t

Amazon Virtual Private Cloud Connectivity Options

Steve Morad

Juillet 2014

Table des matières

Résumé

Amazon Virtual Private Cloud (Amazon VPC) permet aux clients de mettre en service une section privée et isolée du cloud Amazon Web Services (AWS), dans laquelle ils peuvent lancer des ressources AWS en utilisant des gammes d'adresses IP définies par le client. Amazon VPC propose aux clients plusieurs options de connexion de leurs réseaux virtuels AWS à d'autres réseaux distants. Ce document décrit plusieurs options de connectivité réseau courantes à disposition de nos clients. Parmi ces options de connectivité figurent l'intégration des réseaux distants du client à Amazon VPC, ainsi que la connexion de plusieurs Amazon VPC à un réseau virtuel contigu.

Ce livre blanc est destiné aux architectes et ingénieurs réseau d'entreprises ou aux administrateurs d'Amazon VPC qui souhaitent étudier les différentes options de connectivité possibles. Il offre une présentation des diverses options permettant de faciliter les discussions sur la connectivité réseau, et oriente vers d'autres documents et ressources proposant davantage d'informations ou d'exemples.

Introduction

Amazon VPC offre plusieurs options de connectivité réseau dont vous pouvez profiter en fonction de la conception actuelle de votre réseau et de vos exigences. Ces options de connectivité incluent d'exploiter la connexion à Internet ou une connexion AWS Direct Connect comme ossature du réseau et de faire aboutir cette connexion à des points de terminaison aux réseaux gérés par AWS ou par l'utilisateur. Par ailleurs, avec AWS, vous pouvez choisir la façon dont le routage du réseau sera géré entre Amazon VPC et vos réseaux, en tirant parti de l'équipement et des routages du réseau AWS ou de celui de l'utilisateur. Ce livre blanc étudie les options suivantes en offrant une présentation et une comparaison de haut de niveau de chacune d'entre elles :

Options de connectivité du réseau de l'utilisateur à Amazon VPC	
VPN hardware	Décrit l'établissement d'une connexion VPN hardware partant de votre équipement réseau sur un réseau distant vers un équipement réseau géré par AWS et attaché à votre Amazon VPC.
AWS Direct Connect	Décrit l'établissement d'une connexion privée et logique entre votre réseau distant et Amazon VPC, en s'appuyant sur AWS Direct Connect.
AWS Direct Connect + VPN	Décrit l'établissement d'une connexion privée et chiffrée entre votre réseau distant et Amazon VPC, en s'appuyant sur AWS Direct Connect.
AWS VPN CloudHub	Décrit l'établissement d'un modèle en étoile (hub-and-spoke) pour la connexion des succursales distantes.
VPN Software	Décrit l'établissement d'une connexion VPN partant de votre équipement sur un réseau distant vers une appliance VPN Software gérée par l'utilisateur et s'exécutant à l'intérieur d'un Amazon VPC.
Options de connectivité d'Amazon VPC à Amazon VPC	
Appairage de VPC	Décrit l'approche recommandée par AWS pour connecter plusieurs Amazon VPC au sein d'une région utilisant la fonction d'appairage d'Amazon VPC.
VPN Software	Décrit la connexion de plusieurs Amazon VPC en utilisant des connexions VPN établies entre les appliances de VPN Software gérées par l'utilisateur et s'exécutant à l'intérieur de chaque Amazon VPC.
VPN software-hardware	Décrit la connexion de plusieurs Amazon VPC avec une connexion VPN établie entre une appliance de VPN Software gérée par l'utilisateur dans un Amazon VPC et un équipement réseau géré par AWS et attaché à l'autre Amazon VPC.
VPN hardware	Décrit la connexion de plusieurs Amazon VPC, en tirant parti de plusieurs connexions VPN hardware entre votre réseau distant et chacun de vos Amazon VPC.
AWS Direct Connect	Décrit la connexion de plusieurs Amazon VPC, en tirant parti des connexions logiques sur les routeurs AWS Direct Connect gérés par le client.
Options de connectivité de l'utilisateur interne à Amazon VPC	
Accès distant à VPN Software	Outre les options de connectivité du réseau du client à Amazon VPC pour connecter les utilisateurs distants au ressources du VPC, cette section indique comment tirer profit d'une solution d'accès à distance pour offrir un accès au VPN de l'utilisateur final dans un Amazon VPC.

Options de connectivité d'un réseau à Amazon VPC

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

La connectivité du VPC aux réseaux distants du client est optimale en cas d'utilisation de plages d'adresses IP qui ne se chevauchent pas pour chaque réseau connecté. Par exemple, si vous voulez connecter un ou plusieurs VPC à votre réseau domestique, veillez à les configurer avec des plages uniques CIDR (Classless Inter-Domain Routing). Nous vous conseillons d'allouer à chaque VPC un bloc CIDR unique, contigu, sans chevauchement. Pour plus d'informations sur le routage et les contraintes d'Amazon VPC, reportez-vous aux FAQ sur Amazon VPC.[1]

Option	Cas d'utilisation	Avantages	Limites
VPN hardware	Connexion VPN hardware, IPsec, via Internet	Réutilisation de l'équipement et des processus existants du VPN Réutilisation des connexions Internet existantes Le point de terminaison géré par AWS inclut la redondance de centre de données multiples et le basculement automatique Compatible avec les routes statiques ou l'appairage dynamique BGP (Border Gateway Protocol) et les stratégies de routage	La latence, la variabilité et la disponibilité du réseau dépendent des conditions d'Internet Le point de terminaison géré par le client est chargé de mettre en œuvre la redondance et le basculement (si nécessaire) Le périphérique du client doit prendre en charge les protocoles BGP à saut unique (en cas d'exploitation de BGP pour le routage dynamique)
AWS Direct Connect	Connexion réseau dédiée sur des lignes privées	Performances réseau plus prévisibles Coûts de la bande passante réduits Connexions configurées à 1 ou 10 Gb/s Prise en charge de l'appairage BGP et des stratégies de routage	Peut nécessiter la configuration de relations supplémentaires avec les fournisseurs d'hébergement et de téléphonie ou de circuits de réseau

[1] http://aws.amazon.com/vpc/faqs/

Option	Cas d'utilisation	Avantages	Limites
AWS Direct Connect + VPN	Connexion VPN hardware, IPsec, via les lignes privées	Comme dans l'option précédente avec l'ajout d'une connexion VPN IPsec sécurisée	Comme dans l'option précédente avec une petite complexité VPN supplémentaire
AWS VPN CloudHub	Connexion des succursales distantes dans un modèle en étoile (hub-and-spoke) pour la connectivité principale ou de sauvegarde	Réutilisation des connexions Internet existantes et des connexions AWS VPN (par ex., utilisation d'AWS VPN CloudHub comme connectivité de sauvegarde à un réseau MPLS tiers) La passerelle privée virtuelle gérée par AWS inclut la redondance de centre de données multiples et le basculement automatique Compatibilité avec BGP pour l'échange des routes et des priorités de routage (par ex., préférer les connexions MPLS aux connexions AWS VPN de sauvegarde)	La latence, la variabilité et la disponibilité du réseau dépendent d'Internet Les points de terminaison des succursales gérés par le client sont chargés de mettre en œuvre la redondance et le basculement (si nécessaire)
VPN Software	Connexion VPN à base d'appliance logicielle, via Internet	Compatibilité avec une vaste gamme de fournisseurs, produits et protocoles de VPN Solution totalement gérée par le client	Le client est chargé de mettre en œuvre les solutions à haute disponibilité pour tous les points de terminaison du VPN (si nécessaire)

VPN hardware

Amazon VPC offre la possibilité de créer une connexion VPN hardware, IPsec, entre les réseaux distants du client et son Amazon VPC via Internet, comme l'indique la figure 1. Envisagez d'opter pour cette option si vous voulez bénéficier d'un point de terminaison de VPN géré par AWS qui comporte la redondance du centre de données multiples et le basculement automatiques intégrés du côté AWS de la connexion VPN. Même si la figure ne le montre pas, la passerelle réseau privé virtuel (VGW) Amazon représente deux points de terminaison de VPN distincts, situés physiquement dans des centres de données séparés afin d'accroître la disponibilité de votre connexion VPN.

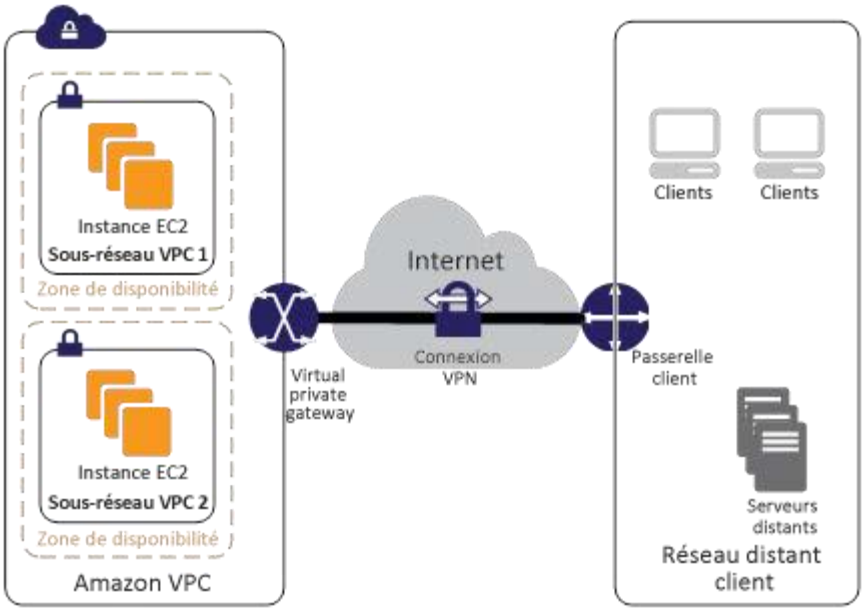

Figure 1 : VPN hardware

La passerelle VGW prend également en charge et encourage les connexions de plusieurs passerelles utilisateur, afin que vous puissiez mettre en œuvre la redondance et le basculement de votre côté de la connexion VPN, comme l'indique la figure 2. Les options de routage dynamique et statique vous sont proposées afin de conférer de la flexibilité à votre configuration de routage. Le routage dynamique tire parti de l'appairage BGP pour échanger les informations de routage entre AWS et ces points de terminaison distants. Avec le routage dynamique, vous pouvez également spécifier des priorités, des stratégies et des poids (métriques) de routage dans vos annonces BGP, ainsi qu'influencer le chemin d'accès réseau entre vos réseaux et AWS.

Il est important de noter que, lorsque BGP est utilisé, les connexions IPsec aussi bien que les connexions BGP doivent être interrompues sur le même périphérique de passerelle utilisateur ; il doit donc être capable de mettre fin aux deux connexions IPsec et BGP.

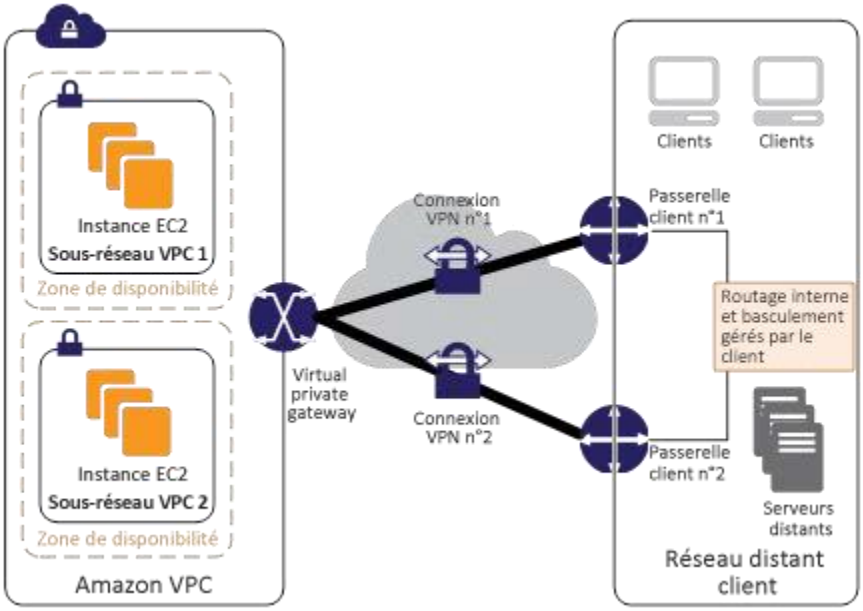

Figure 2 : Connexions VPN hardware redondantes

Ressources supplémentaires

- Ajout d'une passerelle réseau privé virtuel matérielle à votre VPC[2]
- Configuration requise pour le périphérique de la passerelle client[3]
- Périphériques de passerelle client connus pour fonctionner avec Amazon VPC[4]

AWS Direct Connect

AWS Direct Connect facilite l'établissement d'une connexion réseau dédiée d'un réseau sur site vers Amazon VPC. Grâce à AWS Direct Connect, vous pouvez établir une connectivité privée entre AWS et votre centre de données, votre bureau ou votre environnement de colocalisation. Cette connexion privée peut réduire les coûts réseau, augmenter le débit de la bande passante et offrir une expérience réseau plus uniforme que des connexions basées sur Internet.

AWS Direct Connect vous permet d'établir des connexions réseau dédiées (ou des connexions multiples) de 1 ou 10 Gb/s entre les réseaux AWS et un des emplacements d'AWS Direct Connect. Il utilise les VLAN standard de l'industrie pour accéder aux instances Amazon Elastic Compute Cloud (Amazon EC2) s'exécutant dans un Amazon VPC utilisant des adresses IP privées. Vous pouvez faire votre choix dans un écosystème de fournisseurs de services WAN pour l'intégration de votre point de terminaison AWS Direct Connect dans un emplacement AWS Direct Connect avec vos réseaux distants. La figure 3 présente ce schéma.

[2] http://docs.amazonwebservices.com/AmazonVPC/latest/UserGuide/VPC_VPN.html

[3] http://aws.amazon.com/vpc/faqs/#C8

[4] http://aws.amazon.com/vpc/faqs/#C9

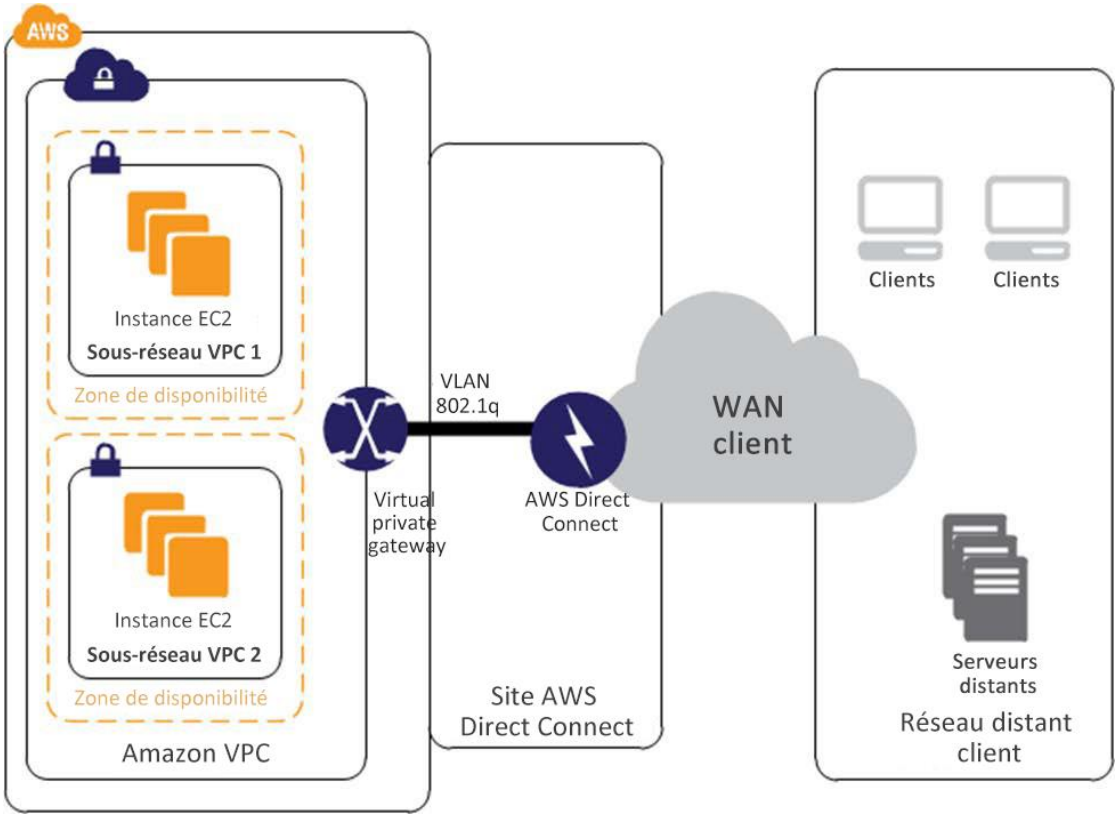

Figure 3 : AWS Direct Connect

Ressources supplémentaires

- Page produit d'AWS Direct Connect[5]
- Emplacements d'AWS Direct Connect[6]
- FAQ sur AWS Direct Connect[7]
- Mise en route d'AWS Direct Connect[8]

[5] http://aws.amazon.com/directconnect/

[6] http://aws.amazon.com/directconnect/#details

[7] http://aws.amazon.com/directconnect/faqs/

[8] http://docs.amazonwebservices.com/DirectConnect/latest/GettingStartedGuide/Welcome.html

AWS Direct Connect + VPN

Avec AWS Direct Connect + VPN, vous pouvez combiner une ou plusieurs connexions réseaux AWS Direct Connect dédiées avec le VPN hardware Amazon VPC. Cette combinaison fournit une connexion privée chiffrée IPsec qui diminue également les coûts du réseau, augmente le débit de la bande passante et offre une expérience réseau plus uniforme que des connexions VPN basées sur Internet.

Vous pouvez utiliser AWS Direct Connect pour établir une connexion réseau dédiée entre votre réseau et une connexion logique vers des ressources AWS publiques, comme un point de terminaison Amazon VGW IPsec. Cette solution combine les avantages de la gestion par AWS de la solution VPN hardware avec une faible latence, une bande passante augmentée, les atouts homogènes de la solution AWS Direct Connect, et une connexion IPsec intégrale et sécurisée. La figure 4 affiche cette option.

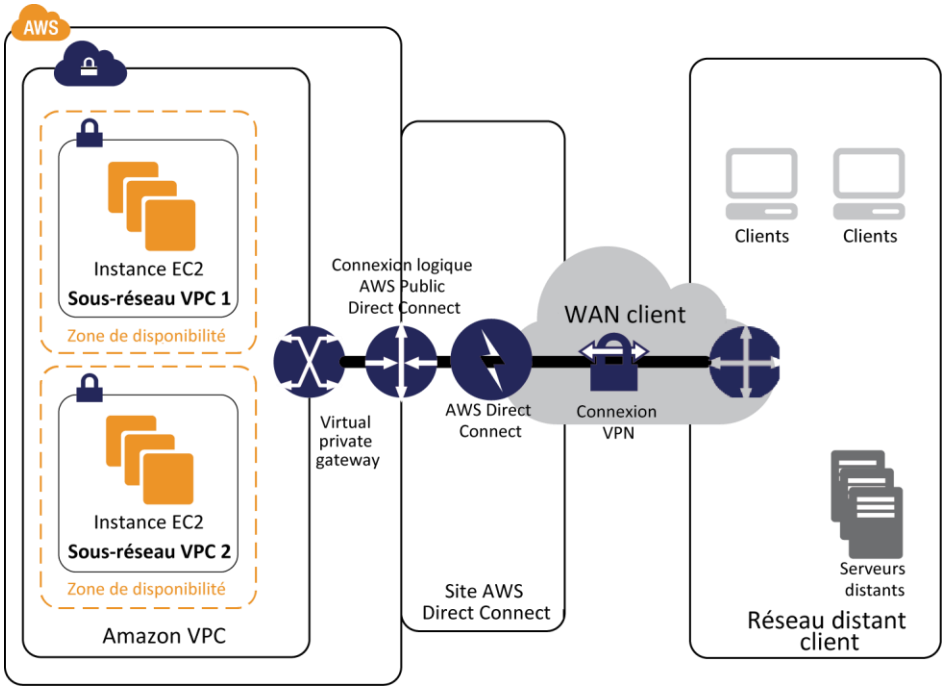

Figure 4 : AWS Direct Connect + VPN

Ressources supplémentaires

- Page produit d'AWS Direct Connect[9]
- FAQ sur AWS Direct Connect[10]
- Ajout d'une passerelle réseau privé virtuel matérielle à votre VPC

[9] http://aws.amazon.com/directconnect/

[10] http://aws.amazon.com/directconnect/faqs/

AWS VPN CloudHub

En vous appuyant sur le VPN hardware et les options AWS Direct Connect décrites précédemment, vous pouvez communiquer en toute sécurité d'un site à l'autre en utilisant AWS VPN CloudHub. L'AWS VPN CloudHub fonctionne sur un simple modèle en étoile (hub and spoke) que vous pouvez utiliser avec ou sans VPC. Utilisez ce modèle si vous avez plusieurs succursales et des connexions Internet existantes et si vous aimeriez implémenter un modèle en étoile (hub and spoke) pratique et potentiellement à bas coût pour une connectivité primaire ou de sauvegarde entre ces bureaux à distance.

La figure 5 décrit l'architecture d'AWS VPN CloudHub : les lignes pointillées bleues indiquent le trafic réseau entre les sites distants qui est acheminé via leurs connexions AWS VPN.

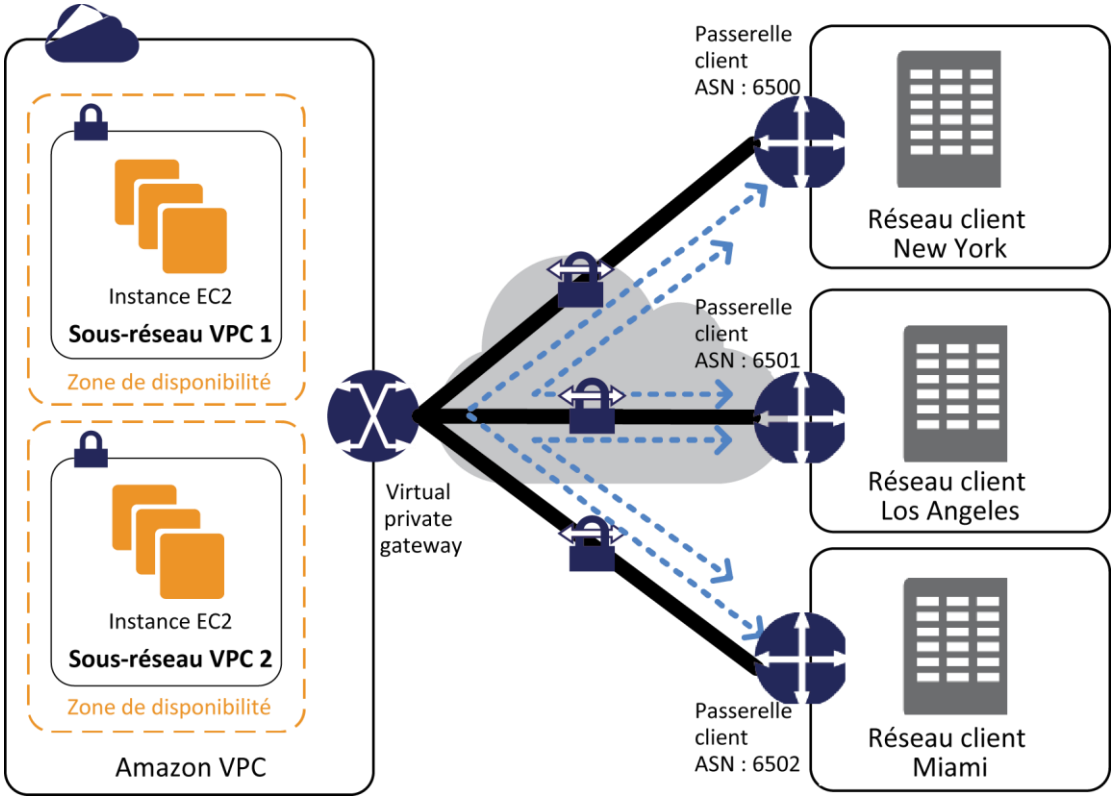

Figure 5 : AWS VPN CloudHub

AWS VPN CloudHub tire profit de la passerelle privée virtuelle Amazon VPC avec plusieurs passerelles, chacune utilisant des numéros de système autonome (ASN) BGP uniques. Vos passerelles publient les routes appropriées (préfixes BGP) via leurs connexions VPN. Ces annonces de routage sont reçues et republiées pour chaque appairage BGP, afin que chaque site puisse envoyer des données vers les autres sites et en recevoir. Les préfixes des réseaux distants pour chaque rayon doivent avoir des ASN uniques et les sites ne doivent pas avoir de plages d'adresses IP se chevauchant. Chaque site peut également envoyer des données au VPC et en recevoir comme s'ils utilisaient une connexion VPN standard.

Cette option peut être combinée avec AWS Direct Connect ou d'autres options de VPN hardware (par ex., plusieurs passerelles par site pour la redondance ou le routage d'ossature que vous fournissez), en fonction de vos exigences.

Ressources supplémentaires

- AWS VPN CloudHub[11]
- Guide d'Amazon VPC VPN
- Configuration requise pour le périphérique de la passerelle client[12]
- Périphériques de passerelle client connus pour fonctionner avec Amazon VPC[13]
- Page produit d'AWS Direct Connect[14]

[11] http://docs.amazonwebservices.com/AmazonVPC/latest/UserGuide/VPN_CloudHub.html

[12] http://aws.amazon.com/vpc/faqs/#C8

[13] http://aws.amazon.com/vpc/faqs/#C9

[14] http://aws.amazon.com/directconnect/

VPN Software

Amazon VPC vous offre la flexibilité nécessaire pour gérer les deux côtés de votre connectivité Amazon VPC en créant une connexion VPN entre votre réseau distant et une appliance VPN Software s'exécutant dans votre réseau Amazon VPC. Cette option est recommandée si vous devez gérer les deux extrémités d'une connexion VPN à des fins de conformité ou pour tirer profit des périphériques de passerelle qui sont actuellement incompatibles avec la solution VPN hardware d'Amazon VPC. La figure 6 affiche cette option.

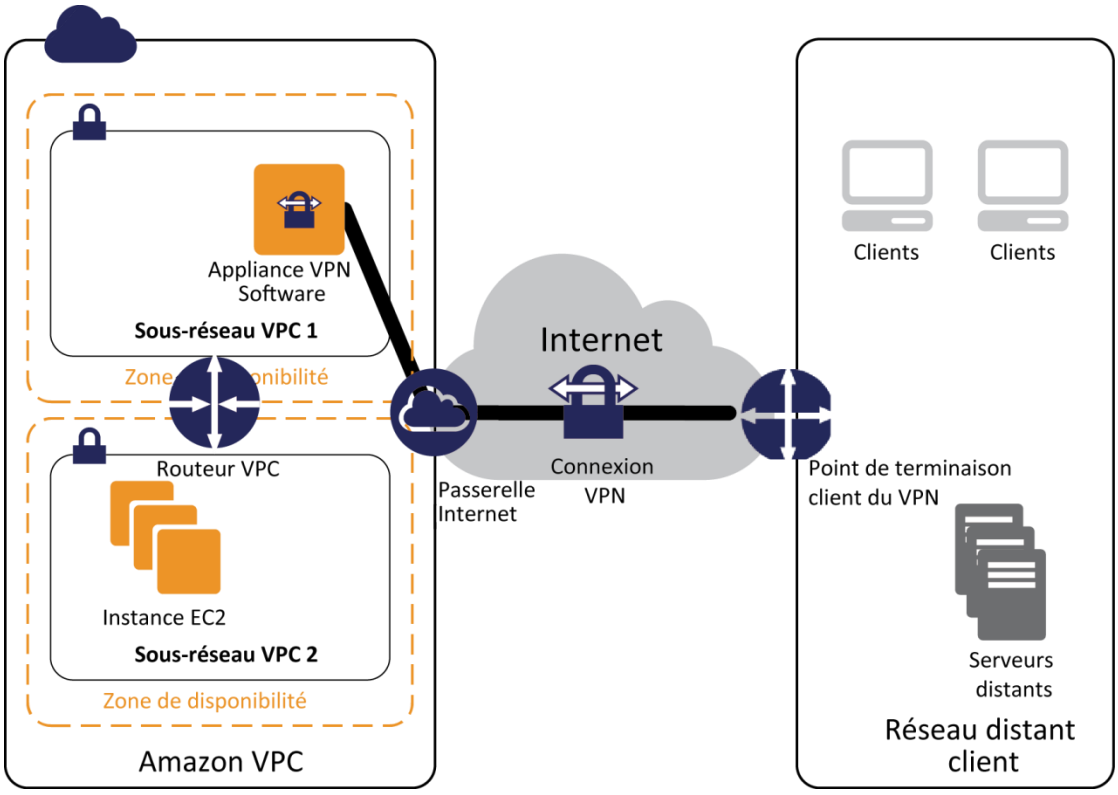

Figure 6 : VPN Software

Vous pouvez effectuer un choix entre un écosystème constitué de plusieurs partenaires et des communautés en Open source qui ont produit les appliances VPN Software qui s'exécutent sur Amazon EC2. Il s'agit de produits développés par des entreprises renommées dans la sécurité comme Check Point, Astaro, OpenVPN Technologies et Microsoft, ainsi que des outils populaires en Open source tels qu'OpenVPN, Openswan et IPsec-Tools. Avec ce choix, vous incombe la responsabilité de gérer l'appliance logicielle, ainsi que la configuration, les correctifs et les mises à niveau.

Veuillez noter que ce modèle introduit un point de défaillance potentiel unique dans la conception du réseau car l'appliance VPN Software s'exécute sur une seule instance Amazon EC2. Pour plus d'informations, consultez l'annexe A : Architecture de haut niveau à haute disponibilité pour les instances VPN Software.

Ressources supplémentaires

- Appliances VPN issues d'AWS Marketplace[15]
- Rappel technique - Connexion de Cisco ASA à l'instance VPC EC2 (IPsec)[16]
- Rappel technique - Connexion de plusieurs VPC avec des instances EC2 (IPsec)[17]
- Rappel technique - Connexion de plusieurs VPC avec des instances EC2 (SSL)[18]

[15] https://aws.amazon.com/marketplace/search/results/ref=brs_navgno_search_box?searchTerms=vpn

[16] http://aws.amazon.com/articles/8800869755706543

[17] Même si ces guides détaillent spécifiquement la connexion de plusieurs Amazon VPC, ils sont facilement adaptables à cette configuration réseau en remplaçant un des VPC par un périphérique VPN sur site se connectant à une appliance de VPN Software IPsec ou SSL, s'exécutant dans un Amazon VPC.

[18] http://aws.amazon.com/articles/0639686206802544

Options de connectivité d'Amazon VPC à Amazon VPC

Utilisez ces modèles de conception lorsque vous voulez intégrer plusieurs Amazon VPC à un réseau virtuel plus important. Ils sont utiles si vous avez besoin de plusieurs VPC pour des raisons de sécurité, de facturation, d'implantation dans plusieurs régions ou d'exigences de refacturation interne, afin d'intégrer plus facilement les ressources AWS entre les différents Amazon VPC. Vous pouvez également combiner ces modèles avec les Options de connectivité de réseau clients américains à Amazon VPC afin de créer un réseau d'entreprise qui s'étende aux réseaux distants et à plusieurs VPC.

La connectivité VPC entre les VPC est optimale en cas d'utilisation de plages d'adresses IP qui ne se chevauchent pas pour chaque VPC connecté. Par exemple, si vous voulez connecter plusieurs VPC, veillez à les configurer avec des plages uniques CIDR (Classless Inter-Domain Routing). Par conséquent, nous vous conseillons d'allouer à chaque VPC un bloc CIDR unique, contigu, sans chevauchement. Pour plus d'informations sur le routage et les contraintes d'Amazon VPC, reportez-vous aux FAQ sur Amazon VPC : http://aws.amazon.com/vpc/faqs/.

Option	Cas d'utilisation	Avantages	Limites
Appairage de VPC	Connectivité réseau fournie par AWS entre deux VPC dans une seule région.	• Tire profit de l'infrastructure de mise en réseau d'AWS dans une région • Ne s'appuie pas sur les instances VPN ou sur une pièce distincte de matériel physique • Ne présente pas de point de défaillance unique • Ne génère pas de goulet d'étranglement sur la bande passante	• Les connexions d'appairage ne sont actuellement prises en charge que dans une région AWS
VPN Software	Connexion VPN à base d'appliance logicielle entre des VPC	• Tire profit de l'équipement de mise en réseau d'AWS en région et dans les canaux Internet entre les régions • Compatibilité avec une vaste gamme de fournisseurs, produits et protocoles de VPN • Est géré entièrement par vos soins	• Vous êtes responsable de la mise en œuvre des solutions à haute disponibilité pour tous les points de terminaison du VPN (si nécessaire) • Les instances VPN peuvent devenir un goulet d'étranglement du réseau

Option	Cas d'utilisation	Avantages	Limites
VPN software-hardware	Connexion d'appliance logicielle à VPN hardware entre des VPC	• Tire profit de l'équipement de mise en réseau d'AWS en région et dans les canaux Internet entre les régions • Le point de terminaison géré par AWS inclut la redondance de centre de données multiples et le basculement automatique	• Vous êtes responsable de la mise en œuvre des solutions à haute disponibilité pour les points de terminaison du VPN de l'appliance logicielle (si nécessaire) • Les instances VPN peuvent devenir un goulet d'étranglement du réseau
VPN hardware	Routage de VPC à VPC géré par vous via des connexions VPN hardware IPsec, avec votre équipement et via Internet	• Réutilisation des connexions VPN Amazon VPC existantes • Le point de terminaison géré par AWS inclut la redondance de centre de données multiples et le basculement automatique • Compatible avec les routes statiques et l'appairage dynamique BGP et les stratégies de routage	• La latence, la variabilité et la disponibilité du réseau dépendent des conditions d'Internet • Le point de terminaison que vous gérez est chargé de mettre en œuvre la redondance et le basculement (si nécessaire)
AWS Direct Connect	Routage de VPC à VPC géré par vous avec votre équipement dans un emplacement AWS Direct Connect et via des lignes privées	• Performances homogènes du réseau • Coûts de bande passante réduits • Connexions configurées à 1 ou 10 Gb/s • Compatibilité avec les routes statiques et l'appairage BGP et les stratégies de routage	• Peut nécessiter la configuration de relations supplémentaires avec les fournisseurs d'hébergement et de téléphonie

Appairage de VPC

Une connexion d'appairage de VPC est une connexion réseau entre deux VPC qui vous permet le routage en utilisant les adresses IP privées de chaque VPC comme s'ils se trouvaient sur le même réseau. Il s'agit de la méthode recommandée par AWS pour la connexion de VPC dans une région. Les connexions d'appairage de VPC peuvent être créées entre vos propres VPC, ou avec un VPC situé dans un autre compte AWS au sein de la même région.

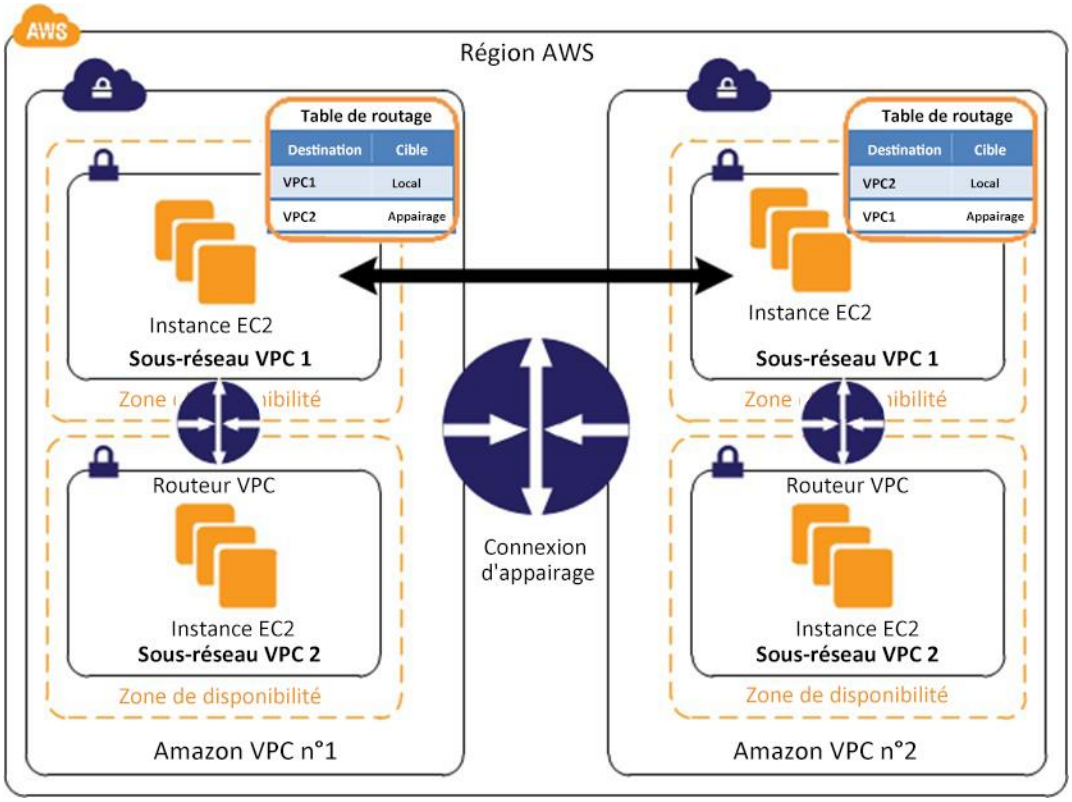

Figure 7 : Appairage de VPC à VPC

AWS utilise l'infrastructure existante d'un VPC pour créer des connexions d'appairage de VPC. Ces connexions ne sont ni une passerelle, ni une connexion VPN et elles ne reposent pas sur un équipement matériel distinct. Elles n'introduisent donc pas de point unique de défaillance potentiel, ni de goulet d'étranglement sur la bande passante du réseau entre les VPC. Par ailleurs, les tables de routage de VPC, les groupes de sécurité et les listes de contrôle d'accès au réseau peuvent être exploitées afin de contrôler les sous-réseaux ou les instances capables d'utiliser la connexion d'appairage de VPC.

Une connexion d'appairage de VPC peut faciliter le transfert des données entre les VPC. Vous pouvez les utiliser pour connecter les VPC lorsque vous avez plusieurs comptes AWS, pour connecter un VPC de gestion ou un VPC de services partagés aux VPC de l'application ou spécifiques du client, ou même pour vous connecter facilement au VPC d'un partenaire. Pour plus d'exemples de cas d'utilisation d'une connexion d'appairage de VPC, reportez-vous au Guide d'appairage d'Amazon VPC.[19]

Ressources supplémentaires

- Guide de l'utilisateur d'Amazon VPC[20]
- Guide d'appairage d'Amazon VPC

[19] http://docs.aws.amazon.com/AmazonVPC/latest/PeeringGuide/

[20] http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-peering.html

VPN Software

Amazon VPC offre la flexibilité du routage de réseau. Vous pouvez ainsi créer des tunnels VPN sécurisés entre deux ou plusieurs appliances VPN Software afin de connecter plusieurs VPC dans un réseau privé virtuel plus important, de sorte que les instances dans chaque VPC peuvent aisément se connecter les unes aux autres à l'aide des adresses IP privées. Cette option est recommandée lorsque vous souhaitez connecter des VPC sur plusieurs régions AWS et gérer les deux extrémités de la connexion VPN en faisant appel à votre fournisseur de VPN Software favori. Cette option utilise une passerelle Internet attachée à chaque VPC afin de faciliter la communication entre les appliances VPN Software.

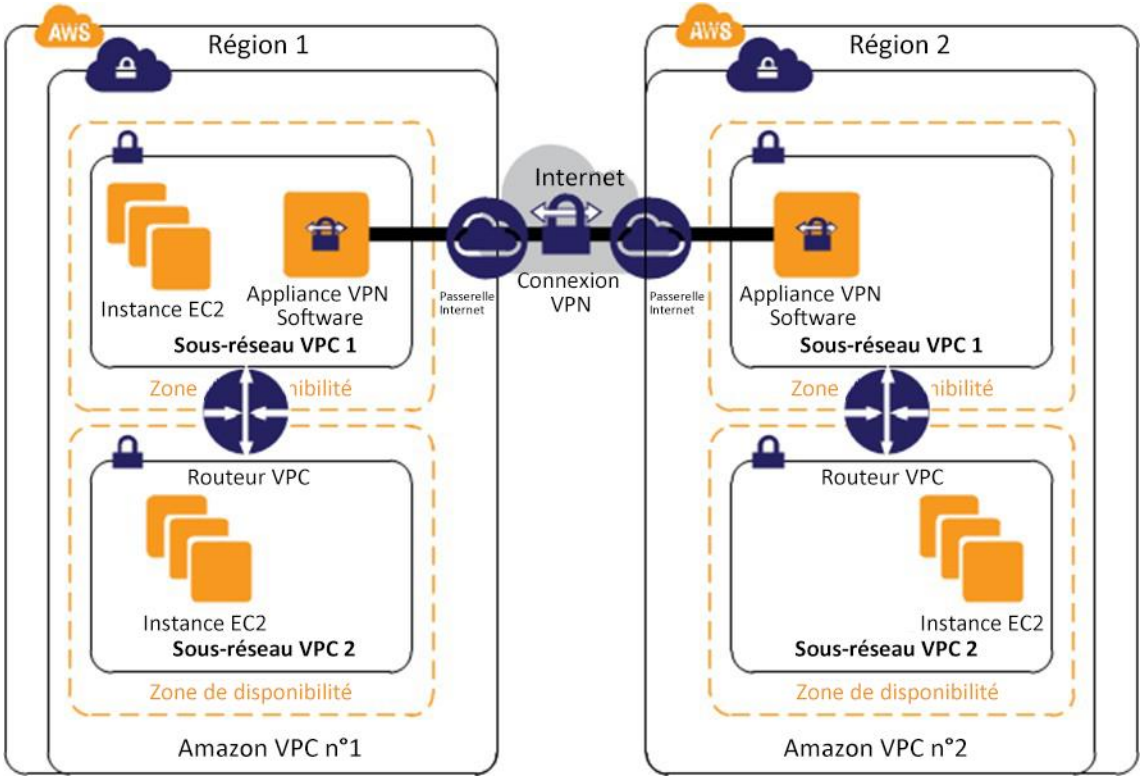

Figure 8 : Routage de VPC à VPC entre les régions

Vous pouvez effectuer un choix entre un écosystème constitué de plusieurs partenaires et des communautés en Open source qui ont produit les appliances VPN Software qui s'exécutent sur Amazon EC2. Il s'agit de produits développés par des entreprises renommées dans la sécurité comme Check Point, Sophos, OpenVPN Technologies et Microsoft, ainsi que des outils populaires en Open source tels qu'OpenVPN, Openswan et IPsec-Tools. Avec ce choix, vous incombe la responsabilité de gérer l'appliance logicielle, ainsi que la configuration, les correctifs et les mises à niveau.

Veuillez noter que ce modèle introduit un point de défaillance potentiel unique dans la conception du réseau car l'appliance VPN Software s'exécute sur une seule instance Amazon EC2. Pour plus d'informations, consultez l'annexe A : Architecture de haut niveau à haute disponibilité pour les instances VPN Software.

Ressources supplémentaires

- Appliances VPN issues d'AWS Marketplace
- Rappel technique - Connexion de plusieurs VPC avec des instances EC2 (IPsec)[21]
- Rappel technique - Connexion de plusieurs VPC avec des instances EC2 (SSL)[22]

VPN software-hardware

Amazon VPC offre la possibilité de combiner les options VPN hardware et VPN Software pour connecter plusieurs VPC. Avec cette configuration, vous pouvez créer des tunnels VPN sécurisés entre une appliance VPN Software et une passerelle privée virtuelle afin de connecter plusieurs VPC dans un réseau privé virtuel plus important, de sorte que les instances dans chaque VPC peuvent aisément se connecter les unes aux autres à l'aide des adresses IP privées. Cette option est recommandée lorsque vous souhaitez connecter des VPC dans plusieurs régions AWS et que vous voulez tirer profit du point de terminaison VPN hardware géré par AWS, qui comporte la redondance du centre de données multiples et le basculement automatiques intégrés du côté VGW de la connexion VPN. Cette option utilise une passerelle privée virtuelle dans un Amazon VPC et une combinaison de passerelle Internet et d'une appliance VPN Software dans un autre Amazon VPC, comme l'indique la figure 9.

[21] http://aws.amazon.com/articles/5472675506466066

[22] http://aws.amazon.com/articles/0639686206802544

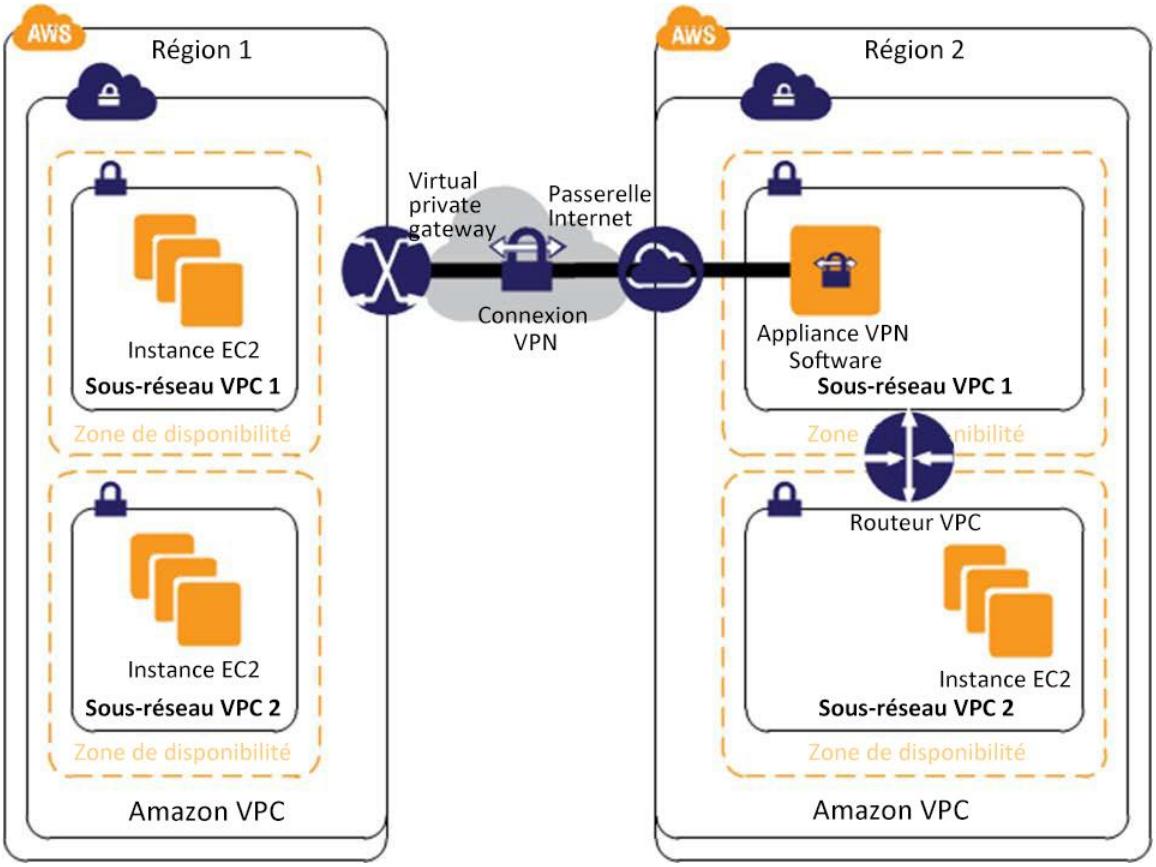

Figure 9 : Routage de VPC à VPC dans une région

Veuillez noter que ce modèle introduit un point de défaillance potentiel unique dans la conception du réseau car l'appliance Astaro Security Gateway s'exécute sur une seule instance Amazon EC2. Pour plus d'informations, consultez l'annexe A : Architecture de haut niveau à haute disponibilité pour les instances VPN Software.

Ressources supplémentaires

- Rappel technique - Connexion de plusieurs VPC avec Sophos Security Gateway[23]
- Configuration de Windows Server 2008 R2 en tant que passerelle client pour Amazon Virtual Private Cloud[24]

[23] http://aws.amazon.com/articles/1909971399457482

[24] http://docs.amazonwebservices.com/AmazonVPC/latest/UserGuide/CustomerGateway-Windows.html

VPN hardware

Amazon VPC offre la possibilité de créer un VPN hardware IPsec pour connecter vos réseaux distants à vos Amazon VPC via Internet. Vous pouvez tirer profit des multiples connexions VPN hardware pour router le trafic entre vos Amazon VPC, comme l'indique la figure 10.

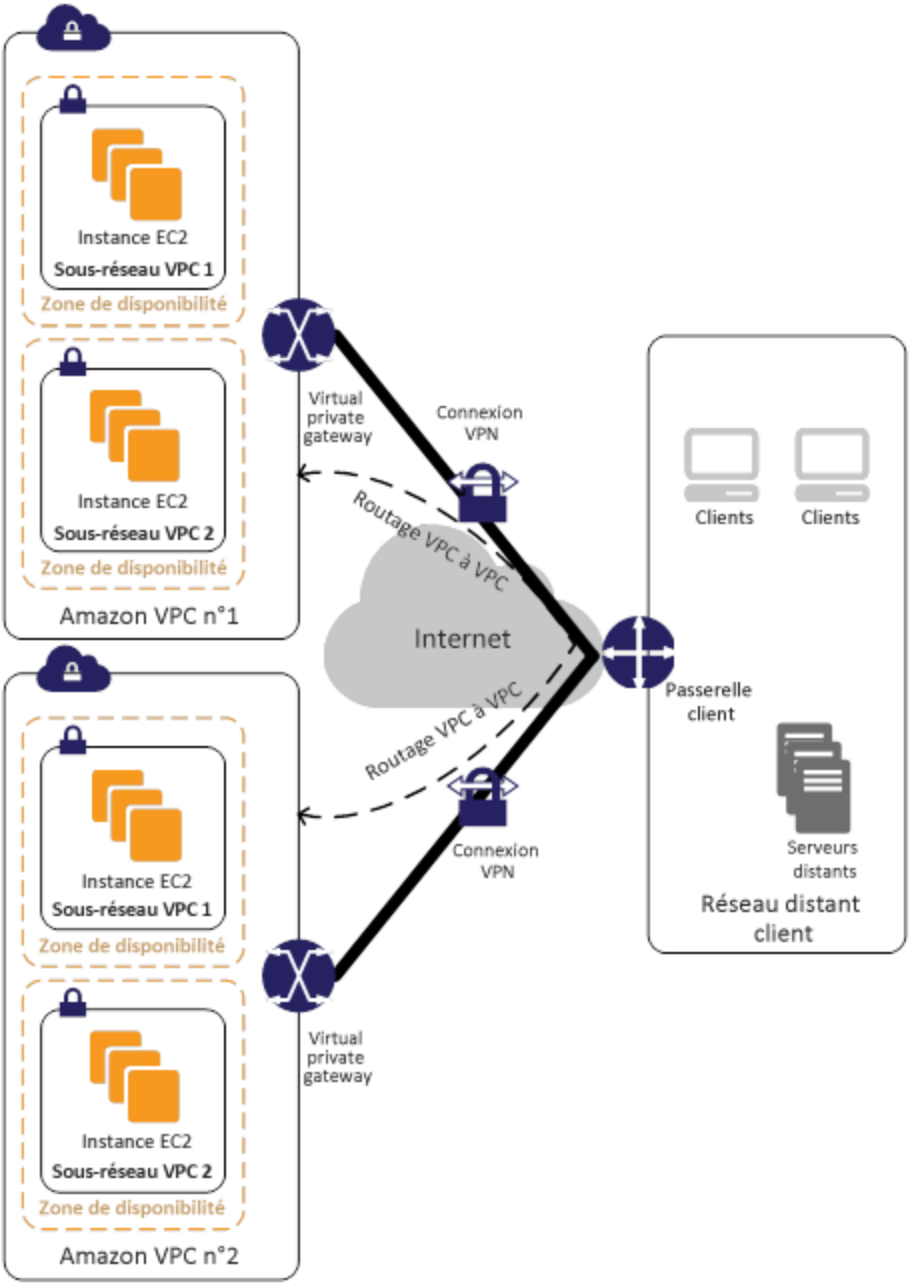

Figure 10 : Routage du trafic entre les VPC

Nous recommandons cette approche lorsque vous souhaitez tirer profit des points de terminaison VPN gérés par AWS, qui comportent la redondance du centre de données multiples et le basculement automatiques intégrés du côté AWS de chaque connexion VPN. Même si la figure ne le montre pas, Amazon VGW représente deux points de terminaison de VPN distincts, situés physiquement dans des centres de données séparés afin d'accroître la disponibilité de chaque connexion VPN.

Amazon VGW prend également en charge les connexions de passerelle client multiples (comme l'indiquent les sections Options de connexion du réseau client avec Amazon VPC et VPN hardware, ainsi que la figure 2), ce qui vous permet de mettre en œuvre la redondance et le basculement de votre côté de la connexion VPN. Cette solution peut également tirer parti de l'appairage BGP pour échanger les informations de routage entre AWS et ces points de terminaison distants. Vous pouvez spécifier des priorités, des stratégies et des poids (métriques) de routage dans vos annonces BGP, afin d'influencer le trafic du chemin d'accès réseau emprunté entre vos réseaux et AWS.

Du point de vue du routage, cette approche n'est pas optimale car le trafic doit passer par Internet pour aller et venir de votre réseau. Elle vous permet cependant de contrôler et de gérer le routage sur vos réseaux locaux et distants, ainsi que de réutiliser les connexions VPN hardware.

Ressources supplémentaires

- Guide de l'utilisateur d'Amazon VPC
- Configuration requise pour le périphérique de la passerelle client
- Périphériques de passerelle client connus pour fonctionner avec Amazon VPC
- Rappel technique - Connexion d'un seul routeur avec plusieurs VPC[25]

AWS Direct Connect

AWS Direct Connect facilite la mise en place d'une connexion réseau privée dédiée de vos locaux vers votre Amazon VPC ou les Amazon VPC. Cette option peut éventuellement réduire les coûts réseau, augmenter le débit de la bande passante et offrir une expérience réseau plus uniforme que les autres options de connectivité VPC à VPC.

Vous pouvez diviser une connexion AWS Direct Connect physique en plusieurs connexions logiques, une pour chaque VPC. Vous pouvez ensuite utiliser ces connexions logiques pour le trafic de routage entre les VPC, comme l'indique la figure 11. Outre le routage intra-régional, vous pouvez vous connecter à des emplacements AWS Direct Connect situés dans d'autres régions en utilisant vos fournisseurs de WAN existants et tirer parti d'AWS Direct Connect pour acheminer le trafic entre des régions sur votre réseau principal WAN.

[25] http://aws.amazon.com/articles/5458758371599914

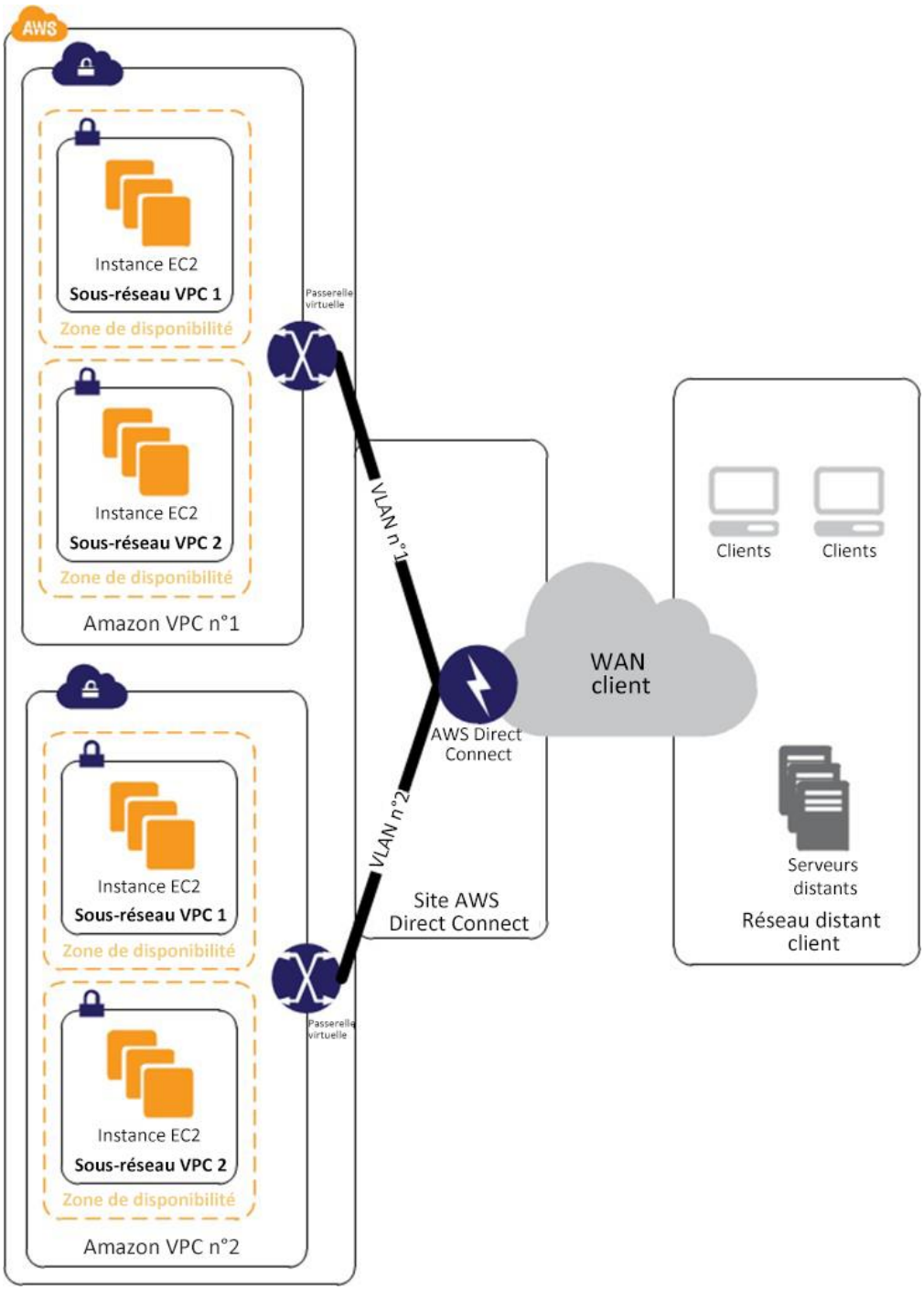

Figure 11 : Routage de VPC à VPC dans une région avec AWS Direct Connect

Nous recommandons cette approche si vous êtes déjà un client d'AWS Direct Connect ou si vous voulez profiter des coûts réseau réduits, du débit de la bande passante plus élevé et de l'expérience réseau plus uniforme d'AWS Direct Connect. AWS Direct Connect peut offrir un routage très rentable, car le trafic peut profiter des connexions par fibres à 1 Go ou 10 Go physiquement attachées au réseau AWS de chaque région. De plus, ce service vous offre une flexibilité optimale pour contrôler et gérer le routage sur vos réseaux locaux et distants, ainsi que la possibilité de réutiliser des connexions AWS Direct Connect.

Ressources supplémentaires

- Page produit d'AWS Direct Connect[26]
- Emplacements d'AWS Direct Connect[27]
- FAQ sur AWS Direct Connect[28]
- Mise en route d'AWS Direct Connect[29]

[26] http://aws.amazon.com/directconnect/

[27] http://aws.amazon.com/directconnect/#details

[28] http://aws.amazon.com/directconnect/faqs/

[29] http://docs.amazonwebservices.com/DirectConnect/latest/GettingStartedGuide/Welcome.html

Options de connectivité de l'utilisateur interne à Amazon VPC

L'accès utilisateur interne aux ressources d'Amazon VPC se fait généralement via les options de votre réseau vers Amazon VPC ou via les VPN Software d'accès à distance pour connecter les utilisateurs internes aux ressources VPC. La première option vous permet de réutiliser vos solutions existantes sur site et d'accès à distance pour gérer l'accès de l'utilisateur final, tout en offrant une expérience transparente de connexion aux ressources hébergées par AWS. Ce document n'a pas pour objectif de décrire plus en détail les solutions internes sur site et d'accès à distance que ne le fait déjà la section Options de connexion du réseau client avec Amazon VPC.

Avec le VPN Software d'accès à distance, vous pouvez tirer profit du faible coût, de l'élasticité et de la sécurité offerts par Amazon Web Services pour mettre en place des solutions d'accès distant tout en offrant une expérience transparente de connexion aux ressources hébergées par AWS. En outre, vous pouvez combiner les VPN Software d'accès distant avec vos options de connexion du réseau avec Amazon VPC pour fournir un accès distant aux réseaux internes, si nécessaire. Cette option est généralement choisie par les petites entreprises équipées de réseaux distants moins étendus ou qui n'ont pas encore créé ou déployé de solutions d'accès à distance pour leurs employés.

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

Option	Cas d'utilisation	Avantages	Limites
Options de connexion du réseau de l'utilisateur à Amazon VPC	Extension virtuelle de votre centre de données dans AWS	Tire parti des stratégies et technologies existantes internes de l'utilisateur final et d'accès à distance	Nécessite des implémentations existantes internes d'utilisateur final et d'accès à distance
Accès distant à VPN Software	Solution basée sur le cloud d'accès à distance vers Amazon VPC et/ou les réseaux internes	Tire parti des services web à faible coût, élastiques et sécurisés proposés par AWS pour la mise en place d'une solution d'accès à distance	Peut s'avérer redondant si des implémentations internes et d'accès à distance existent déjà

Accès distant à VPN Software

Vous pouvez effectuer votre choix dans un écosystème constitué de plusieurs partenaires et des communautés en Open source qui ont produit des solutions d'accès à distance qui s'exécutent sur Amazon EC2. Ces solutions incluent des produits développés par des entreprises renommées de sécurité comme Check Point, Sophos, OpenVPN Technologies et Microsoft. La figure 12 présente une solution simple d'accès à distance tirant profit de la base de données utilisateur interne à distance.

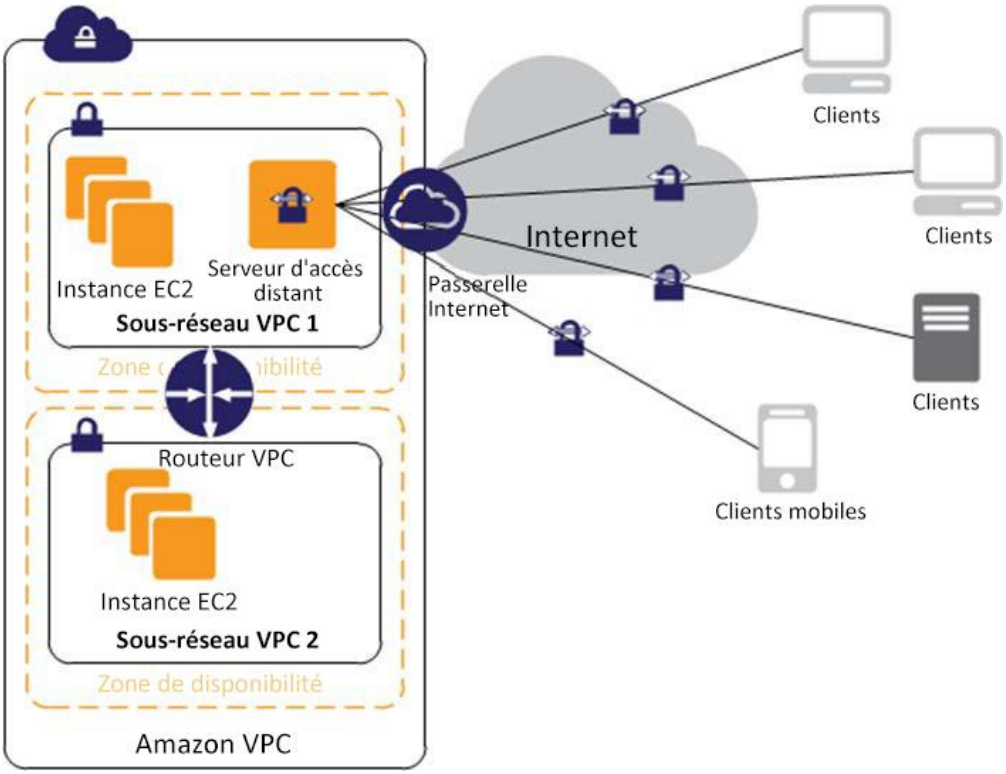

Figure 12 : Solution d'accès à distance

Les solutions d'accès à distance varient en termes de complexité, prennent en charge plusieurs options d'authentification du client (y compris l'authentification multi-facteurs) et peuvent être intégrées avec Amazon VPC ou avec des solutions de gestion d'accès et d'identité hébergées à distance (en exploitant une des options de connexion du réseau à Amazon VPC) comme Microsoft Active Directory ou d'autres solutions LDAP/d'authentification multi-facteurs. La figure 13 illustre cette combinaison permettant au serveur d'accès à distance de tirer parti des solutions de gestion d'accès interne, si nécessaire.

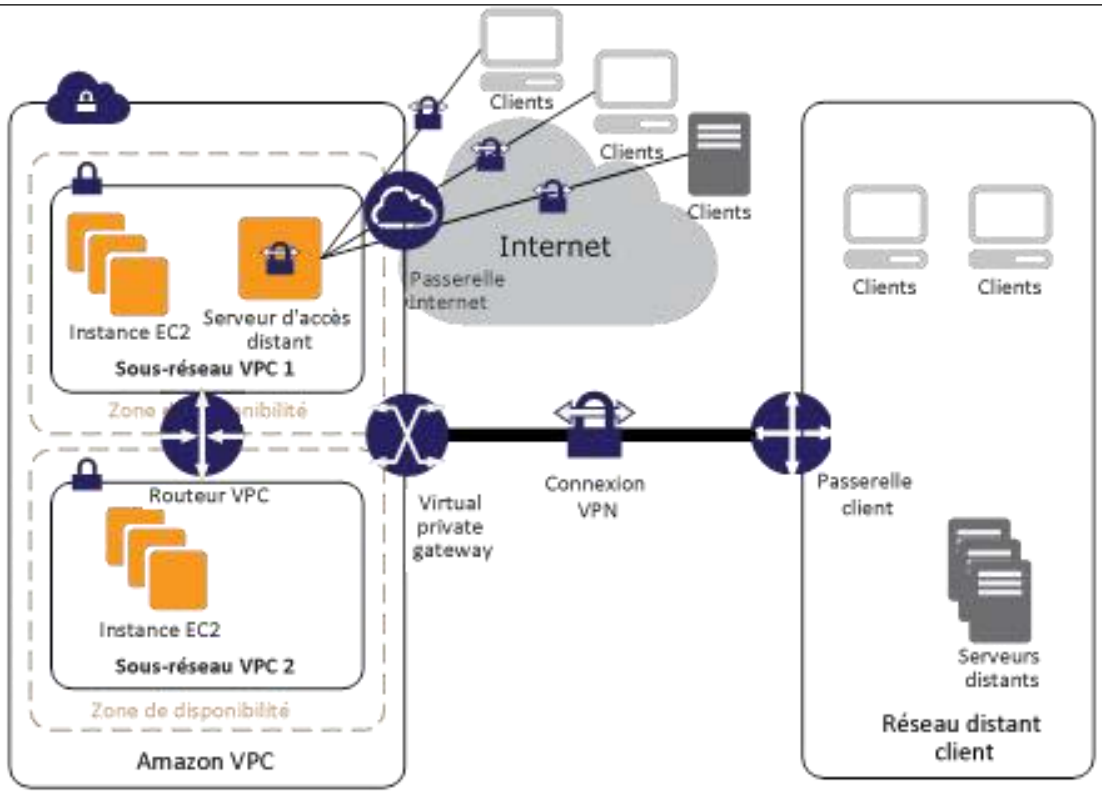

Figure 13 : Solution de combinaison d'accès à distance

Tout comme avec les options de VPN Software, le client est responsable de la gestion du logiciel d'accès à distance, notamment de la gestion de l'utilisateur, de la configuration, des correctifs et des mises à niveau. Par ailleurs, veuillez noter que ce modèle introduit un point de défaillance potentiel unique 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 l'annexe A : Architecture de haut niveau à haute disponibilité pour les instances VPN Software.

Ressources supplémentaires

- Appliances VPN issues d'AWS Marketplace
- Guide de démarrage rapide d'OpenVPN Access Server[30]

[30] http://docs.openvpn.net/how-to-tutorialsguides/virtual-platforms/amazon-ec2-appliance-ami-quick-start-guide/

Conclusion

AWS vous offre un certain nombre d'options de connectivité efficaces et sécurisées pour vous aider à profiter pleinement d'AWS lors de l'intégration de vos réseaux distants à Amazon VPC. Les options répertoriées dans ce livre blanc mettent en avant plusieurs options et schémas de connectivité dont certains ont grandement bénéficié pour intégrer, avec succès, leurs réseaux distants ou plusieurs réseaux Amazon VPC. Nous espérons que ces options vous aideront à choisir le mécanisme le plus approprié pour connecter l'infrastructure nécessaire pour exploiter votre activité, que celle-ci soit installée physiquement sur site ou hébergée.

Annexe A : Architecture de haut niveau à haute disponibilité pour les instances VPN Software

La création d'une connexion VPC résistante pour les instances VPN Software nécessite l'installation et la configuration de plusieurs instances VPN, ainsi qu'une instance de surveillance de l'état des connexions VPN.

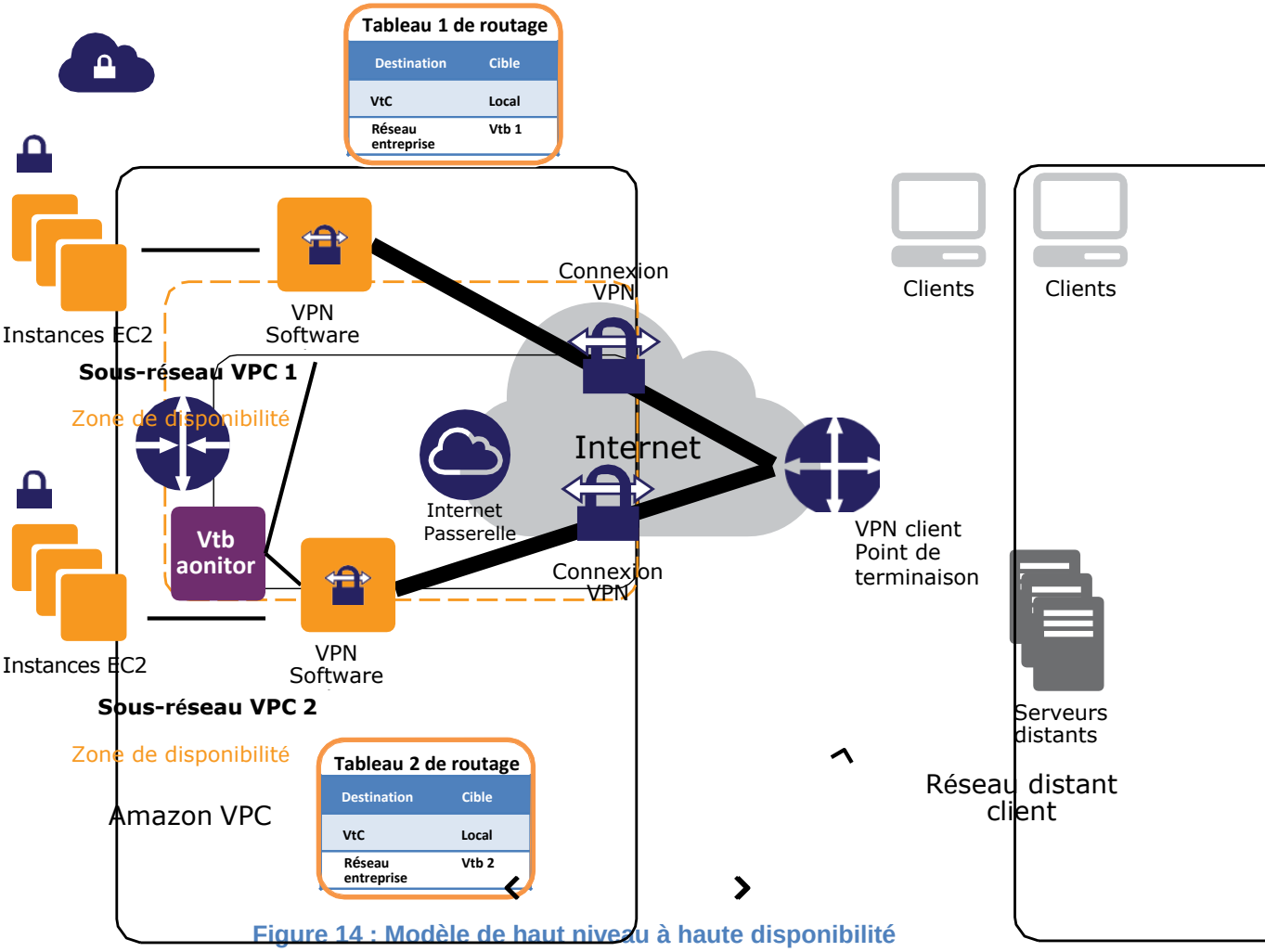

Figure 14 : Modèle de haut niveau à haute disponibilité

Nous vous recommandons de configurer vos tableaux de routage VPC de manière à tirer parti de toutes les instances VPN simultanément en dirigeant le trafic sortant de tous les sous-réseaux dans une zone de disponibilité via ses instances VPN correspondantes dans la même zone de disponibilité. Chaque instance de VPN fournira alors la connectivité VPN pour les instances qui partagent la même zone de disponibilité.

Instance(s) de supervision du VPN

Le contrôleur du VPN est une instance personnalisée qui vous sera nécessaire pour créer et développer des scripts de surveillance à exécuter. Cette instance est conçue pour s'exécuter et superviser l'état de la connexion VPN et des instances VPN. Si une instance ou une connexion VPN dysfonctionne, le contrôleur doit arrêter, résilier ou redémarrer l'instance VPN tout en redirigeant le trafic issu des sous-réseaux affectés vers l'instance VPN qui fonctionne, jusqu'à ce que les connexions soient de nouveau fonctionnelles. Etant donné que les exigences des clients varient, AWS ne fournit aucune consigne précise d'installation de cette instance de supervision. Un exemple de script d'activation des instances à haute disponibilité entre NAT peut toutefois être utilisé comme point de départ de création d'une solution à haute disponibilité pour les instances VPN Software. Prenez le temps de réfléchir à la logique business nécessaire pour déclencher une notification et/ou tenter de réparer automatiquement la connectivité au réseau en cas de panne d'une connexion VPN.