Pour plus d'informations sur le routage et les contraintes d'Amazon VPC, consultez les questions fréquemment posées sur Amazon VPC.

Option	Cas d’utilisation	Avantages	Limites
AWS Site-to-Site VPN	Connexion VPN IPSec gérée par AWS via Internet à un VPC individuel	Réutiliser l'équipement et les processus VPN existants Réutiliser les connexions Internet existantes Service VPN haute disponibilité géré par AWS Prend en charge les routes statiques ou les politiques de peering et de routage dynamiques du Border Gateway Protocol (BGP)	La latence, la variabilité et la disponibilité du réseau dépendent des conditions Internet Vous êtes responsable de la mise en œuvre de la redondance et du basculement (si nécessaire) Le périphérique distant doit prendre en charge le BGP à saut unique (lors de l'utilisation du BGP pour le routage dynamique)

Option	Cas d'utilisation	Avantages	Limites
AWS Transit Gateway + VPN de site à site AWS	Connexion VPN IPSec gérée par AWS via Internet à un routeur régional pour plusieurs VPC	Identique à l'option précédente Hub de réseau régional à haute disponibilité et évolutivité géré par AWS pour un maximum de 5 000 pièces jointes	Identique à l'option précédente
AWS Direct Connect	Connexion réseau dédiée via des lignes privées	Performances réseau plus prévisibles Coûts de bande passante réduits Prend en charge les politiques de peering et de routage BGP	Cela peut nécessite r des relations supplémentaires avec des fournisseurs de télécommunications et d'hébergement ou la mise en service de nouveaux circuits réseau
AWS Direct Connect + AWS Transit Gateway	Connexion réseau dédiée via des lignes privées au routeur régional pour plusieurs VPC	Identique à l'option précédente Hub de réseau régional à haute disponibilité et évolutivité géré par AWS pour un maximum de 5 000 pièces jointes	Identique à l'option précédente

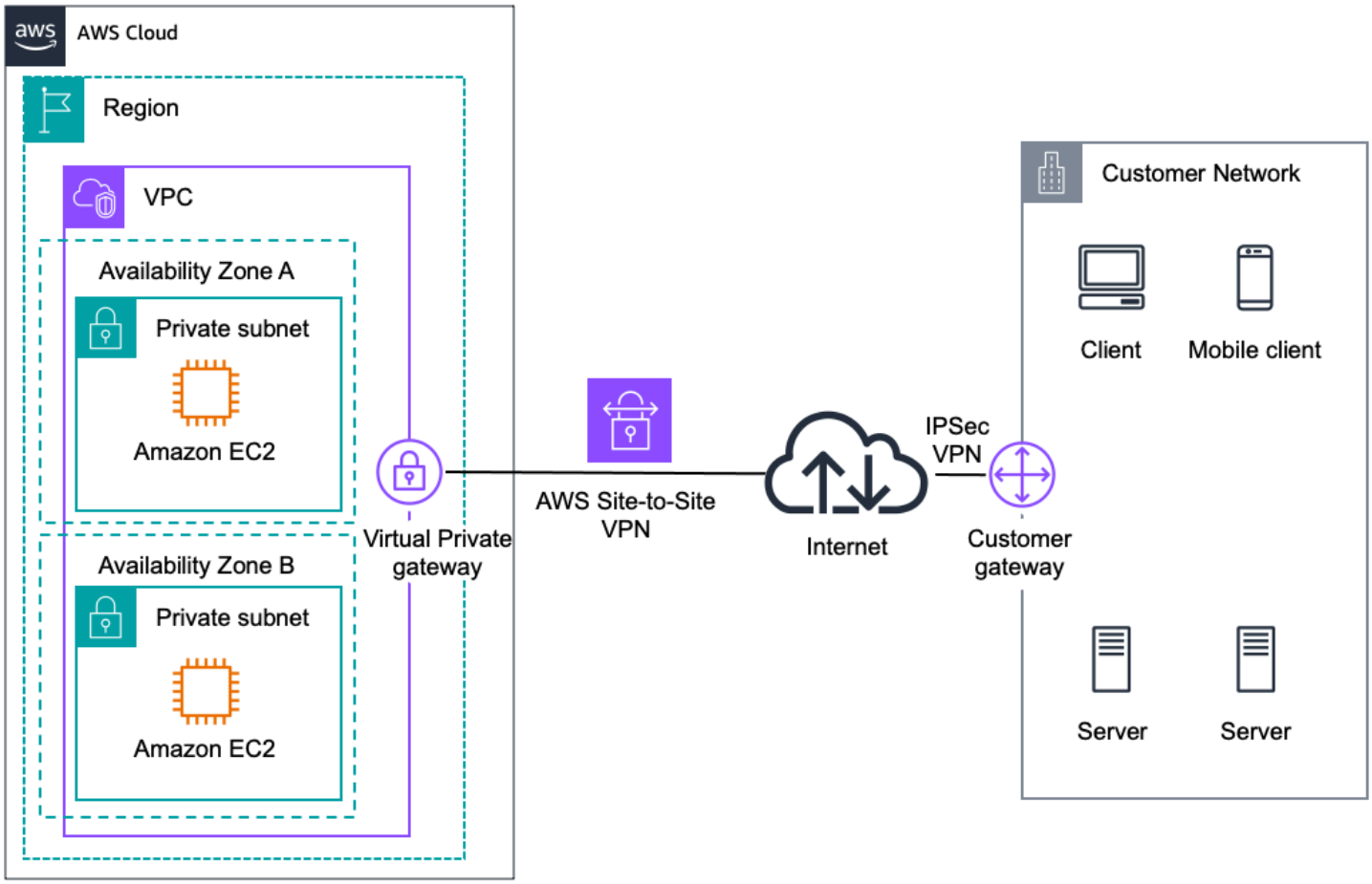
Option	Cas d'utilisation	Avantages	Limites
AWS Direct Connect + VPN de site à site AWS	Connexion VPN IPSec via des lignes privées	Performances réseau plus prévisibles Coûts de bande passante réduits Prend en charge les politiques de peering et de routage BGP sur AWS Direct Connect Réutiliser l'équipement et les processus VPN existants Service VPN haute disponibilité géré par AWS Prend en charge les routes statiques ou les politiques de peering et de routage dynamiques du Border Gateway Protocol (BGP) sur les connexions VPN	Peut nécessiter des relations supplémentaires avec des fournisseurs de télécommunications et d'hébergement ou la mise en service de nouveaux circuits réseau Vous êtes responsable de la mise en œuvre de la redondance et du basculement (si nécessaire) Le périphérique distant doit prendre en charge le BGP à saut unique (lors de l'utilisation du BGP pour le routage dynamique)

Option	Cas d'utilisation	Avantages	Limites
AWS Direct Connect + AWS Transit Gateway + VPN de site à site AWS	Connexion VPN IPSec via des lignes privées au routeur régional pour plusieurs VPC	Identique à l'option précédente Hub de réseau régional à haute disponibilité et évolutivité géré par AWS pour un maximum de 5 000 pièces jointes	Identique à l'option précédente
AWS VPN CloudHub	Connectez les succursales distantes dans un hub-and-spoke modèle de connectivité principale ou de sauvegarde	Réutiliser les connexions Internet et les AWS VPN connexions existantes Service VPN haute disponibilité géré par AWS Supporte le BGP pour échanger des itinéraires et des priorités de routage	La latence, la variabilité et la disponibilité du réseau dépendent d'Internet Les terminaux des succursales gérés par l'utilisateur sont responsables de la mise en œuvre de la redondance et du basculement (si nécessaire)
AWS Transit Gateway + Solutions SD-WAN	Connectez les succursales et les bureaux distants à un réseau étendu défini par logiciel en utilisant le AWS backbone ou Internet comme réseau de transit.	Prend en charge un plus large éventail de fournisseurs, de produits et de protocoles SD-WAN Certaines solutions de fournisseurs sont intégrées aux services natifs d'AWS.	Vous êtes responsable de la mise en œuvre de la haute disponibilité (HA) des appliances SD-WAN si elles sont placées dans un Amazon VPC.

Option	Cas d'utilisation	Avantages	Limites
Logiciel VPN	Connexion VPN via Internet basée sur une appliance logicielle	Prend en charge un plus large éventail de fournisseurs, de produits et de protocoles VPN Solution entièrement gérée par le client	Vous êtes responsable de la mise en œuvre de solutions HA (haute disponibilité) pour tous les points de terminaison VPN (si nécessaire)

AWS Site-to-Site VPN

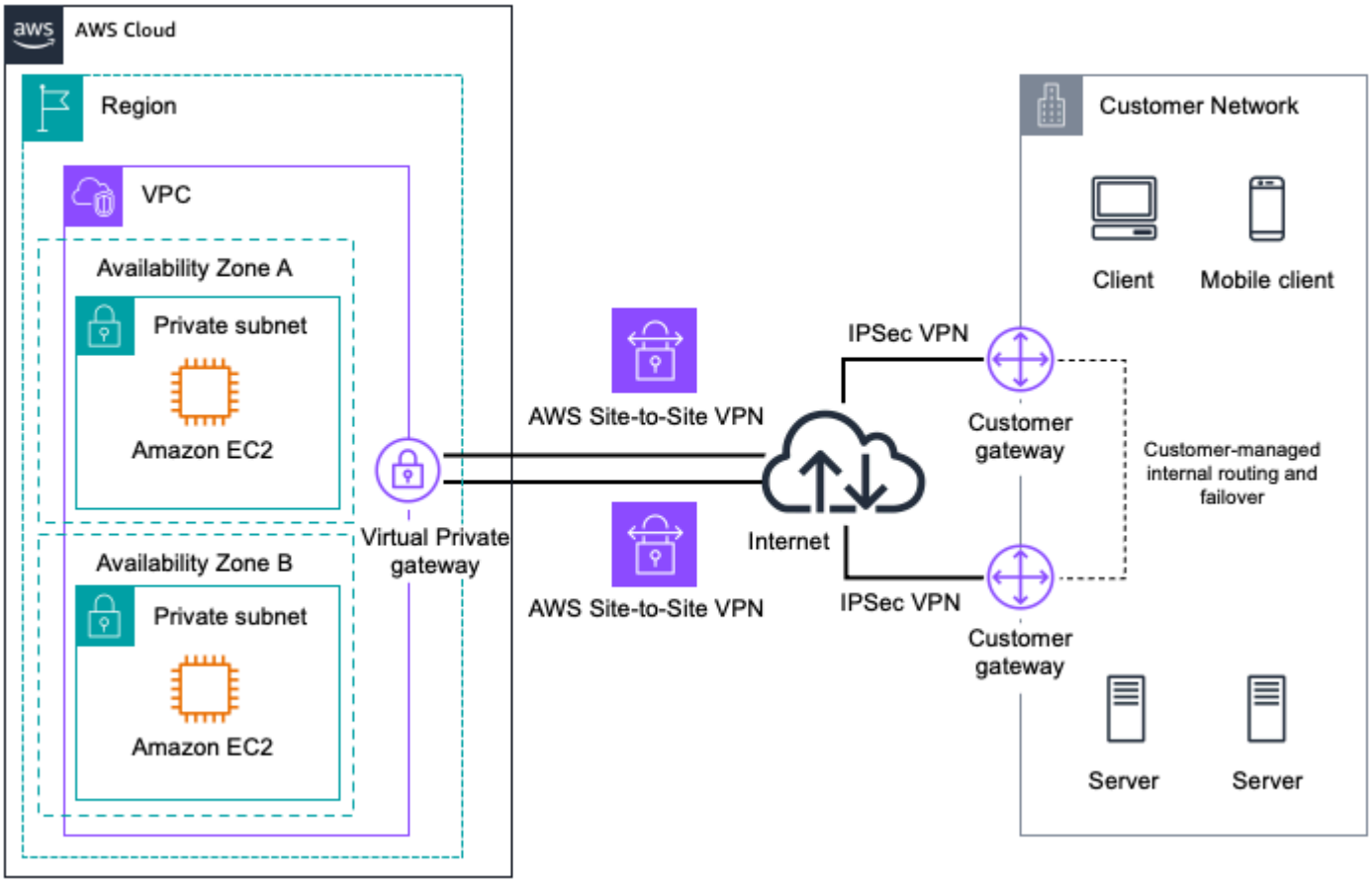
Amazon VPC offre la possibilité de créer une connexion VPN IPSec entre vos réseaux distants et Amazon VPC via Internet, comme le montre la figure suivante.



AWS Managed VPN

Envisagez d'adopter cette approche lorsque vous souhaitez tirer parti d'un point de terminaison VPN géré par AWS qui inclut une redondance et un basculement automatisés intégrés au côté AWS de la connexion VPN.

La passerelle privée virtuelle prend également en charge et encourage les connexions à plusieurs passerelles utilisateur afin que vous puissiez implémenter la redondance et le basculement sur incident de votre côté de la connexion VPN, comme le montre la figure suivante.



Redundant AWS Site-to-Site VPN Connections

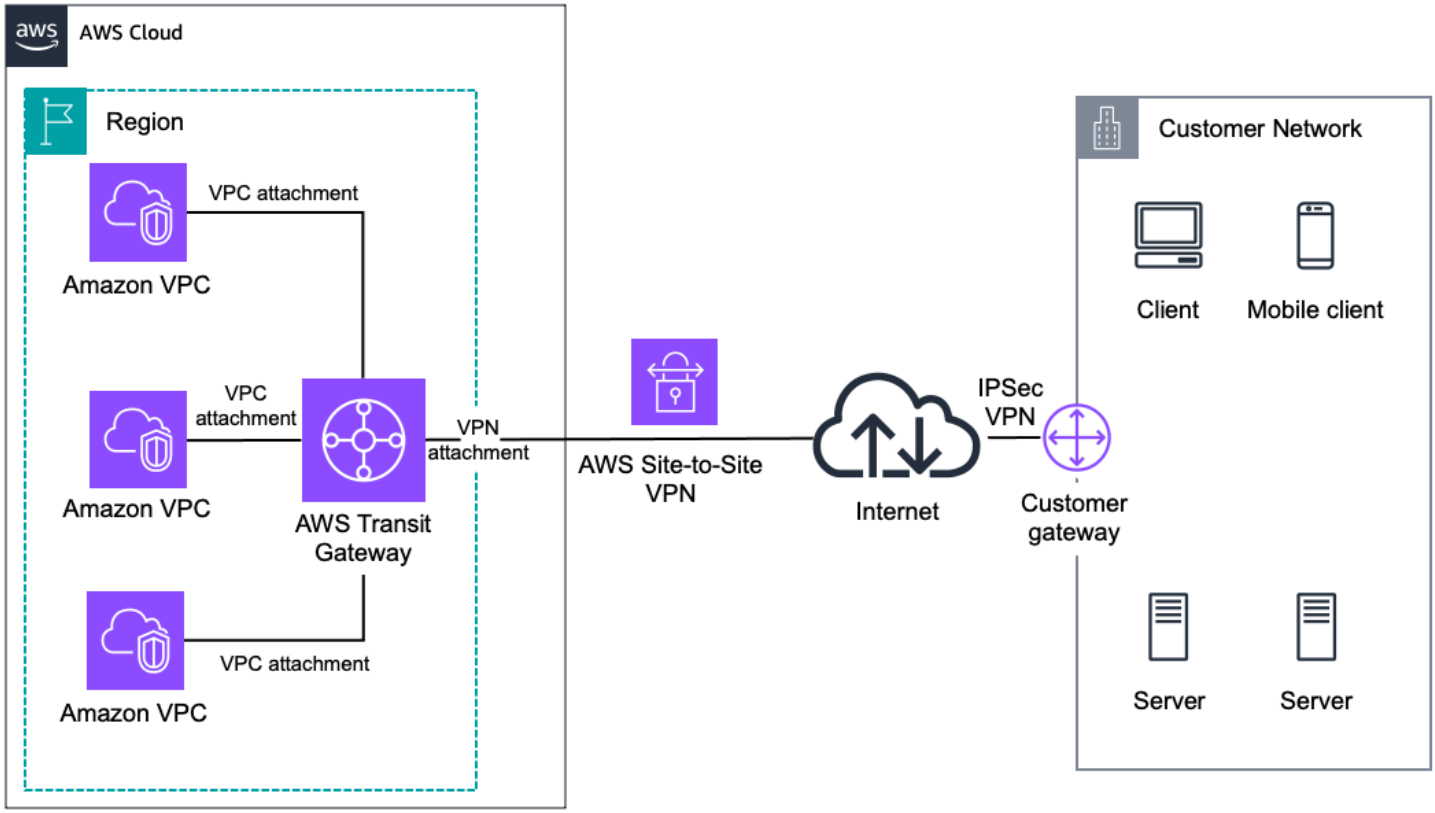
Des options de routage dynamiques et statiques sont proposées pour vous donner de la flexibilité dans votre configuration de routage. Le routage dynamique utilise le peering BGP pour échanger des informations de routage entre AWS et ces points de terminaison distants. Avec le routage dynamique, vous pouvez également spécifier les priorités, les politiques et les pondérations (métriques) de routage dans vos publicités BGP et influencer le chemin réseau entre vos réseaux et AWS. Il est important de noter que lorsque vous utilisez le protocole BGP, les sessions IPsec et BGP doivent être terminées sur le même périphérique de passerelle utilisateur. Il doit donc être capable de mettre fin aux sessions IPsec et BGP.

Ressources supplémentaires

- Guide de l'utilisateur AWS Site-to-Site VPN
- Exigences relatives aux dispositifs de passerelle client
- Appareils de passerelle client testés avec Amazon VPC

AWS Transit Gateway + VPN de site à site AWS

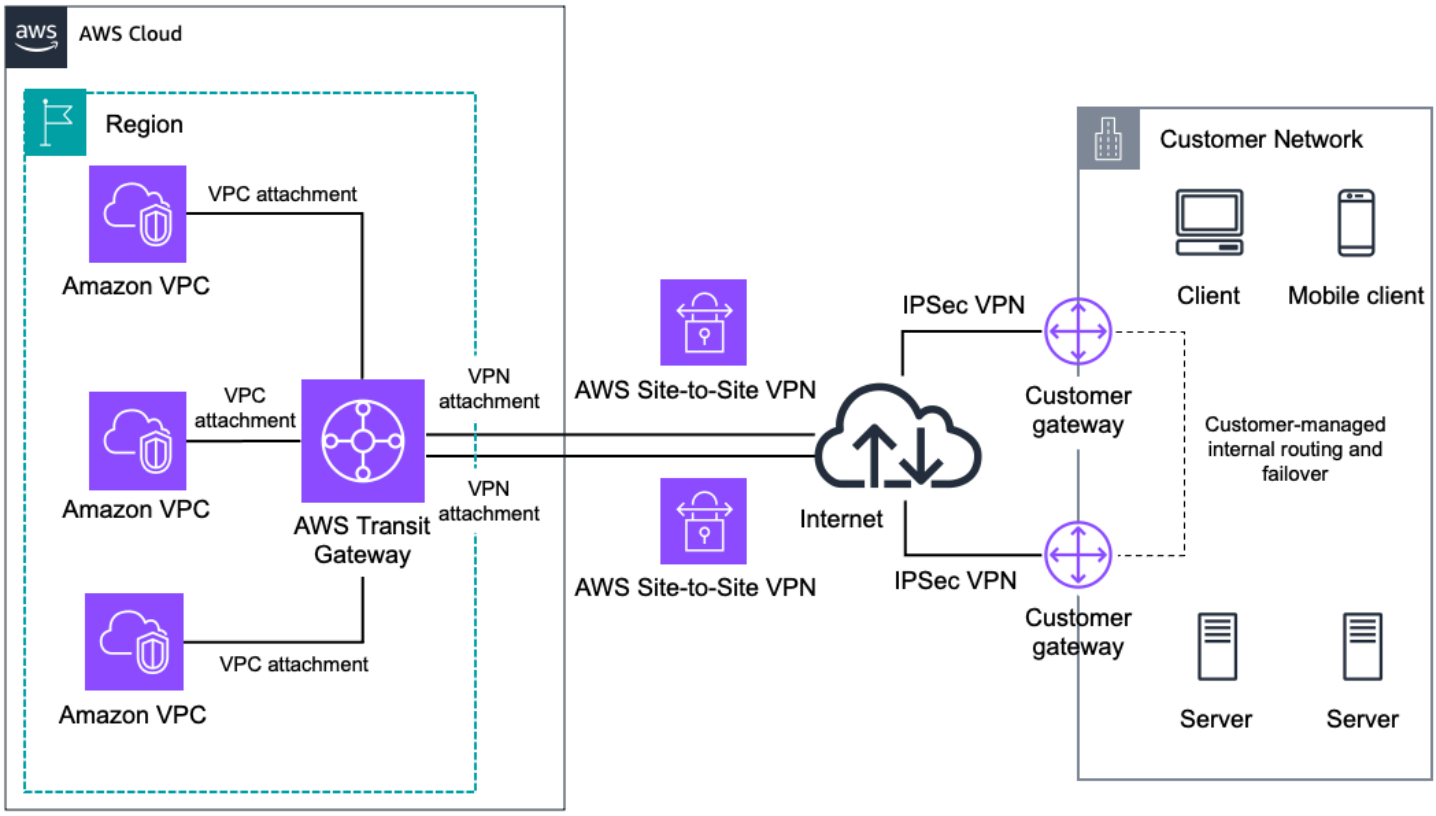
AWS Transit Gateway est un hub de transit régional à haute disponibilité et évolutivité géré par AWS, utilisé pour interconnecter les VPC et les réseaux des clients. Le VPN AWS Transit Gateway +, qui utilise le rattachement au VPN Transit Gateway, offre la possibilité de créer une connexion VPN IPsec entre votre réseau distant et Transit Gateway via Internet, comme illustré dans la figure suivante.



AWS Transit Gateway and AWS Site-to-Site VPN

Envisagez d'utiliser cette approche lorsque vous souhaitez tirer parti d'un point de terminaison VPN géré par AWS pour vous connecter à plusieurs VPC dans la même région sans les coûts supplémentaires et la gestion de plusieurs connexions VPN IPsec à plusieurs VPC Amazon.

AWS Transit Gateway prend également en charge et encourage les connexions à plusieurs passerelles utilisateur afin que vous puissiez implémenter la redondance et le basculement sur incident de votre côté de la connexion VPN, comme illustré dans la figure suivante.



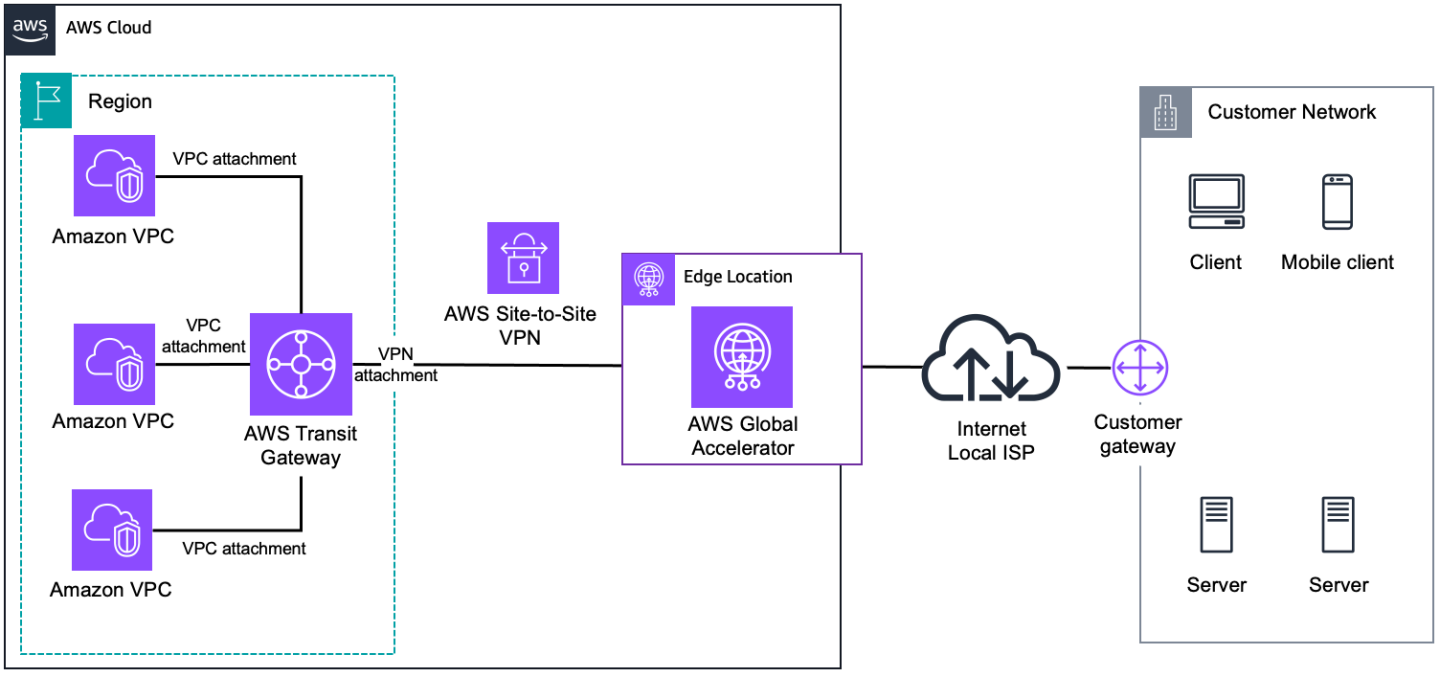
AWS Transit Gateway and Redundant VPN

Des options de routage dynamiques et statiques sont proposées pour vous donner de la flexibilité dans votre configuration de routage sur la pièce jointe IPSec du VPN Transit Gateway. Le routage dynamique utilise le peering BGP pour échanger des informations de routage entre AWS et ces points de terminaison distants. Avec le routage dynamique, vous pouvez également spécifier les priorités, les politiques et les pondérations (métriques) de routage dans vos publicités BGP et influencer le chemin réseau entre vos réseaux et AWS. Il est important de noter que lorsque vous utilisez le protocole BGP, les sessions IPsec et BGP doivent être terminées sur le même périphérique de passerelle utilisateur. Il doit donc être capable de mettre fin aux sessions IPsec et BGP.

Par connexion VPN, vous pouvez atteindre 1,25 Gbit/s de débit et 140 000 paquets par seconde. Lorsque vous mettez fin aux connexions VPN dans le Transit Gateway, vous pouvez utiliser le

routage ECMP (Equal Cost Multi-Path) pour obtenir une bande passante VPN plus élevée en agrégeant plusieurs tunnels VPN. Pour utiliser l'ECMP, vous devez configurer le routage dynamique dans les connexions VPN. L'ECMP n'est pas pris en charge avec le routage statique.

En outre, vous pouvez activer l'accélération de vos connexions VPN de site à site AWS. Une connexion VPN accélérée utilise AWS Global Accelerator pour acheminer le trafic de votre réseau vers l'emplacement périphérique AWS le plus proche de votre dispositif de passerelle client. Vous pouvez utiliser cette option pour éviter les perturbations du réseau susceptibles de se produire lorsque le trafic est acheminé sur l'Internet public. L'accélération n'est prise en charge que pour les connexions VPN associées à un Transit Gateway, comme le montre la figure suivante :



Accelerated AWS Site-to-Site VPN

Enfin, en ce qui concerne l'adressage IP, les connexions VPN de site à site sur un réseau prennent en AWS Transit Gateway charge à la fois le trafic IPv4 et IPv6. Les règles suivantes s’appliquent :

- L'IPv6 n'est pris en charge que pour les adresses IP internes du tunnel VPN. Les adresses IP externes des AWS points de terminaison sont des adresses IPv4 publiques. L'adresse IP de la passerelle client doit être une adresse IPv4 publique.
- Une connexion Site-to-Site VPN ne peut pas prendre en charge le trafic IPv4 et IPv6. Si votre connectivité hybride nécessite une communication à double pile, vous devez créer différents tunnels VPN pour le trafic IPv4 et IPv6.

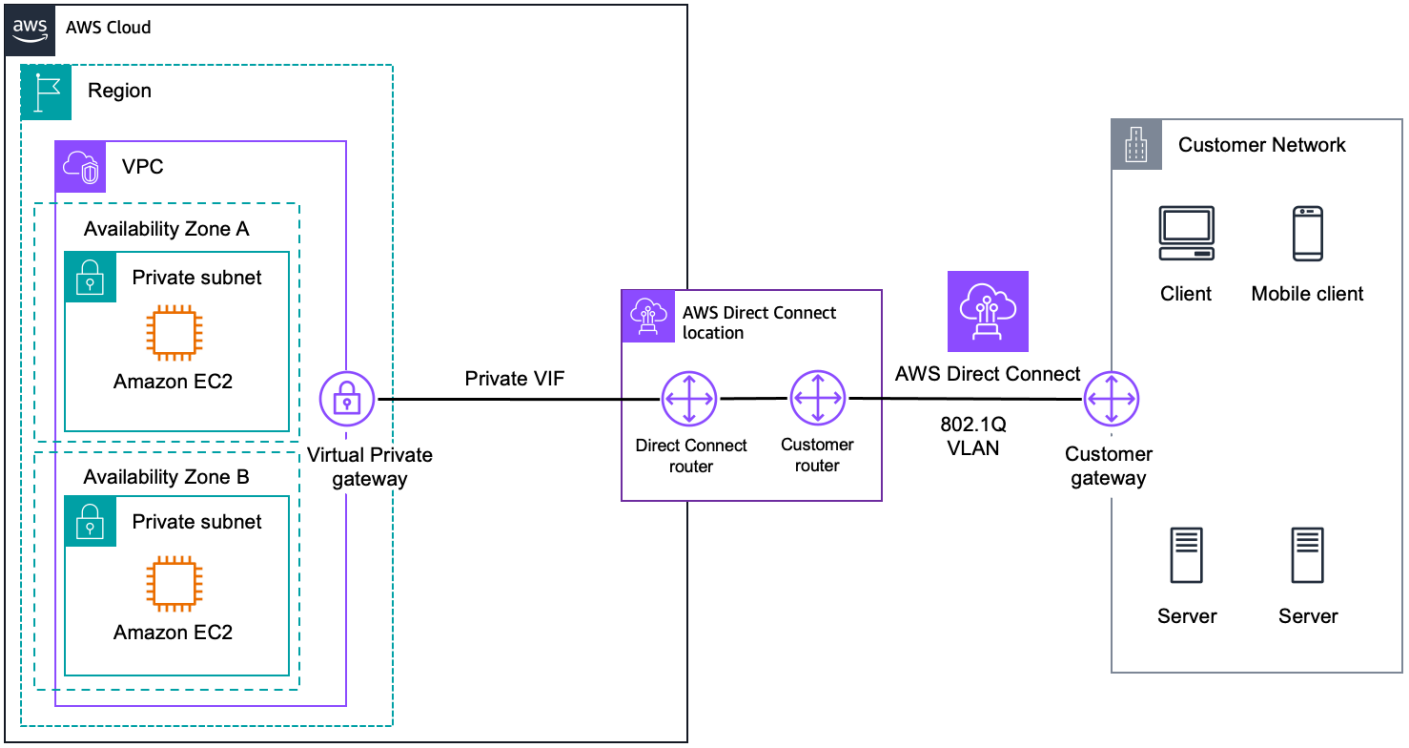
Ressources supplémentaires

- Pièces jointes VPN Transit Gateway
- Passerelle client
- Utilisation du VPN de site à site
- Connexions VPN de site à site accélérées

AWS Direct Connect

AWS Direct Connectpermet d'établir facilement une connexion dédiée entre un réseau sur site et un ou plusieurs VPC. AWS Direct Connect peuvent réduire les coûts du réseau, augmenter le débit de bande passante et fournir une expérience réseau plus cohérente que les connexions Internet. Il utilise des VLAN 802.1Q conformes aux normes du secteur pour se connecter à Amazon VPC à l'aide d'adresses IP privées. Les VLAN sont configurés à l'aide d'interfaces virtuelles (VIF), et vous pouvez configurer trois types de VIF différents :

- Interface virtuelle publique : établissez une connectivité entre les terminaux AWS publics et votre environnement de centre de données, de bureau ou de colocation.
- Interface virtuelle de transit : établissez une connectivité privée entre AWS Transit Gateway votre centre de données, votre bureau ou votre environnement de colocation. Cette option de connectivité est abordée dans la section???.
- Interface virtuelle privée : établissez une connectivité privée entre les ressources Amazon VPC et votre environnement de centre de données, de bureau ou de colocation. L'utilisation de VIFs privés est illustrée dans la figure suivante.



AWS Direct Connect

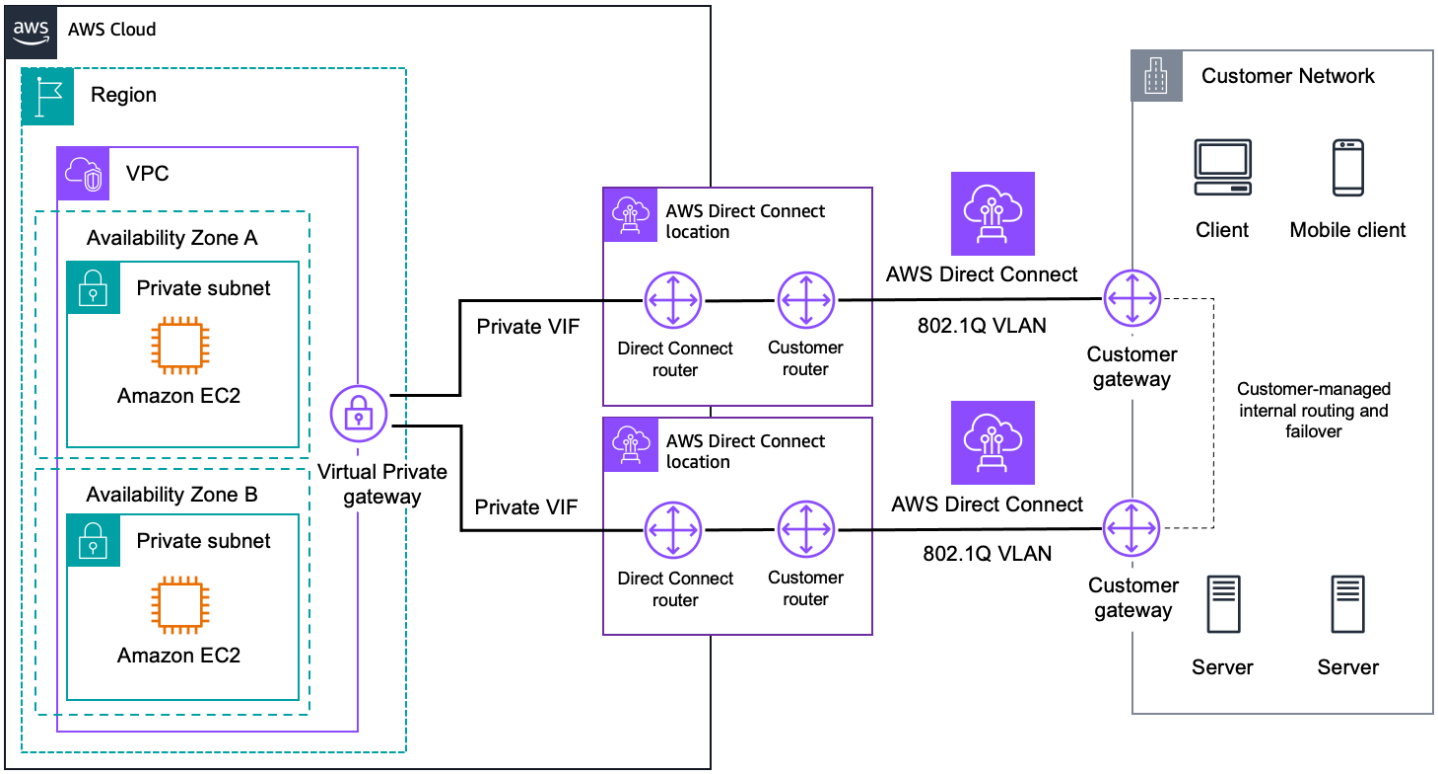
Vous pouvez établir une connectivité au AWS backbone en AWS Direct Connect établissant une connexion croisée avec AWS les appareils d'un emplacement Direct Connect. Vous pouvez accéder à n'importe quelle AWS région depuis n'importe lequel de nos sites Direct Connect (à l'exception de la Chine). Si vous ne disposez pas d'équipement sur un site, vous pouvez choisir parmi un écosystème de fournisseurs de services WAN pour intégrer votre AWS Direct Connect point de terminaison sur un AWS Direct Connect site à vos réseaux distants.

Avec AWS Direct Connect, vous disposez de deux types de connexion :

- Connexions dédiées, où une connexion Ethernet physique est associée à un seul client. Vous pouvez commander des vitesses de port de 1, 10 ou 100 Gbit/s. Vous devrez peut-être travailler avec un AWS Direct Connect partenaire du programme de partenariat pour vous aider à établir des circuits réseau entre une AWS Direct Connect connexion et votre centre de données, votre bureau ou votre environnement de colocation.
- Connexions hébergées, où une connexion Ethernet physique est fournie par un AWS Direct Connect partenaire et partagée avec vous. Vous pouvez commander des vitesses de port comprises entre 50 Mbits/s et 10 Gbit/s. Votre travail avec le partenaire concerne à la fois la AWS Direct Connect connexion qu'il a établie et les circuits réseau entre une AWS Direct Connect connexion et votre centre de données, votre bureau ou votre environnement de colocation.

Pour les connexions dédiées, vous pouvez également utiliser un groupe d'agrégation de liens (LAG) pour agréger plusieurs connexions sur un seul AWS Direct Connect point de terminaison. Vous les traitez comme une seule connexion gérée. Vous pouvez agréger jusqu'à quatre connexions de 1 ou 10 Gbit/s et jusqu'à deux connexions de 100 Gbit/s.

Lorsque vous discutez de la haute disponibilité dans AWS Direct Connect, nous vous recommandons d'utiliser des AWS Direct Connect connexions supplémentaires. Le AWS Direct Connect Resiliency Toolkit fournit des conseils pour établir des connexions réseau hautement résilientes entre AWS votre centre de données, votre bureau ou votre environnement de colocation. La figure suivante montre un exemple d'option de connectivité à haute résilience, avec deux AWS Direct Connect connexions terminées à deux endroits différents AWS Direct Connect .

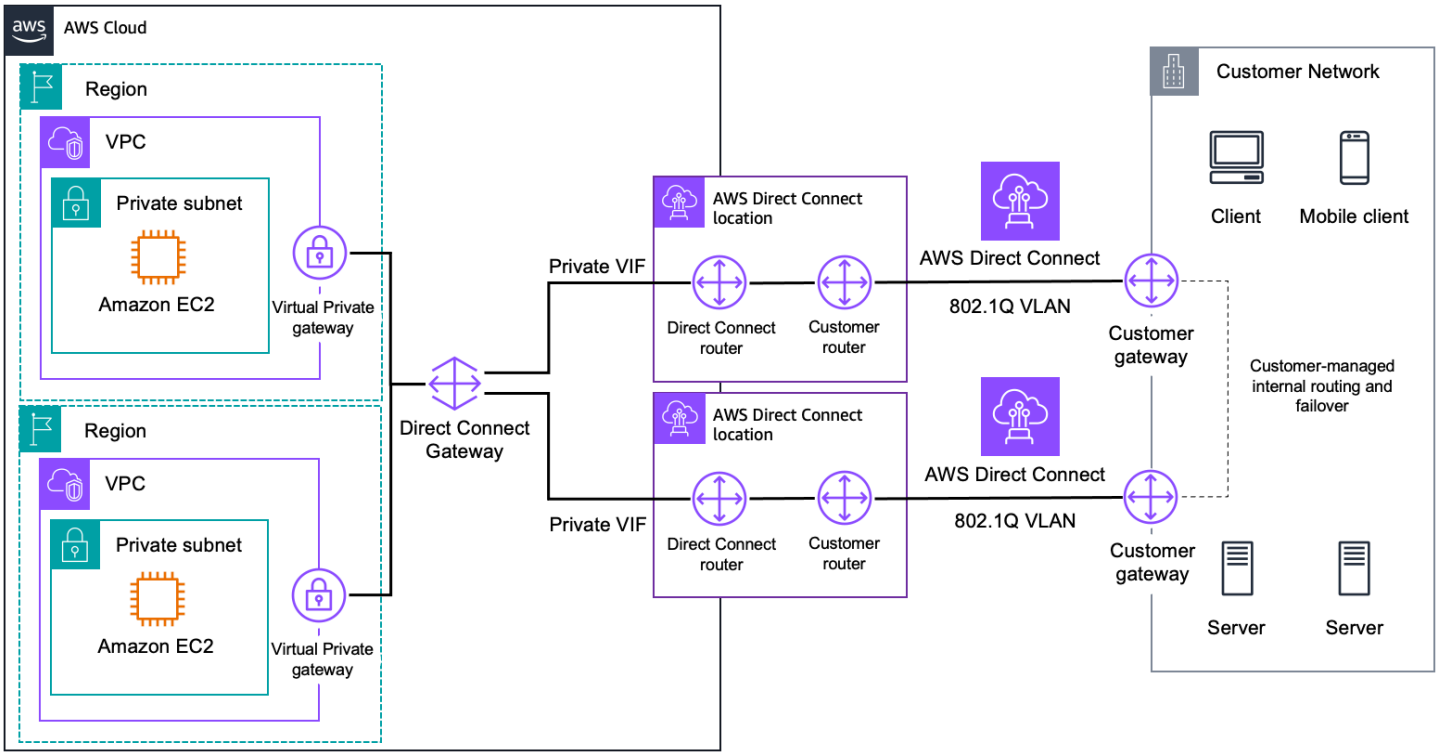


Redondant AWS Direct Connect

AWS Direct Connect n'est pas crypté par défaut. Pour les connexions dédiées de 10 ou 100 Gbit/s, vous pouvez utiliser la sécurité MAC (MacSec) comme option de chiffrement. Pour les connexions de 1 Gbit/s ou moins, vous pouvez créer des tunnels VPN au-dessus de la connexion. Cette option est abordée dans les AWS Direct Connect + AWS Transit Gateway + VPN de site à site AWS sections AWS Direct Connect + VPN de site à site AWS et sections.

L'une des ressources importantes AWS Direct Connect est la passerelle Direct Connect, qui est une ressource disponible dans le monde entier pour permettre des connexions à plusieurs Amazon

VPC ou Transit Gateway dans différentes régions ou AWS comptes. Cette ressource vous permet également de vous connecter à n'importe quel VPC ou Transit Gateway participant à partir d'un VIF privé ou d'un VIF de transit, réduisant ainsi AWS Direct Connect la gestion, comme le montre la figure suivante.



AWS Direct Connect Gateway

En ce qui concerne l'adressage IP, les interfaces AWS Direct Connect virtuelles prennent en charge les sessions BGP IPv4 et IPv6 pour un fonctionnement à double pile.

- La configuration IPv4 des VIF privées et de transit utilise soit des adresses IPv4 générées par AWS, soit des adresses que vous avez configurées. Pour l'appairage BGP IPv4 de VIF publics, vous devez spécifier un CIDR IPv4 public /31 unique dont vous êtes propriétaire (ou envoyer une demande pour qu'un bloc d'adresse CIDR soit attribué).
- Pour tous les types d'appairage BGP IPv6 de VIF, AWS attribue un CIDR /125, qui n'est pas configurable.

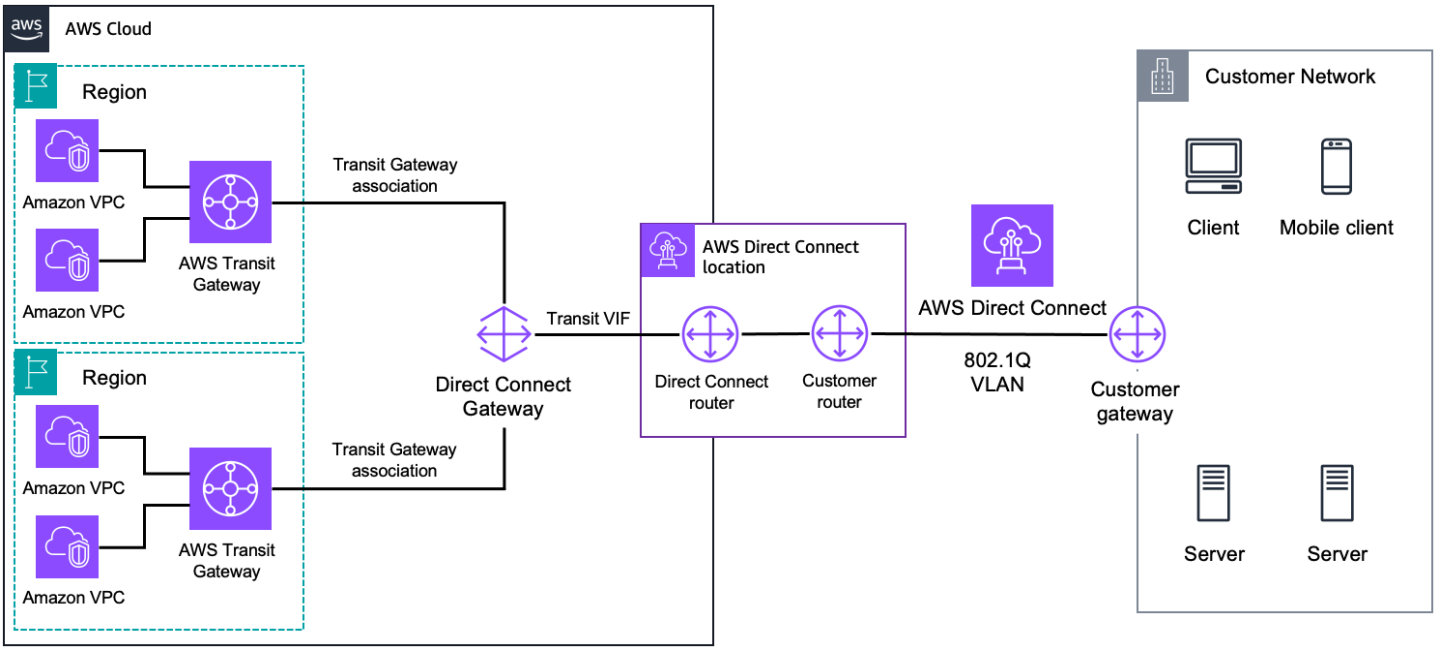
Ressources supplémentaires

- AWS Direct Connect Guide de l'utilisateur
- AWS Direct Connect interfaces virtuelles

- AWS Direct Connect passerelles
- AWS Direct Connect Boîte à outils de résilience
- AWS Direct Connect Sécurité MAC
- AWS Direct Connect emplacements
- AWS Direct Connect Partenaires de livraison

AWS Direct Connect + AWS Transit Gateway

AWS Direct Connect+ AWS Transit Gateway, en utilisant l'attachement du VIF de transit à la passerelle Direct Connect, permet à votre réseau de connecter plusieurs routeurs centralisés régionaux via une connexion dédiée privée. Le schéma suivant montre la connexion à deux routeurs.



AWS Direct Connect and AWS Transit Gateway

Chacun AWS Transit Gateway est un hub de transit réseau permettant d'interconnecter les VPC d'une même région, consolidant ainsi la configuration de routage Amazon VPC en un seul endroit. Cette solution simplifie la gestion des connexions entre un Amazon VPC et vos réseaux via une connexion privée, ce qui permet de réduire les coûts du réseau, d'augmenter le débit de bande passante et de fournir une expérience réseau plus cohérente que les connexions Internet.

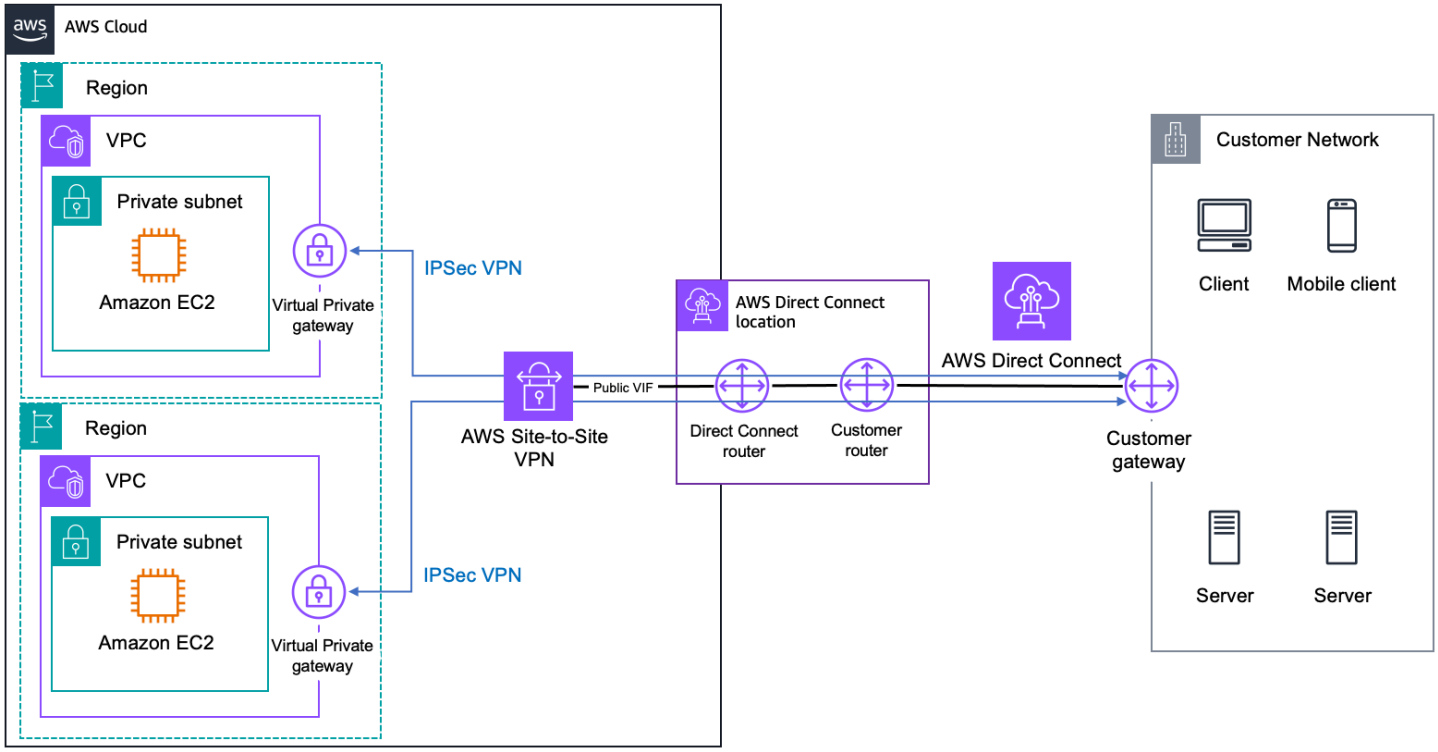
Ressources supplémentaires

- Guide de l'utilisateur AWS Direct Connect

- Groupes d'agrégation de liens dans AWS Direct Connect
- Article de blog : Intégration de connexions hébergées inférieures à 1 Gbit/s avec AWS Transit Gateway

AWS Direct Connect + VPN de site à site AWS

Avec AWS Direct Connect+ AWS Site-to-Site VPN, vous pouvez combiner des AWS Direct Connect connexions avec une solution VPN gérée par AWS. AWS Direct Connect les VIF publics établissent une connexion réseau dédiée entre votre réseau et les ressources AWS publiques, telles qu'un point de terminaison VPN AWS Site-to-Site. Une fois que vous avez établi la connexion au service, vous pouvez créer des connexions IPsec aux passerelles privées virtuelles Amazon VPC correspondantes. La figure suivante illustre cette option.



AWS Direct Connect and AWS Site-to-Site VPN

Cette solution combine les avantages d'une connexion IPsec end-to-end sécurisée avec une faible latence et une bande passante accrue AWS Direct Connect afin de fournir une expérience réseau plus cohérente que les connexions VPN basées sur Internet. Une session de connexion BGP est établie entre AWS Direct Connect et votre routeur sur le VIF public. Une autre session BGP ou une route statique sera établie entre la passerelle privée virtuelle et votre routeur sur les tunnels VPN IPSec.

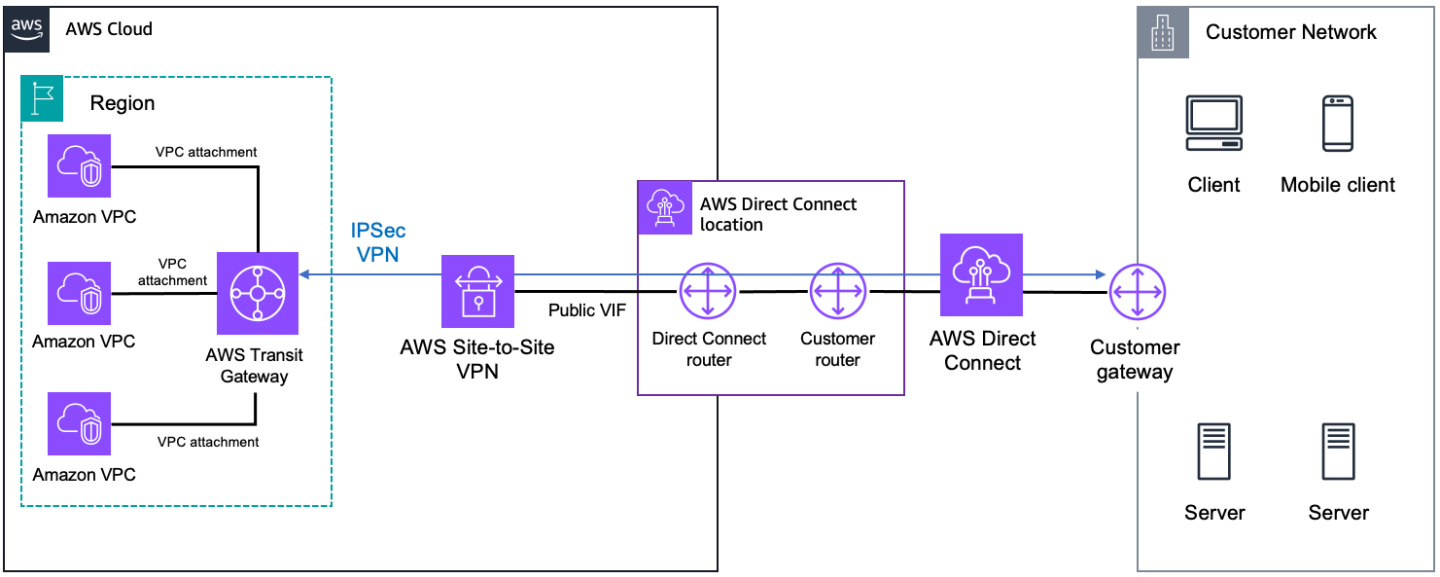
Ressources supplémentaires

- AWS Direct Connect
- AWS Direct Connect interfaces virtuelles
- Guide de l'utilisateur AWS Site-to-Site VPN

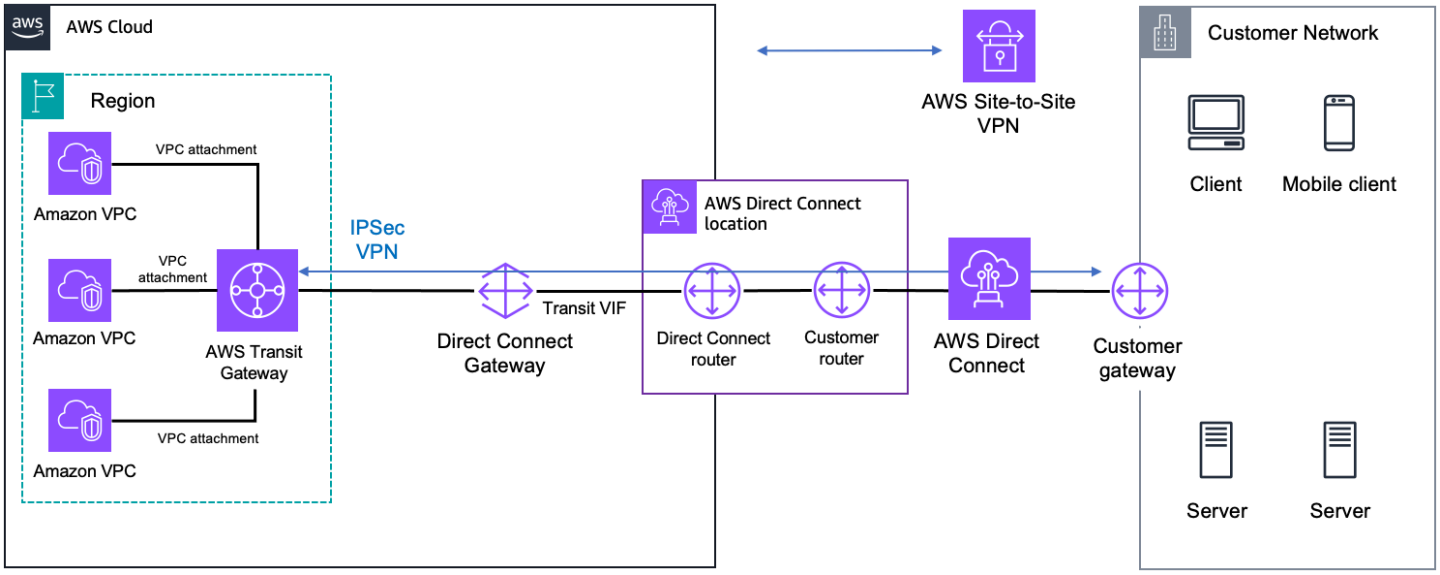
AWS Direct Connect + AWS Transit Gateway + VPN de site à site AWS

Avec AWS Direct Connect+ AWS Transit Gateway+ le VPN Site-to-Site AWS, vous pouvez activer des connexions end-to-end cryptées IPsec entre vos réseaux et un routeur centralisé régional pour les Amazon VPC via une connexion dédiée privée.

Vous pouvez utiliser des VIF AWS Direct Connect publics pour établir d'abord une connexion réseau dédiée entre votre réseau et les ressources AWS publiques, telles que les points de terminaison VPN AWS Site-to-Site. Une fois cette connexion établie, vous pouvez créer une connexion IPSec vers AWS Transit Gateway. La figure suivante illustre cette option.



AWS Direct Connect, AWS Transit Gateway, and AWS Site-to-Site VPN (public VIF)



AWS Direct Connect, AWS Transit Gateway, and AWS Site-to-Site VPN (transit VIF)

Envisagez d'adopter cette approche lorsque vous souhaitez simplifier la gestion et minimiser le coût des connexions VPN IPSec vers plusieurs Amazon VPC dans la même région, avec les avantages d'une faible latence et d'une expérience réseau cohérente d'une connexion dédiée privée par rapport à un VPN basé sur Internet. Une session BGP est établie entre AWS Direct Connect et votre routeur en utilisant le VIF public ou de transit. Une autre session BGP ou une route statique sera établie entre AWS Transit Gateway et votre routeur sur le tunnel VPN IPSec.

Ressources supplémentaires

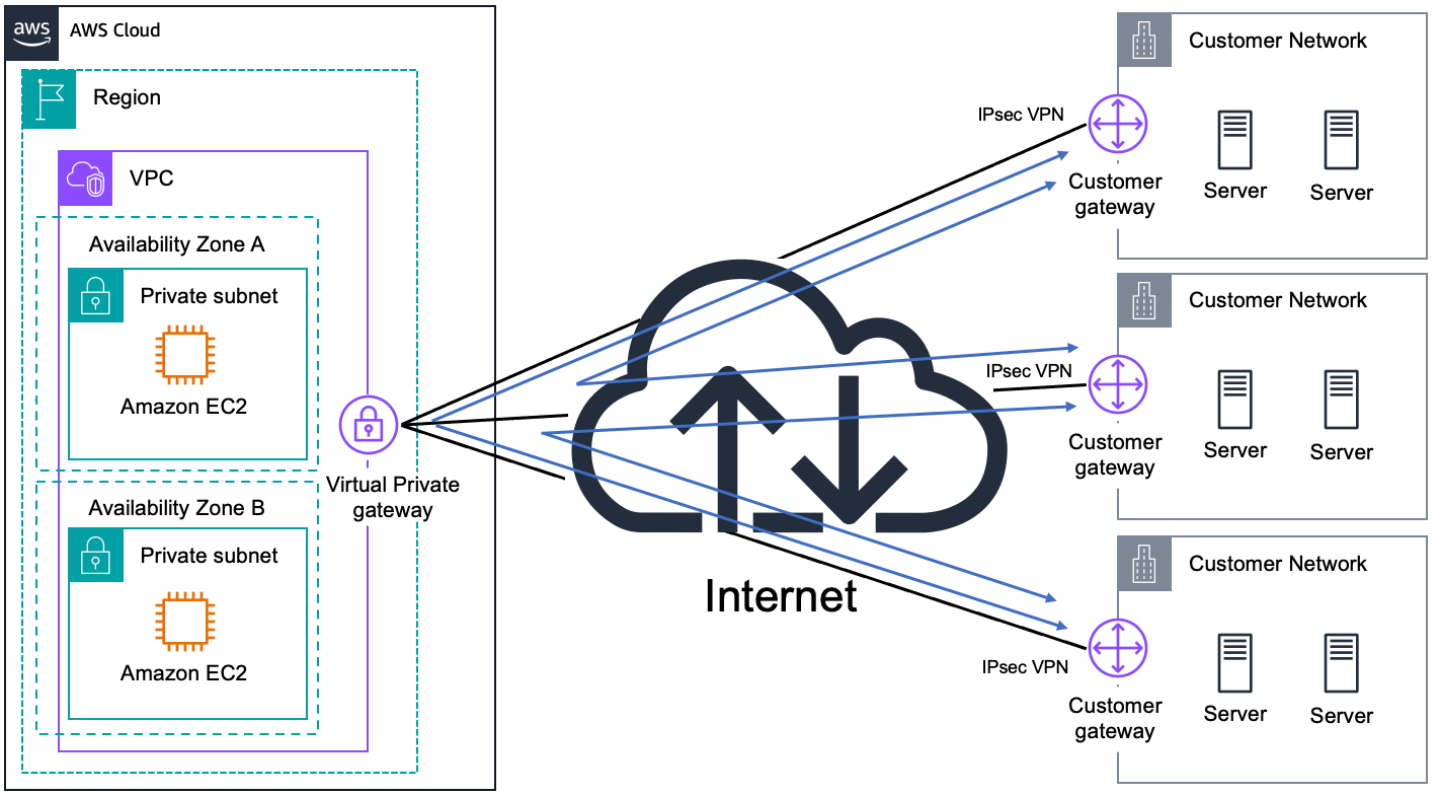
- Interfaces virtuelles AWS Direct Connect
- Pièces jointes VPN Transit Gateway
- Exigences relatives aux dispositifs de passerelle client
- Appareils de passerelle client testés avec Amazon VPC
- VPN de site à site AWS : VPN IP privé avec AWS Direct Connect

AWS VPN CloudHub

En vous appuyant sur les options VPN gérées par AWS décrites précédemment, vous pouvez communiquer en toute sécurité d'un site à l'autre à l'aide du AWS VPN CloudHub. AWS VPN CloudHub Il fonctionne sur un hub-and-spoke modèle simple que vous pouvez utiliser avec ou sans VPC. Utilisez cette approche si vous disposez de plusieurs succursales et de connexions

Internet existantes et que vous souhaitez mettre en œuvre un hub-and-spoke modèle pratique et potentiellement peu coûteux pour la connectivité principale ou de sauvegarde entre ces bureaux distants.

La figure suivante montre l' AWS VPN CloudHub architecture, avec des lignes indiquant le trafic réseau entre les sites distants acheminé via leurs AWS VPN connexions.



AWS VPN CloudHub

AWS VPN CloudHub utilise une passerelle privée virtuelle Amazon VPC avec plusieurs passerelles client, chacune utilisant des numéros de système autonome (ASN) BGP uniques. Les plages d'adresses IP des sites distants ne doivent pas se chevaucher. Vos passerelles annoncent les itinéraires appropriés (préfixes BGP) via leurs connexions VPN. Ces publicités de routage sont reçues et rediffusées auprès de chaque homologue BGP afin que chaque site puisse envoyer des données aux autres sites et en recevoir.

Ressources supplémentaires

- Fournir une communication sécurisée entre les sites à l'aide d'un VPN CloudHub
- Guide de l'utilisateur AWS Site-to-Site VPN
- Exigences relatives aux dispositifs de passerelle client

- Appareils de passerelle client testés avec Amazon VPC

AWS Transit Gateway + Solutions SD-WAN

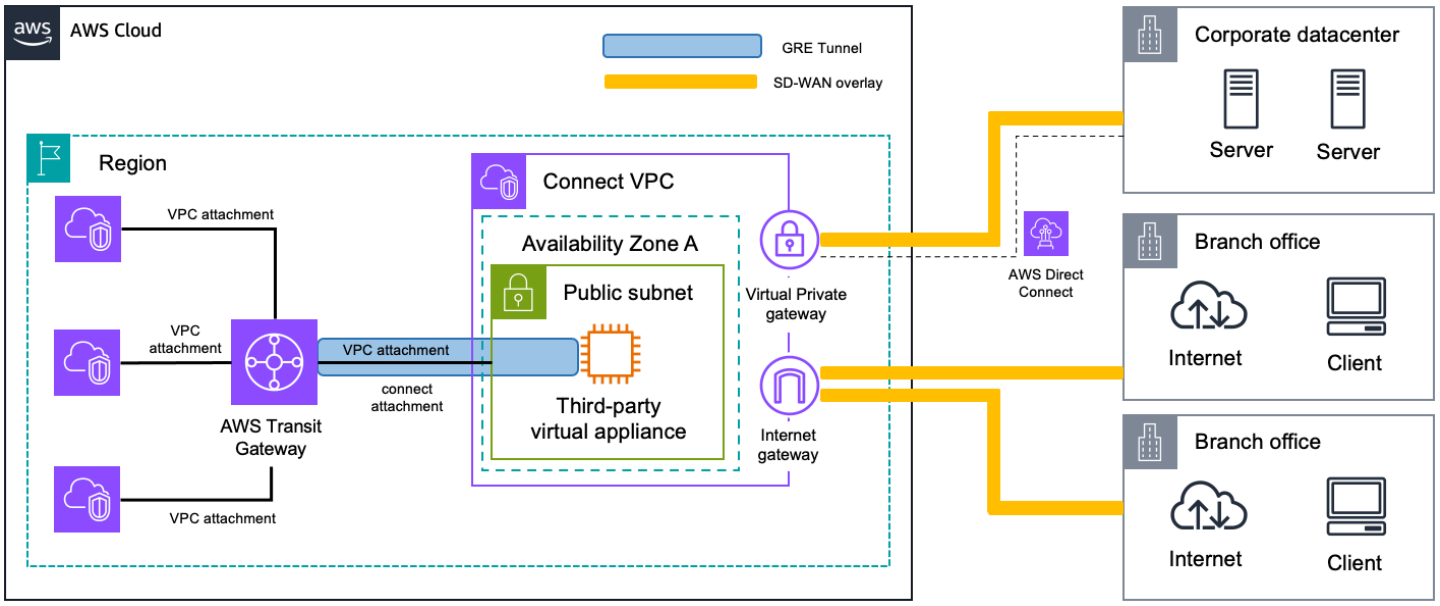
Les réseaux étendus définis par logiciel (SD-WAN) sont utilisés pour connecter vos centres de données, bureaux ou environnements de colocation via différents réseaux de transport (tels que l'Internet public, les réseaux MPLS ou le backbone AWS AWS Direct Connect), en gérant le trafic automatiquement et dynamiquement sur le chemin le plus approprié et le plus efficace en fonction des conditions du réseau, du type d'application ou des exigences de qualité de service (QoS).

Utilisez cette approche si vous avez une topologie réseau complexe, avec plusieurs centres de données, bureaux ou environnements de colocation qui doivent communiquer entre eux et avec AWS. Les solutions SD-WAN peuvent vous aider à gérer efficacement ce type de réseau.

Lorsque vous parlez de la connexion d'un réseau SD-WAN à AWS, AWS Transit Gateway fournit un hub de transit régional géré, hautement disponible et évolutif pour interconnecter les VPC et votre réseau SD-WAN. Les pièces jointes Transit Gateway connect constituent un moyen natif de connecter votre infrastructure et vos appareils SD-WAN à AWS. Cela permet d'étendre facilement votre SD-WAN à AWS sans avoir à configurer de VPN IPSec.

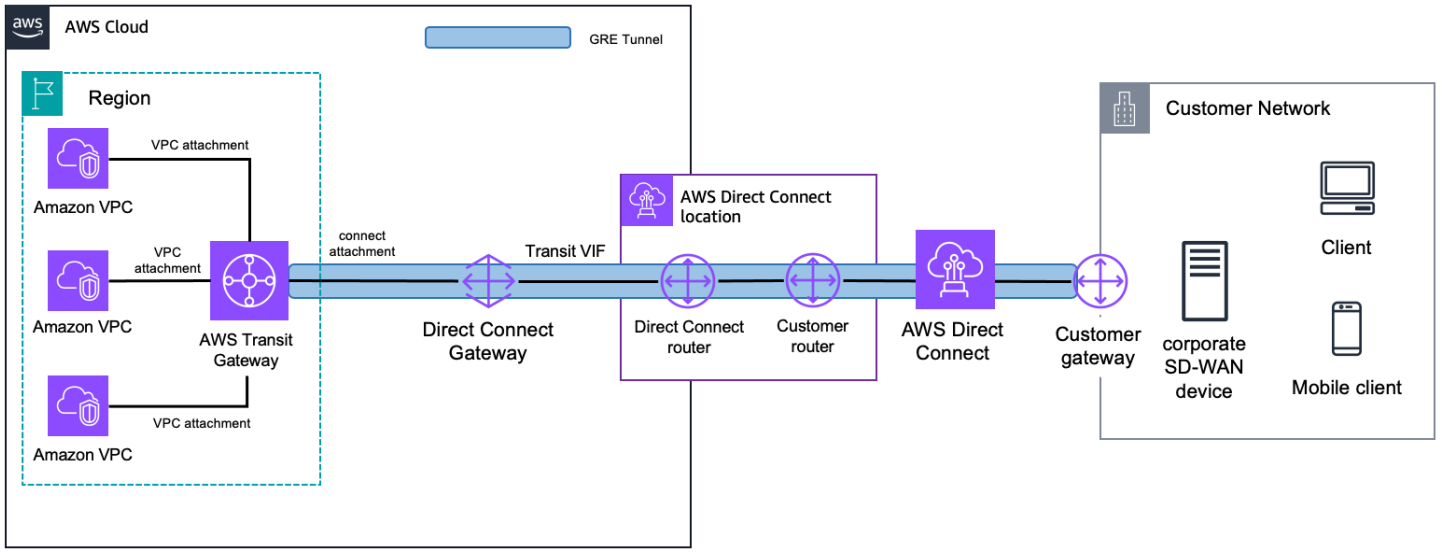
Les pièces jointes Transit Gateway Connect prennent en charge l'encapsulation de routage générique (GRE) pour des performances de bande passante supérieures à celles d'une connexion VPN. Il prend en charge le protocole BGP (Border Gateway Protocol) pour le routage dynamique et élimine le besoin de configurer des itinéraires statiques. Cela simplifie la conception du réseau et réduit les coûts d'exploitation associés. En outre, son intégration à Transit Gateway Network Manager fournit une visibilité avancée grâce à la topologie du réseau mondial, aux mesures de performance du niveau des attachements et aux données de télémétrie.

Lorsque vous intégrez votre réseau SD-WAN à Transit Gateway à l'aide de pièces jointes, vous avez deux modèles communs. La première consiste à placer les appliances virtuelles du réseau SD-WAN dans un VPC au sein d'AWS. Ensuite, vous utilisez une pièce jointe VPC comme transport sous-jacent pour la pièce jointe Transit Gateway connect entre les dispositifs virtuels et le Transit Gateway, comme le montre la figure suivante.



SD-WAN connectivity with AWS Transit Gateway (virtual appliance in AWS)

Vous pouvez également étendre et segmenter votre trafic SD-WAN vers AWS sans ajouter d'infrastructure supplémentaire. Vous pouvez créer des pièces jointes Transit Gateway connect en utilisant une AWS Direct Connect connexion comme transport sous-jacent, comme le montre la figure suivante.



SD-WAN connectivity with AWS Transit Gateway (Direct Connect as transport)

Certaines considérations doivent être prises en compte lors de l'utilisation des pièces jointes de Transit Gateway connect :

- Vous pouvez créer des pièces jointes sur les passerelles de transport en commun existantes.

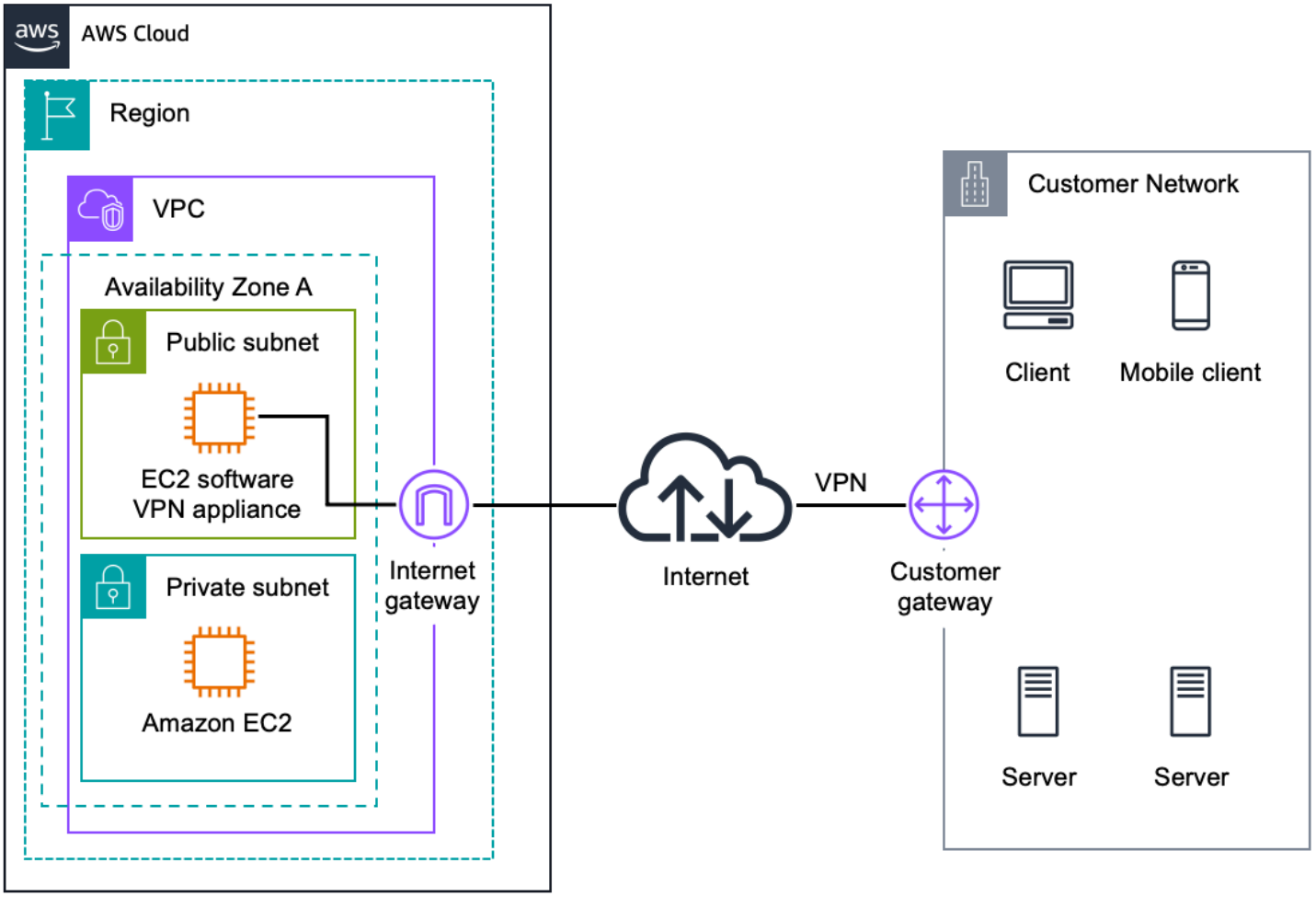
- Les appliances tierces doivent être configurées avec un tunnel GRE afin d'envoyer et de recevoir du trafic depuis Transit Gateway à l'aide de pièces jointes de connexion. L'appliance doit être configurée avec BGP pour les mises à jour dynamiques des itinéraires et les contrôles de santé.
- Les pièces jointes Connect ne prennent pas en charge les itinéraires statiques.
- Les accessoires Transit Gateway connect prennent en charge une bande passante maximale de cinq Gbit/s par tunnel GRE. Une bande passante supérieure à cinq Gbit/s peut être atteinte en annonçant les mêmes préfixes sur plusieurs homologues Connect (tunnels GRE) pour la même pièce jointe Connect.
- Un maximum de quatre homologues Connect sont pris en charge pour chaque pièce jointe Connect.
- Les pièces jointes Transit Gateway Connect prennent en charge le protocole IPv6 et les publicités de routage dynamiques via des extensions multiprotocoles pour BGP (MBGP ou MP-BGP).

Ressources supplémentaires

- Accessoires de peering Transit Gateway
- Exigences et considérations
- Article de blog : Simplifiez la connectivité SD-WAN avec AWS Transit Gateway Connect

Logiciel VPN

Amazon VPC vous offre la flexibilité de gérer entièrement les deux côtés de votre connectivité Amazon VPC en créant une connexion VPN entre votre réseau distant et une appliance VPN logicielle exécutée sur votre réseau Amazon VPC. Cette option est recommandée si vous devez gérer les deux extrémités de la connexion VPN, soit pour des raisons de conformité, soit pour tirer parti de dispositifs de passerelle qui ne sont pas actuellement pris en charge par la solution VPN d'Amazon VPC. La figure suivante illustre cette option.



Logiciel VPN de site à site

Vous pouvez choisir parmi un écosystème de plusieurs partenaires et communautés open source qui ont produit des appliances VPN logicielles qui s'exécutent sur Amazon EC2. Ce choix s'accompagne de la responsabilité de gérer l'appliance logicielle, y compris la configuration, les correctifs et les mises à niveau.

Notez que cette conception introduit un point de défaillance unique potentiel dans la conception du réseau car l'appliance VPN logicielle s'exécute sur une seule instance Amazon EC2. Pour plus d'informations, consultez Annexe A : Architecture HA de haut niveau pour les instances VPN logicielles Architecture pour les instances VPN logicielles.

Ressources supplémentaires

- Appliances VPN disponibles dans AWS Marketplace
- Fiche technique - Connexion de Cisco ASA à une instance VPC EC2 (IPsec)

- Fiche technique - Connexion de plusieurs VPC avec des instances EC2 (IPsec)
- Fiche technique - Connexion de plusieurs VPC avec des instances EC2 (SSL)

Options de connectivité entre Amazon VPC et Amazon VPC

Utilisez ces modèles de conception lorsque vous souhaitez intégrer plusieurs Amazon VPC dans un réseau virtuel plus vaste. Cela est utile si vous avez besoin de plusieurs VPC pour des raisons de sécurité, de facturation, de présence dans plusieurs régions ou d'exigences internes en matière de rétrofacturation, afin d'intégrer plus facilement les ressources AWS entre les VPC Amazon. Vous pouvez également combiner ces modèles avec les options de connectivité réseau vers Amazon VPC pour créer un réseau d'entreprise qui couvre des réseaux distants et plusieurs VPC.

La connectivité VPC entre VPC est optimale lorsque des plages d'adresses IP ne se chevauchent pas pour chaque VPC connecté. Par exemple, si vous souhaitez connecter plusieurs VPC, assurez-vous que chaque VPC est configuré avec des plages CIDR (Classless Inter-Domain Routing) uniques. Par conséquent, nous vous conseillons d'allouer un bloc CIDR unique, contigu et ne se chevauchant pas, à utiliser par chaque VPC. Pour plus d'informations sur le routage et les contraintes d'Amazon VPC, consultez les questions fréquemment posées sur Amazon VPC.

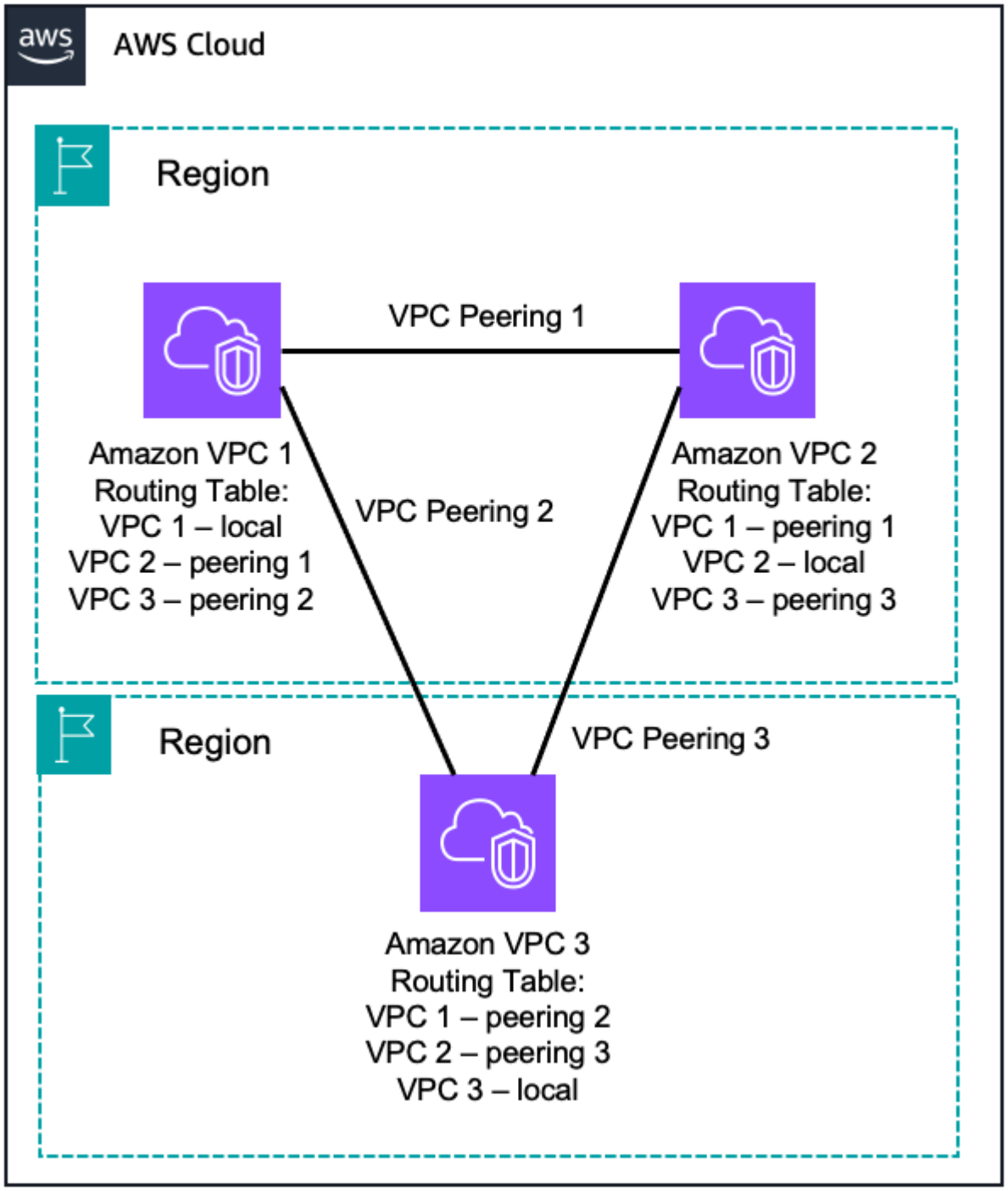
Option	Cas d'utilisation	Avantages	Limites
Appairage de VPC	Connectivité réseau fournie par AWS entre deux VPC.	Exploite l'infrastructure réseau évolutive gérée par AWS	Le peering VPC ne prend pas en charge les relations d'appairage transitives Difficile à gérer à grande échelle
AWS Transit Gateway	Connectivité de routeur régional fournie par AWS pour les VPC	Service de haute disponibilité et d'évolutivité géré par AWS Hub réseau régional pouvant accueillir jusqu'à 5 000 pièces jointes	Le peering de Transit Gateway ne prend en charge que les itinéraires statiques
AWS PrivateLink	Connectivité réseau fournie par AWS entre	Exploite l'infrastructure réseau	Les services VPC Endpoint ne sont

Option	Cas d'utilisation	Avantages	Limites
	deux VPC à l'aide de points de terminaison d'interface	évolutive gérée par AWS	disponibles que dans la région AWS dans laquelle ils ont été créés
Logiciel VPN	Connexions VPN basées sur des dispositifs logiciels entre des VPC	Supporte un large éventail de fournisseurs, de produits et de protocoles VPN Entièrement géré par vous	Vous êtes responsable de la mise en œuvre de solutions HA pour tous les points de terminaison VPN (si nécessaire) Les instances VPN pourraient devenir un goulot d'étranglement du réseau
Logiciel VPN vers AWS Site-to-Site VPN	Connexion entre l'appliance logicielle et le VPN entre les VPC	Connexion VPN VPC haute disponibilité gérée par AWS Supporte un large éventail de fournisseurs de VPN et de produits que vous gérez Supporte les routes statiques et les politiques de peering et de routage BGP dynamiques	Vous êtes responsable de la mise en œuvre des solutions HA pour les points de terminaison VPN de l'appliance logicielle (si nécessaire) Les instances VPN pourraient devenir un goulot d'étranglement du réseau Protocole VPN IPSec uniquement pour le VPN géré par AWS

Appairage de VPC

Une connexion d'appairage de VPC est une connexion réseau entre deux VPC qui permet le routage en utilisant les adresses IP privées de chaque VPC comme s'ils se trouvaient sur le même réseau. Les connexions d'appairage VPC peuvent être créées entre vos propres VPC ou avec un VPC d'un autre compte AWS. Le peering VPC prend également en charge le peering interrégional.

Le trafic utilisant le peering VPC interrégional reste toujours sur le backbone mondial d'AWS et ne traverse jamais l'Internet public, réduisant ainsi les vecteurs de menaces, tels que les exploits courants et les attaques DDoS.



VPC-to-VPC Peering

AWS utilise l'infrastructure existante d'un VPC pour créer des connexions d'appairage VPC et ne repose pas sur un matériel physique distinct. Ils n'introduisent donc pas de point de défaillance unique potentiel ni de goulot d'étranglement de la bande passante réseau entre les VPC. En outre, les tables de routage VPC, les groupes de sécurité et les listes de contrôle d'accès réseau peuvent

être utilisés pour contrôler les sous-réseaux ou les instances capables d'utiliser la connexion d'appairage VPC.

Les Amazon VPC ne prennent pas en charge le peering transitif, ce qui signifie que vous ne pouvez pas communiquer entre deux VPC qui ne sont pas directement appairés en utilisant un troisième VPC comme transit. Si vous souhaitez que tous vos VPC communiquent entre eux à l'aide de l'appairage VPC, vous devez créer des connexions d'appairage VPC 1:1 entre chacun d'eux. Vous pouvez également utiliser AWS Transit Gateway AWS Cloud WAN pour faire office de hub de transit réseau.

Le trafic IPv4 et IPv6 est pris en charge dans les connexions d'appairage VPC. Toutefois, deux VPC ne peuvent pas être appairés si leur bloc d'adresse CIDR IPv4 principal se chevauche, quels que soient les blocs d'adresse CIDR IPv4 ou IPv6 secondaires utilisés. Tenez-en compte lorsque vous attribuez le bloc CIDR principal à vos VPC si vous prévoyez d'utiliser le peering VPC entre eux.

Ressources supplémentaires

- Peering Amazon VPC
- Qu'est-ce que le peering VPC ?

AWS Transit Gateway

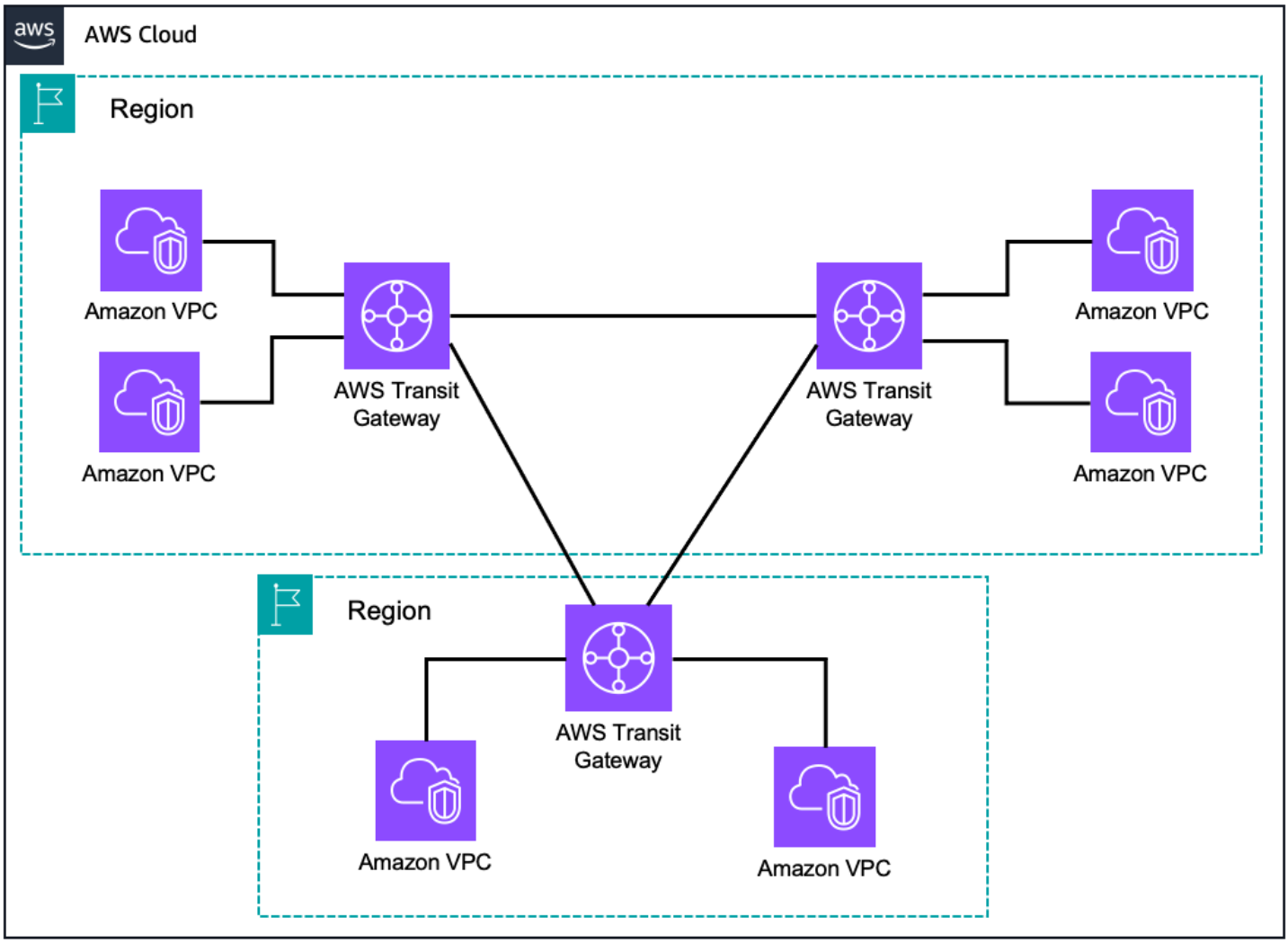
AWS Transit Gatewayest un service hautement disponible et évolutif destiné à consolider la configuration de routage des VPC AWS pour une région dotée d'une architecture. hub-and-spoke Chaque VPC en étoile doit uniquement se connecter au Transit Gateway pour accéder aux autres VPC connectés. Le trafic IPv4 et IPv6 est pris en charge dansAWS Transit Gateway.

Vous pouvez tirer parti de plusieurs tables de routage, associations et propagations de Transit Gateway pour segmenter votre trafic au sein d'un même Transit Gateway. Vous serez en mesure de gérer différents domaines de routage (par exemple, le trafic de production et le trafic hors production) à partir d'un point de gestion unique, en veillant à ce que ces domaines de routage ne puissent pas communiquer entre eux.

Vous pouvez également tirer parti de l' hub-and-spoke architecture créée par Transit Gateway pour centraliser l'accès aux services partagés tels que l'inspection du trafic, l'accès aux terminaux VPC d'interface ou le trafic de sortie via une passerelle NAT ou des instances NAT. Cette centralisation simplifie la gestion de ces ressources dans plusieurs VPC et permet un meilleur contrôle à mesure que vous étendez votre présence dans AWS.

Les passerelles de transit peuvent être couplées entre elles au sein d'une même région AWS ou entre différentes régions AWS. AWS Transit Gatewayle trafic reste toujours sur le backbone mondial d'AWS et ne traverse jamais l'Internet public, réduisant ainsi les vecteurs de menaces tels que les exploits courants et les attaques DDoS.

Avec un grand nombre de VPC, Transit Gateway simplifie la gestion des communications VPC à VPC via le peering VPC, comme le montre la figure suivante.



AWS Transit Gateway

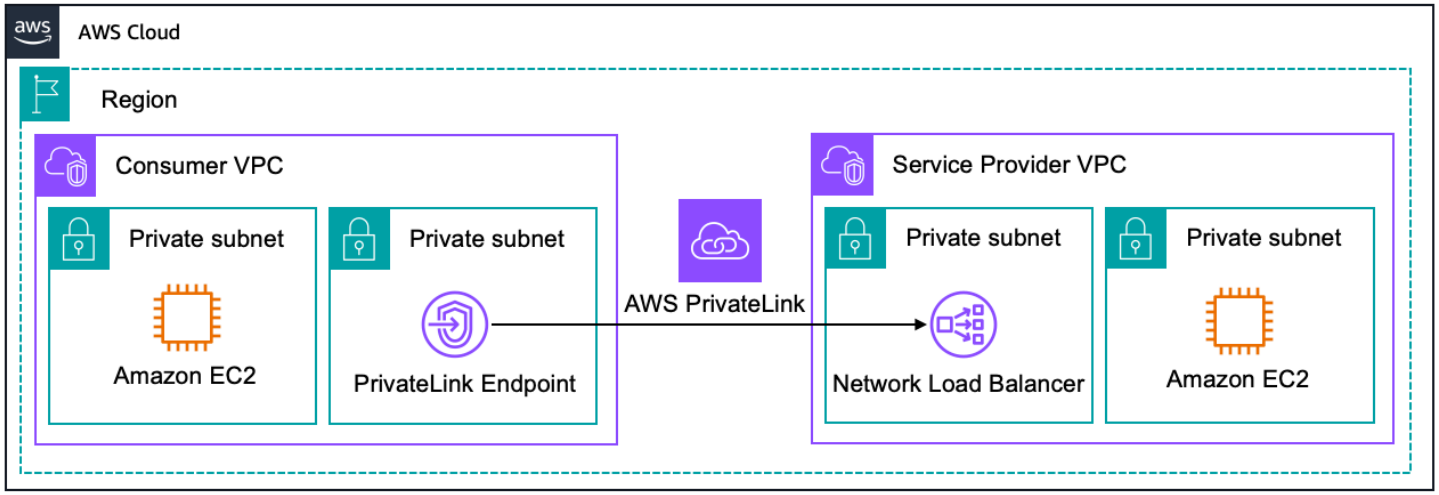
Pour une visibilité centralisée du trafic IP à destination et en provenance de vos passerelles de transit, vous pouvez publier les journaux de flux de transit sur Amazon CloudWatch Logs et Amazon S3. Les données du journal de flux sont collectées en dehors du chemin d'accès de votre trafic réseau et n'affectent donc pas le débit réseau ou la latence.

Ressources supplémentaires

- Passerelle de transit Amazon VPC
- Accessoires de peering Transit Gateway
- Travaillez avec Transit Gateways
- Enregistrement du trafic réseau à l'aide de Transit Gateway Flow Logs

AWS PrivateLink

AWS PrivateLinkvous permet de vous connecter à certains services AWS, à des services hébergés par d'autres comptes AWS (appelés services de point de terminaison) et à des services AWS Marketplace partenaires pris en charge, via des adresses IP privées dans votre VPC. Les points de terminaison de l'interface sont créés directement dans votre VPC, à l'aide d'interfaces réseau élastiques et d'adresses IP dans les sous-réseaux de votre VPC. Cela signifie que les groupes de sécurité VPC peuvent être utilisés pour gérer l'accès aux points de terminaison.



AWS PrivateLink

Nous recommandons cette approche si vous souhaitez utiliser les services proposés par un autre VPC en toute sécurité au sein d'un réseau AWS, en utilisant des adresses IP privées. AWS PrivateLinkC'est également une bonne solution lorsque les adresses IP des VPC se chevauchent.

AWS PrivateLinkprend entièrement en charge IPv6, mais les deux VPC de destination, les sous-réseaux VPC, le Network Load Balancer et les noms DNS doivent être activés ou modifiés pour utiliser le dual-stack. Une fois ces conditions préalables remplies, IPv6 peut être activé lors de la configuration du service pour le point de terminaison.

Contrôles d'accès à AWS PrivateLink

Les points de terminaison de l'interface sont créés directement dans votre VPC à l'aide d'interfaces réseau élastiques et d'adresses IP dans les sous-réseaux de votre VPC. Cela signifie que les groupes de sécurité VPC peuvent être utilisés pour gérer l'accès réseau aux points de terminaison.

Lorsque vous créez un point de terminaison d'interface ou un point de terminaison de passerelle, vous pouvez également joindre une politique de point de terminaison. La politique de point de terminaison contrôle quels principaux AWS (comptes AWS, utilisateurs IAM et rôles) peuvent utiliser le point de terminaison VPC pour accéder au service de point de terminaison.

Vous ne pouvez pas attacher plus d'une stratégie à un point de terminaison. Cependant, vous pouvez modifier la politique de point de terminaison à tout moment.

Une politique de point de terminaison ne remplace ni ne remplace les politiques utilisateur IAM ou les politiques spécifiques au service (telles que les politiques relatives aux compartiments Amazon S3). Si vous utilisez un point de terminaison d'interface pour vous connecter à Amazon S3, vous pouvez également utiliser les politiques de compartiment Amazon S3 pour contrôler l'accès aux compartiments depuis des points de terminaison ou des VPC spécifiques.

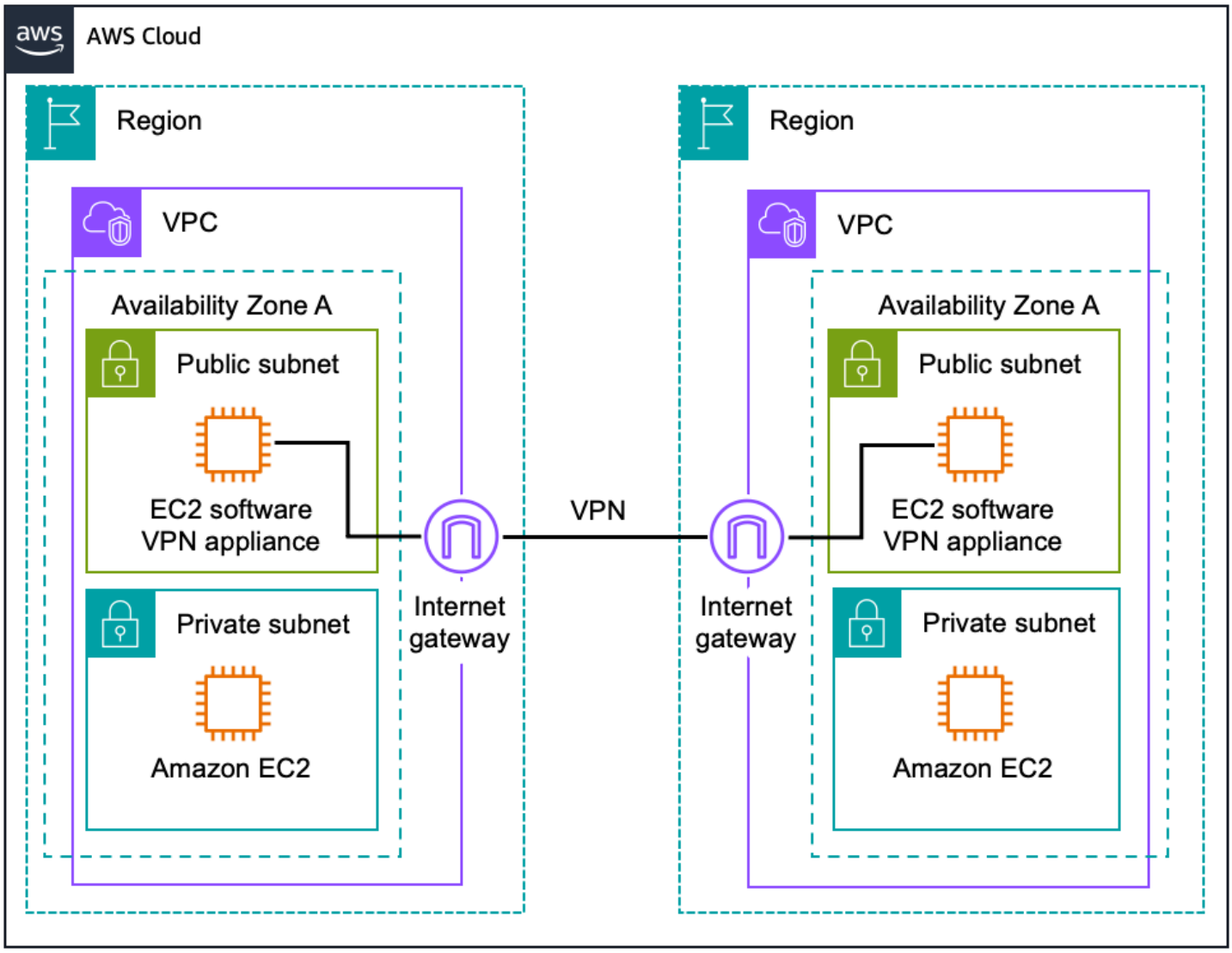
Ressources supplémentaires

- Points de terminaison VPC d'interface () AWS PrivateLink
- Services de point de terminaison VPC () AWS PrivateLink
- Article de blog : Accélérez votre adoption d'IPv6 grâce PrivateLink aux services et aux terminaux
- Article de blog : Connexion de réseaux dont les plages d'adresses IP se chevauchent
- AWS PrivateLinkPartenaires

Logiciel VPN

Amazon VPC fournit une flexibilité de routage réseau. Cela inclut la possibilité de créer des tunnels VPN sécurisés entre deux ou plusieurs appliances VPN logicielles afin de connecter plusieurs VPC à un réseau privé virtuel plus vaste afin que les instances de chaque VPC puissent se connecter facilement les unes aux autres à l'aide d'adresses IP privées. Cette option est recommandée lorsque vous souhaitez gérer les deux extrémités de la connexion VPN à l'aide de votre fournisseur de

logiciel VPN préféré. Cette option utilise une passerelle Internet attachée à chaque VPC pour faciliter la communication entre les appliances VPN logicielles.



Software Site-to-Site VPN VPC-to-VPC Routing

Vous pouvez choisir parmi un écosystème de plusieurs partenaires et communautés open source qui ont produit des appliances VPN logicielles qui s'exécutent sur Amazon EC2. Ce choix s'accompagne de la responsabilité de gérer l'appliance logicielle, y compris la configuration, les correctifs et les mises à niveau.

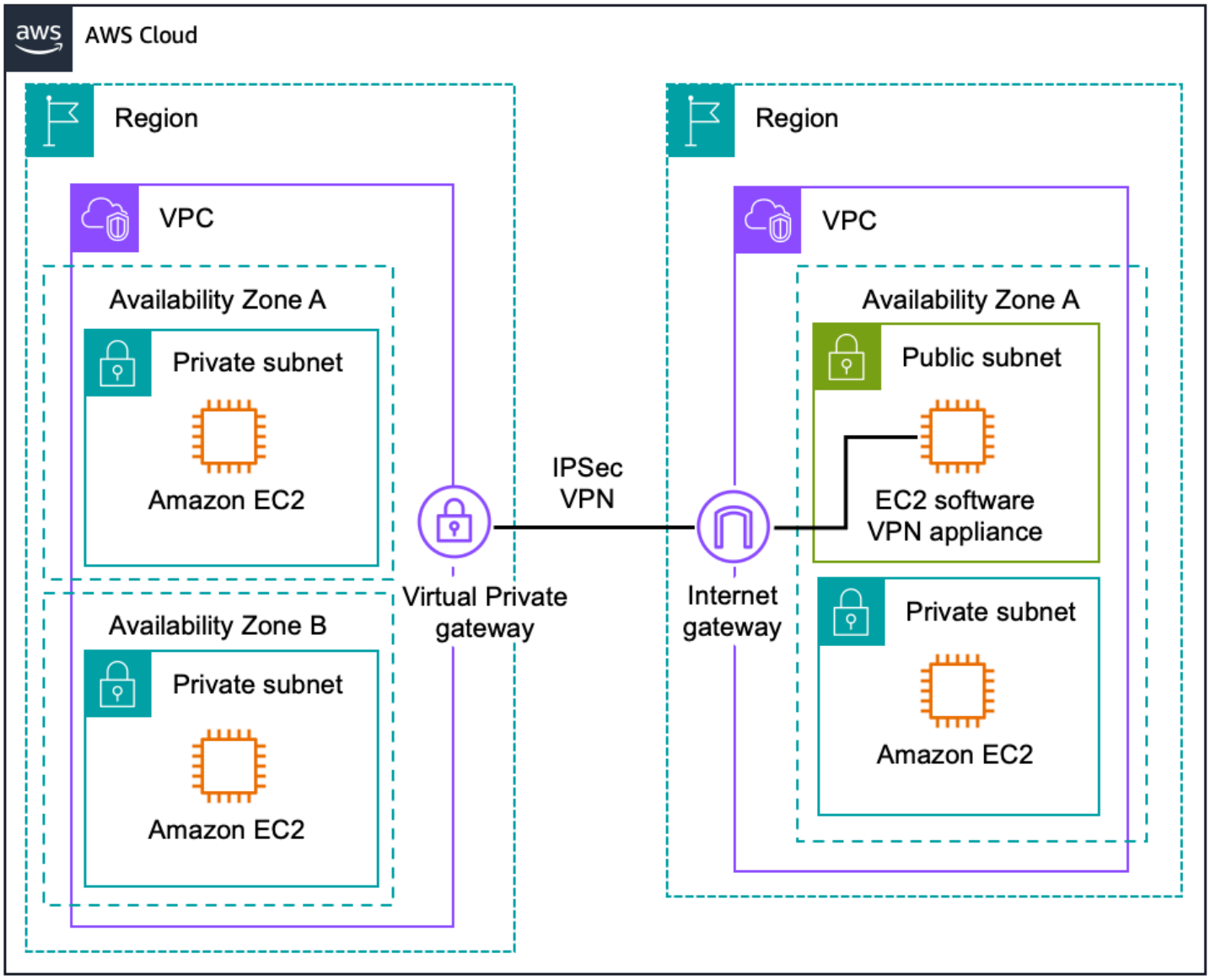
Notez que cette conception introduit un point de défaillance unique potentiel dans la conception du réseau car l'appliance VPN logicielle s'exécute sur une seule instance Amazon EC2. Pour plus d'informations, consultez Annexe A : Architecture HA de haut niveau pour les instances VPN logicielles.

Ressources supplémentaires

- Appliances VPN disponibles auprès du AWS Marketplace
- Fiche technique - Connexion de plusieurs VPC avec des instances EC2 (IPsec)
- Fiche technique - Connexion de plusieurs VPC avec des instances EC2 (SSL)

Logiciel VPN vers AWS Site-to-Site VPN

Amazon VPC offre la flexibilité nécessaire pour combiner les options VPN gérées par AWS et VPN logiciel pour connecter plusieurs VPC. Grâce à cette conception, vous pouvez créer des tunnels VPN sécurisés entre une appliance VPN logicielle et une passerelle privée virtuelle, permettant aux instances de chaque VPC de se connecter facilement les unes aux autres à l'aide d'adresses IP privées. Cette option utilise une passerelle privée virtuelle dans un Amazon VPC et une combinaison d'une passerelle Internet et d'une appliance VPN logicielle dans un autre Amazon VPC, comme illustré dans la figure suivante.



Software VPN to AWS Site-to-Site VPN VPC-to-VPC Routing

Notez que cette conception introduit un point de défaillance unique potentiel dans la conception du réseau. Pour plus d'informations, consultez Annexe A : Architecture HA de haut niveau pour les instances VPN logicielles.

Ressources supplémentaires

- Appliances VPN disponibles auprès du AWS Marketplace
- Guide de l'utilisateur AWS Site-to-Site VPN
- Exigences relatives aux dispositifs de passerelle client

Options d'accès à distance logicielle à Amazon VPC

Avec le VPN d'accès à distance logiciel, vous pouvez tirer parti de services peu coûteux, élastiques et sécurisés pour mettre en œuvre des solutions d'accès à distance tout en offrant une expérience fluide de connexion aux ressources hébergées par AWS. Cette option est généralement préférée par les petites entreprises dotées de réseaux distants moins étendus ou qui n'ont pas encore conçu et déployé de solutions d'accès à distance pour leurs employés.

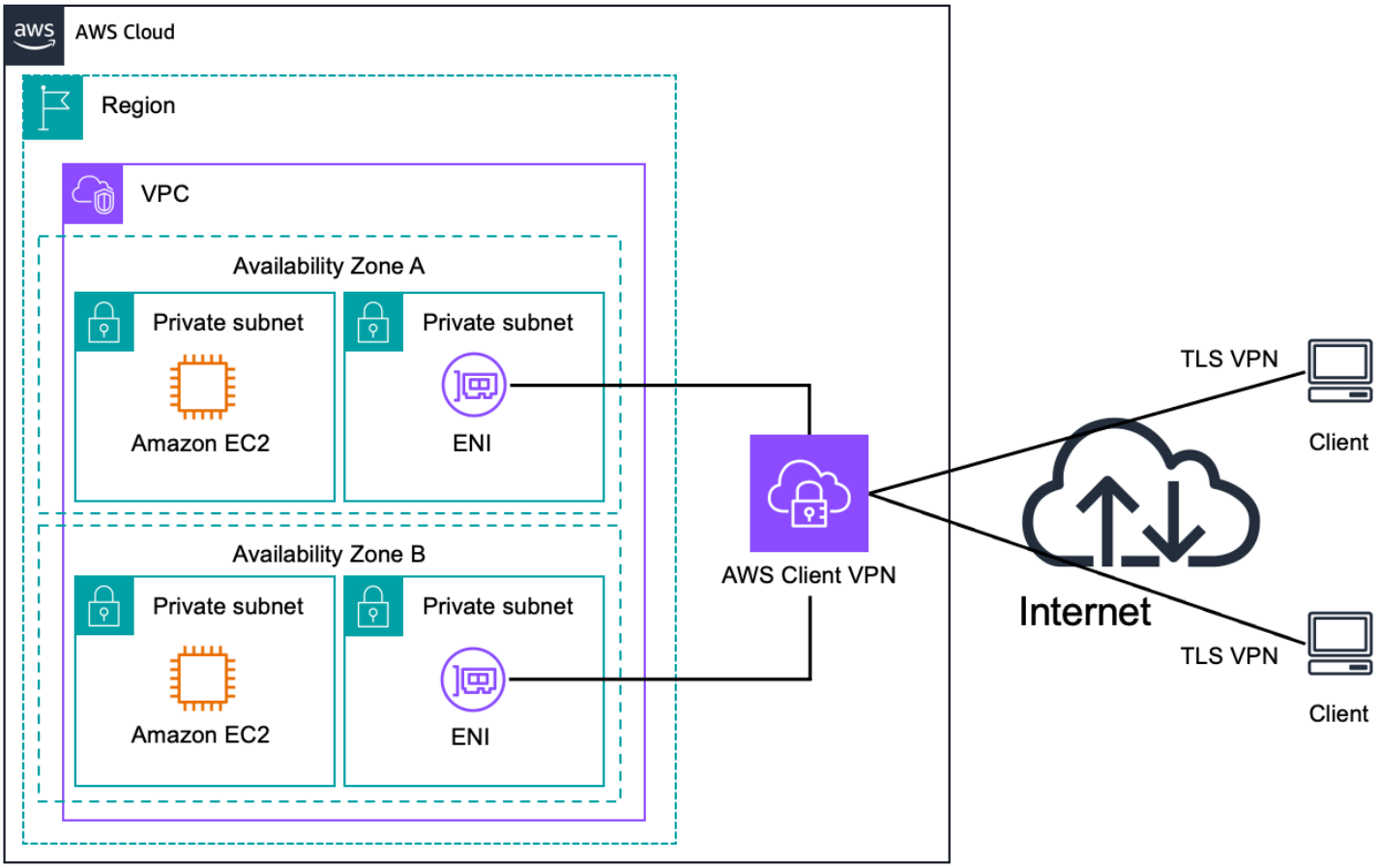
Vous pouvez combiner ces modèles avec les options de Options de connectivité entre le réseau et Amazon VPC connectivité et Options de connectivité entre Amazon VPC et Amazon VPC créer un réseau qui couvre des réseaux distants et plusieurs VPC.

Le tableau suivant décrit les avantages et les limites de ces options.

Option	Cas d'utilisation	Avantages	Limites
AWS Client VPN	Solution d'accès à distance gérée par AWS à Amazon VPC et/ou à des réseaux internes	Service de haute disponibilité et d'évolutivité géré par AWS	Clients OpenVPN uniquement
Logiciel client VPN	Solution logicielle d'accès à distance d'une appliance VPN à Amazon VPC et/ou à des réseaux internes	Prend en charge un plus large éventail de fournisseurs, de produits et de protocoles VPN Solution entièrement gérée par le client	Vous êtes responsable de la mise en œuvre des solutions HA

AWS Client VPN

Client VPN AWS est un service de haute disponibilité et d'évolutivité géré par AWS qui permet un accès à distance sécurisé aux logiciels. Il offre la possibilité de créer une connexion TLS sécurisée entre les clients distants et vos Amazon VPC, afin d'accéder en toute sécurité aux ressources AWS et sur site via Internet, comme le montre la figure suivante.



AWS Client VPN Remote Access

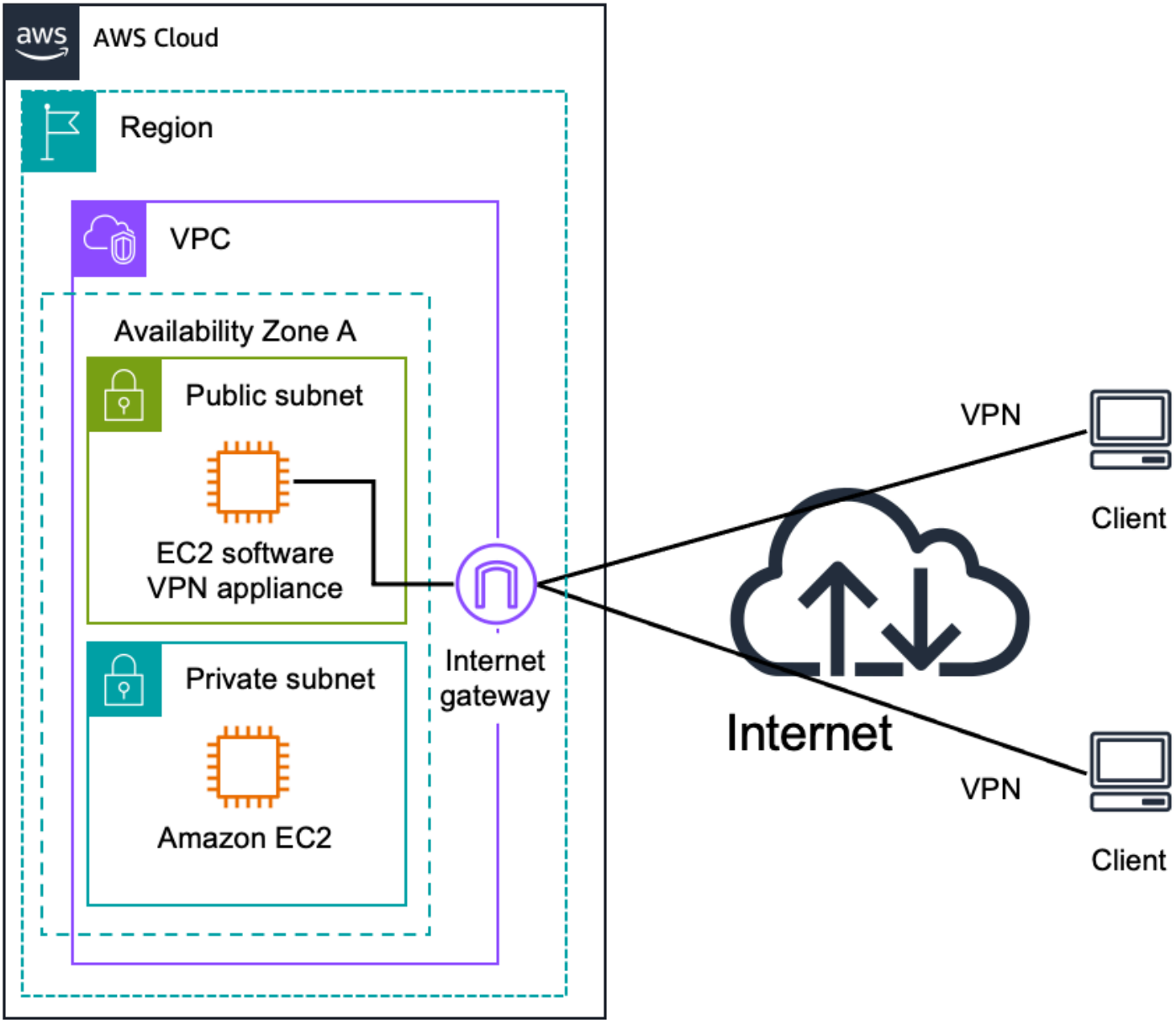
Les clients distants peuvent être le Client VPN pour ordinateur de bureau AWS ou des clients VPN OpenVPN tiers, avec authentification par Active Directory ou par certificat mutuel.

Ressources supplémentaires

- Guide de l'administrateur AWS Client VPN

Logiciel client VPN

Vous pouvez choisir parmi un écosystème de plusieurs partenaires et communautés open source qui ont produit des solutions d'accès à distance qui s'exécutent sur Amazon EC2. Ces solutions offrent une grande flexibilité quant à l'utilisation du protocole de sécurité pour l'accès à distance à vos Amazon VPC, afin d'accéder en toute sécurité aux ressources AWS et sur site via Internet, comme le montre la figure suivante.



Software Client VPN Remote Access

Les solutions d'accès à distance varient en complexité, prennent en charge plusieurs options d'authentification des clients (y compris l'authentification multifactorielle) et peuvent être intégrées à Amazon VPC ou à des solutions de gestion des identités et des accès hébergées à distance (en tirant parti de l'une des options Network-to-Amazon VPC) comme Microsoft Active Directory ou d'autres solutions d'authentification LDAP/multifactorielle.

Vous êtes responsable de la gestion du logiciel d'accès à distance, notamment de la gestion des utilisateurs, de la configuration, des correctifs et des mises à niveau. Cette conception introduit un point de défaillance unique potentiel dans la conception du réseau car le serveur d'accès à distance

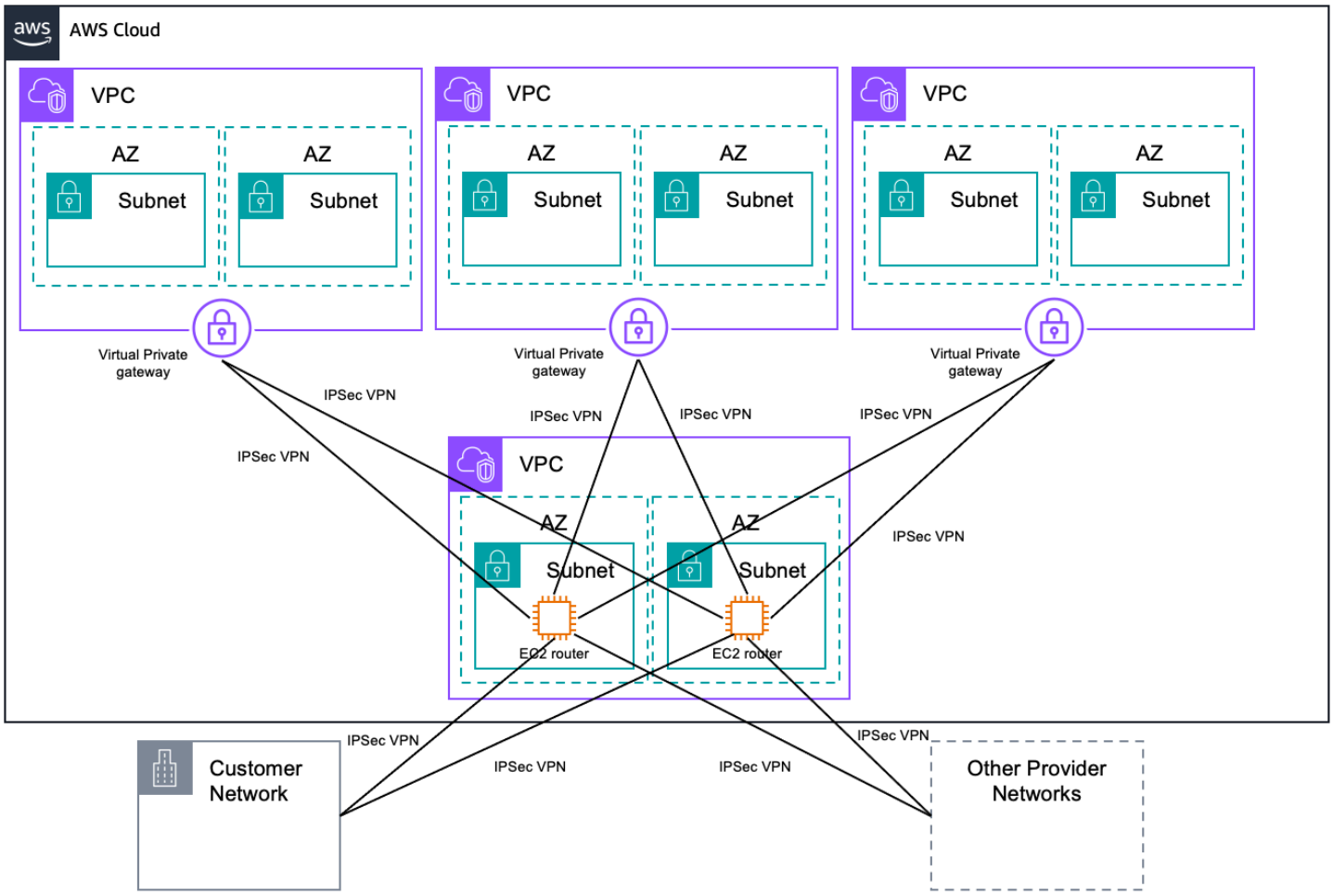
s'exécute sur une seule instance Amazon EC2. Pour plus d’informations, consultez Annexe A : Architecture HA de haut niveau pour les instances VPN logicielles.

Ressources supplémentaires

- Appliances VPN disponibles auprès du AWS Marketplace
- Guide de démarrage rapide du serveur d'accès OpenVPN

VPC de transit

En vous appuyant sur les conceptions de VPN logiciel mentionnées ci-dessus, vous pouvez créer un réseau de transit mondial sur AWS. Un VPC de transit est une stratégie courante pour connecter plusieurs VPC géographiquement dispersés et des réseaux distants afin de créer un centre de transit réseau mondial. Un VPC en transit simplifie la gestion du réseau et limite le nombre de connexions requises pour connecter plusieurs VPC et réseaux distants. La figure suivante illustre cette conception.



Transit VPC

Outre le routage réseau direct entre les VPC et les réseaux locaux, cette conception permet également au VPC de transit de mettre en œuvre des règles de routage plus complexes, telles que la traduction d'adresses réseau entre des plages de réseaux qui se chevauchent, ou d'ajouter un filtrage ou une inspection de paquets supplémentaires au niveau du réseau. La conception du VPC de transit peut être utilisée pour prendre en charge des cas d'utilisation importants tels que les réseaux privés, la connectivité partagée et l'utilisation d'AWS entre comptes.

Ressources supplémentaires

- AWS Transit Gateway
- Cisco Catalyst 8000V pour SD-WAN et routage AWS Marketplace

Réseau étendu dans le cloud AWS

AWS Cloud WAN est un réseau étendu (WAN) géré par l'intention, décrit par une politique que vous définissez qui unifie votre centre de données, vos succursales et vos réseaux AWS. Bien que vous puissiez créer votre propre réseau mondial en interconnectant plusieurs passerelles de transit entre les régions, le Cloud WAN fournit des fonctionnalités intégrées d'automatisation, de segmentation et de gestion de configuration conçues spécifiquement pour créer et exploiter des réseaux mondiaux, sur la base de votre politique réseau principale. Le Cloud WAN a ajouté des fonctionnalités telles que les attachements automatisés aux VPC, la surveillance intégrée des performances et la configuration centralisée.

La politique du réseau principal est rédigée dans un langage déclaratif qui définit les segments, le routage de la région AWS et la manière dont les pièces jointes doivent être mappées aux segments. Avec une politique réseau de base, vous pouvez décrire votre intention en matière de contrôle d'accès et de routage du trafic, tandis qu'AWS Cloud WAN gère les détails de configuration du réseau.

Le cloud WAN est géré dans AWS Network Manager, ce qui vous permet de gérer et de visualiser de manière centralisée votre réseau central Cloud WAN et vos réseaux Transit Gateway sur les comptes AWS, les régions et les sites sur site. Network Manager vous fournit plusieurs visualisations de tableau de bord pour vous aider à visualiser et à surveiller tous les aspects de votre réseau mondial. Certains des tableaux de bord incluent :

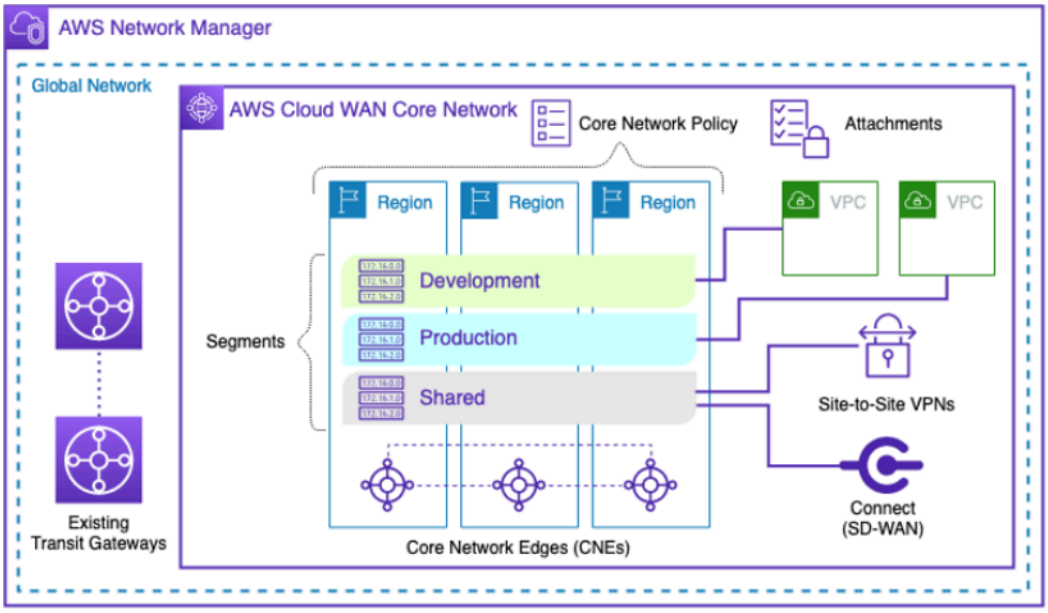
- Des cartes du monde qui indiquent où se trouvent les ressources de votre réseau, telles que les emplacements périphériques, les appareils et les pièces jointes.
- Surveillance qui utilise CloudWatch les événements pour suivre 15 mois de statistiques, vous donnant ainsi une meilleure idée des performances de vos réseaux.
- Suivi des événements qui diffuse les événements en temps réel vers un tableau de bord des événements.
- Schémas topologiques et logiques de vos réseaux de passerelles de transit et de vos passerelles de transit.

Transit Gateway et Cloud WAN permettent une connectivité centralisée entre les VPC et les sites sur site. Transit Gateway est un hub de connectivité réseau régional idéal pour les clients qui opèrent dans quelques régions AWS, qui souhaitent gérer leur propre configuration de peering et de routage, ou qui préfèrent utiliser leur propre automatisation. Le cloud WAN est idéal pour les clients

qui souhaitent définir leur réseau mondial par le biais de politiques et faire en sorte que le service implémente automatiquement les composants sous-jacents.

À savoir

- Le CNE (Core network edge) hérite de nombreuses caractéristiques de Transit Gateway, telles que le débit par attachement VPC.
- Le Cloud WAN prend en charge les protocoles IPv4 et IPv6.
- Actuellement, le Cloud WAN ne prend pas en charge les AWS Direct Connect pièces jointes de manière native. Pour pouvoir l'utiliser AWS Direct Connect avec Cloud WAN, vous avez besoin d'une passerelle de transit connectée à une AWS Direct Connect passerelle, puis d'une passerelle de transit couplée au Cloud WAN.
- Pour les grands réseaux comportant de nombreuses modifications, envisagez de créer un réseau mondial distinct de développement et de test dans lequel vous pourrez valider les modifications.



AWS Cloud WAN

Ressources supplémentaires

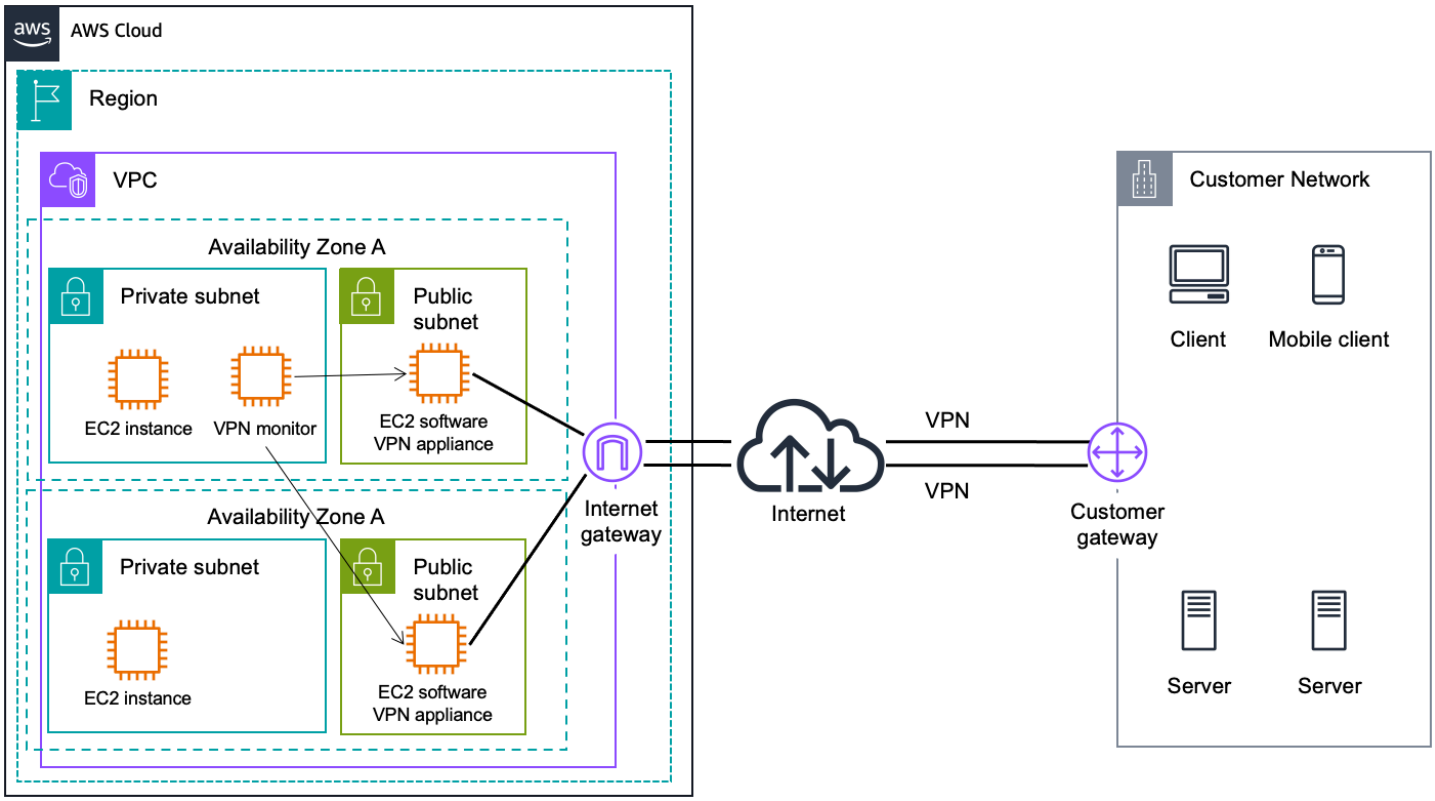
- Documentation sur le WAN dans le cloud AWS
- Article de blog : Modèles de migration et d'interopérabilité avec AWS Cloud WAN et AWS Transit Gateway

Conclusion

AWS propose un certain nombre d'options de connectivité efficaces et sécurisées pour vous aider à tirer le meilleur parti d'AWS lors de l'intégration de vos réseaux distants à Amazon VPC. Les options proposées dans ce livre blanc mettent en évidence plusieurs options et modèles de connectivité que des clients ont utilisés pour intégrer avec succès leurs réseaux distants ou plusieurs réseaux Amazon VPC. Vous pouvez utiliser les informations fournies ici pour déterminer le mécanisme le plus approprié pour connecter l'infrastructure nécessaire au fonctionnement de votre entreprise, quel que soit son emplacement physique ou son hébergement.

Annexe A : Architecture HA de haut niveau pour les instances VPN logicielles

La création d'une connexion VPC entièrement résiliente pour les instances VPN logicielles nécessite l'installation et la configuration de plusieurs instances VPN et d'une instance de surveillance pour surveiller l'état des connexions VPN.



Logiciel VPN HA de haut niveau

Nous vous recommandons de configurer vos tables de routage VPC pour tirer parti de toutes les instances VPN simultanément en dirigeant le trafic de tous les sous-réseaux d'une zone de disponibilité vers ses instances VPN respectives situées dans la même zone de disponibilité. Chaque instance VPN fournit ensuite une connectivité VPN aux instances qui partagent la même zone de disponibilité.

Surveillance des VPN

Pour surveiller un appareil VPN basé sur un logiciel, vous pouvez créer un moniteur VPN. Le moniteur VPN est une instance personnalisée dont vous aurez besoin pour exécuter les scripts

de surveillance VPN. Cette instance est destinée à exécuter et à surveiller l'état de la connexion VPN et des instances VPN. En cas de panne d'une instance ou d'une connexion VPN, le moniteur doit arrêter, résilier ou redémarrer l'instance VPN tout en redirigeant le trafic des sous-réseaux concernés vers l'instance VPN fonctionnelle jusqu'à ce que les deux connexions soient à nouveau fonctionnelles. Étant donné que les exigences des clients varient, AWS ne fournit actuellement aucune directive prescriptive pour la configuration de cette instance de surveillance. Cependant, un exemple de script permettant d'activer la haute disponibilité entre les instances NAT peut être utilisé comme point de départ pour créer une solution HA pour les instances VPN logicielles. Nous vous recommandons de réfléchir à la logique métier nécessaire pour envoyer une notification ou tenter de réparer automatiquement la connectivité réseau en cas de panne de connexion VPN.

En outre, vous pouvez surveiller les tunnels VPN gérés par AWS à l'aide CloudWatch des métriques Amazon, qui collectent les points de données du service VPN sous forme de métriques lisibles en temps quasi réel. Chaque connexion VPN collecte et publie diverses métriques de tunnel sur Amazon CloudWatch. Ces mesures vous permettent de surveiller l'état et l'activité du tunnel et de créer des actions automatisées.

Collaborateurs

Les personnes qui ont contribué à ce document incluent :

- Daniel Yu, responsable de compte technique senior, AWS Enterprise Support
- Garvit Singh, concepteur de solutions, architecture de solutions AWS
- Steve Morad, directeur principal, concepteurs de solutions, architecture de solutions AWS
- Sohaib Tahir, architecte de solutions, architecture de solutions AWS
- Fiona Armada, architecte de solutions principale, architecture de solutions AWS
- Pablo Sánchez Carmona, architecte de solutions spécialisé dans les réseaux, AWS Solution Architecture
- Tony Hawke, spécialiste principal des réseaux, responsable des comptes techniques, AWS Enterprise Support

Révisions du document

Pour être informé des mises à jour de ce livre blanc, abonnez-vous au flux RSS.

Modification	Description	Date
Livre blanc mis à jour	AWS Cloud WAN et Transit Gateway ont ajouté des options de connexion, des diagrammes mis à jour et des informations à tout moment.	5 avril 2023
Livre blanc mis à jour	Ajout d'options VPN pour AWS Transit Gateway et AWS Client, mise à jour de diagrammes et d'informations.	6 juin 2020
Mise à jour mineure	Modification mineure visant à corriger la référence à l'applian ce VPN logicielle.	20 mai 2020
Livre blanc mis à jour	Informations mises à jour partout. Concentrez-vous sur les conceptions/fonctionnalités suivantes : VPC de transit, passerelle Direct Connect et. AWS PrivateLink	1er janvier 2018
Publication initiale	Les options de connectivité Amazon Virtual Private Cloud ont été publiées.	1 juillet 2014

Mentions légales

Les clients sont responsables de leur propre évaluation indépendante des informations contenues dans ce document. Le présent document : (a) est fourni à titre informatif uniquement, (b) représente les offres et pratiques actuelles de produits AWS, qui sont susceptibles d'être modifiées sans préavis, et (c) ne crée aucun engagement ou assurance de la part d'AWS et de ses affiliés, fournisseurs ou concédants de licences. Les produits ou services AWS sont fournis « en l'état » sans garantie, représentation ou condition, de quelque nature que ce soit, explicite ou implicite. Les responsabilités et obligations d'AWS envers ses clients sont déterminées par les contrats AWS, et le présent document ne fait pas partie d'un contrat entre AWS et ses clients, ni le modifie.

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.