aws

Guide de l’utilisateur

AWS Site-to-Site VPN

AWS Site-to-Site VPN: Guide de l’utilisateur

Table of Contents

Qu'est-ce que c'est AWS Site-to-Site VPN ?

Par défaut, une instance que vous lancez au sein d'un Amazon VPC ne peut pas communiquer avec un réseau local (AWS Cloud) et un appareil distant. Par exemple, il peut s'agir d'un site ou d'un appareil sur site. Vous pouvez activer l'accès à vos appareils distants depuis votre VPC en créant une connexion AWS Site-to-Site VPN(Site-to-Site VPN) et en configurant le routage pour faire passer le trafic via cette connexion.

Bien que le terme connexion VPN soit un terme général, dans cette documentation, une connexion VPN fait référence à la connexion entre votre VPC et votre propre réseau local. Site-to-Site Le VPN prend en charge les connexions VPN de sécurité par protocole Internet (IPsec).

Table des matières

Concepts

Les concepts clés du Site-to-Site VPN sont les suivants :

- Connexion VPN : connexion sécurisée entre votre équipement sur site et votre VPCs.
- Tunnel VPN : lien chiffré où les données peuvent transiter par le réseau client vers ou depuis AWS.

  Chaque connexion VPN comprend deux tunnels VPN que vous pouvez utiliser simultanément pour une haute disponibilité.
- Passerelle client :AWS ressource qui fournit des informations AWS sur votre dispositif de passerelle client.
- Dispositif de passerelle client : appareil physique ou application logicielle situé de votre côté de la connexion Site-to-Site VPN.
- Passerelle cible : terme générique désignant le point de terminaison VPN du côté Amazon de la connexion Site-to-Site VPN.

- Passerelle privée virtuelle : une passerelle privée virtuelle est le point de terminaison VPN du côté Amazon de votre connexion Site-to-Site VPN qui peut être rattaché à un seul VPC.
- Passerelle de transit : hub de transit qui peut être utilisé pour interconnecter plusieurs VPCs réseaux locaux et comme point de terminaison VPN pour le côté Amazon de la Site-to-Site connexion VPN.
- Tunnel à large bande passante : configuration de tunnel qui prend en charge une bande passante maximale de 5 Gbit/s par tunnel, contre 1,25 Gbit/s standard. Disponible pour les connexions VPN connectées à Transit Gateway ou Cloud WAN.

Site-to-Site Fonctionnalités du VPN

Les fonctionnalités suivantes sont prises en charge sur AWS Site-to-Site VPN les connexions :

- Échange de clés Internet version 2 (IKEv2)
- NAT Traversal
- ASN à 4 octets compris entre 1 et 2147483647 pour une configuration de passerelle privée virtuelle (VGW). Pour plus d'informations, consultez Options de passerelle client pour votre AWS Site-to-Site VPN connexion.
- ASN à 2 octets pour Customer Gateway (CGW) compris entre 1 et 65 535. Pour plus d'informations, consultez Options de passerelle client pour votre AWS Site-to-Site VPN connexion.
- CloudWatch métriques
- Adresses IP réutilisables pour vos passerelles client
- Options de chiffrement supplémentaires, notamment chiffrement AES 256 bits, hachage SHA-2 et groupes Diffie-Hellman supplémentaires
- Options de tunnel configurables
- ASN privé personnalisé pour le côté Amazon d'une session BGP
- Certificat privé d'une autorité de certification subordonnée de Autorité de certification privée AWS
- Support pour le IPv6 support pour le AWS Site-to-Site VPN
  - IPv6 pour les adresses IP du tunnel interne (IP du paquet)
  - IPv6 pour les adresses IP des tunnels extérieurs (IP des tunnels) sur Transit Gateway et Cloud WAN
- Support de IPv6 migration complet avec les combinaisons suivantes :
  - IPv6 IP du tunnel extérieur avec IP du paquet IPv6 intérieur (IPv6-in-IPv6)

- IPv6 IP du tunnel extérieur avec IP du paquet IPv4 intérieur (IPv4-in-IPv6)

Site-to-Site Limites du VPN

Les limites d'une connexion Site-to-Site VPN sont les suivantes.

- IPv6 le trafic n'est pas pris en charge pour les connexions VPN sur une passerelle privée virtuelle. IPv6 pour le tunnel extérieur n' IPs est pris en charge que sur Transit Gateway et Cloud WAN.
- Une Site-to-Site VPN connexion ne prend pas en charge Path MTU Discovery.
- Une seule connexion Site-to-Site VPN ne peut pas prendre en charge à la fois IPv6 le trafic IPv4 et le trafic. Vous avez besoin de connexions VPN distinctes pour le transport IPv4 et IPv6 les paquets.
- Les connexions VPN IP privées ne prennent pas en charge IPv6 les adresses pour le tunnel extérieur IPs.
- Vous ne pouvez pas modifier une connexion IPv4 VPN existante pour l'utiliser IPv6. Vous devez supprimer la connexion existante et en créer une nouvelle.

En outre, tenez compte des points suivants lorsque vous utilisez Site-to-Site un VPN.

- Lorsque vous vous connectez VPCs à un réseau local commun, nous vous recommandons d'utiliser des blocs CIDR qui ne se chevauchent pas pour vos réseaux.

Site-to-Site Ressources VPN

Vous pouvez créer, accéder et gérer vos ressources Site-to-Site VPN à l'aide de l'une des interfaces suivantes :

- Console de gestion AWS— Fournit une interface Web que vous pouvez utiliser pour accéder à vos ressources Site-to-Site VPN.
- AWS Command Line Interface(AWS CLI) — Fournit des commandes pour un large éventail de AWS services, y compris Amazon VPC, et est compatible avec Windows, macOS et Linux. Les lignes de commande sont incluses dans la AWS Site-to-Site VPN référence de ligne de commande plus large EC2
  - Pour des informations générales sur l'interface de ligne de commande, consultez AWS Command Line Interface.

- Pour la liste des EC2 commandes disponibles, y compris les commandes Site-to-Site VPN, consultez la section Référence de ligne de EC2 commande.

  > **Note**
  >
  > La référence à la ligne de commande ne fait pas la différence entre les commandes Site-to-Site VPN et le plus grand ensemble de EC2 commandes

- AWS SDKs— Fournissez des informations spécifiques à la langue APIs et prend en charge de nombreux détails de connexion, tels que le calcul des signatures, la gestion des nouvelles tentatives de demande et la gestion des erreurs. Pour de plus amples informations, veuillez consulter AWS SDKs.
- API de requête : Fournit des actions d'API de bas niveau appelées à l'aide de demandes HTTPS. L'utilisation de l'API de requête est le moyen le plus direct d'accéder à Amazon VPC;, mais elle nécessite que votre application gère les détails de bas niveau, tels que la génération d'un hachage pour signer la demande et le traitement des erreurs. Pour plus d'informations, consultez le Amazon EC2 API Reference.

Tarification

Vous êtes facturé pour chaque heure de connexion VPN pendant laquelle votre connexion VPN est fournie et disponible. Pour plus d'informations, consultez AWS Site-to-Site VPN la section Tarification de la connexion Site-to-Site VPN accélérée.

Le transfert de données depuis Amazon EC2 vers Internet vous est facturé. Pour plus d'informations, consultez la section Transfert de données sur la page de tarification d' EC2 Amazon On-Demand.

Lorsque vous créez une connexion VPN accélérée, nous créons et gérons deux accélérateurs en votre nom. Vous êtes facturé à un tarif horaire et aux frais de transfert de données pour chaque accélérateur. Pour en savoir plus, consultez Pricing AWS Global Accelerator (Tarification).

L'utilisation d' IPv6 adresses avec vos connexions Site-to-Site VPN ne comporte aucun frais supplémentaire.

Comment ? AWS Site-to-Site VPN fonctionnement

Une connexion Site-to-Site VPN comprend les éléments suivants :

- Une passerelle réseau privé virtuel ou une passerelle de transit
- Un périphérique de passerelle client
- Une passerelle client

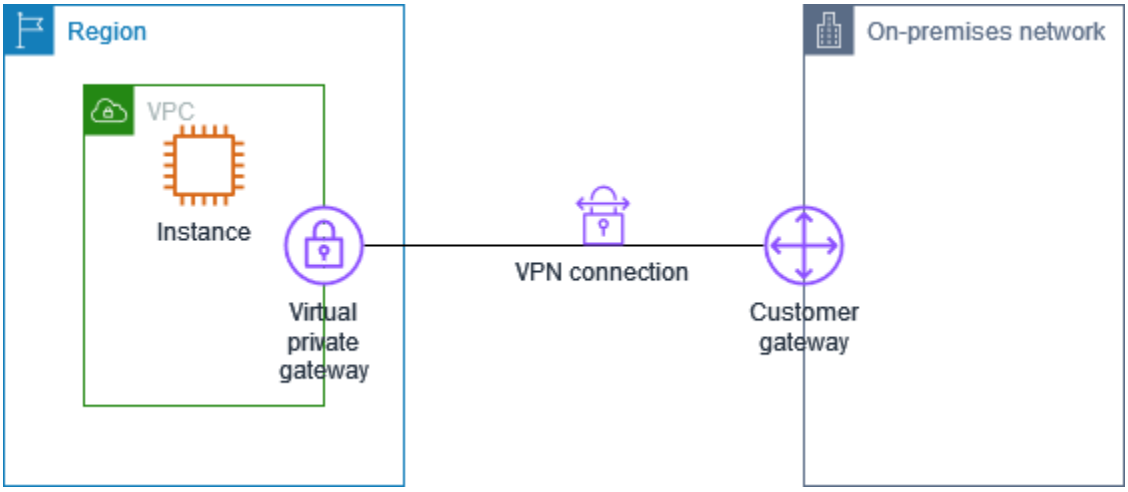
La connexion VPN propose deux tunnels VPN entre une passerelle privée virtuelle ou une passerelle de transit sur le AWS côté, et une passerelle client sur site.

Pour plus d'informations sur les quotas Site-to-Site VPN, consultezAWS Site-to-Site VPN quotas.

Passerelle réseau privé virtuel

Une passerelle privée virtuelle est le concentrateur Site-to-Site VPN situé du côté Amazon de la connexion Site-to-Site VPN. Vous créez une passerelle privée virtuelle et vous l'associez à un cloud privé virtuel (VPC) avec des ressources qui doivent accéder à la Site-to-Site connexion VPN.

Le schéma suivant montre une connexion VPN entre un VPC et votre réseau sur site à l'aide d'une passerelle réseau privé virtuel.



Lorsque vous créez une passerelle réseau privé virtuel, vous pouvez spécifier le numéro d'ASN (Autonomous System Number) privé pour le côté Amazon de la passerelle. Si vous ne spécifiez pas d'ASN, la passerelle réseau privé virtuel est créée avec l'ASN par défaut (64512). Une fois la passerelle réseau privé virtuel créée, vous ne pouvez pas modifier l'ASN. Pour vérifier l'ASN de votre

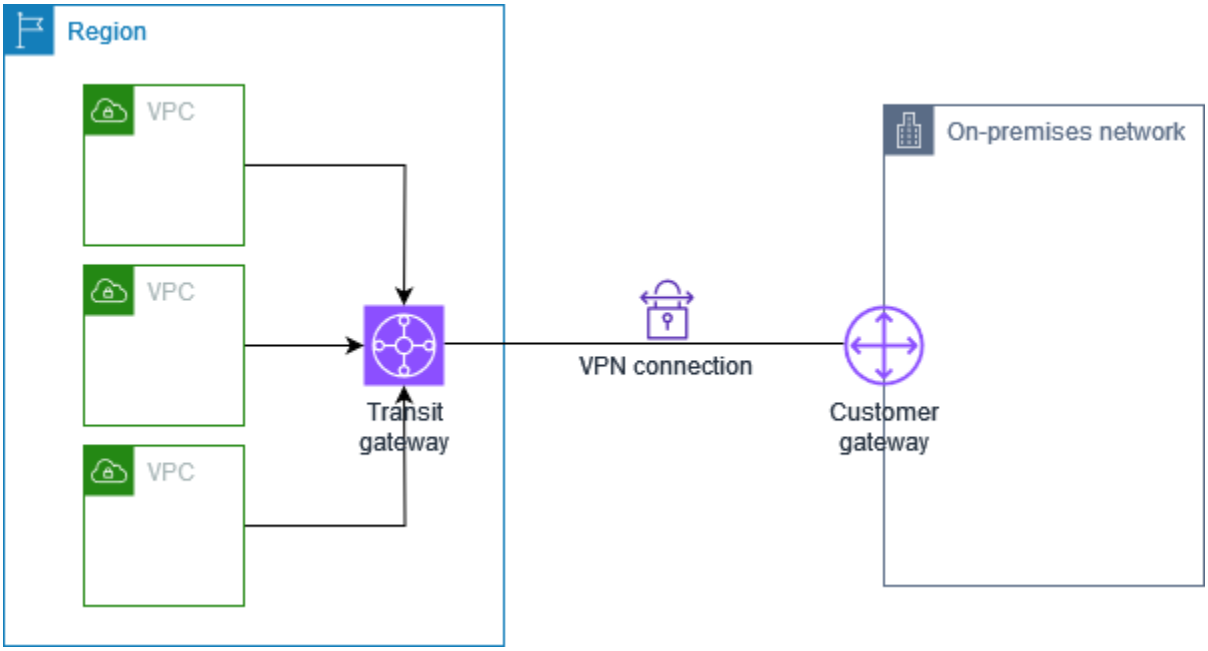
passerelle réseau privé virtuel, affichez ses informations sur la page Passerelles réseau privé virtuel de la console Amazon VPC ou utilisez la commande describe-vpn-gateways (AWS CLI).

> **Note**
>
> Les passerelles privées virtuelles ne prennent pas en charge le protocole IPv6 pour les connexions Site-to-Site VPN. Si vous avez besoin du support IPv6, utilisez une passerelle de transit ou un Cloud WAN pour votre connexion VPN.

Passerelle de transit

Une passerelle de transit est un hub de transit que vous pouvez utiliser pour relier vos VPC et vos réseaux sur site. Pour plus d'informations, consultez Passerelles de transit Amazon VPC. Vous pouvez créer une connexion Site-to-Site VPN en tant que pièce jointe sur une passerelle de transit.

Le schéma suivant montre une connexion VPN entre plusieurs VPC et votre réseau sur site à l'aide d'une passerelle de transit. La passerelle de transit comporte trois attachements de VPC et un attachement de VPN.



Votre connexion Site-to-Site VPN sur une passerelle de transit peut prendre en charge le trafic IPv4 ou IPv6 à l'intérieur des tunnels VPN (adresses IP internes). En outre, les passerelles de transit prennent en charge les adresses IPv6 pour les adresses IP des tunnels extérieurs. Pour de plus amples informations, veuillez consulter IPv4 et IPv6 trafic entrant AWS Site-to-Site VPN.

Vous pouvez modifier la passerelle cible d'une connexion Site-to-Site VPN d'une passerelle privée virtuelle à une passerelle de transit. Pour de plus amples informations, veuillez consulter the section called "Modification de la passerelle cible d'une connexion VPN".

Périphérique de passerelle client

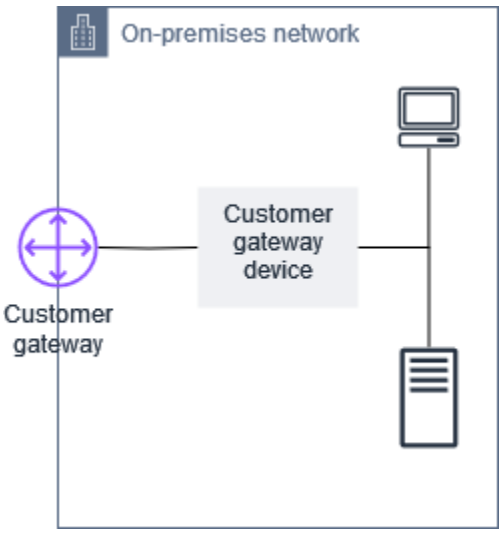
Un dispositif de passerelle client est un appareil physique ou une application logicielle qui se trouve de votre côté de la connexion Site-to-Site VPN. Vous configurez l'appareil pour qu'il fonctionne avec la connexion Site-to-Site VPN. Pour de plus amples informations, veuillez consulter AWS Site-to-Site VPN dispositifs de passerelle client.

Par défaut, votre dispositif de passerelle client doit ouvrir les tunnels pour votre connexion Site-to-Site VPN en générant du trafic et en lançant le processus de négociation IKE (Internet Key Exchange). Vous pouvez configurer votre connexion Site-to-Site VPN pour spécifier qui AWS doit plutôt lancer le processus de négociation IKE. Pour de plus amples informations, veuillez consulter AWS Site-to-Site VPN options d'initiation du tunnel.

Si vous utilisez IPv6 pour les adresses IP des tunnels extérieurs, votre dispositif de passerelle client doit prendre en charge l'adressage IPv6 et être en mesure d'établir des tunnels IPsec avec des points de terminaison IPv6.

Passerelle client

Une passerelle client est une ressource que vous créez dans AWS et qui représente le périphérique de passerelle client dans votre réseau local. Lorsque vous créez une passerelle client, vous fournissez des informations sur votre appareil à AWS. Pour de plus amples informations, veuillez consulter the section called "Options de passerelle client".



Pour utiliser Amazon VPC avec une connexion Site-to-Site VPN, vous ou votre administrateur réseau devez également configurer le dispositif ou l'application de passerelle client sur votre réseau distant. Lorsque vous créez la connexion Site-to-Site VPN, nous vous fournissons les informations de configuration requises et c'est généralement votre administrateur réseau qui effectue cette configuration. Pour plus d'informations sur les exigences et la configuration de la passerelle client, consultez AWS Site-to-Site VPN dispositifs de passerelle client.

Passerelle client IPv6

Lorsque vous créez une passerelle client à utiliser avec les adresses IP des tunnels extérieurs IPv6, vous spécifiez une adresse IPv6 au lieu d'une adresse IPv4. Vous pouvez créer une passerelle client IPv6 à l'aide de la console AWS de gestion ou de la AWS CLI.

Pour créer une passerelle client IPv6 à l'aide de la AWS CLI, utilisez la commande suivante :

```
aws ec2 create-customer-gateway --Ipv6-address 2001:0db8:85a3:0000:0000:8a2e:0370:7334
 --bgp-asn 65051 --type ipsec.1 --region us-west-1
```

L'adresse IPv6 doit être une adresse IPv6 valide et routable par Internet pour votre dispositif de passerelle client.

Connexions VPN IPv6

Site-to-Site Les connexions VPN prennent en charge les configurations IPv6 suivantes :

- Tunnel extérieur IPv4 avec paquets internes IPv4 : fonctionnalité VPN IPv4 de base prise en charge sur Virtual Private Gateway (VGW), Transit Gateway (TGW) et Cloud WAN.

- Tunnel extérieur IPv4 avec paquets internes IPv6 : autorise l'IPv6 applications/transport dans le tunnel VPN. Pris en charge sur TGW et Cloud WAN (non pris en charge sur VGW).
- Tunnel extérieur IPv6 avec paquets internes IPv6 - Permet une migration IPv6 complète avec des adresses IPv6 pour les adresses IP du tunnel extérieur et les adresses IP des paquets internes. Pris en charge sur TGW et Cloud WAN.
- Tunnel extérieur IPv6 avec paquets internes IPv4 : autorise l'adressage du tunnel extérieur IPv6 tout en prenant en charge les applications IPv4 existantes au sein du tunnel. Pris en charge sur TGW et Cloud WAN.

Pour créer une connexion VPN avec les adresses IP des tunnels extérieurs IPv6, vous devez le spécifier `OutsideIPAddressType=Ipv6` lors de la création de la connexion VPN. AWS configure automatiquement les adresses IPv6 des tunnels extérieurs pour le côté AWS des tunnels VPN.

Exemple de commande CLI pour créer une connexion VPN avec des adresses IP de tunnel extérieur IPv6 et des adresses IP de tunnel interne IPv6 :

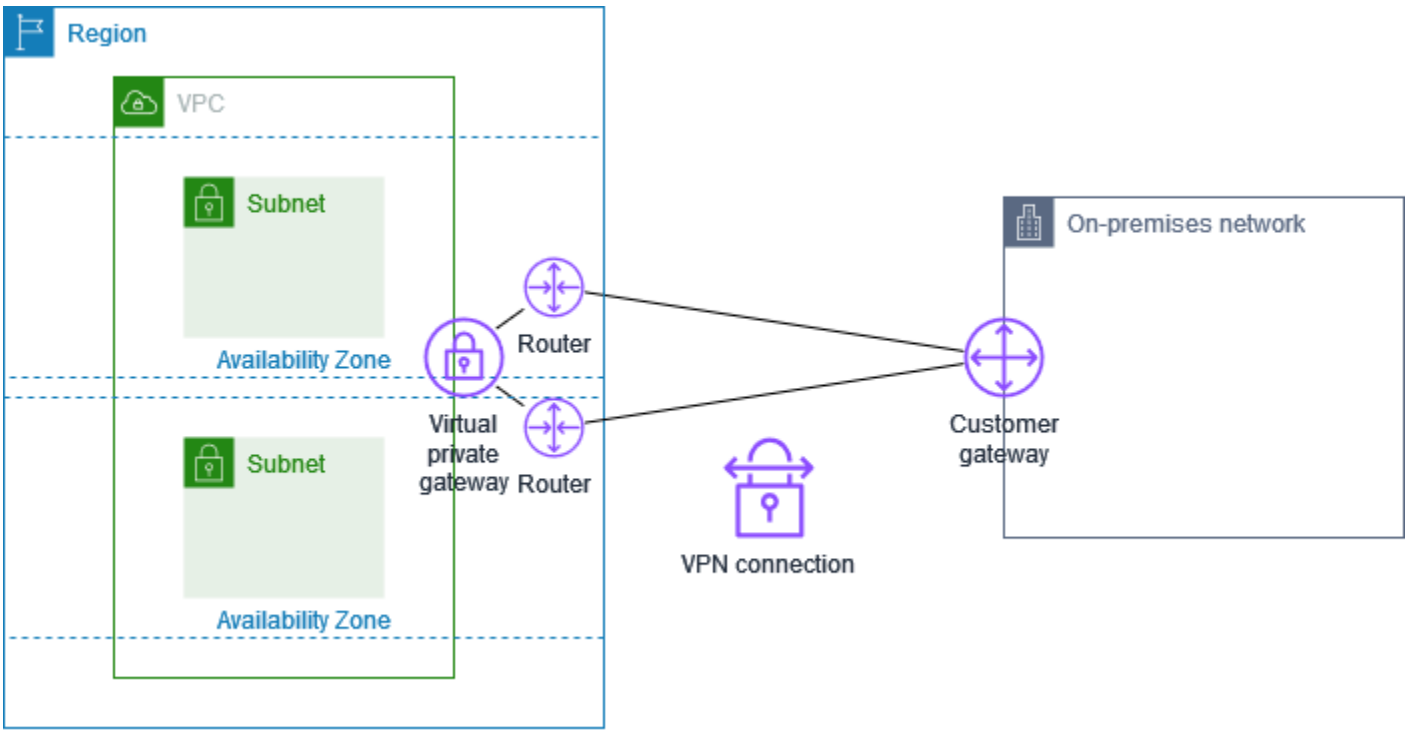
```
aws ec2 create-vpn-connection --type ipsec.1 --transit-gateway-id
 tgw-12312312312312312 --customer-gateway-id cgw-001122334455aabbc --options
 OutsideIPAddressType=Ipv6,TunnelInsideIpVersion=ipv6,TunnelOptions=[{StartupAction=start},
{StartupAction=start}]
```

Vous pouvez consulter les adresses IPv6 attribuées à votre connexion VPN à l'aide de la commande `describe-vpn-connection` CLI.

Options de tunnel pour votre AWS Site-to-Site VPN connexion

Vous utilisez une connexion Site-to-Site VPN pour connecter votre réseau distant à un VPC. Chaque connexion Site-to-Site VPN possède deux tunnels, chaque tunnel utilisant une adresse IP publique unique. Il est important de configurer deux tunnels pour la redondance. Lorsqu'un tunnel devient indisponible (par exemple, en cas d'arrêt pour maintenance), le trafic réseau est automatiquement acheminé vers le tunnel disponible pour cette connexion Site-to-Site VPN spécifique.

Le schéma suivant illustre les deux tunnels d'une connexion VPN. Chaque tunnel se termine dans une zone de disponibilité différente afin d'améliorer la disponibilité. Le trafic provenant du réseau local AWS utilise les deux tunnels. Le trafic AWS en provenance du réseau local préfère l'un des tunnels, mais peut automatiquement basculer vers l'autre tunnel en cas de défaillance AWS latérale.



Lorsque vous créez une connexion Site-to-Site VPN, vous téléchargez un fichier de configuration spécifique à votre dispositif de passerelle client qui contient des informations pour configurer l'appareil, notamment des informations pour configurer chaque tunnel. Vous pouvez éventuellement spécifier vous-même certaines options du tunnel lorsque vous créez la connexion Site-to-Site VPN. Sinon, AWS fournit des valeurs par défaut.

Options de bande passante du tunnel

Vous pouvez configurer la capacité de bande passante de vos tunnels VPN :

- Bande passante standard : jusqu'à 1,25 Gbit/s par tunnel (par défaut)
- Tunnel à large bande passante (LBT) : jusqu'à 5 Gbit/s par tunnel

Les tunnels à large bande passante ne sont disponibles que pour les connexions VPN connectées à Transit Gateway ou Cloud WAN. Pour de plus amples informations, veuillez consulter Tunnels à large bande passante.

> **Note**
>
> Site-to-Site Les points de terminaison du tunnel VPN évaluent les propositions provenant de votre passerelle client en commençant par la valeur configurée la plus faible de la liste

ci-dessous, quelle que soit la commande de proposition émanant de la passerelle client. Vous pouvez utiliser la `modify-vpn-connection-options` commande pour restreindre la liste des options que les AWS points de terminaison accepteront. Pour plus d'informations, consultez modify-vpn-connection-options dans Amazon EC2 Command Line Reference (Référence de ligne de commande Amazon EC2).

Tunnels à large bande passante

Les tunnels à large bande passante vous permettent de configurer des tunnels Site-to-Site VPN qui prennent en charge jusqu'à 5 Gbit/s de bande passante par tunnel, contre 1,25 Gbit/s standard. Des tunnels à large bande passante sont disponibles pour les connexions VPN connectées à Transit Gateway ou Cloud WAN. Cela élimine ou réduit le besoin de déployer des protocoles complexes tels que l'ECMP (Equal Cost Multi Path) pour obtenir une bande passante plus élevée et garantir une bande passante de tunnel constante de 5 Gbit/s par tunnel. Les tunnels à large bande passante sont conçus pour être utilisés dans les cas d'utilisation suivants :

- Connectivité des centres de données : Supportez les applications hybrides gourmandes en bande passante, les migrations de mégadonnées ou les architectures de reprise après sinistre qui nécessitent une connectivité à haute capacité entre les charges de travail AWS et les centres de données sur site.
- Sauvegarde Direct Connect : fournissez une connectivité de sauvegarde ou de superposition pour les circuits Direct Connect à haute capacité (10 Gbit/s et plus) vers les centres de données sur site ou les installations de colocation.

Disponibilité dans les Régions

Les tunnels à large bande passante sont disponibles dans toutes les régions, à l'exception des suivantes :

Unavailable Régions AWS

AWS Région	Description
ap-southeast-4	Asie-Pacifique (Melbourne)
ca-west-1	Canada-Ouest (Calgary)

AWS Région	Description
eu-central-2	Europe (Zurich)
il-central-1	Israël (Tel Aviv)
me-central-1	Moyen-Orient (EAU)

Exigences et limitations

- Disponible uniquement pour les connexions VPN connectées à une passerelle de transit ou au Cloud WAN. Non pris en charge pour les pièces jointes de Virtual Private Gateway.
- Les deux tunnels d'une connexion VPN doivent utiliser la même configuration de bande passante (1,25 Gbit/s ou 5 Gbit/s dans les deux cas).
- Le VPN accéléré n'est pas pris en charge.
- Toutes les autres fonctionnalités VPN de base, telles que le VPN IP privé, le routage et la maintenance des tunnels, fonctionnent de la même manière avec le tunnel à large bande passante.
- La limite de MTU reste de 1 500 octets. En savoir plus sur la façon d'ajuster les tailles MTU et MSS en fonction des algorithmes utilisés.
- Vous pouvez modifier la bande passante du tunnel des connexions VPN existantes. Pour de plus amples informations, veuillez consulter Modifier la bande passante du tunnel.
- Les passerelles client (CGW) dotées uniquement d'une adresse IP fixe peuvent être utilisées avec les tunnels à large bande passante.
- Les passerelles client (CGW) sans adresse IP ne peuvent pas être utilisées avec des tunnels à large bande passante.
- Les tunnels à large bande passante ne prennent pas en charge les modifications du NAT-T port lorsque le tunnel est établi.
- Les paquets nécessitant une fragmentation peuvent être moins performants. En savoir plus.

Tarification des tunnels à large bande passante

Vous trouverez des informations sur les tarifs des connexions VPN à large bande passante sur la page de tarification des AWS VPN.

Échelle au-delà de 5 Gbit/s

Pour les besoins en bande passante supérieurs à 5 Gbit/s par tunnel, vous pouvez utiliser l'ECMP sur plusieurs connexions VPN. Par exemple, vous pouvez atteindre une bande passante de 20 Gbit/s en déployant deux connexions VPN avec des tunnels à large bande passante et en utilisant l'ECMP dans les quatre tunnels.

Configurer les options de tunnel pour AWS Site-to-Site VPN

Cette section fournit des conseils complets sur la configuration des options de tunnel pour les AWS Site-to-Site VPN connexions, en abordant les paramètres essentiels tels que la détection des pairs morts, les versions IKE et les paramètres de chiffrement. Vous pouvez personnaliser ces options de tunnel pour optimiser la sécurité, les performances et la compatibilité de votre connexion VPN avec votre infrastructure réseau sur site.

Voici les options de tunnel que vous pouvez configurer.

> **Note**
>
> Certaines options de tunnel comportent plusieurs valeurs par défaut. Par exemple, les versions IKE comportent deux valeurs d'option de tunnel par défaut : `ikev1` et`ikev2`. Toutes les valeurs par défaut seront associées à cette option de tunnel si vous ne choisissez pas de valeurs spécifiques. Cliquez pour supprimer toute valeur par défaut que vous ne souhaitez pas associer à l'option de tunnel. Par exemple, si vous souhaitez uniquement l'utiliser `ikev1` pour la version IKE, cliquez `ikev2` pour la supprimer.

Expiration du délai d'attente de la fonction Dead Peer Detection (DPD)

Nombre de secondes au bout duquel le délai d'attente de la fonction DPD arrive à expiration. Un délai d'expiration du DDP de 30 secondes signifie que le point de terminaison VPN considérera que l'homologue est mort 30 secondes après l'échec du premier maintien en vie. Vous pouvez spécifier 30 secondes ou plus.

Valeur par défaut : 40

Action d'expiration du délai d'attente de la fonction Dead Peer Detection

Action à effectuer après l'expiration du délai d'attente de la fonction Dead peer detection (DPD). Vous pouvez spécifier les valeurs suivantes :

- `Clear` : fin de la session IKE lors de l'expiration du délai d'attente de la fonction Dead Peer Detection (arrêt du tunnel et effacement des routes)
- `None` : aucune action lors de l'expiration du délai d'attente de la fonction Dead Peer Detection
- `Restart` : redémarrage de la session IKE lors de l'expiration du délai d'attente de la fonction Dead Peer Detection

Pour plus d'informations, consultez AWS Site-to-Site VPN options d'initiation du tunnel.

Par défaut: `Clear`

Options de journalisation de VPN

Grâce aux journaux Site-to-Site VPN, vous pouvez accéder à des informations détaillées sur l'établissement du tunnel de sécurité IP (IPsec), les négociations relatives à l'échange de clés Internet (IKE) et les messages du protocole de détection des pairs morts (DDP).

Pour de plus amples informations, veuillez consulter AWS Site-to-Site VPN journaux.

Formats de journal disponibles :`json`, `text`

Versions IKE

Versions IKE autorisées pour le tunnel VPN. Vous pouvez spécifier une ou plusieurs valeurs par défaut.

Valeurs par défaut :`ikev1`, `ikev2`

Bloc d'adresses CIDR IPv4 internes du tunnel

Plage d'adresses IPv4 internes du tunnel VPN. Vous pouvez spécifier un bloc d'adresse CIDR d'une taille de /30 dans la plage `169.254.0.0/16`. Le bloc CIDR doit être unique pour toutes les connexions Site-to-Site VPN qui utilisent la même passerelle privée virtuelle.

> **Note**
>
> Le bloc d'adresse CIDR n'a pas besoin d'être unique sur l'ensemble des connexions d'une passerelle de transit. Cependant, s'il n'est pas unique, cela peut créer un conflit sur votre passerelle client. Procédez avec prudence lorsque vous réutilisez le même bloc CIDR sur plusieurs connexions Site-to-Site VPN sur une passerelle de transit.

Les blocs d'adresse CIDR suivants sont réservés et ne peuvent pas être utilisés :

- `169.254.0.0/30`

- `169.254.1.0/30`
- `169.254.2.0/30`
- `169.254.3.0/30`
- `169.254.4.0/30`
- `169.254.5.0/30`
- `169.254.169.252/30`

Valeur par défaut : bloc d'adresses CIDR IPV4 de taille /30 de la plage `169.254.0.0/16`.

Pre-shared rangement des clés

Type de stockage pour la clé pré-partagée :

- Standard — La clé pré-partagée est stockée directement dans le service Site-to-Site VPN.
- Secrets Manager — La clé pré-partagée est stockée à l'aide AWS Secrets Manager de. Pour plus d'informations sur Secrets Manager, consultezFonctionnalités de sécurité améliorées à l'aide de Secrets Manager.

Bande passante du tunnel

Bande passante prise en charge pour le tunnel.

- Standard — La bande passante du tunnel est définie sur un maximum de 1,25 Gbit/s par tunnel (par défaut).
- Grande : bande passante maximale de 5 Gbit/s par tunnel.

> **Note**
>
> Large n'est disponible que pour les connexions VPN connectées à une passerelle de transit ou au Cloud WAN. Il n'est pas pris en charge pour les connexions Virtual Private Gateway.

Bloc d'adresses CIDR IPv6 internes du tunnel

(Connexions VPN IPv6 uniquement) Plage d'adresses IPv6 internes du tunnel VPN. Vous pouvez spécifier un bloc d'adresses CIDR d'une taille de /126 de la plage `fd00::/8` locale. Le bloc CIDR doit être unique pour toutes les connexions Site-to-Site VPN qui utilisent la même passerelle de transit. Si vous ne spécifiez aucun sous-réseau IPv6, Amazon sélectionne automatiquement un sous-réseau /128 dans cette plage. Que vous spécifiez le sous-réseau ou qu'Amazon le sélectionne, Amazon utilise la première adresse IPv6 utilisable du sous-réseau pour son côté de la connexion, et votre côté utilise la deuxième adresse IPv6 utilisable.

Valeur par défaut : bloc d'adresses CIDR IPv6 de taille /126 de la plage `fd00::/8` locale.

Type d'adresse IP du tunnel extérieur

Type d'adresse IP pour les adresses IP des tunnels extérieurs (externes). Vous pouvez spécifier l'une des options suivantes :

- `PrivateIpv4`: utilisez une adresse IPv4 privée pour déployer des connexions Site-to-Site VPN via Direct Connect.
- `PublicIpv4`: (Par défaut) Utilisez des adresses IPv4 pour les adresses IP du tunnel extérieur.
- `Ipv6`: utilisez des adresses IPv6 pour les adresses IP des tunnels extérieurs. Cette option n'est disponible que pour les connexions VPN sur une passerelle de transit ou sur le Cloud WAN.

Lorsque vous sélectionnez`Ipv6`, AWS configure automatiquement les adresses IPv6 des tunnels extérieurs pour le côté AWS des tunnels VPN. Votre dispositif de passerelle client doit prendre en charge l'adressage IPv6 et être capable d'établir des tunnels IPsec avec des points de terminaison IPv6.

Valeur par défaut : `PublicIpv4`

CIDR de réseau IPv4 local

(Connexion VPN IPv4 uniquement) La plage d'adresses CIDR utilisée lors de la négociation de la phase 2 de l'IKE pour le côté client (sur site) du tunnel VPN. Cette plage est utilisée pour proposer des itinéraires mais n'impose pas de restrictions de trafic car elle AWS utilise exclusivement des VPN basés sur des itinéraires. Policy-based Les VPN ne sont pas pris en charge car ils limiteraient la capacité AWSà prendre en charge les protocoles de routage dynamiques et les architectures multirégionales. Cela doit inclure les plages d'adresses IP de votre réseau local qui doivent communiquer via le tunnel VPN. Des configurations de table de routage, des NACL et des groupes de sécurité appropriés doivent être utilisés pour contrôler le flux de trafic réel.

Par défaut : 0,0.0. 0/0

CIDR réseau IPv4 distant

(Connexion VPN IPv4 uniquement) La plage d'adresses CIDR utilisée lors de la négociation de la phase 2 de l'IKE pour le AWS côté du tunnel VPN. Cette plage est utilisée pour proposer des itinéraires mais n'impose pas de restrictions de trafic, étant donné qu'AWS utilise exclusivement des VPN basés sur des itinéraires. AWS ne prend pas en charge les VPN basés sur des politiques car ils n'offrent pas la flexibilité requise pour les scénarios de routage complexes et sont incompatibles avec des fonctionnalités telles que les passerelles de transit et le VPN à coût égal Multi-Path (ECMP). Pour les VPC, il s'agit généralement de la plage CIDR de votre VPC. Pour

les passerelles de transit, cela peut inclure plusieurs plages d'adresses CIDR provenant de VPC connectés ou d'un autre réseau.

Par défaut : 0,0.0. 0/0

CIDR de réseau IPv6 local

(Connexion VPN IPv6 uniquement) Plage CIDR IPv6 côté passerelle client (sur site) autorisée à communiquer via les tunnels VPN.

Par défaut : ::/0

CIDR de réseau IPv6 distant

(Connexion VPN IPv6 uniquement) La plage d'adresses CIDR IPv6 du AWS côté autorisé à communiquer via les tunnels VPN.

Par défaut : ::/0

Numéros de groupe de la phase 1 Diffie-Hellman (DH)

Numéros de groupe DH autorisés pour le tunnel VPN pour la phase 1 des négociations IKE. Vous pouvez spécifier une ou plusieurs valeurs par défaut.

Valeurs par défaut : 2, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24

Numéros de groupe de la phase 2 Diffie-Hellman (DH)

Numéros de groupe DH autorisés pour le tunnel VPN pour la phase 2 des négociations IKE. Vous pouvez spécifier une ou plusieurs valeurs par défaut.

Valeurs par défaut : 2, 5, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24

Algorithmes de chiffrement de la phase 1

Algorithmes de chiffrement autorisés pour le tunnel VPN pour la phase 1 des négociations IKE. Vous pouvez spécifier une ou plusieurs valeurs par défaut.

Valeurs par défaut : AES128, AES256, AES128-GCM-16 AES256-GCM-16

Algorithmes de chiffrement de la phase 2

Algorithmes de chiffrement autorisés pour le tunnel VPN pour la phase 2 des négociations IKE. Vous pouvez spécifier une ou plusieurs valeurs par défaut.

Valeurs par défaut : AES128, AES256, AES128-GCM-16 AES256-GCM-16

Algorithmes d'intégrité de la phase 1

Algorithmes d'intégrité autorisés pour le tunnel VPN pour la phase 1 des négociations IKE. Vous pouvez spécifier une ou plusieurs valeurs par défaut.

Valeurs par défaut : SHA1,,, SHA2-256 SHA2-384 SHA2-512

Algorithmes d'intégrité de la phase 2

Algorithmes d'intégrité autorisés pour le tunnel VPN pour la phase 2 des négociations IKE. Vous pouvez spécifier une ou plusieurs valeurs par défaut.

Valeurs par défaut : SHA1,,, SHA2-256 SHA2-384 SHA2-512

Durée de vie phase 1

> **Note**
>
> AWS initialisez de nouvelles touches avec les valeurs temporelles définies dans les champs Durée de vie de la phase 1 et Durée de vie de la phase 2. Si ces durées de vie sont différentes des valeurs de liaison négociées, la connectivité du tunnel risque d'être interrompue.

Durée de vie en secondes de la phase 1 de la négociation IKE. Vous pouvez spécifier un nombre compris entre 900 et 28 800.

Valeur par défaut : 28 800 (8 heures)

Durée de vie phase 2

> **Note**
>
> AWS initialisez de nouvelles touches avec les valeurs temporelles définies dans les champs Durée de vie de la phase 1 et Durée de vie de la phase 2. Si ces durées de vie sont différentes des valeurs de liaison négociées, la connectivité du tunnel risque d'être interrompue.

Durée de vie en secondes de la phase 2 de la négociation IKE. Vous pouvez spécifier un nombre compris entre 900 et 3 600. Le nombre que vous spécifiez doit être inférieur au nombre de secondes de la durée de vie de la phase 1.

Valeur par défaut : 3 600 (1 heure)

Pre-shared clé (PSK)

Clé prépartagée (pre-shared key, PSK) permettant d'établir l'association de sécurité IKE (internet key exchange) initiale entre la passerelle cible et la passerelle client.

La clé pré-partagée doit comporter entre 8 et 64 caractères et ne peut pas commencer par un zéro (0). Les caractères autorisés sont les caractères alphanumériques, les points (.) et les traits de soulignement (_).

Valeur par défaut : chaîne alphanumérique de 32 caractères.

Fuzz du changement de clé

Pourcentage de la fenêtre de changement de clé (déterminé par le temps de la marge du changement de clé) dans laquelle le temps de changement de clé est sélectionné aléatoirement.

Vous pouvez spécifier une valeur de pourcentage comprise entre 0 et 100.

Par défaut : 100

Durée de marge du changement de clé

Durée de marge en secondes avant l'expiration de la durée de vie des phases 1 et 2, pendant laquelle le AWS côté de la connexion VPN effectue une nouvelle clé IKE.

Vous pouvez spécifier un nombre compris entre 60 et la moitié de la valeur de la durée de vie de la phase 2.

L'heure exacte du changement de clé est sélectionnée aléatoirement en fonction de la valeur du fuzz de changement de clé.

Valeur par défaut : 270 (4,5 minutes)

Paquets de taille de la fenêtre de réexécution

Nombre de paquets dans une fenêtre de réexécution IKE.

Vous pouvez spécifier une valeur comprise entre 64 et 2 048.

Par défaut: 1024

Action de démarrage

Action à effectuer lors de l'établissement du tunnel pour une connexion VPN. Vous pouvez spécifier les éléments suivants :

- `Start`: AWS lance la négociation IKE pour ouvrir le tunnel. Prise en charge uniquement si votre passerelle client est configurée avec une adresse IP.
- `Add` : votre périphérique de passerelle client doit lancer la négociation IKE pour activer le tunnel.

Pour plus d'informations, consultez AWS Site-to-Site VPN options d'initiation du tunnel.

Par défaut: `Add`

Contrôle du cycle de vie des points de terminaison de tunnel

Le contrôle du cycle de vie des points de terminaison de tunnel permet de contrôler le calendrier de remplacement des points de terminaison.

Pour de plus amples informations, veuillez consulter AWS Site-to-Site VPN contrôle du cycle de vie des terminaux du tunnel.

Par défaut: `Off`

Vous pouvez spécifier les options de tunnel lorsque vous créez une connexion Site-to-Site VPN, ou vous pouvez modifier les options de tunnel pour une connexion VPN existante. Pour plus d'informations, consultez les rubriques suivantes :

- Étape 5 : Création d'une connexion VPN
- Modifier les options AWS Site-to-Site VPN du tunnel

AWS Site-to-Site VPN options d'authentification du tunnel

Vous pouvez utiliser des clés ou des certificats pré-partagés pour authentifier les points de terminaison de votre tunnel Site-to-Site VPN.

Clés prépartagées

Une clé pré-partagée (PSK) est l'option d'authentification par défaut pour les tunnels Site-to-Site VPN. Lorsque vous créez un tunnel, vous pouvez soit spécifier votre propre PSK, soit autoriser AWS à en générer un automatiquement pour vous. Le PSK est stocké selon l'une des méthodes suivantes :

- Directement dans le service Site-to-Site VPN. Pour de plus amples informations, veuillez consulter Site-to-Site Dispositifs de passerelle client VPN.

- AWS Secrets Manager Pour une sécurité renforcée. Pour plus d'informations sur l'utilisation de Secrets Manager pour stocker un PSK, consultezFonctionnalités de sécurité améliorées à l'aide de Secrets Manager.

La chaîne PSK est ensuite utilisée lors de la configuration de votre dispositif de passerelle client.

Certificat privé de Autorité de certification privée AWS

Si vous ne souhaitez pas utiliser de clés prépartagées, vous pouvez utiliser un certificat privé provenant de Autorité de certification privée AWS pour authentifier votre VPN.

Vous devez créer un certificat privé à partir d'une autorité de certification subordonnée à l'aide d' Autorité de certification privée AWS (Autorité de certification privée AWS). Pour signer l'autorité de certification subordonnée ACM, vous pouvez utiliser une autorité de certification racine ACM ou une autorité de certification externe. Pour de plus amples informations sur la création d'un certificat privé, veuillez consulter Création et gestion d'une autorité de certification privée dans le Guide de l'utilisateur Autorité de certification privée AWS .

Vous devez créer un rôle lié à un service pour générer et utiliser le certificat du AWS côté du point de terminaison du tunnel Site-to-Site VPN. Pour de plus amples informations, veuillez consulter the section called “Service-linked rôles”.

> **Note**
>
> Pour faciliter les rotations de certification fluides, tout certificat doté de la même chaîne d'autorité de certification que celle initialement spécifiée dans l'appel d'`CreateCustomerGateway`API est suffisant pour établir une connexion VPN.

Si vous ne spécifiez pas l'adresse IP de votre périphérique de passerelle client, nous ne vérifions pas l'adresse IP. Cette opération vous permet de déplacer le périphérique de passerelle client vers une adresse IP différente sans avoir à reconfigurer la connexion VPN.

Site-to-Site Le VPN effectue la vérification de la chaîne de certificats sur le certificat de la passerelle client lorsque vous créez un certificat VPN. Outre les contrôles d'autorité de certification et de validité de base, le Site-to-Site VPN vérifie si les extensions X.509 sont présentes, notamment l'identifiant de clé d'autorité, l'identifiant de clé d'objet et les contraintes de base.

AWS Site-to-Site VPN options d'initiation du tunnel

Par défaut, votre dispositif de passerelle client doit ouvrir les tunnels pour votre connexion Site-to-Site VPN en générant du trafic et en lançant le processus de négociation IKE (Internet Key Exchange). Vous pouvez configurer vos tunnels VPN pour spécifier qui AWS doit plutôt lancer ou redémarrer le processus de négociation IKE.

Options de lancement IKE du tunnel VPN

Les options de lancement IKE suivantes sont disponibles. Vous pouvez implémenter l'une ou les deux options, pour l'un ou les deux tunnels de votre connexion Site-to-Site VPN. Consultez Options de tunnel VPN pour plus de détails sur ces paramètres d'option de tunnel en particulier et les autres.

- Action de démarrage : action à effectuer lors de l'établissement du tunnel VPN pour une connexion VPN nouvelle ou modifiée. Par défaut, votre périphérique de passerelle client lance le processus de négociation IKE pour activer le tunnel. Vous pouvez spécifier qu'il AWS doit plutôt lancer le processus de négociation IKE.
- Action de l'expiration du délai d'attente DPD : action à effectuer après l'expiration du délai d'attente de la fonction Dead Peer Detection (DPD). Par défaut, la session IKE est arrêtée, le tunnel est arrêté et les routes sont supprimées. Vous pouvez spécifier qu' AWS il doit redémarrer la session IKE lorsque le délai d'expiration du délai DDP se produit, ou vous pouvez spécifier qu' AWS il ne doit prendre aucune mesure lorsque le délai d'expiration du délai DDP se produit.

Règles et limitations

Les règles et limitations suivantes s'appliquent :

- Pour lancer une négociation IKE, AWS l'adresse IP publique de votre passerelle client est requise. Si vous avez configuré l'authentification basée sur des certificats pour votre connexion VPN et que vous n'avez pas spécifié d'adresse IP lorsque vous avez créé la ressource de passerelle client dans AWS, vous devez créer une nouvelle passerelle client et spécifier l'adresse IP. Ensuite, modifiez la connexion VPN et spécifiez la nouvelle passerelle client. Pour de plus amples informations, veuillez consulter Modifier la passerelle client pour une AWS Site-to-Site VPN connexion.
- L'initiation IKE (action de démarrage) depuis le AWS côté de la connexion VPN n'est prise en charge IKEv2 que pour.

- Si vous utilisez l'initiation IKE depuis le AWS côté de la connexion VPN, aucun paramètre de délai d'expiration n'est inclus. Il essaiera continuellement d'établir une connexion jusqu'à ce qu'elle soit établie. En outre, le AWS côté de la connexion VPN relancera la négociation IKE lorsqu'il recevra un message de suppression de la SA provenant de votre passerelle client.
- Si votre dispositif de passerelle client se trouve derrière un pare-feu ou un autre appareil utilisant la traduction d'adresses réseau (NAT), une identité (IDr) doit être configurée. Pour plus d'informations sur IDr, consultez la RFC 7296.

Si vous ne configurez pas l'initiation IKE par le AWS côté pour votre tunnel VPN et que la connexion VPN est inactive (généralement 10 secondes, selon votre configuration), le tunnel risque de tomber en panne. Pour éviter cela, vous pouvez utiliser un outil de surveillance du réseau pour générer des tests ping keepalive.

Utilisation des options de lancement du tunnel VPN

Pour de plus amples informations sur l'utilisation des options de lancement du tunnel VPN, veuillez consulter les rubriques suivantes :

- Pour créer une nouvelle connexion VPN et spécifier les options de lancement du tunnel VPN : Étape 5 : Création d'une connexion VPN
- Pour modifier les options de lancement du tunnel VPN pour une connexion VPN existante : Modifier les options AWS Site-to-Site VPN du tunnel

AWS Site-to-Site VPN remplacement des extrémités des tunnels

Votre connexion Site-to-Site VPN se compose de deux tunnels VPN pour la redondance. Parfois, l'un des points de terminaison du tunnel VPN ou les deux sont remplacés lorsque vous AWS effectuez des mises à jour du tunnel ou lorsque vous modifiez votre connexion VPN. Lors du remplacement d'un point de terminaison de tunnel, la connectivité sur le tunnel peut être interrompue pendant que le nouveau point de terminaison du tunnel est alloué.

Rubriques

- Remplacement des points de terminaison à l'initiative du client
- Remplacement des points de terminaison gérés par AWS
- AWS Site-to-Site VPN contrôle du cycle de vie des terminaux du tunnel

Remplacement des points de terminaison à l'initiative du client

Lorsque vous modifiez les composants suivants de votre connexion VPN, un ou les deux points de terminaison de votre tunnel est remplacé.

Modification	Action d'API	Impact sur le tunnel
Modifier la passerelle cible pour la connexion VPN	ModifyVpnConnection	Les deux tunnels sont indisponibles pendant que les nouveaux points de terminaison de tunnel sont alloués.
Modifier la passerelle client pour la connexion VPN	ModifyVpnConnection	Les deux tunnels sont indisponibles pendant que les nouveaux points de terminaison de tunnel sont alloués.
Modifier les options de connexion VPN	ModifyVpnConnectionOptions	Les deux tunnels sont indisponibles pendant que les nouveaux points de terminaison de tunnel sont alloués.
Modifier les options du tunnel VPN	ModifyVpnTunnelOptions	Le tunnel modifié est indisponible pendant la mise à jour.

Remplacement des points de terminaison gérés par AWS

AWS Site-to-Site VPN est un service géré qui applique régulièrement des mises à jour aux points de terminaison de votre tunnel VPN. Ces mises à jour se produisent pour diverses raisons, notamment :

- Pour appliquer des mises à niveau générales, telles que des correctifs, des améliorations de la résilience et d'autres optimisations
- Pour retirer le matériel sous-jacent
- Lorsque la surveillance automatisée détermine qu'un point de terminaison de tunnel VPN est non sain

AWS applique les mises à jour des points de terminaison du tunnel à un tunnel de votre connexion VPN à la fois. Lors d'une mise à jour du point de terminaison de tunnel, votre connexion VPN risque de subir une brève perte de redondance. Il est donc important de configurer les deux tunnels dans votre connexion VPN pour une haute disponibilité.

AWS Site-to-Site VPN contrôle du cycle de vie des terminaux du tunnel

Le contrôle du cycle de vie des terminaux du tunnel permet de contrôler le calendrier des remplacements des terminaux et peut aider à minimiser les interruptions de connectivité lors des remplacements AWS gérés des terminaux du tunnel. Grâce à cette fonctionnalité, vous pouvez choisir d'accepter les mises à jour AWS gérées des points de terminaison du tunnel au moment qui convient le mieux à votre entreprise. Utilisez cette fonction si vous avez des besoins professionnels à court terme ou si vous ne pouvez prendre en charge qu'un seul tunnel par connexion VPN.

> **Note**
>
> Dans de rares circonstances, des mises à jour critiques AWS peuvent être appliquées immédiatement aux points de terminaison du tunnel, même si la fonctionnalité de contrôle du cycle de vie des points de terminaison du tunnel est activée.

Rubriques

Fonctionnement du contrôle du cycle de vie des points de terminaison de tunnel

Activez la fonction de contrôle du cycle de vie des points de terminaison de tunnel pour les tunnels individuels au sein d'une connexion VPN. Elle peut être activée au moment de la création du VPN ou en modifiant les options de tunnel pour une connexion VPN existante.

Une fois le contrôle du cycle de vie des points de terminaison de tunnel activé, vous bénéficierez d'une visibilité supplémentaire sur les prochains événements de maintenance du tunnel de deux manières :

- Vous recevrez des AWS Health notifications concernant les prochains remplacements des terminaux du tunnel.
- L'état de la maintenance en attente, ainsi que les horodatages Maintenance auto appliquée après et Dernière maintenance appliquée, peuvent être consultés dans le Console de gestion AWS ou à l'aide de la commande get-vpn-tunnel-replacement AWS CLI -status.

Lorsqu'une maintenance des points de terminaison de tunnel est disponible, vous avez la possibilité d'accepter la mise à jour au moment qui vous convient, avant l'horodatage de la Maintenance appliquée automatiquement après donnée.

Si vous n'appliquez pas de mises à jour avant la date d'application automatique de la maintenance, vous AWS effectuerez automatiquement le remplacement du point de terminaison du tunnel peu après, dans le cadre du cycle de mise à jour de maintenance régulier.

Activer le contrôle du cycle de vie des terminaux du AWS Site-to-Site VPN tunnel

Le contrôle du cycle de vie des terminaux peut être activé sur une connexion VPN existante ou nouvelle. Cela peut être fait en utilisant le Console de gestion AWS ou AWS CLI.

> **Note**
>
> Par défaut, lorsque vous activez la fonction pour une connexion VPN existante, le remplacement du point de terminaison de tunnel sera lancé en même temps. Si vous souhaitez activer la fonction, mais ne pas lancer immédiatement le remplacement du point de terminaison de tunnel, vous pouvez utiliser l'option Ignorer le remplacement du tunnel.

Existing VPN connection

Les étapes suivantes montrent comment activer le contrôle du cycle de vie des points de terminaison de tunnel sur une connexion VPN existante.

Pour activer le contrôle du cycle de vie des terminaux du tunnel à l'aide du Console de gestion AWS

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation de gauche, choisissez Site-to-Site VPN Connections.
3. Sélectionnez la connexion appropriée sous Connexions VPN.
4. Sélectionnez Actions, puis Modifier les options de tunnel VPN.
5. Sélectionnez le tunnel spécifique que vous souhaitez modifier en choisissant la bonne Adresse IP externe du tunnel VPN.
6. Sous Contrôle du cycle de vie des points de terminaison de tunnel, cochez la case Activer.
7. (Facultatif) Sélectionnez Ignorer le remplacement du tunnel.
8. Sélectionnez Enregistrer les modifications.

Pour activer le contrôle du cycle de vie des terminaux du tunnel à l'aide du AWS CLI

Utilisez la modify-vpn-tunnel-optionscommande pour activer le contrôle du cycle de vie des points de terminaison du tunnel.

New VPN connection

Les étapes suivantes montrent comment activer le contrôle du cycle de vie des points de terminaison de tunnel lors de la création d'une connexion VPN.

Pour activer le contrôle du cycle de vie des terminaux du tunnel lors de la création d'une nouvelle connexion VPN à l'aide du Console de gestion AWS

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Site-to-Site VPN Connections.
3. Choisissez Create VPN connection (Créer une connexion VPN).
4. Dans les sections Options Tunnel 1 et Options Tunnel 2, sous Contrôle du cycle de vie des points de terminaison de tunnel, sélectionnez Activer.
5. Choisissez Créer une connexion VPN.

Pour activer le contrôle du cycle de vie des terminaux du tunnel lors de la création d'une nouvelle connexion VPN à l'aide du AWS CLI

Utilisez la create-vpn-connectioncommande pour activer le contrôle du cycle de vie des points de terminaison du tunnel.

Vérifiez si le contrôle du cycle de vie des points de terminaison du AWS Site-to-Site VPN tunnel est activé

Vous pouvez vérifier si le contrôle du cycle de vie des points de terminaison du tunnel est activé sur un tunnel VPN existant à l'aide de la CLI Console de gestion AWS ou.

- Si le contrôle du cycle de vie des points de terminaison du tunnel est désactivé et que vous souhaitez l'activer, consultezActiver le contrôle du cycle de vie des points de terminaison de tunnel.
- Si le contrôle du cycle de vie des points de terminaison du tunnel est activé et que vous souhaitez le désactiver, consultezDésactiver le contrôle du cycle de vie des points de terminaison de tunnel.

Pour vérifier si le contrôle du cycle de vie des points de terminaison du tunnel est activé à l'aide du Console de gestion AWS

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation de gauche, choisissez Site-to-Site VPN Connections.
3. Sélectionnez la connexion appropriée sous Connexions VPN.
4. Sélectionnez l'onglet Détails du tunnel.
5. Dans les détails du tunnel, recherchez Contrôle du cycle de vie des points de terminaison de tunnel, qui indiquera si la fonction est Activée ou Désactivée.

Pour vérifier si le contrôle du cycle de vie des points de terminaison du tunnel est activé à l'aide du AWS CLI

Utilisez la describe-vpn-connectionscommande pour vérifier si le contrôle du cycle de vie des points de terminaison du tunnel est activé.

Vérifiez les mises à jour disponibles sur les AWS Site-to-Site VPN tunnels

Après avoir activé la fonction de contrôle du cycle de vie des points de terminaison de tunnel, vous pouvez voir si une mise à jour de maintenance est disponible pour votre connexion VPN avec la Console de gestion AWS ou l'interface de ligne de commande. La vérification de la disponibilité d'une mise à jour du tunnel Site-to-Site VPN ne télécharge ni ne déploie automatiquement la mise à jour. Vous pouvez choisir à quel moment vous souhaitez le déployer. Pour connaître les étapes

de téléchargement et de déploiement d'une mise à jour, consultezAccepter une mise à jour de maintenance.

Pour vérifier les mises à jour disponibles à l'aide du Console de gestion AWS

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation de gauche, choisissez Site-to-Site VPN Connections.
3. Sélectionnez la connexion appropriée sous Connexions VPN.
4. Sélectionnez l'onglet Détails du tunnel.
5. Consultez la colonne Maintenance en attente. Le statut sera soit Disponible, soit Aucun.

Pour vérifier les mises à jour disponibles à l'aide du AWS CLI

Utilisez la commande get-vpn-tunnel-replacement-status pour vérifier les mises à jour disponibles.

Accepter une mise à jour de maintenance AWS Site-to-Site VPN du tunnel

Lorsqu'une mise à jour de maintenance est disponible, vous pouvez l'accepter à l'aide de la CLI Console de gestion AWS or. Vous pouvez choisir d'accepter la mise à jour de maintenance du tunnel Site-to-Site VPN au moment qui vous convient. Une fois que vous aurez accepté la mise à jour de maintenance, elle sera déployée.

> **Note**
>
> Si vous n'acceptez pas la mise à jour de maintenance, elle AWS sera automatiquement déployée au cours d'un cycle de mise à jour de maintenance régulier.

Pour accepter une mise à jour de maintenance disponible à l'aide du Console de gestion AWS

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation de gauche, choisissez Site-to-Site VPN Connections.
3. Sélectionnez la connexion appropriée sous Connexions VPN.
4. Choisissez Actions, puis Remplacer le tunnel VPN.
5. Sélectionnez le tunnel spécifique que vous souhaitez remplacer en choisissant la bonne Adresse IP externe du tunnel VPN.
6. Choisissez Remplacer.

Pour accepter une mise à jour de maintenance disponible à l'aide du AWS CLI

Utilisez la replace-vpn-tunnelcommande pour accepter une mise à jour de maintenance disponible.

Désactiver AWS Site-to-Site VPN le contrôle du cycle de vie des terminaux du tunnel

Si vous ne souhaitez plus utiliser la fonctionnalité de contrôle du cycle de vie des points de terminaison du tunnel, vous pouvez la désactiver à l'aide du Console de gestion AWS ou du AWS CLI. Lorsque vous désactivez cette fonction, AWS déploiera automatiquement des mises à jour de maintenance régulièrement, qui peuvent avoir lieu pendant vos heures de travail. Pour éviter tout impact sur votre activité, nous vous recommandons vivement de configurer les deux tunnels dans votre connexion VPN pour une haute disponibilité.

> **Note**
>
> Bien qu'une maintenance en attente soit disponible, vous ne pouvez pas spécifier l'option Ignorer le remplacement du tunnel lorsque vous désactivez la fonction. Vous pouvez toujours désactiver cette fonctionnalité sans utiliser l'option Ignorer le remplacement du tunnel, mais vous AWS déploierez automatiquement les mises à jour de maintenance en attente disponibles en lançant immédiatement le remplacement du point de terminaison du tunnel.

Pour désactiver le contrôle du cycle de vie des terminaux du tunnel à l'aide du Console de gestion AWS

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation de gauche, choisissez Site-to-Site VPN Connections.
3. Sélectionnez la connexion appropriée sous Connexions VPN.
4. Sélectionnez Actions, puis Modifier les options de tunnel VPN.
5. Sélectionnez le tunnel spécifique que vous souhaitez modifier en choisissant la bonne Adresse IP externe du tunnel VPN.
6. Pour désactiver le contrôle du cycle de vie des points de terminaison de tunnel, sous Contrôle du cycle de vie des points de terminaison de tunnel, décochez la case Activer.
7. (Facultatif) Sélectionnez Ignorer le remplacement du tunnel.
8. Sélectionnez Enregistrer les modifications.

Pour désactiver le contrôle du cycle de vie des terminaux du tunnel à l'aide du AWS CLI

Utilisez la modify-vpn-tunnel-optionscommande pour désactiver le contrôle du cycle de vie des points de terminaison du tunnel.

Options de passerelle client pour votre AWS Site-to-Site VPN connexion

Le tableau suivant décrit les informations dont vous aurez besoin pour créer une ressource de passerelle client dans AWS.

Élément	Description
(Facultatif) Identification de nom	Crée une identification avec la clé « Nom » et la valeur que vous spécifiez.
(Routage dynamique uniquement) Numéro d'ASN (Autonomous System Number) BGP (Border Gateway Protocol) de la passerelle client.	Un ASN compris entre 1 et 4 294 967 295 est pris en charge. Vous pouvez utiliser un numéro ASN public existant affecté à votre réseau, à l'exception des numéros suivants : • 7224 — Réservé dans toutes les régions • 9059 — Réservé dans la région `eu-west-1` • 10124 — Réservé dans la région `ap-northeast-1` • 17943 — Réservé dans la région `ap-southeast-1` Si vous n'avez pas d'ASN public, vous pouvez utiliser un ASN privé compris entre 64 512 et 65 534 ou entre 4 200 000 000 et 4 294 967 294. L'ASN par défaut est 64512. Pour plus d'informations sur le routage, consultezAWS Site-to-Site VPN options de routage.
Adresse IP de l'interface externe du dispositif de passerelle client.	L'adresse IP doit être statique et peut être IPv4 soit IPv6.

Élément	Description
	Pour les IPv4 adresses : si votre dispositif de passerelle client se trouve derrière un périphéri que de traduction d'adresses réseau (NAT), utilisez l'adresse IP de votre périphérique NAT. Assurez-vous également que les paquets UDP sur le port 500 (et le port 4500, si la traversée NAT est utilisée) sont autorisés à passer entre votre réseau et les AWS Site-to-Site VPN points de terminaison. Pour plus d'informations, consultez Règles de pare-feu. Pour les IPv6 adresses : l'adresse doit être une adresse valide pouvant être routée par Internet IPv6 . IPv6 les adresses ne sont prises en charge que pour les connexions VPN sur une passerelle de transit ou un Cloud WAN. Aucune adresse IP n'est requise lorsque vous utilisez un certificat privé Autorité de certifica tion privée AWS et un VPN public.

Élément	Description
(Facultatif) Certificat privé d'une autorité de certification subordonnée utilisant AWS Certificate Manager (ACM).	Si vous souhaitez utiliser l'authentification basée sur le certificat, fournissez l'ARN d'un certificat privé ACM qui sera utilisé sur votre périphérique de passerelle client. Lorsque vous créez une passerelle client, vous pouvez configurer la passerelle client pour utiliser des certificats Autorité de certification privée AWS privés afin d'authentifier le Site-to-Site VPN. Lorsque vous choisissez d'utiliser cette option, vous créez une autorité de certification privée (CA) entièrement AWS hébergée pour un usage interne par votre organisation. Le certificat de l'autorité de certification racine et les certificats de l'autorité de certification subordonnée sont stockés et gérés par Autorité de certification privée AWS. Avant de créer la passerelle client, vous créez un certificat privé à partir d'une autorité de certification subordonnée en utilisant Autorité de certification privée AWS, puis vous spécifiez le certificat lorsque vous configurez la passerell e client. Pour de plus amples informations sur la création d'un certificat privé, veuillez consulter Création et gestion d'une autorité de certification privée dans le Guide de l'utilisateur Autorité de certification privée AWS .
Appareil (Facultatif).	Nom de l'appareil de passerelle client associé à cette passerelle client.

IPv6 options de passerelle client

Lorsque vous créez une passerelle client avec une IPv6 adresse, tenez compte des points suivants :

- IPv6 les passerelles client ne sont prises en charge que pour les connexions VPN sur une passerelle de transit ou sur le Cloud WAN.
- L' IPv6 adresse doit être une adresse valide et routable par Internet IPv6 .
- Votre dispositif de passerelle client doit prendre en charge l' IPv6 adressage et être capable d'établir des IPsec tunnels avec les IPv6 points de terminaison.
- Pour créer une passerelle IPv6 client à l'aide de l'AWS CLI, utilisez une IPv6 adresse pour le `--ip-address` paramètre :

```
aws ec2 create-customer-gateway --ip-address 2001:0db8:85a3:0000:0000:8a2e:0370:7334
 --bgp-asn 65051 --type ipsec.1 --region us-west-1
```

AWS Site-to-Site VPN Connexions accélérées

Vous pouvez éventuellement activer l'accélération pour votre connexion Site-to-Site VPN. Une connexion Site-to-Site VPN accélérée (connexion VPN accélérée) permet AWS Global Accelerator d'acheminer le trafic de votre réseau local vers l'emplacement AWS périphérique le plus proche de votre passerelle client.AWS Global Accelerator optimise le chemin réseau, en utilisant le réseau AWS mondial exempt de congestion pour acheminer le trafic vers le point de terminaison offrant les meilleures performances applicatives (pour plus d'informations, voir). AWS Global Accelerator Vous pouvez utiliser une connexion VPN accélérée pour éviter les perturbations réseau qui peuvent survenir lorsque le trafic est routé sur l'Internet public.

Lorsque vous créez une connexion VPN accélérée, nous créons et gérons deux accélérateurs pour votre compte, un pour chaque tunnel VPN. Vous ne pouvez pas afficher ou gérer vous-même ces accélérateurs à l'aide de la AWS Global Accelerator console ou APIs.

Pour plus d'informations sur les AWS régions qui prennent en charge les connexions VPN accélérées, consultez le Site-to-SiteVPN AWS accéléré FAQs.

Activation de l'accélération

Par défaut, lorsque vous créez une connexion Site-to-Site VPN, l'accélération est désactivée. Vous pouvez éventuellement activer l'accélération lorsque vous créez une nouvelle pièce jointe Site-to-Site

VPN sur une passerelle de transit. Pour plus d'informations et pour connaître les étapes, consultez Création d'une AWS Site-to-Site VPN connexion.

Les connexions VPN accélérées utilisent un pool distinct d'adresses IP pour les adresses IP du point de terminaison du tunnel. Les adresses IP des deux tunnels VPN sont sélectionnées dans deux zones réseau distinctes.

Règles et restrictions

Pour utiliser une connexion VPN accélérée, les règles suivantes s'appliquent :

- L'accélération n'est prise en charge que pour les connexions Site-to-Site VPN associées à une passerelle de transit. Les passerelles réseau privé virtuel ne prennent pas en charge les connexions VPN accélérées.
- Une connexion Site-to-Site VPN accélérée ne peut pas être utilisée avec une interface virtuelle AWS Direct Connect publique.
- Vous ne pouvez pas activer ou désactiver l'accélération pour une connexion Site-to-Site VPN existante. Au lieu de cela, vous pouvez créer une nouvelle connexion Site-to-Site VPN avec l'accélération activée ou désactivée selon vos besoins. Configurez ensuite votre dispositif de passerelle client pour qu'il utilise la nouvelle connexion Site-to-Site VPN et supprimez l'ancienne connexion Site-to-Site VPN.
- NAT-traversal (NAT-T) est requis pour une connexion VPN accélérée et est activé par défaut. Si vous avez téléchargé un fichier de configuration depuis la console Amazon VPC, vérifiez le paramètre NAT-T et ajustez-le si nécessaire.
- La négociation IKE pour les tunnels VPN accélérés doit être lancée depuis le dispositif de passerelle du client. Les deux options de tunnel qui affectent ce comportement sont `Startup Action` et`DPD Timeout Action`. Pour plus d'informations, consultez Options de tunnel VPN et Options de lancement du tunnel VPN.
- Site-to-Site Les connexions VPN qui utilisent l'authentification basée sur des certificats peuvent ne pas être compatibles avec AWS Global Accelerator, en raison de la prise en charge limitée de la fragmentation des paquets dans Global Accelerator. Pour plus d'informations, consultez Fonctionnement de AWS Global Accelerator. Si vous avez besoin d'une connexion VPN accélérée qui utilise l'authentification basée sur des certificats, votre périphérique de passerelle client doit prendre en charge la fragmentation IKE. Si ce n'est pas le cas, n'activez pas votre VPN pour l'accélération.

AWS Site-to-Site VPN options de routage

AWS recommande de faire de la publicité pour des itinéraires BGP spécifiques afin d'influencer les décisions de routage dans la passerelle privée virtuelle. Consultez la documentation de votre fournisseur pour connaître les commandes spécifiques à votre appareil.

Lorsque vous créez plusieurs connexions VPN, la passerelle réseau privé virtuel envoie le trafic réseau vers la connexion VPN appropriée à l'aide de routes affectées statiquement ou d'annonces de routes BGP. Le choix de la route dépend de la façon dont la connexion VPN a été configurée. Les routes affectées statiquement sont préférées aux routes annoncées par BGP lorsque des routes identiques existent dans la passerelle réseau privé virtuel. Si vous sélectionnez l'option d'utiliser une annonce BGP, vous ne pouvez pas spécifier de routes statiques.

Pour plus d'informations sur la priorité de route, consultez Tables de routage et priorité des itinéraires.

Lorsque vous créez une connexion Site-to-Site VPN, vous devez effectuer les opérations suivantes :

- Spécifiez le type de routage que vous prévoyez d'utiliser (statique ou dynamique)
- Mettez à jour la table de routage de votre sous-réseau

Le nombre de routes que vous pouvez ajouter à une table de routage est limité. Pour plus d'informations, consultez la section Tables de routage dans Quotas Amazon VPC dans le Guide de l'utilisateur Amazon VPC.

Rubriques

Routage statique et dynamique dans AWS Site-to-Site VPN

Le type de routage que vous sélectionnez peut dépendre de la marque et du modèle de votre périphériques de passerelle client. Si votre dispositif de passerelle client prend en charge le protocole BGP (Border Gateway Protocol), spécifiez le routage dynamique lorsque vous configurez votre

connexion Site-to-Site VPN. Si votre périphérique de passerelle client ne prend pas en charge le BGP, spécifiez un routage statique.

> **Note**
>
> Site-to-Site Les concentrateurs VPN ne prennent en charge que le routage BGP. Le routage statique n'est pas pris en charge pour les connexions VPN qui utilisent un concentrateur Site-to-Site VPN.

Si vous utilisez un appareil qui prend en charge la publicité BGP, vous ne spécifiez pas de routes statiques vers la connexion Site-to-Site VPN, car l'appareil utilise le protocole BGP pour annoncer ses itinéraires vers la passerelle privée virtuelle. Si vous utilisez un périphérique qui ne prend pas en charge les annonces BGP, vous devez sélectionner un routage statique et entrer les routes (préfixes IP) pour votre réseau qui doivent être communiquées à la passerelle réseau privé virtuel.

Nous vous recommandons d'utiliser des périphériques compatibles avec BGP, quand c'est possible, puisque le protocole BGP offre de solides contrôles de détection du caractère vivant qui peuvent assister le failover vers le second tunnel VPN si le premier tunnel s'arrête. Les périphériques qui ne prennent pas en charge BGP peuvent également exécuter des vérifications de l'état pour assister le failover vers le second tunnel lorsque c'est nécessaire.

Vous devez configurer votre dispositif de passerelle client pour acheminer le trafic de votre réseau local vers la connexion Site-to-Site VPN. La configuration dépend de la marque et du modèle de votre périphérique. Pour de plus amples informations, veuillez consulter AWS Site-to-Site VPN dispositifs de passerelle client.

Tables de routage et priorité des AWS Site-to-Site VPN itinéraires

Les tables de routage déterminent où le trafic réseau de votre VPC est dirigé. Dans votre table de routage VPC, vous devez ajouter une route pour votre réseau distant et spécifier la passerelle réseau privé virtuel comme cible. Cela permet au trafic de votre VPC destiné à votre réseau distant de s'acheminer via la passerelle réseau privé virtuel et sur l'un des tunnels VPN. Vous pouvez autoriser la propagation du routage pour votre table de routage pour automatiquement propager vos routes réseau vers la table pour vous.

Nous utilisons la route la plus spécifique de votre table de routage qui correspond au trafic afin de déterminer comment router le trafic (correspondance de préfixe le plus long). Si votre table

de routage comporte des routes qui se chevauchent ou correspondent, les règles suivantes s'appliquent :

- Si les routes propagées à partir d'une connexion Site-to-Site VPN ou d'une Direct Connect connexion se chevauchent avec la route locale de votre VPC, la route locale est préférable, même si les routes propagées sont plus spécifiques.
- Si les routes propagées à partir d'une connexion ou d'une Direct Connect connexion Site-to-Site VPN ont le même bloc d'adresse CIDR de destination que les autres routes statiques existantes (la correspondance de préfixe la plus longue ne peut pas être appliquée), nous donnons la priorité aux routes statiques dont les cibles sont une passerelle Internet, une passerelle privée virtuelle, une interface réseau, un identifiant d'instance, une connexion d'appairage VPC, une passerelle NAT, une passerelle de transit ou un point de terminaison VPC de passerelle.

Par exemple, la table de routage suivante a une route statique vers une passerelle Internet et une route propagée vers une passerelle réseau privé virtuel. Les deux routes ont pour destination : `172.31.0.0/24`. Dans ce cas, tout le trafic destiné à l'adresse `172.31.0.0/24` est routé vers la passerelle Internet. Il s'agit d'une route statique qui a donc priorité sur la route propagée.

Destination	Cible
10.0.0.0/16	Locale
172.31.0.0/24	vgw-11223344556677889 (propagée)
172.31.0.0/24	igw-12345678901234567 (statique)

Seuls les préfixes IP connus de la passerelle réseau privé virtuel, que ce soit par une annonce BGP ou une entrée de routage statique, peuvent recevoir du trafic sortant de votre VPC. La passerelle réseau privé virtuel n'achemine pas d'autre trafic destiné en dehors des annonces BGP reçues, des saisies de routage statique ou du CIDR de VPC attaché. Les passerelles privées virtuelles ne prennent pas en charge le IPv6 trafic.

Quand une passerelle réseau privé virtuel reçoit des informations de routage, elle utilise la sélection des chemins pour déterminer comment acheminer le trafic. La correspondance de préfixe la plus longue s'applique si tous les points de terminaison sont sains. L'état du point de terminaison d'un tunnel est prioritaire par rapport aux autres attributs de routage. Cette priorité s'applique aux VPNs passerelles privées virtuelles et aux passerelles de transit. Si les préfixes sont les mêmes, la

passerelle réseau privé virtuel donne la priorité suivante aux routes, de la route la plus préférée à la route la moins préférée :

- Routes propagées par BGP à partir d'une connexion Direct Connect

  Les routes Blackhole ne sont pas propagées vers une passerelle client Site-to-Site VPN via BGP.
- Routes statiques ajoutées manuellement pour une connexion Site-to-Site VPN
- Routes propagées par BGP à partir d'une connexion VPN Site-to-Site
- Pour les préfixes correspondants lorsque chaque connexion Site-to-Site VPN utilise BGP, le PATH AS est comparé et le préfixe avec le plus court AS PATH est préféré.

  > **Note**
  >
  > AWS recommande vivement d'utiliser des dispositifs de passerelle client qui prennent en charge le routage asymétrique.
  > Pour les périphériques de passerelle client qui prennent en charge l'acheminement asymétrique, nous déconseillons d'utiliser le préfixe AS PATH, afin de garantir que les deux tunnels ont le même AS PATH. Cela permet de s'assurer que la valeur multi-exit discriminator (MED) que nous avons définie sur un tunnel lors des mises à jour du point de terminaison du tunnel VPN est utilisée pour déterminer la priorité du tunnel.
  > Pour les périphériques de passerelle client qui ne prennent pas en charge l'acheminement asymétrique, vous pouvez utiliser AS PATH prepending et Local Preference pour préférer un tunnel à l'autre. Toutefois, lorsque le chemin de sortie change, cela peut entraîner une baisse du trafic.
- Lorsque les AS PATHs ont la même longueur et si le premier AS de l'AS_SEQUENCE est le même sur plusieurs chemins, multi-exit discriminators (MEDs) sont comparés. Le chemin avec la valeur MED la plus faible est préféré.

La priorité de route est affectée lors des mises à jour des points de terminaison du tunnel VPN.

Sur une connexion Site-to-Site VPN, AWS sélectionne l'un des deux tunnels redondants comme chemin de sortie principal. Cette sélection peut parfois changer, et nous vous recommandons fortement de configurer les deux tunnels pour une haute disponibilité, et permet un routage asymétrique. L'état du point de terminaison d'un tunnel est prioritaire par rapport aux autres attributs de routage. Cette priorité s'applique aux VPNs passerelles privées virtuelles et aux passerelles de transit.

Pour une passerelle privée virtuelle, un tunnel pour toutes les connexions Site-to-Site VPN de la passerelle sera sélectionné. Pour utiliser plusieurs tunnels, nous vous recommandons d'utiliser le protocole ECMP (Equal Cost Multipath), qui est pris en charge pour les connexions Site-to-Site VPN sur une passerelle de transit. Pour plus d'informations, consultez Passerelles de transit dans Passerelles de transit Amazon VPC. L'ECMP n'est pas pris en charge pour les connexions Site-to-Site VPN sur une passerelle privée virtuelle.

Pour les connexions Site-to-Site VPN qui utilisent le protocole BGP, le tunnel principal peut être identifié par la valeur multi-exit discriminator (MED). Nous vous recommandons de publier des itinéraires BGP plus spécifiques pour influencer les décisions de routage.

Pour les connexions Site-to-Site VPN qui utilisent le routage statique, le tunnel principal peut être identifié par des statistiques ou des métriques de trafic.

Routage pendant les mises à jour des points de terminaison du tunnel VPN

Une connexion Site-to-Site VPN consiste en deux tunnels VPN entre un dispositif de passerelle client et une passerelle privée virtuelle ou une passerelle de transit. Nous vous recommandons de configurer les deux tunnels pour la redondance. De temps en temps, effectue AWS également une maintenance de routine sur votre connexion VPN, ce qui peut désactiver brièvement l'un des deux tunnels de votre connexion VPN. Pour de plus amples informations, veuillez consulter Notifications de remplacement des points de terminaison du tunnel.

Lorsque nous effectuons des mises à jour sur un tunnel VPN, nous définissons une valeur MED (multi-exit discriminator) inférieure sur l'autre tunnel. Si vous avez configuré votre périphérique de passerelle client afin qu'il utilise les deux tunnels, votre connexion VPN utilise l'autre tunnel (en amont) pendant le processus de mise à jour du point de terminaison du tunnel.

> **Note**
>
> - Pour vous assurer que le tunnel en amont avec la valeur MED inférieure est préféré, assurez-vous que votre périphérique de passerelle client utilise les mêmes valeurs de poids et de préférence locale pour les deux tunnels (les valeurs de poids et de préférence locale ont une priorité plus élevée que la valeur MED).

IPv4 et IPv6 trafic entrant AWS Site-to-Site VPN

Votre connexion Site-to-Site VPN sur une passerelle de transit peut prendre en charge le IPv4 trafic ou le IPv6 trafic à l'intérieur des tunnels VPN. Par défaut, une connexion Site-to-Site VPN prend en charge le IPv4 trafic à l'intérieur des tunnels VPN. Vous pouvez configurer une nouvelle connexion Site-to-Site VPN pour prendre en charge le IPv6 trafic à l'intérieur des tunnels VPN. Ensuite, si votre VPC et votre réseau local sont configurés pour l' IPv6 adressage, vous pouvez envoyer IPv6 du trafic via la connexion VPN.

Si vous activez IPv6 les tunnels VPN pour votre connexion Site-to-Site VPN, chaque tunnel possède deux blocs CIDR. L'un est un bloc d'adresse IPv4 CIDR de taille /30 et l'autre est un bloc d'adresse CIDR de taille /126 IPv6 .

IPv4 et IPv6 support

Site-to-Site Les connexions VPN prennent en charge les configurations IP suivantes :

- IPv4 tunnel extérieur avec paquets IPv4 internes : fonctionnalité IPv4 VPN de base prise en charge sur les passerelles privées virtuelles, les passerelles de transit et le Cloud WAN.
- IPv4 tunnel extérieur avec paquets IPv6 internes - Autorise les IPv6 applications/le transport dans le tunnel VPN. Pris en charge sur les passerelles de transit et le Cloud WAN. Cela n'est pas pris en charge pour les passerelles privées virtuelles.
- IPv6 tunnel extérieur avec paquets IPv6 internes - Permet une IPv6 migration complète avec des IPv6 adresses à la fois pour le tunnel externe IPs et pour le paquet interne IPs. Pris en charge à la fois pour les passerelles de transit et le Cloud WAN.
- IPv6 tunnel extérieur avec paquets IPv4 internes - Permet l'adressage du tunnel IPv6 externe tout en prenant en charge IPv4 les applications existantes au sein du tunnel. Pris en charge à la fois pour les passerelles de transit et le Cloud WAN.

Les règles suivantes s’appliquent :

- IPv6 les adresses du tunnel extérieur ne IPs sont prises en charge que sur les connexions Site-to-Site VPN terminées sur une passerelle de transit ou sur le Cloud WAN. Site-to-Site Les connexions VPN sur une passerelle privée virtuelle ne prennent pas en charge IPv6 le tunnel IPs extérieur.
- Lorsque vous utilisez IPv6 un tunnel externe IPs, vous devez attribuer IPv6 des adresses à la fois du AWS côté de la connexion VPN et de la passerelle client pour les deux tunnels VPN.

- Vous ne pouvez pas activer le IPv6 support pour une connexion Site-to-Site VPN existante. Vous devez supprimer la connexion existante et en créer une nouvelle.
- Une connexion Site-to-Site VPN ne peut pas prendre en charge à la fois IPv6 le trafic IPv4 et le trafic. Les paquets encapsulés internes peuvent être l'un IPv6 ou l'autre IPv4, mais pas les deux. Vous avez besoin de connexions Site-to-Site VPN distinctes pour le transport IPv4 et IPv6 les paquets.
- Les adresses IP privées VPNs ne prennent pas en charge IPv6 les adresses pour le tunnel extérieur IPs. Ils utilisent des adresses RFC 1918 ou CGNAT. Pour plus d'informations sur la RFC 1918, consultez la RFC 1918 - Allocation d'adresses pour les réseaux Internet privés.
- IPv6 VPNs supportent les mêmes limites de débit (Gbit/s et PPS), de MTU et de route que. IPv4 VPNs
- Le IPSec chiffrement et l'échange de clés fonctionnent de la même manière pour les deux IPv4 et IPv6 VPNs.

Pour plus d'informations sur la création d'une connexion VPN avec IPv6 assistance, voir Création d'une connexion VPN dans Commencer avec un Site-to-Site VPN.

AWS Site-to-Site VPN Concentrateurs

AWS Site-to-Site VPN Concentrator est une nouvelle fonctionnalité qui simplifie la connectivité multisite pour les entreprises distribuées. Le concentrateur VPN convient aux clients qui ont besoin de connecter plus de 25 sites distants à AWS, chaque site nécessitant une faible bande passante (moins de 100 Mbits/s).

Services et fonctionnalités de passerelle pris en charge

Les concentrateurs VPN ne sont pris en charge qu'avec Transit Gateway. Cette fonctionnalité n'est pas prise en charge avec Cloud WAN ou Virtual Private Gateway.

Le tableau suivant décrit les fonctionnalités prises en charge par Site-to-Site VPN Concentrator :

Fonction	Pris en charge ?
IPv6	Oui
Connexions VPN Direct Connect privées	Non

Fonction	Pris en charge ?
VPN accéléré	Oui
Plusieurs appareils de passerelle client depuis le même site	Oui. Cependant, chaque dispositif de passerelle client doit avoir une adresse IP unique.
Restrictions géographiques	Non Vous pouvez associer un site situé dans n'importe quelle région à un concentrateur de n'importe quelle AWS région.
Site-to-Site Journaux VPN	Oui. Vous pouvez générer des journaux VPN pour tous les sites connectés au Concentra tor ou individuellement.
Support pour le chiffrement de Transit Gateway	Non

Bande passante

Actuellement, les concentrateurs Site-to-Site VPN prennent en charge une bande passante globale de 5 Gbit/s. Chaque site peut prendre en charge une bande passante maximale de 100 Mbits/s. Toutefois, si vous avez besoin d'une bande passante plus élevée, contactez AWS Support.

Routage

Site-to-Site Les concentrateurs VPN prennent uniquement en charge le routage BGP (Border Gateway Protocol). Le routage statique n'est pas pris en charge.

Toutes les passerelles client connectées au Site-to-Site VPNConcentrator utilisent le même attachement Site-to-Site VPN Concentrator à la passerelle de transit pour le routage. Chaque site connecté au concentrateur Site-to-Site VPN peut envoyer un maximum de 5 000 itinéraires de la passerelle de transit vers une passerelle client et 1 000 itinéraires de la passerelle client vers la passerelle de transit.

Allocation d'adresses IP

Chaque connexion VPN via le concentrateur Site-to-Site VPN aura toujours une adresse IP AWS unique (une par tunnel).

Contrôle

Les connexions VPN via des concentrateurs Site-to-Site VPN prennent en charge les mêmes métriques que les connexions VPN classiques.

Lorsque vous activez les journaux de flux de la passerelle de transit sur la pièce jointe du concentrateur VPN, vous verrez les journaux de flux pour tout le trafic entrant et sortant de tous les sites distants connectés au concentrateur.

Entretien des tunnels

La maintenance des tunnels fonctionne de la même manière que les tunnels Site-to-Site VPN standard existants pour les deux points de terminaison lors de l'utilisation d'un concentrateur Site-to-Site VPN. Pour plus d'informations, consultez Remplacements de points de terminaison.

Tarification

Les informations relatives à la tarification de Site-to-Site VPN Concentrator sont disponibles sur la page de tarification du VPN AWS.

Commencez avec AWS Site-to-Site VPN

Pour configurer une AWS Site-to-Site VPN connexion, procédez comme suit. Lors de la création, vous devez spécifier une passerelle privée virtuelle, une passerelle de transit, un concentrateur Site-to-Site VPN ou « Non associé » comme type de passerelle cible. Si vous spécifiez « Non associé », vous pouvez choisir le type de passerelle cible ultérieurement, ou vous pouvez l'utiliser comme pièce jointe VPN pour AWS Cloud WAN. Ce didacticiel vous aide à créer une connexion VPN en utilisant une passerelle réseau privé virtuel. Il considère que vous disposez déjà d'un VPC doté d'un ou plusieurs sous-réseaux.

Pour configurer une connexion VPN en utilisant une passerelle réseau privé virtuel, procédez comme suit :

Tâches

- Conditions préalables
- Étape 1 : Création d'une passerelle client
- Étape 2 : Création d'une passerelle cible
- Étape 3 : Configuration du routage
- Étape 3 : Mise à jour du groupe de sécurité
- Étape 5 : Création d'une connexion VPN
- Étape 6 : Téléchargement du fichier de configuration
- Étape 7 : Configuration de l'appareil de passerelle client

Tâches associées

- Pour créer une connexion VPN pour AWS Cloud WAN, consultezCréez une connexion VPN Cloud WAN à l'aide de la CLI ou de l'API.
- Pour créer une connexion VPN sur une passerelle de transit, consultez Création d'une connexion VPN.

Conditions préalables

Vous avez besoin des informations suivantes pour installer et configurer les composants d'une connexion VPN.

Élément	Informations
Périphérique de passerelle client	Périphérique physique ou logiciel de votre côté de la connexion VPN. Vous avez besoin du fournisseur (par exemple, Cisco), de la plateforme (par exemple, routeurs ISR) et de la version du logiciel (par exemple, IOS 12.4)
Passerelle client	Pour créer la ressource de passerelle client dans AWS, vous avez besoin des informations suivantes : • Adresse IP routable par Internet de l'interface externe du périphérique • Type de routage : statique ou dynamique • Pour le routage dynamique, numéro d'ASN (Autonomous System Number) BGP (Border Gateway Protocol) • (Facultatif) Certificat privé Autorité de certification privée AWS pour authentifier votre VPN Pour de plus amples informations, veuillez consulter Options de passerelle client.
(Facultatif) L'ASN du AWS côté de la session BGP	Vous le spécifiez lorsque vous créez une passerelle réseau privé virtuel ou une passerell e de transit. Si vous ne spécifiez pas de valeur, l'ASN par défaut s'applique. Pour plus d'informa tions, consultez Passerelle réseau privé virtuel.
Connexion VPN	Pour créer la connexion VPN, vous avez besoin des informations suivantes : • Pour le routage statique, préfixes IP de votre réseau privé.

Élément	Informations
	• (Facultatif) Options de tunnel de chaque tunnel VPN. Pour de plus amples informations, veuillez consulter Options de tunnel pour votre AWS Site-to-Site VPN connexion.

Étape 1 : Création d'une passerelle client

Une passerelle client fournit des informations AWS sur votre dispositif de passerelle client ou votre application logicielle. Pour de plus amples informations, veuillez consulter Passerelle client.

Si vous prévoyez d'utiliser un certificat privé pour authentifier votre VPN, créez un certificat privé auprès d'une autorité de certification subordonnée à l'aide de. Autorité de certification privée AWS Pour de plus amples informations sur la création d'un certificat privé, veuillez consulter Création et gestion d'une autorité de certification privée dans le Guide de l'utilisateur Autorité de certification privée AWS .

> **Note**
>
> Vous devez spécifier une adresse IP ou l'Amazon Resource Name (ARN) du certificat privé.

Pour créer une passerelle client avec la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Passerelles client.
3. Choisissez Créer la passerelle client.
4. (Facultatif) Pour Name tag (Étiquette de nom), entrez un nom pour votre passerelle client. Une identification est alors créée avec la clé `Name` et la valeur que vous spécifiez.
5. Dans BGP ASN (Version du moteur de cache), saisissez le numéro d'ASN (Autonomous System Number) BGP (Border Gateway Protocol) de votre passerelle client.
6. Pour le type d'adresse IP, sélectionnez l'une des options suivantes :
   - IPv4- (Par défaut) Spécifiez une IPv4 adresse pour votre dispositif de passerelle client.
   - IPv6- Spécifiez une IPv6 adresse pour votre dispositif de passerelle client. Cette option est requise lors de la création d'une connexion VPN avec un tunnel IPv6 extérieur IPs.

7. Pour l'adresse IP, entrez l'adresse IP statique routable par Internet de votre dispositif de passerelle client. Si votre appareil de passerelle client est situé derrière un appareil NAT activé pour NAT-T, utilisez l'adresse IP publique de l'appareil NAT.
8. (Facultatif) Si vous souhaitez utiliser un certificat privé, pour ARN du certificat, choisissez l'Amazon Resource Name (ARN) du certificat privé.
9. (Facultatif) Pour Appareil, saisissez un nom pour l'appareil de passerelle client associé à cette passerelle client.
10. Choisissez Créer la passerelle client.

Pour créer une passerelle client à l'aide de la ligne de commande ou de l'API

- CreateCustomerGateway(API de requête Amazon EC2)
- create-customer-gateway (AWS CLI)

  Exemple de création d'une passerelle IPv6 client :

```
aws ec2 create-customer-gateway --ipv6-address
 2001:0db8:85a3:0000:0000:8a2e:0370:7334 --bgp-asn 65051 --type ipsec.1 --region us-
west-1
```

- New-EC2CustomerGateway (AWS Tools for Windows PowerShell)

Étape 2 : Création d'une passerelle cible

Pour établir une connexion VPN entre votre VPC et votre réseau local, vous devez créer une passerelle cible du AWS côté de la connexion. La passerelle cible peut être une passerelle réseau privé virtuel ou une passerelle de transit.

Créer une passerelle réseau privé virtuel

Lorsque vous créez une passerelle réseau privé virtuel, vous pouvez spécifier le numéro d'ASN (Autonomous System Number) privé pour le côté Amazon de la passerelle. Ce numéro d'ASN doit être différent de celui spécifié pour la passerelle client.

Après avoir créé une passerelle réseau privé virtuel, vous devez l'attacher à votre VPC.

Pour créer une passerelle réseau privé virtuel et l'attacher à votre VPC

1. Dans le volet de navigation, choisissez Passerelles réseau privé virtuel.
2. Cliquez sur Create virtual private gateway (Créer une passerelle réseau privé virtuel).
3. (Facultatif) Pour Identification de nom, saisissez un nom pour la passerelle réseau privé virtuel. Une identification est alors créée avec la clé `Name` et la valeur que vous spécifiez.
4. Pour Numéro de système autonome (ASN), conservez la sélection par défaut, ASN par défaut Amazon, pour utiliser l'ASN par défaut Amazon. Sinon, choisissez ASN personnalisé et entrez une valeur. Pour un ASN de 16 bits, la valeur doit être comprise entre 64512 et 65534. Pour un ASN de 32 bits, la valeur doit être comprise entre 4200000000 et 4294967294.
5. Cliquez sur Create virtual private gateway (Créer une passerelle réseau privé virtuel).
6. Sélectionnez la passerelle réseau privé virtuel que vous avez créée, puis choisissez Actions, Attach to VPC (Attacher au VPC).
7. Dans Disponible VPCs, choisissez votre VPC, puis choisissez Attacher au VPC.

Pour créer une passerelle réseau privé virtuel à l'aide de la ligne de commande ou de l'API

- CreateVpnGateway(API de requête Amazon EC2)
- create-vpn-gateway (AWS CLI)
- New-EC2VpnGateway (AWS Tools for Windows PowerShell)

Pour attacher une passerelle réseau privé virtuel à un VPC à l'aide de la ligne de commande ou de l'API

- AttachVpnGateway(API de requête Amazon EC2)
- attach-vpn-gateway (AWS CLI)
- Add-EC2VpnGateway (AWS Tools for Windows PowerShell)

Créer une passerelle de transit

Pour plus d'informations sur la création d'une passerelle de transit, consultez Passerelles de transit dans Passerelles de transit Amazon VPC.

Étape 3 : Configuration du routage

Pour permettre aux instances de votre VPC d'atteindre la passerelle client, vous devez configurer la table de routage pour y inclure les routes utilisées par la connexion VPN et les diriger vers la passerelle réseau privé virtuel ou la passerelle de transit.

(Passerelle réseau privé virtuel) Activer la propagation de route dans votre table de routage

Vous pouvez activer la propagation des itinéraires pour votre table de routage afin de propager automatiquement les itinéraires Site-to-Site VPN.

Pour un routage statique, les préfixes IP statiques que vous spécifiez dans votre configuration VPN sont propagés vers la table de routage lorsque la connexion VPN a le statut UP. De même, pour un routage dynamique, les routes publiées par BGP depuis votre passerelle client sont propagées vers la table de routage quand la connexion VPN a le statut UP.

> **Note**
>
> Si votre connexion est interrompue mais que la connexion VPN reste à l'état UP (en fonction), toutes les routes propagées qui se trouvent dans votre table de routage ne sont pas automatiquement supprimées. Gardez cela à l'esprit si, par exemple, vous voulez que le trafic soit transféré à une route statique en cas de besoin. Dans ce cas, vous devrez peut-être désactiver la propagation de route pour supprimer les routes propagées.

Pour activer la propagation de route avec la console

1. Dans le volet de navigation, choisissez Route tables (Tables de routage).
2. Sélectionnez la table de routage associée au sous-réseau.
3. Dans l'onglet Propagation de routage, choisissez Modifier la propagation de routage. Sélectionnez la passerelle réseau privé virtuel que vous avez créée dans la procédure précédente, puis choisissez Enregistrer.

> **Note**
>
> Si vous n'autorisez pas la propagation de routage, vous devez saisir manuellement les routes statiques utilisées par votre connexion VPN. Pour ce faire, sélectionnez votre table de routage et choisissez Routes, Modifier. Pour Destination, ajoutez la route statique utilisée par votre connexion Site-to-Site VPN. Pour Cible, sélectionnez l'ID de passerelle réseau privé virtuel et choisissez Enregistrer.

Pour désactiver la propagation de route avec la console

1. Dans le volet de navigation, choisissez Route tables (Tables de routage).
2. Sélectionnez la table de routage associée au sous-réseau.
3. Dans l'onglet Propagation de routage, choisissez Modifier la propagation de routage. Décochez la case Propager correspondant à la passerelle réseau privé virtuel.
4. Choisissez Enregistrer.

Pour activer la propagation de route à l'aide de la ligne de commande ou d'une API

- EnableVgwRoutePropagation(API de requête Amazon EC2)
- enable-vgw-route-propagation (AWS CLI)
- Enable-EC2VgwRoutePropagation (AWS Tools for Windows PowerShell)

Pour désactiver la propagation de route à l'aide de la ligne de commande ou d'une API

- DisableVgwRoutePropagation(API de requête Amazon EC2)
- disable-vgw-route-propagation (AWS CLI)
- Disable-EC2VgwRoutePropagation (AWS Tools for Windows PowerShell)

(Passerelle de transit) Ajouter une route à votre table de routage

Si vous avez activé la propagation de la table de routage pour votre passerelle de transit, les routes de l'attachement VPN sont propagées vers la table de routage de la passerelle de transit. Pour plus d'informations, consultez Routage dans Passerelles de transit Amazon VPC.

Si vous attachez un VPC à votre passerelle de transit et que vous souhaitez permettre aux ressources du VPC d'atteindre votre passerelle client, vous devez ajouter à votre table de routage de sous-réseau une route pointant vers la passerelle de transit.

Pour ajouter une route vers une table de routage de VPC

1. Dans le volet de navigation, choisissez Tables de routage.
2. Choisissez la table de routage associée à votre VPC.
3. Dans l'onglet Routes, choisissez Edit routes (Modifier les routes).
4. Choisissez Ajouter une route.
5. Pour Destination, saisissez la plage d'adresses IP de destination. Pour Cible, choisissez la passerelle de transit.
6. Sélectionnez Enregistrer les modifications.

Étape 3 : Mise à jour du groupe de sécurité

Pour autoriser l'accès aux instances dans votre VPC à partir de votre réseau, vous devez mettre à jour les règles des groupes de sécurité afin de permettre l'accès SSH, RDP et ICMP entrant.

Pour ajouter des règles à votre groupe de sécurité afin d'autoriser l'accès

1. Dans le panneau de navigation, choisissez Groupes de sécurité.
2. Sélectionnez le groupe de sécurité pour les instances de votre VPC auxquelles vous souhaitez autoriser l'accès.
3. Sous l'onglet Inbound Rules (Règles entrantes), sélectionnez Edit inbound rules (Modifier les règles entrantes).
4. Ajoutez des règles qui autorisent l'accès SSH, RDP et ICMP entrant depuis votre réseau, puis choisissez Enregistrer les règles. Pour en savoir plus, consultez Utilisation de règles de groupe de sécurité dans le Guide de l'utilisateur Amazon VPC.

Étape 5 : Création d'une connexion VPN

Créez la connexion VPN en utilisant la passerelle client en association avec la passerelle réseau privé virtuel ou la passerelle de transit que vous avez créée précédemment.

Pour créer une connexion VPN :

1. Dans le volet de navigation, sélectionnez Connexions Site-to-Site VPN.
2. Choisissez Create VPN connection (Créer une connexion VPN).
3. (Facultatif) Pour Identification de nom, saisissez un nom pour votre connexion VPN. Cette étape crée une balise avec une clé de `Name` et la valeur que vous spécifiez.
4. Pour Target Gateway Type (Type de passerelle cible), choisissez Virtual Private Gateway (Passerelle réseau privé virtuel) ou Transit Gateway (Passerelle de transit). Ensuite, choisissez la passerelle réseau privé virtuel ou la passerelle de transit que vous avez créée précédemment.
5. Pour Passerelle client, sélectionnez Existante, puis choisissez la passerelle client que vous avez créée précédemment à partir de ID de passerelle client.
6. Sélectionnez l'une des options de routage selon que votre dispositif de passerelle client prend en charge le protocole BGP (Border Gateway Protocol) :

   - Si votre périphérique de passerelle client prend en charge BGP, choisissez Dynamique (nécessite BGP).
   - Si votre périphérique de passerelle client ne prend pas en charge BGP, choisissez Statique. Pour Préfixes IP statiques, spécifiez chaque préfixe IP pour le réseau privé de votre connexion VPN.
7. Choisissez le type de stockage de clés pré-partagé :

   - Standard — La clé pré-partagée est stockée directement dans le service Site-to-Site VPN.
   - Secrets Manager — La clé pré-partagée est stockée à l'aide AWS Secrets Manager de. Pour plus d'informations sur Secrets Manager, consultezFonctionnalités de sécurité améliorées à l'aide de Secrets Manager.
8. Si votre type de passerelle cible est une passerelle de transit, pour la version Tunnel inside IP, spécifiez si les tunnels VPN prennent en charge le IPv6 trafic IPv4 ou le trafic. IPv6 le trafic n'est pris en charge que pour les connexions VPN sur une passerelle de transit.
9. Si vous avez spécifié IPv4la version Tunnel inside IP, vous pouvez éventuellement spécifier les plages IPv4 CIDR pour la passerelle client et AWS les côtés autorisés à communiquer via les tunnels VPN. La valeur par défaut est `0.0.0.0/0`.

   Si vous avez spécifié IPv6la version Tunnel inside IP, vous pouvez éventuellement spécifier les plages IPv6 CIDR pour la passerelle client et AWS les côtés autorisés à communiquer via les tunnels VPN. La valeur par défaut pour les deux plages est `::/0`.
10. Pour le type d'adresse IP externe, sélectionnez l'une des options suivantes :

- PublicIpv4 - (Par défaut) Utilisez les IPv4 adresses du tunnel extérieur IPs.
- IPv6- Utilisez IPv6 les adresses du tunnel extérieur IPs. Cette option n'est disponible que pour les connexions VPN sur une passerelle de transit ou sur le Cloud WAN.

11. (Facultatif) Pour Options de tunnel, vous pouvez spécifier les informations suivantes pour chaque tunnel :

    - Un bloc IPv4 CIDR de taille /30 issu de la `169.254.0.0/16` plage des adresses du tunnel IPv4 intérieur.
    - Si vous avez spécifié IPv6pour la version IP du tunnel intérieur, un bloc d'adresse IPv6 CIDR /126 dans la `fd00::/8` plage des adresses du tunnel IPv6 intérieur.
    - La clé pré-partagée (PSK) IKE. Les versions suivantes sont prises en charge : IKEv1 ou IKEv2.
    - Pour modifier les options avancées de votre tunnel, choisissez Modifier les options du tunnel. Pour de plus amples informations, veuillez consulter Options de tunnel VPN.

12. Choisissez Create VPN connection (Créer une connexion VPN). La création de la connexion VPN peut prendre quelques minutes.

Pour créer une connexion VPN à l'aide de la ligne de commande ou de l'API

- CreateVpnConnection(API de requête Amazon EC2)
- create-vpn-connection (AWS CLI)

  Exemple de création d'une connexion VPN avec un tunnel IPv6 extérieur IPs et un tunnel IPv6 intérieur IPs :

```
aws ec2 create-vpn-connection --type ipsec.1 --transit-gateway-id
 tgw-12312312312312312 --customer-gateway-id cgw-001122334455aabbc --options
 OutsideIPAddressType=IPv6,TunnelInsideIpVersion=ipv6,TunnelOptions=[{StartupAction=start},
{StartupAction=start}]
```

  Exemple de création d'une connexion VPN avec un tunnel IPv6 extérieur IPs et un tunnel IPv4 intérieur IPs :

```
aws ec2 create-vpn-connection --type ipsec.1 --transit-gateway-id
 tgw-12312312312312312 --customer-gateway-id cgw-001122334455aabbc --options
```

```
 OutsideIPAddressType=IPv6,TunnelInsideIpVersion=ipv4,TunnelOptions=[{StartupAction=start},
{StartupAction=start}]
```

- New-EC2VpnConnection (AWS Tools for Windows PowerShell)

Étape 6 : Téléchargement du fichier de configuration

Après avoir créé la connexion VPN, vous pouvez télécharger un exemple de fichier de configuration à utiliser pour configurer l'appareil de passerelle client.

> **Important**
>
> Le fichier de configuration présenté est un simple exemple et peut ne pas correspondre entièrement aux paramètres de connexion VPN que vous souhaitez. Il spécifie les exigences minimales pour une connexion VPN de AES128 SHA1, et Diffie-Hellman groupe 2 dans la plupart des AWS régions, et, AES128 SHA2, et Diffie-Hellman groupe 14 dans les régions. AWS GovCloud Il spécifie également des clés prépartagées pour l'authentification. Vous devez modifier l'exemple de fichier de configuration pour tirer parti des algorithmes de sécurité supplémentaires, des groupes Diffie-Hellman, des certificats privés et du trafic. IPv6 Nous avons intégré la IKEv2 prise en charge des fichiers de configuration pour de nombreux appareils de passerelle client courants et nous continuerons d'ajouter des fichiers supplémentaires au fil du temps. Pour obtenir la liste des fichiers de configuration pris en IKEv2 charge, consultezAWS Site-to-Site VPN dispositifs de passerelle client.

Permissions

Pour charger correctement l'écran de configuration du téléchargement depuis le Console de gestion AWS, vous devez vous assurer que votre rôle ou utilisateur IAM est autorisé à accéder à l'Amazon APIs EC2 `GetVpnConnectionDeviceTypes` suivant : et. `GetVpnConnectionDeviceSampleConfiguration`

Pour télécharger le fichier de configuration en utilisant la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Connexions Site-to-Site VPN.
3. Sélectionnez votre connexion VPN, puis choisissez Télécharger la configuration.

4. Sélectionnez le fournisseur, la plateforme, les logiciels et la version IKE qui correspondent à votre appareil de passerelle client. Si votre périphérique n'est pas répertorié, choisissez Generic (Générique).
5. Choisissez Téléchargement.

Pour télécharger un exemple de fichier de configuration à l'aide de la ligne de commande ou de l'API

- GetVpnConnectionDeviceTypes(API Amazon EC2)
- GetVpnConnectionDeviceSampleConfiguration(API de requête Amazon EC2)
- get-vpn-connection-device-types ()AWS CLI
- get-vpn-connection-device-exemple de configuration ()AWS CLI

Étape 7 : Configuration de l'appareil de passerelle client

Utilisez l'exemple de fichier de configuration pour configurer votre périphérique de passerelle client. Un appareil de passerelle client est une appliance physique ou logicielle située de votre côté de la connexion VPN. Pour de plus amples informations, veuillez consulter AWS Site-to-Site VPN dispositifs de passerelle client.

AWS Site-to-Site VPN scénarios architecturaux

Voici des scénarios dans lesquels vous pouvez créer plusieurs connexions VPN avec un ou plusieurs périphériques de passerelle client.

Plusieurs connexions VPN utilisant le même périphérique de passerelle client

Vous pouvez créer des connexions VPN supplémentaires entre votre site local et d'autres sites VPCs en utilisant le même dispositif de passerelle client. De plus, vous pouvez réutiliser la même adresse IP de passerelle client pour chacune de ces connexions VPN.

Plusieurs dispositifs de passerelle client vers une seule passerelle privée virtuelle (Site-to-Site VPN CloudHub)

Vous pouvez établir plusieurs connexions VPN sur une passerelle réseau privé virtuel à partir de plusieurs passerelles client. Cela vous permet d'avoir plusieurs sites connectés au AWS VPN CloudHub. Pour de plus amples informations, veuillez consulter Communication sécurisée entre les AWS Site-to-Site VPN connexions à l'aide d'un VPN CloudHub. Lorsque vous disposez de passerelles client dans plusieurs sites géographiques, chacune d'entre elles doit publier un ensemble unique de plages d'adresses IP propres à chaque emplacement.

Connexion VPN redondante utilisant un deuxième périphérique de passerelle client

Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre périphérique de passerelle client, vous pouvez configurer une seconde connexion VPN vers votre VPC en utilisant un second périphérique de passerelle client. Pour de plus amples informations, veuillez consulter Redondant AWS Site-to-Site VPN connexions pour basculement. Lorsque vous établissez des passerelles client redondantes dans un même emplacement, ces dernières doivent publier les mêmes plages d'adresses IP.

Les architectures Site-to-Site VPN les plus courantes sont les suivantes :

- Connexions VPN uniques et multiples
- the section called “Connexions VPN redondantes”
- Communications sécurisées entre les connexions VPN à l'aide du VPN CloudHub

AWS Site-to-Site VPN exemples de connexions VPN uniques et multiples

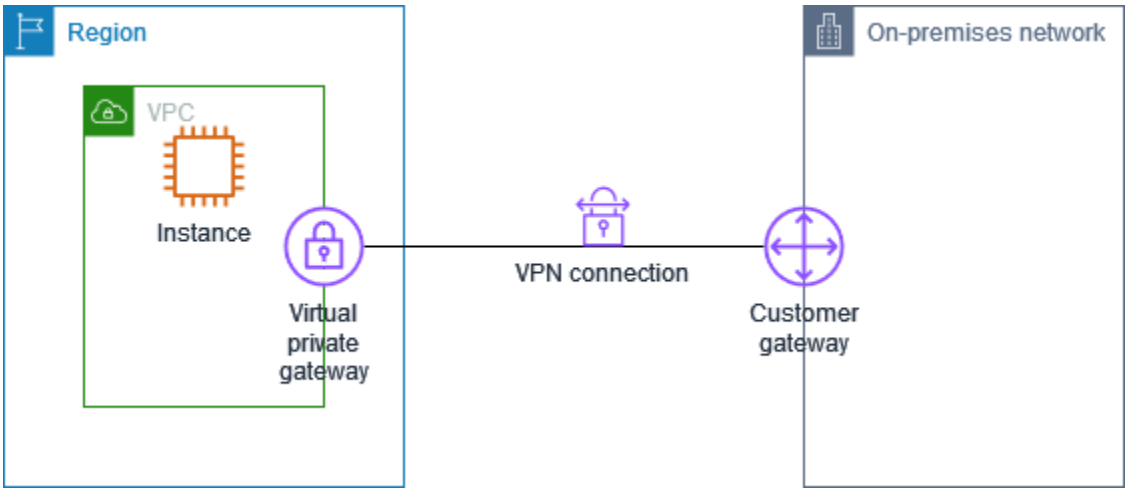
Les diagrammes suivants illustrent les connexions Site-to-Site VPN uniques et multiples.

Exemples

- Connexion Site-to-Site VPN unique
- Connexion Site-to-Site VPN unique avec passerelle de transit
- Connexions Site-to-Site VPN multiples
- Connexions Site-to-Site VPN multiples avec une passerelle de transit
- Site-to-Site Connexion VPN avec Direct Connect
- Connexion Site-to-Site VPN IP privée avec Direct Connect

Connexion Site-to-Site VPN unique

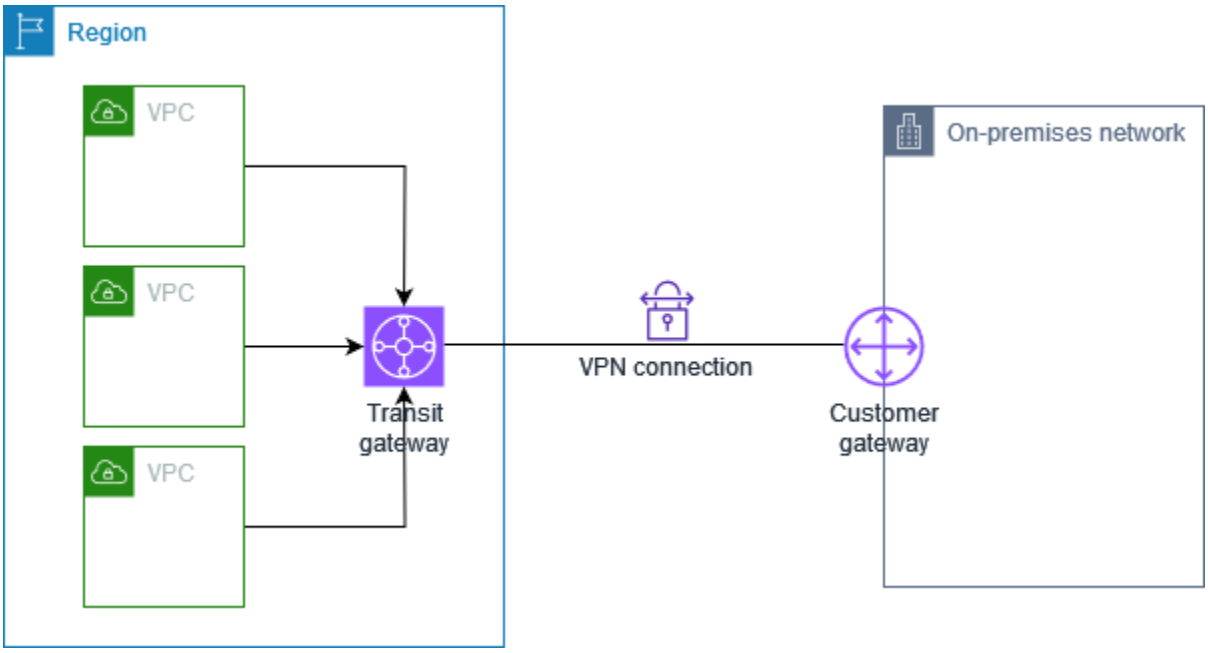
Le VPC a une passerelle réseau privé virtuel attachée et votre réseau sur site (distant) comprend un périphérique de passerelle client que vous devez configurer pour activer la connexion VPN. Vous devez mettre à jour les tables de routage de VPC afin que le trafic de votre VPC lié à votre réseau soit acheminé vers la passerelle réseau privé virtuel.



Pour connaître la procédure à suivre pour configurer ce scénario, consultez Commencez avec AWS Site-to-Site VPN.

Connexion Site-to-Site VPN unique avec passerelle de transit

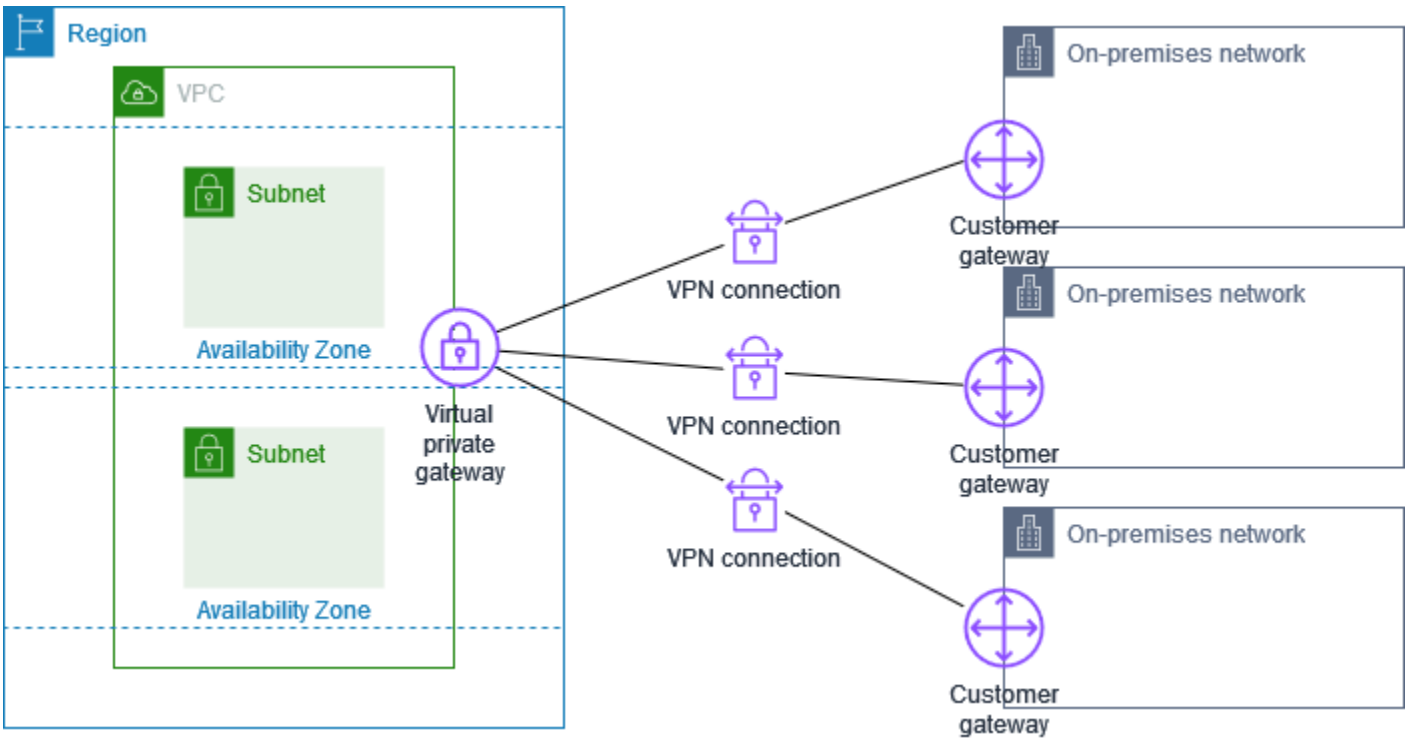
Le VPC a une passerelle de transit attachée et votre réseau sur site (distant) comprend un périphérique de passerelle client que vous devez configurer pour permettre la connexion VPN. Vous devez mettre à jour les tables de routage de VPC afin que le trafic de votre VPC lié à votre réseau soit acheminé vers la passerelle de transit.



Pour connaître la procédure à suivre pour configurer ce scénario, consultez Commencez avec AWS Site-to-Site VPN.

Connexions Site-to-Site VPN multiples

Le VPC est associé à une passerelle privée virtuelle, et vous disposez de plusieurs connexions Site-to-Site VPN vers plusieurs sites sur site. Vous configurez le routage afin que le trafic de votre VPC lié à votre réseau soit acheminé vers la passerelle réseau privé virtuel.

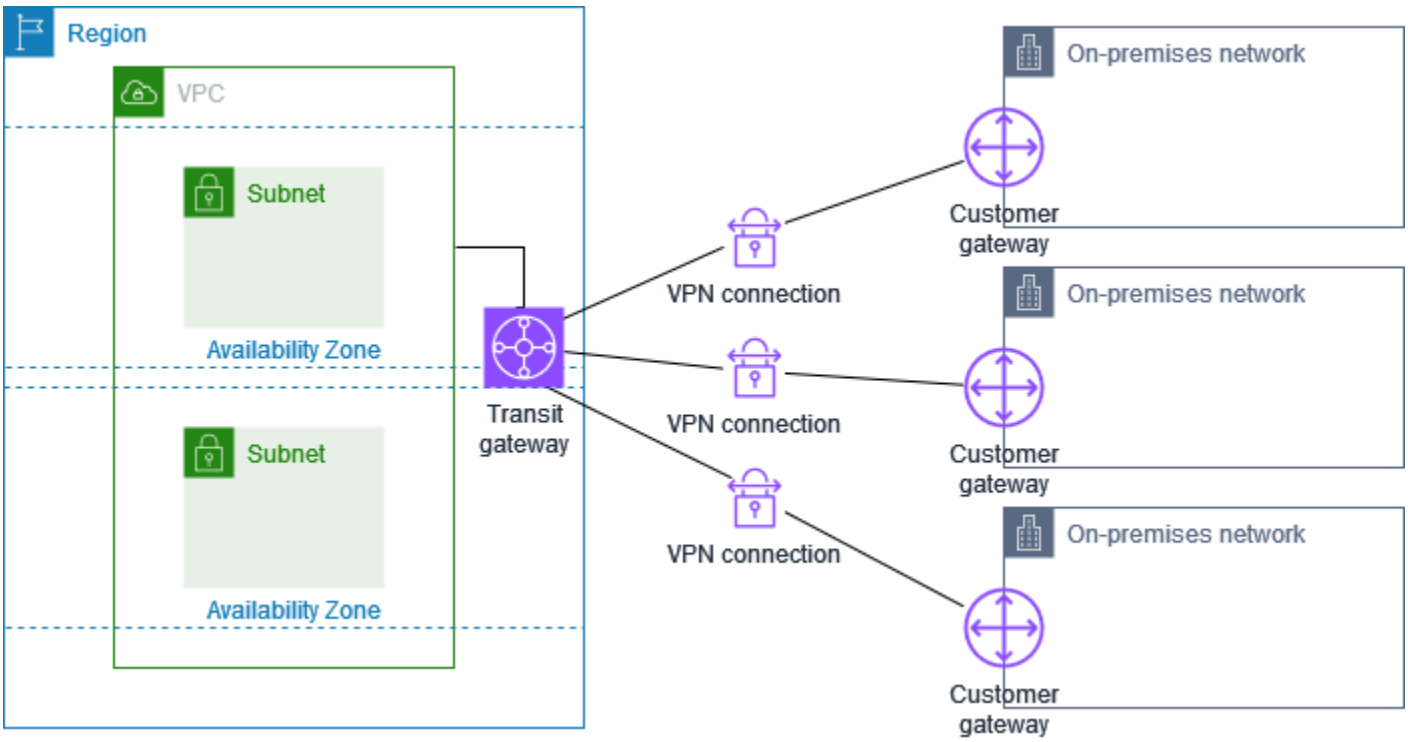


Lorsque vous créez plusieurs connexions Site-to-Site VPN vers un seul VPC, vous pouvez configurer une deuxième passerelle client pour créer une connexion redondante vers le même emplacement externe. Pour de plus amples informations, veuillez consulter Redondant AWS Site-to-Site VPN connexions pour basculement.

Vous pouvez également utiliser ce scénario pour créer des connexions Site-to-Site VPN vers plusieurs sites géographiques et sécuriser les communications entre les sites. Pour de plus amples informations, veuillez consulter Communication sécurisée entre les AWS Site-to-Site VPN connexions à l'aide d'un VPN CloudHub.

Connexions Site-to-Site VPN multiples avec une passerelle de transit

Le VPC possède une passerelle de transit attachée, et vous disposez de plusieurs connexions Site-to-Site VPN vers plusieurs sites sur site. Vous configurez le routage afin que le trafic de votre VPC lié à vos réseaux soit acheminé vers la passerelle de transit.

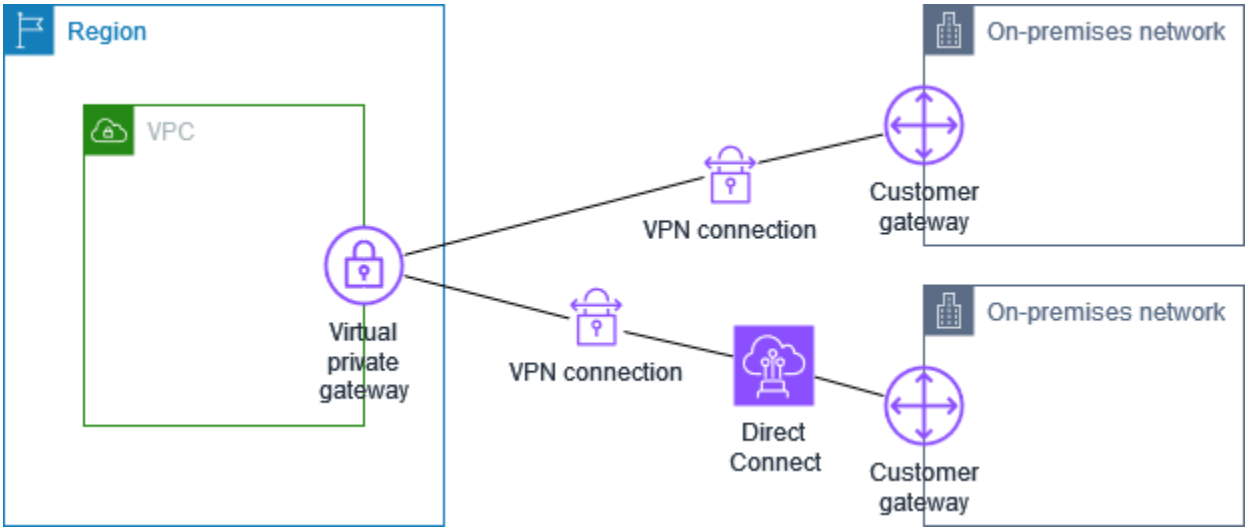


Lorsque vous créez plusieurs connexions Site-to-Site VPN vers une seule passerelle de transit, vous pouvez configurer une deuxième passerelle client pour créer une connexion redondante vers le même emplacement externe.

Vous pouvez également utiliser ce scénario pour créer des connexions Site-to-Site VPN vers plusieurs sites géographiques et sécuriser les communications entre les sites.

Site-to-Site Connexion VPN avec Direct Connect

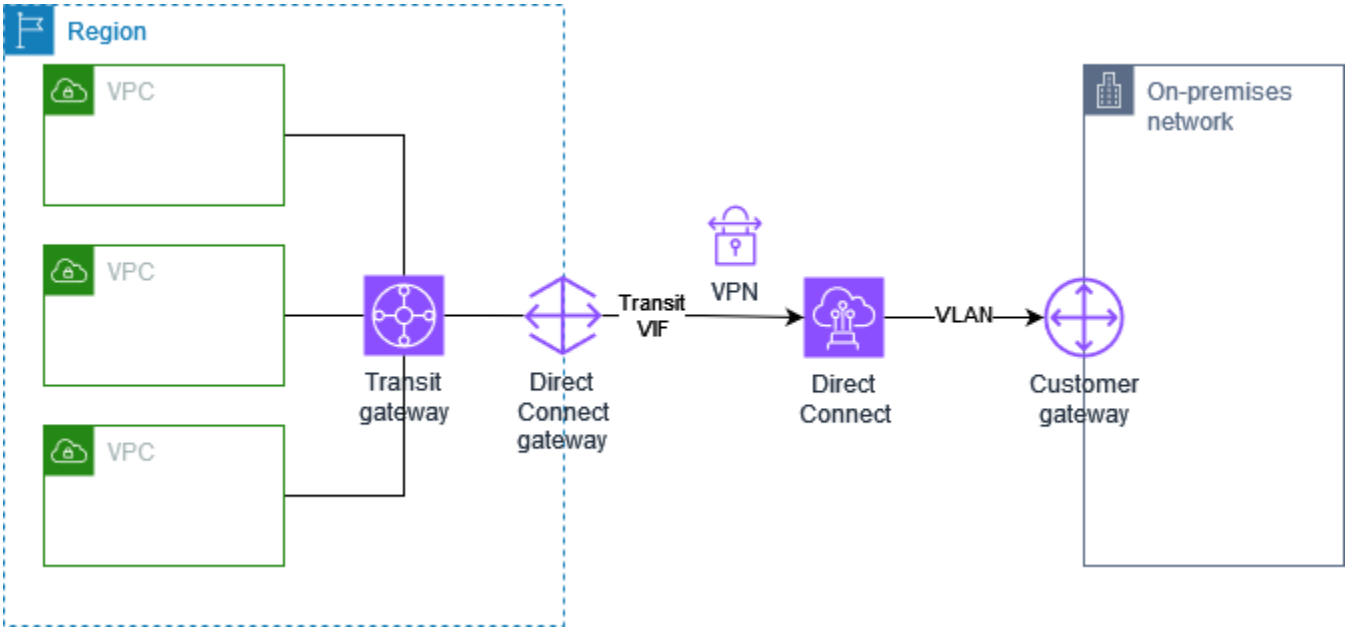
Le VPC possède une passerelle privée virtuelle attachée et se connecte à votre réseau sur site (distant) via. AWS Direct Connect Vous pouvez configurer une interface virtuelle Direct Connect publique pour établir une connexion réseau dédiée entre votre réseau et les AWS ressources publiques via une passerelle privée virtuelle. Vous configurez le routage de telle sorte que tout trafic provenant du VPC à destination de votre réseau soit acheminé vers la passerelle privée virtuelle et la Direct Connect connexion.



Lorsque les deux connexions Direct Connect et la connexion VPN sont configurées sur la même passerelle privée virtuelle, l'ajout ou la suppression d'objets peut faire passer la passerelle privée virtuelle à l'état « attache ». Cela indique qu'une modification est apportée au routage interne qui basculera entre Direct Connect et la connexion VPN afin de minimiser les interruptions et les pertes de paquets. Après cela, la passerelle réseau privé virtuel revient à l'état « attachée ».

Connexion Site-to-Site VPN IP privée avec Direct Connect

Avec un Site-to-Site VPN IP privé, vous pouvez chiffrer Direct Connect le trafic entre votre réseau local AWS sans utiliser d'adresses IP publiques. Le VPN IP privé Direct Connect garantit que le trafic entre les réseaux locaux AWS et sur site est à la fois sécurisé et privé, ce qui permet aux clients de se conformer aux obligations réglementaires et de sécurité.



Pour obtenir des conseils sur le choix de la bonne solution VPN, voir Sélection de la bonne solution AWS VPN : un cadre décisionnel.

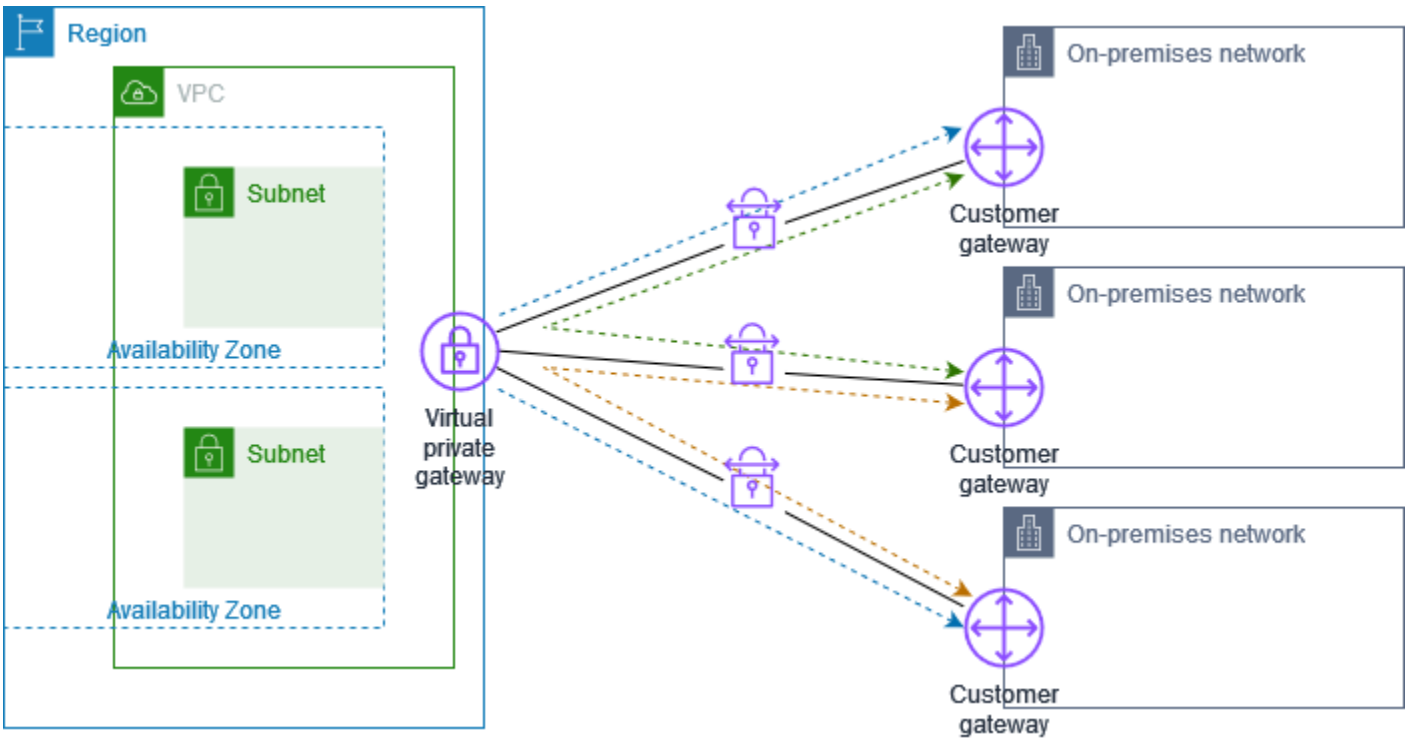
Pour plus d'informations, consultez le billet de blog suivant : Présentation des VPN IP AWS Site-to-Site VPN privés.

Communication sécurisée entre les AWS Site-to-Site VPN connexions à l'aide d'un VPN CloudHub

Si vous disposez de plusieurs AWS Site-to-Site VPN connexions, vous pouvez assurer une communication sécurisée entre les sites à l'aide du AWS VPN CloudHub. Cela permet à vos sites de communiquer entre eux et pas uniquement avec les ressources dans votre VPC. Le VPN CloudHub fonctionne selon un hub-and-spoke modèle simple que vous pouvez utiliser avec ou sans VPC. Cette conception convient si vous avez plusieurs succursales et des 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 secours entre ces sites.

Présentation de

Le schéma suivant montre l' CloudHub architecture du VPN. Les lignes pointillées indiquent le trafic réseau entre des sites distants acheminé via les connexions VPN. Les sites ne doivent pas avoir de plages d'adresses IP qui se chevauchent.



Pour ce scénario, procédez comme suit :

1. Créez une passerelle réseau privé virtuel unique.
2. Créez plusieurs passerelles client, chacune avec l'adresse IP publique de la passerelle. Vous devez utiliser un numéro d'ASN (Autonomous System Number) BGP (Border Gateway Protocol) unique pour chaque passerelle client.
3. Créez une connexion Site-to-Site VPN routée dynamiquement entre chaque passerelle client et la passerelle privée virtuelle commune.
4. Configurez chaque passerelle client pour publier un préfixe propre à un site (tel que 10.0.0.0/24, 10.0.1.0/24) sur la passerelle réseau privé virtuel. Ces annonces de routage sont reçues et ré-publiées pour chaque BGP pair, pour permettre à chaque site d'envoyer des données vers les autres sites et d'en recevoir. Cela se fait à l'aide des instructions réseau contenues dans les fichiers de configuration VPN pour la connexion Site-to-Site VPN. Les relevés du réseau sont légèrement différents en fonction du type de routeur que vous utilisez.
5. Configurez les routes dans vos tables de routage de sous-réseau pour permettre aux instances de votre VPC de communiquer avec vos sites. Pour de plus amples informations, veuillez consulter (Passerelle réseau privé virtuel) Activer la propagation de route dans votre table de routage. Vous pouvez configurer une route agrégée dans votre table de routage (par exemple, 10.0.0.0/16). Utilisez des préfixes plus spécifiques entre les passerelles client et la passerelle réseau privé virtuel.

Les sites qui utilisent Direct Connect des connexions à la passerelle privée virtuelle peuvent également faire partie du AWS VPN CloudHub. Par exemple, le siège social de votre entreprise à New York peut être Direct Connect connecté au VPC et vos succursales peuvent utiliser des connexions Site-to-Site VPN avec le VPC. Les succursales de Los Angeles et de Miami peuvent envoyer et recevoir des données entre elles et avec le siège de votre entreprise, le tout à l'aide du AWS VPN CloudHub.

Tarification

Pour utiliser AWS un VPN CloudHub, vous payez les tarifs habituels de connexion Site-to-Site VPN Amazon VPC. Le tarif de la connexion vous est facturé pour chaque heure de connexion de chaque VPN à la passerelle réseau privé virtuel. Lorsque vous envoyez des données d'un site à un autre à l'aide du AWS VPN CloudHub, l'envoi de données de votre site vers la passerelle privée virtuelle est gratuit. Vous payez uniquement les tarifs de transfert de données AWS standard pour les données qui sont transmises de la passerelle réseau privé virtuel vers votre point de terminaison.

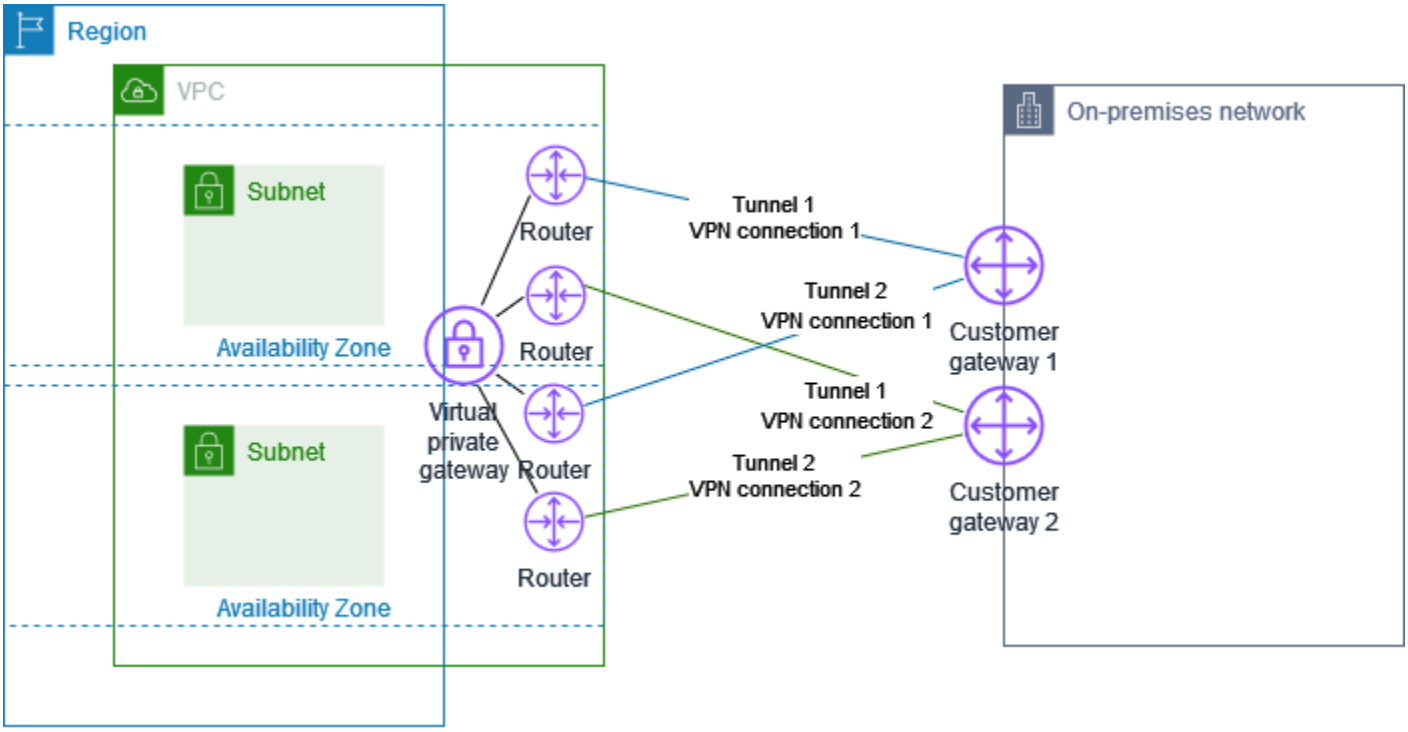
Par exemple, si vous avez un site à Los Angeles et un deuxième site à New York et que les deux sites disposent d'une connexion Site-to-Site VPN à la passerelle privée virtuelle, vous payez le tarif horaire pour chaque connexion Site-to-Site VPN (donc si le tarif était de 0,05 dollar de l'heure, ce serait un total de 0,10 dollar de l'heure). Vous payez également les tarifs de transfert de AWS données standard pour toutes les données que vous envoyez de Los Angeles à New York (et vice versa) Site-to-Site via chaque connexion VPN. Le trafic réseau envoyé via la connexion Site-to-Site VPN à la passerelle privée virtuelle est gratuit, mais le trafic réseau envoyé via la connexion Site-to-Site VPN de la passerelle privée virtuelle au point de terminaison est facturé au taux de transfert de AWS données standard.

Pour en savoir plus, consultez Site-to-Site Tarification de connexion VPN.

Redondant AWS Site-to-Site VPN connexions pour basculement

Pour vous protéger contre une perte de connectivité en cas d'indisponibilité de votre dispositif de passerelle client, vous pouvez configurer une deuxième connexion Site-to-Site VPN vers votre VPC et votre passerelle privée virtuelle en ajoutant un deuxième dispositif de passerelle client. En utilisant des connexions VPN et des périphériques de passerelle client redondantes, vous pouvez effectuer une opération de maintenance sur l'un de vos périphériques pendant que le trafic continue d'être acheminé via la seconde connexion VPN.

Le schéma suivant illustre deux connexions VPN. Chaque connexion VPN possède ses propres tunnels et sa propre passerelle client.



Pour ce scénario, procédez comme suit :

- Configurez une deuxième connexion Site-to-Site VPN en utilisant la même passerelle privée virtuelle et en créant une nouvelle passerelle client. L'adresse IP de la passerelle client pour la deuxième connexion Site-to-Site VPN doit être accessible au public.
- Configurez un second périphérique de passerelle client. Les deux appareils doivent annoncer les mêmes plages IP sur la passerelle réseau privé virtuel. Nous utilisons le routage BGP pour déterminer le chemin pour le trafic. En cas de défaillance d'une des passerelles client, la passerelle réseau privé virtuel dirige tout le trafic vers celle qui est opérationnelle.

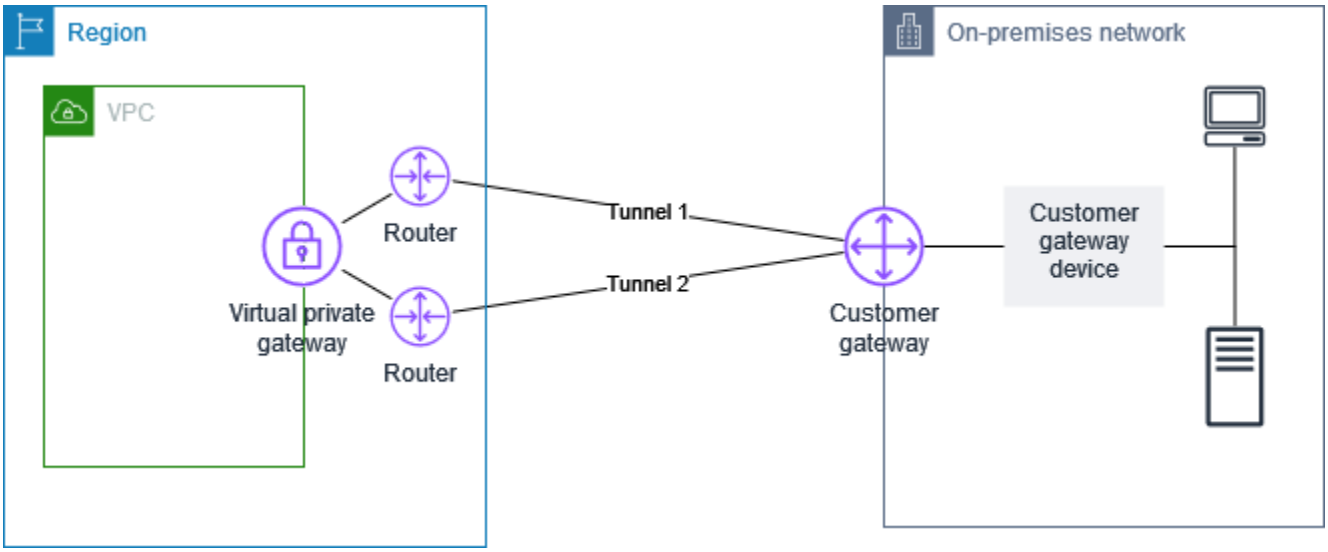
Les connexions Site-to-Site VPN routées dynamiquement utilisent le protocole BGP (Border Gateway Protocol) pour échanger des informations de routage entre les passerelles de vos clients et les passerelles privées virtuelles. Les connexions Site-to-Site VPN à routage statique nécessitent que vous saisissiez des itinéraires statiques pour le réseau distant situé de votre côté de la passerelle client. BGP-advertised et les informations d'itinéraire saisies de manière statique permettent aux passerelles des deux côtés de déterminer quels tunnels sont disponibles et de rediriger le trafic en cas de panne. Nous vous recommandons de configurer votre réseau pour utiliser les informations de routage fournies par BGP (si disponible) pour sélectionner un chemin disponible. La configuration exacte dépend de l'architecture de votre réseau.

Pour plus d'informations sur la création et la configuration d'une passerelle client et d'une connexion Site-to-Site VPN, consultezCommencez avec AWS Site-to-Site VPN.

AWS Site-to-Site VPN dispositifs de passerelle client

Un dispositif de passerelle client est une appliance physique ou logicielle que vous possédez ou gérez sur votre réseau local (de votre côté d'une connexion Site-to-Site VPN). Vous ou votre administrateur réseau devez configurer l'appareil pour qu'il fonctionne avec la connexion Site-to-Site VPN.

Le diagramme suivant illustre votre réseau, le périphérique de passerelle client et la connexion VPN qui mène à une passerelle réseau privé virtuel qui est attachée à votre VPC. Les deux lignes entre la passerelle client et la passerelle réseau privé virtuel représentent les tunnels de la connexion VPN. En cas de panne d'un appareil AWS, votre connexion VPN bascule automatiquement vers le second tunnel afin que votre accès ne soit pas interrompu. De temps en temps, effectue AWS également une maintenance de routine sur la connexion VPN, ce qui peut désactiver brièvement l'un des deux tunnels de votre connexion VPN. Pour de plus amples informations, veuillez consulter AWS Site-to-Site VPN remplacement des extrémités des tunnels. Lorsque vous configurez votre périphérique de passerelle client, il est donc important de le configurer afin qu'il utilise les deux tunnels.



Pour plus d'informations sur la configuration d'une connexion VPN, consultez Commencez avec AWS Site-to-Site VPN. Au cours de ce processus, vous créez une ressource de passerelle client dans AWS, qui fournit des informations AWS sur votre appareil, par exemple son adresse IP destinée au public. Pour de plus amples informations, veuillez consulter Options de passerelle client pour votre AWS Site-to-Site VPN connexion. La ressource de passerelle client dans AWS ne configure ni ne crée le dispositif de passerelle client. Vous devez configurer l'appareil vous-même.

Vous trouverez également des dispositifs de VPN logiciel sur AWS Marketplace.

Exigences relatives à un AWS Site-to-Site VPN Appareil de passerelle client

AWS prend en charge un certain nombre de dispositifs de passerelle client Site-to-Site VPN, pour lesquels nous fournissons des fichiers de configuration téléchargeables. Pour obtenir la liste des appareils pris en charge et les étapes de téléchargement des fichiers de configuration, consultezFichiers de configuration de routage statiques et dynamiques.

Si votre appareil ne figure pas dans la liste des appareils pris en charge, la section suivante décrit les exigences auxquelles l'appareil doit satisfaire pour établir une connexion Site-to-Site VPN.

La configuration de votre périphérique de passerelle client est composée de 4 éléments principaux. Les symboles suivants représentent chaque partie de la configuration.

IKE	Association de sécurité IKE (Internet Key Exchange). Cette association est nécessaire pour échanger les clés utilisées pour établir l'association de sécurité IPsec.
IPsec	Association de sécurité IPsec. Cette association gère, entre autres, le chiffrement et l'authentification du tunnel.
Tunnel	Interface du tunnel. Cette interface reçoit le trafic allant vers le tunnel et en revenant.
BGP	(Facultatif) Appairage Border Gateway Protocol (BGP). Pour les périphériques utilisant BGP, cet appairage échange les routes entre le périphérique de passerelle client et la passerelle réseau privé virtuel.

Le tableau ci-dessous répertorie les conditions que le périphérique de passerelle client doit respecter, la RFC concernée (pour information) et des commentaires sur ces conditions.

Chaque connexion VPN se compose de deux tunnels distincts. Chaque tunnel comporte une association de sécurité IKE, une association de sécurité IPsec et un appairage BGP. Vous êtes limité à une paire d'association de sécurité (SA) unique par tunnel (une entrante et une sortante), et donc à deux paires de SA uniques au total pour deux tunnels (quatre SA). Certains périphériques utilisent un VPN basé sur une stratégie et créent autant de SA que d'entrées ACL (liste de contrôle d'accès). Par conséquent, vous pouvez être amené à regrouper vos règles, puis à définir des filtres afin de ne pas autoriser le trafic non souhaité.

Par défaut, le tunnel VPN est activé lorsque le trafic est généré et que la négociation IKE est lancée depuis votre côté de la connexion VPN. Vous pouvez configurer la connexion VPN pour lancer la négociation IKE du AWS côté de la connexion à la place. Pour de plus amples informations, veuillez consulter AWS Site-to-Site VPN options d'initiation du tunnel.

Les points de terminaison VPN prennent en charge le changement de clé et peuvent initier les renégociations lorsque la phase 1 est sur le point d'expirer si la passerelle client n'a envoyé aucun trafic de renégociation.

Exigence	RFC	Commentaires
Établir une association de sécurité IKE IKE	RFC 2409 RFC 7296	L'association de sécurité IKE est d'abord établie entre la passerelle privée virtuelle et le dispositif de passerelle client à l'aide d'une clé pré-partagée ou d'un certificat privé utilisé Autorité de certification privée AWS comme authentificateur. Une fois l'association établie, IKE négocie une clé éphémère afin de sécuriser les futurs messages IKE. Il doit y avoir un accord complet entre les paramètres, y compris les paramètres de chiffrement et d'authentification. Lorsque vous créez une connexion VPN dans AWS, vous pouvez spécifier votre propre clé pré-partagée pour chaque tunnel, ou vous pouvez laisser en AWS générer une pour vous. Vous pouvez également spécifier le certificat privé Autorité de certification privée AWS à utiliser pour votre dispositif de passerelle client. Pour plus d'informations sur la configuration des tunnels VPN, consultez Options de tunnel pour votre AWS Site-to-Site VPN connexion. Les versions suivantes sont prises en charge : IKEv1 et IKEv2. Nous prenons en charge le mode Principal uniquement avec la version IKEv1.

Exigence	RFC	Commentaires
		Le service Site-to-Site VPN est une solution basée sur les itinéraires. Si vous utilisez une configuration basée sur des stratégies, vous devez limiter votre configura tion à une seule association de sécurité.
Établir des associations de sécurité IPsec en mode tunnel IPsec	RFC 4301	Grâce à la clé éphémère IKE, des clés sont établies entre la passerelle réseau privé virtuel et le périphéri que de passerelle client de façon à former une association de sécurité (SA) IPsec. Le trafic entre les passerelles est chiffré et déchiffré à l'aide de cette SA. Les clés éphémères utilisées pour chiffrer le trafic au sein de la SA IPsec font l'objet d'une rotation automatique et régulière par IKE afin de garantir la confidentialité des communications.
Utiliser la fonction de chiffrement AES 128 bits ou 256 bits	RFC 3602	La fonction de chiffrement est utilisée pour garantir la confidentialité pour les associations de sécurité IKE et IPsec.
Utiliser la fonction de hachage SHA-1 or SHA-2 (256)	RFC 2404	Cette fonction de hachage est utilisée pour authentifier les associations de sécurité IKE et IPsec.
Utilisez Diffie-Hellman Perfect Forward Secrecy.	RFC 2409	IKE établit des clés éphémères Diffie-Hellman afin de sécuriser toutes les communications entre les dispositi fs de passerelle client et les passerelles privées virtuelles. Les groupes suivants sont pris en charge : • Phase 1 : groupes 2, 14-24 • Phase 2 : groupes 2, 5, 14-24

Exigence	RFC	Commentaires
(Connexions Dynamically-routed VPN) Utiliser la détection IPSec Dead Peer	RFC 3706	Le mécanisme DPD (Dead Peer Detection) permet aux périphériques VPN de savoir rapidement quand une condition réseau empêche la transmission de paquets sur Internet. Lorsque cette situation se produit, les passerelles suppriment les associations de sécurité et tentent d'en créer de nouvelles. Au cours de ce processus, l'autre tunnel IPsec est utilisé dans la mesure du possible.
(connexions Dynamically-routed VPN) Lier le tunnel à l'interface logique (VPN basé sur la route) Tunnel	Aucune	Votre périphérique doit pouvoir relier le tunnel IPsec à une interface logique. L'interface logique comporte une adresse IP qui est utilisée pour établir l'appairage BGP avec la passerelle réseau privé virtuel. Cette interface logique ne doit exécuter aucune encapsulation supplémentaire (par exemple, GRE ou IP dans IP). Votre interface doit être définie sur une unité de transmission maximale (MTU) de 1 399 octets.
(Connexions Dynamically-routed VPN) Établissez des peerings BGP BGP	RFC 4271	Le protocole BGP permet d'échanger des routes entre le périphérique de passerelle client et la passerelle réseau privé virtuel pour les périphériques qui l'utilisent. L'ensemble du trafic BGP est chiffré et transmis via l'association de sécurité IPsec. Le protocole BGP est requis pour les deux passerelles afin d'échanger les préfixes IP qui sont accessibles via l'association de sécurité IPsec.

Une connexion AWS VPN ne prend pas en charge Path MTU Discovery (RFC 1191).

Si vous disposez d'un pare-feu entre votre périphérique de passerelle client et Internet, consultez Règles de pare-feu pour un AWS Site-to-Site VPN Appareil de passerelle client.

Les meilleures pratiques pour un AWS Site-to-Site VPN Appareil de passerelle client

Utiliser IKEv2

Nous vous recommandons vivement d'utiliser IKEv2 pour votre Site-to-Site connexion VPN. IKEv2 est un protocole plus simple, plus robuste et plus sécurisé que le protocole IKEv1. Vous ne devez utiliser IKEv1 que si votre dispositif de passerelle client ne prend pas en charge IKEv2. Pour plus de détails sur les différences entre IKEv1 et IKEv2, voir l'annexe A de la RFC7296.

Réinitialiser le drapeau « Don't Fragment (DF) » (Ne pas fragmenter) dans les paquets

Certains paquets comportent un indicateur, appelé indicateur DF (Don't Fragment, Ne pas fragmenter), indiquant qu'il ne faut pas les fragmenter. Si les paquets comportent cet indicateur, les passerelles génèrent un message ICMP indiquant que la taille PMTU (Path MTU) a été dépassée. Dans certains cas, les applications n'incluent pas de mécanismes appropriés pour traiter ces messages ICMP et réduire la quantité de données transmises dans chaque paquet. Certains périphériques VPN peuvent remplacer l'indicateur DF et fragmenter les paquets sans condition si nécessaire. Si votre passerelle client possède cette fonctionnalité, nous vous recommandons de l'utiliser le cas échéant. Consultez RFC 791 pour plus de détails.

Pratiquer une fragmentation par paquets IP avant le chiffrement

Si les paquets envoyés via votre connexion Site-to-Site VPN dépassent la taille de la MTU, ils doivent être fragmentés. Pour éviter une baisse des performances, nous vous recommandons de configurer votre dispositif de passerelle client pour fragmenter les paquets avant qu'ils ne soient chiffrés. Site-to-Site Le VPN réassemble ensuite tous les paquets fragmentés avant de les transférer vers la destination suivante, afin d'obtenir des flux de paquets par seconde plus élevés sur le réseau. AWS Consultez RFC 4459 pour plus de détails.

Assurez-vous que la taille des paquets ne dépasse pas la MTU pour les réseaux de destination

Étant donné que le Site-to-Site VPN réassemble tous les paquets fragmentés reçus de la passerelle de votre client avant de les transférer vers la destination suivante, n'oubliez pas qu'il peut y avoir des size/MTU considérations relatives aux paquets pour les réseaux de destination sur lesquels ces paquets seront ensuite transférés, par exemple Direct Connect, ou avec certains protocoles, tels que Radius.

Ajustement des tailles MTU et MSS en fonction des algorithmes utilisés

Les paquets TCP sont souvent le type de paquet le plus courant dans les tunnels IPSec. Site-to-Site Le VPN prend en charge une unité de transmission maximale (MTU) de 1446 octets et une taille de segment maximale (MSS) correspondante de 1406 octets. Cependant, les algorithmes de chiffrement ont des tailles d'en-tête variables et peuvent empêcher d'atteindre ces valeurs maximales. Pour obtenir des performances optimales en évitant la fragmentation, nous vous recommandons de définir la MTU et la MSS en fonction des algorithmes utilisés.

Utilisez le tableau suivant pour configurer votre système afin MTU/MSS d'éviter la fragmentation et d'obtenir des performances optimales :

Algorithme de chiffrement	Algorithme de hachage	NAT-Traversal	MTU	MSS (IPv4)	MME () IPv6-in-IPv4
AES-GCM-16	N/A	désactivées	1446	1406	1386
AES-GCM-16	N/A	activé	1438	1398	1378
AES-CBC	SHA1/SHA2-256	désactivées	1438	1398	1378
AES-CBC	SHA1/SHA2-256	activé	1422	1382	1362
AES-CBC	SHA2-384	désactivées	1422	1382	1362
AES-CBC	SHA2-384	activé	1422	1382	1362
AES-CBC	SHA2-512	désactivées	1422	1382	1362
AES-CBC	SHA2-512	activé	1406	1366	1346

> **Note**
>
> Les AES-GCM algorithmes couvrent à la fois le chiffrement et l'authentification, il n'y a donc pas de choix d'algorithme d'authentification distinct qui affecterait le MTU.

Désactiver les identifiants uniques IKE

Certains dispositifs de passerelle client prennent en charge un paramètre garantissant qu'il existe au maximum une association de sécurité de phase 1 par configuration de tunnel. Ce paramètre peut entraîner des états de phase 2 incohérents entre les homologues VPN. Si votre dispositif de passerelle client prend en charge ce paramètre, nous vous recommandons de le désactiver.

Règles de pare-feu pour un AWS Site-to-Site VPN Appareil de passerelle client

Vous devez disposer d'une adresse IP statique à utiliser comme point de terminaison pour les tunnels IPsec qui connectent votre dispositif de passerelle client aux points de AWS Site-to-Site VPN terminaison. Si un pare-feu est en place entre AWS et votre dispositif de passerelle client, les règles décrites dans les tableaux suivants doivent être en place pour établir les tunnels IPsec. Les adresses IP du AWS côté -side figureront dans le fichier de configuration.

Entrant (depuis Internet)

Règle entrante I1	
IP Source	Adresse IP extérieure Tunnel1
IP Dest	Passerelle client
Protocole	UDP
Port source	500
Destination	500
Règle entrante I2	
IP Source	Adresse IP extérieure Tunnel2
IP Dest	Passerelle client
Protocole	UDP
Port source	500
Port de destination	500
Règle entrante I3	

IP Source	Adresse IP extérieure Tunnel1
IP Dest	Passerelle client
Protocole	IP 50 (ESP)
Règle entrante I4	
IP Source	Adresse IP extérieure Tunnel2
IP Dest	Passerelle client
Protocole	IP 50 (ESP)

Sortant (vers Internet)

Règle sortante O1	
IP Source	Passerelle client
IP Dest	Adresse IP extérieure Tunnel1
Protocole	UDP
Port source	500
Port de destination	500
Règle sortante O2	
IP Source	Passerelle client
IP Dest	Adresse IP extérieure Tunnel2
Protocole	UDP
Port source	500
Port de destination	500
Règle sortante O3	

IP Source	Passerelle client
IP Dest	Adresse IP extérieure Tunnel1
Protocole	IP 50 (ESP)
Règle sortante O4	
IP Source	Passerelle client
IP Dest	Adresse IP extérieure Tunnel2
Protocole	IP 50 (ESP)

Les règles I1, I2, O1 et O2 permettent la transmission des paquets IKE. Les règles I3, I4, O3 et O4 permettent la transmission des paquets IPsec contenant le trafic réseau chiffré.

> **Note**
>
> Si vous utilisez la traversée NAT (NAT-T) sur votre appareil, assurez-vous que le trafic UDP sur le port 4500 est également autorisé à passer entre votre réseau et les AWS Site-to-Site VPN points de terminaison. Vérifiez si votre appareil fait de la publicité NAT-T.

Fichiers de configuration statiques et dynamiques pour un AWS Site-to-Site VPN Appareil de passerelle client

Après avoir créé la connexion VPN, vous avez également la possibilité de télécharger un exemple de fichier de configuration fourni par AWS depuis la console Amazon VPC ou via l'API EC2. Pour plus d'informations, consultez Étape 6 : Téléchargement du fichier de configuration. Vous pouvez également télécharger des fichiers .zip contenant des exemples de configurations spécifiques pour le routage statique ou dynamique à partir de ces pages respectives.

L'exemple de fichier de configuration AWS fourni contient des informations spécifiques à votre connexion VPN que vous pouvez utiliser pour configurer votre dispositif de passerelle client. Ces fichiers de configuration spécifiques au périphérique sont disponibles uniquement pour les périphériques testés par AWS. Si votre périphérique de passerelle client spécifique n'est pas répertorié, vous pouvez commencer par télécharger un fichier de configuration générique.

Important

Le fichier de configuration n'est qu'un exemple et il se peut qu'il ne corresponde pas entièrement aux paramètres de connexion Site-to-Site VPN que vous avez définis. Il spécifie les exigences minimales pour une connexion Site-to-Site VPN AES128, SHA1 et Diffie-Hellman groupe 2 dans la plupart des AWS régions, et AES128, SHA2 et Diffie-Hellman groupe 14 dans les régions. AWS GovCloud Il spécifie également des clés prépartagées pour l'authentification. Vous devez modifier l'exemple de fichier de configuration pour tirer parti des algorithmes de sécurité supplémentaires, Diffie-Hellman des groupes, des certificats privés et du trafic IPv6.

Note

Ces fichiers de configuration spécifiques à l'appareil sont fournis dans AWS la mesure du possible. Bien qu'ils aient été testés par AWS, ces tests sont limités. Si vous rencontrez un problème avec les fichiers de configuration, vous devrez peut-être contacter le fournisseur concerné pour obtenir une assistance supplémentaire.

Le tableau suivant contient la liste des périphériques pour lesquels il est possible de télécharger un exemple de fichier de configuration mis à jour pour prendre en charge IKEv2. Nous avons introduit la prise en charge d'IKEv2 dans les fichiers de configuration pour de nombreux périphériques de passerelle client très répandus et continuerons d'ajouter des fichiers supplémentaires au fil du temps. Cette liste sera mise à jour à mesure que d'autres exemples de fichiers de configuration seront ajoutés.

Vendor	Plateforme	Logiciels
AXGATE	NF	AOS 3.2+
AXGATE	UTM	IOS 2.1+
Checkpoint	Gaia	R80.10+
Cisco Meraki	MX Series	15.12+ (WebUI)
Cisco Systems, Inc.	ASA 5500 Series	ASA 9.7+ VTI

Vendor	Plateforme	Logiciels
Cisco Systems, Inc.	CSRv AMI	IOS 12.4+
Fortinet	Fortigate 40+ Series	FortiOS 6.4.4+ (GUI)
Juniper Networks, Inc.	J-Series Routeurs	JunOS 9.5+
Juniper Networks, Inc.	Routeurs SRX	JunOS 11.0+
Mikrotik	RouterOS	6,44.3
Palo Alto Networks	PA Series	PANOS 7.0+
SonicWall	NSA, TZ	OS 6.5
Sophos	Par-feu Sophos	v19+
Strongswan	Ubuntu 16.04	Strongswan 5.5.1+
Yamaha	Routeurs RTX	Rev.10.01.16+

Fichiers de configuration de routage statique téléchargeables pour un dispositif de passerelle AWS Site-to-Site VPN client

Pour télécharger un exemple de fichier de configuration avec des valeurs spécifiques à la configuration de votre connexion Site-to-Site VPN, utilisez la console Amazon VPC, la ligne de AWS commande ou l'API Amazon EC2. Pour de plus amples informations, veuillez consulter Étape 6 : Téléchargement du fichier de configuration.

Vous pouvez également télécharger des exemples de fichiers de configuration génériques pour le routage statique qui n'incluent pas de valeurs spécifiques à la configuration de votre connexion Site-to-Site VPN : static-routing-examples.zip

Les fichiers utilisent des valeurs d'espace réservé pour certains composants. Par exemple, ils utilisent :

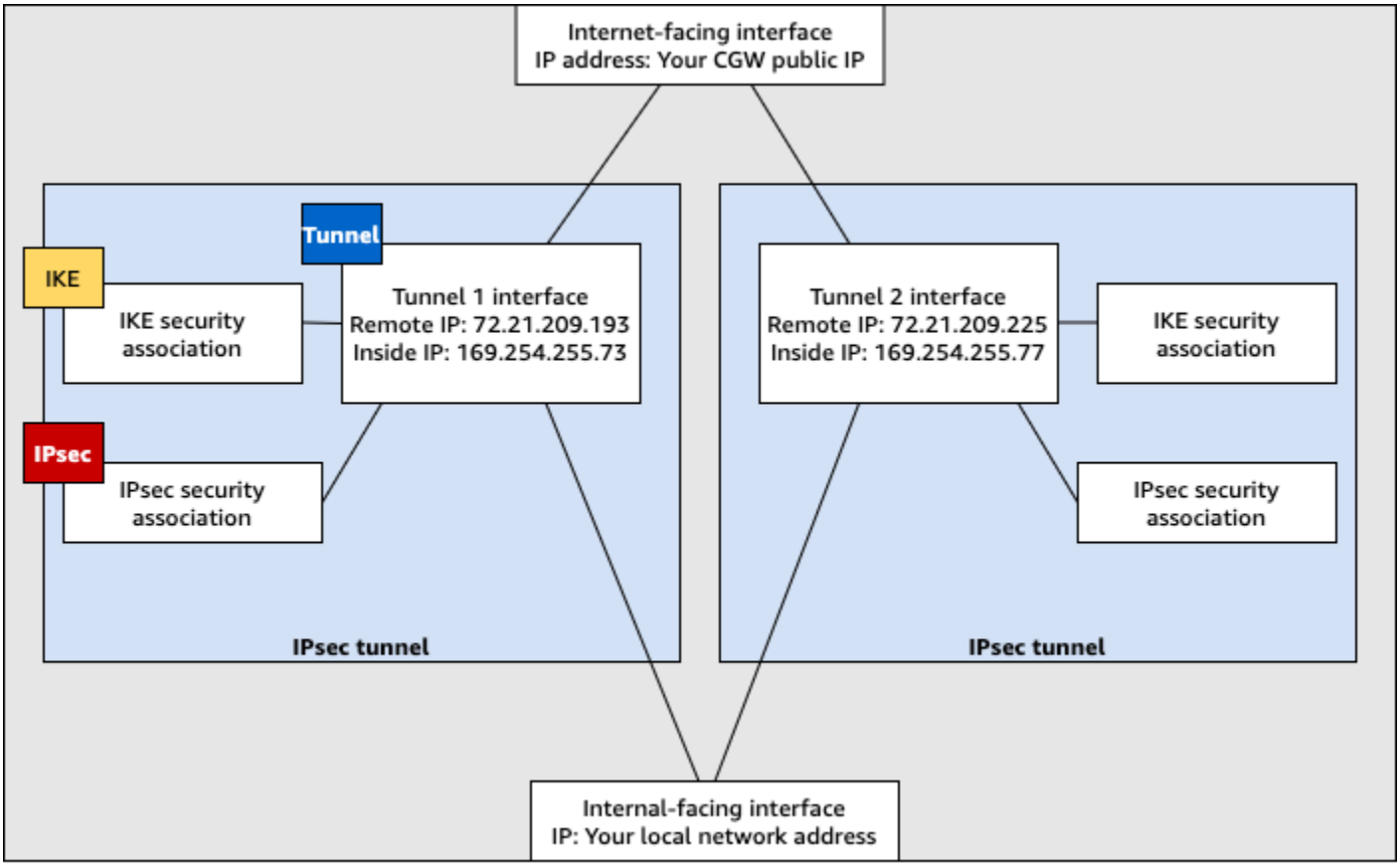
- Des exemples de valeurs pour l'ID de connexion VPN, l'ID de passerelle client et l'ID de passerelle réseau privé virtuel

- Espaces réservés aux AWS points de terminaison d'adresses IP distants (*AWS_ENDPOINT_1*et) *AWS_ENDPOINT_2*
- Un espace réservé pour l'adresse IP de l'interface externe routable par Internet sur le dispositif de passerelle client () *your-cgw-ip-address*
- Un espace réservé pour la valeur clé pré-partagée () pre-shared-key
- Des exemples de valeurs pour le tunnel à l'intérieur des adresses IP.
- Exemples de valeurs pour le paramètre MTU.

> **Note**
>
> Les paramètres MTU fournis dans les exemples de fichiers de configuration ne sont que des exemples. Veuillez vous référer à Les meilleures pratiques pour un AWS Site-to-Site VPN Appareil de passerelle client pour obtenir des informations sur la définition de la valeur MTU optimale pour votre situation.

En plus de fournir des valeurs d'espace réservé, les fichiers spécifient les exigences minimales pour une connexion Site-to-Site VPN de AES128, SHA1, et du groupe Diffie-Hellman 2 dans la plupart des AWS régions, et AES128 SHA2, et du groupe Diffie-Hellman 14 dans les régions. AWS GovCloud Ils spécifient également des clés prépartagées pour l'authentification. Vous devez modifier l'exemple de fichier de configuration pour tirer parti des algorithmes de sécurité supplémentaires, des groupes Diffie-Hellman, des certificats privés et du trafic. IPv6

Le diagramme suivant fournit une vue d'ensemble des différents composants configurés sur le périphérique de passerelle client. Il inclut des exemples de valeurs pour les adresses IP de l'interface tunnel.



Configuration du routage statique pour un dispositif de passerelle AWS Site-to-Site VPN client

Voici quelques exemples de procédures pour configurer un périphérique de passerelle client à l'aide de son interface utilisateur (si disponible).

Check Point

Voici les étapes à suivre pour configurer votre dispositif de passerelle client s'il s'agit d'un appareil Check Point Security Gateway exécutant la version R77.10 ou une version ultérieure, à l'aide du système d'exploitation Gaia et de Check Point. SmartDashboard Vous pouvez également consulter l'article VPC de Check Point Security IPsec Gateway sur le VPC d'Amazon Web Services sur le Check Point Support Center.

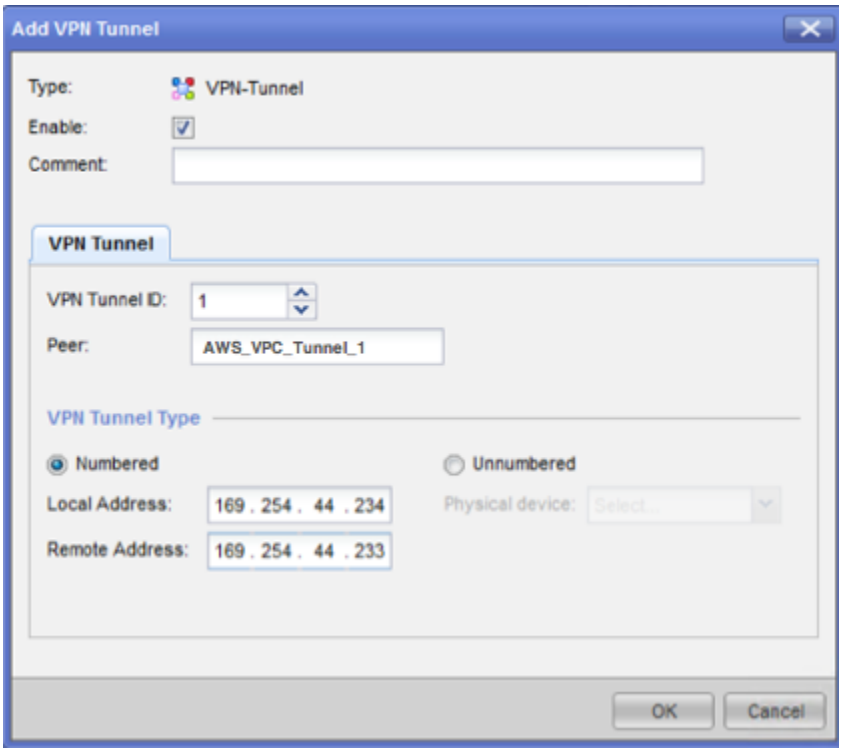
Pour configurer l'interface du tunnel

La première étape consiste à créer les tunnels VPN et à fournir les adresses IP privées (internes) de la passerelle client et de la passerelle réseau privé virtuel pour chaque tunnel. Pour créer le

premier tunnel, utilisez les informations fournies dans la section `IPSec Tunnel #1` du fichier de configuration. Pour créer le second tunnel, utilisez les valeurs fournies dans la section `IPSec Tunnel #2` du fichier de configuration.

1. Ouvrez le portail Gaia de votre périphérique Check Point Security Gateway.
2. Sélectionnez successivement Network Interfaces, Add, VPN tunnel.
3. Dans la boîte de dialogue, configurez les paramètres comme suit et choisissez OK lorsque vous avez terminé :

   - Pour VPN Tunnel ID, entrez une valeur unique, telle que 1.
   - Pour Peer, entrez un nom unique pour votre tunnel, tel que `AWS_VPC_Tunnel_1` ou `AWS_VPC_Tunnel_2`.
   - Vérifiez que Numbered (Numéroté) est sélectionné et, pour Local Address (Adresse locale), entrez l'adresse IP spécifiée pour `CGW Tunnel IP` dans le fichier de configuration (`169.254.44.234`, par exemple).
   - Pour Remote Address, entrez l'adresse IP spécifiée pour `VGW Tunnel IP` dans le fichier de configuration (`169.254.44.233`, par exemple).



4. Connectez-vous à votre passerelle de sécurité via SSH. Si vous utilisez le shell autre que celui par défaut, choisissez clish en exécutant la commande suivante : `clish`

5. Pour tunnel 1, exécutez la commande suivante :

```
set interface vpnt1 mtu 1436
```

   Pour tunnel 2, exécutez la commande suivante :

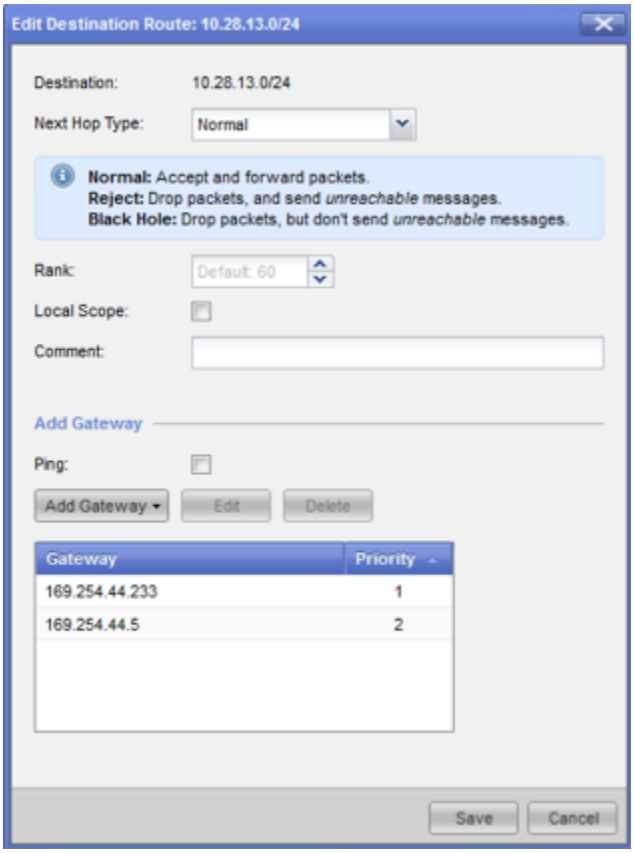
```
set interface vpnt2 mtu 1436
```

6. Répétez ces étapes pour créer un second tunnel, à l'aide des informations de la section `IPSec Tunnel #2` du fichier de configuration.

Pour configurer les itinéraires statiques

Dans cette étape, spécifiez la route statique vers le sous-réseau dans le VPC de chaque tunnel pour vous permettre d'acheminer le trafic via les interfaces de tunnel. Le second tunnel permet un basculement en cas de problème avec le premier tunnel. Si un problème est détecté, la stratégie basée sur la route statique est supprimée de la table de routage et la deuxième route est activée. Vous devez également activer la passerelle Check Point pour effectuer un test ping sur l'autre extrémité du tunnel et vérifier que le tunnel est opérationnel.

1. Dans le portail Gaia, choisissez IPv4 Static Routes, puis Ajouter.
2. Spécifiez le CIDR de votre sous-réseau : par exemple, `10.28.13.0/24`.
3. Choisissez Add Gateway, IP Address.
4. Entrez l'adresse IP spécifiée pour `VGW Tunnel IP` dans le fichier de configuration (par exemple, `169.254.44.233`) et spécifiez une priorité égale à 1.
5. Sélectionnez Ping.
6. Répétez les étapes 3 et 4 pour le second tunnel, à l'aide de la valeur `VGW Tunnel IP` de la section `IPSec Tunnel #2` du fichier de configuration. Spécifiez une priorité égale à 2.



7. Choisissez Enregistrer.

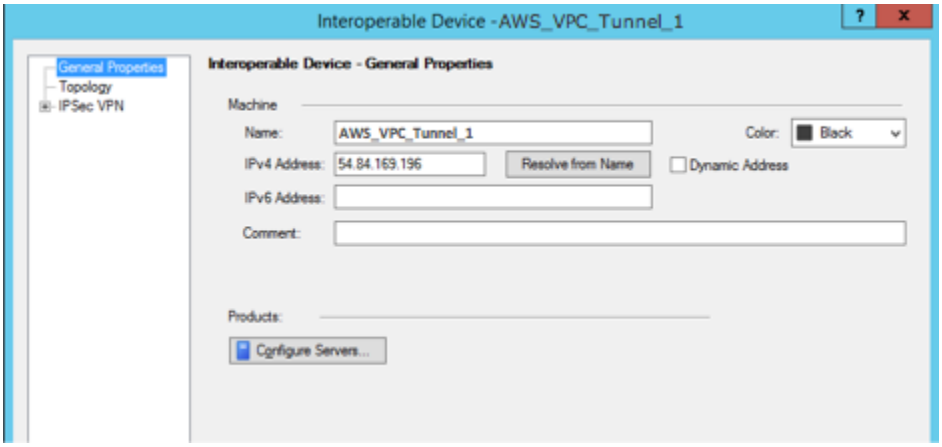
Si vous utilisez un cluster, répétez les étapes précédentes pour les autres membres du cluster.

Pour définir un nouvel objet réseau

Dans cette étape, vous créez un objet réseau pour chaque tunnel VPN, en spécifiant les adresses IP publiques (externes) de la passerelle réseau privé virtuel. Par la suite, vous ajoutez ces objets réseau en tant que passerelles satellite pour votre communauté VPN. Vous devez également créer un groupe vide comme espace réservé du domaine VPN.

1. Ouvrez le point de contrôle SmartDashboard.
2. Pour Groups, ouvrez le menu contextuel et choisissez Groups, Simple Group. Vous pouvez utiliser le même groupe pour chaque objet réseau.
3. Pour Network Objects, ouvrez le menu contextuel (clic droit) et choisissez New, Interoperable Device.
4. Pour Name (Nom), entrez le nom que vous avez fourni pour votre tunnel : `AWS_VPC_Tunnel_1` ou `AWS_VPC_Tunnel_2`, par exemple.

5. Pour IPv4 Adresse, entrez l'adresse IP externe de la passerelle privée virtuelle fournie dans le fichier de configuration, par exemple,`54.84.169.196`. Enregistrez vos paramètres et fermez la boîte de dialogue.



6. Dans le volet SmartDashboard, ouvrez les propriétés de votre passerelle et dans le volet des catégories, sélectionnez Topology.
7. Pour récupérer la configuration de l'interface, choisissez Get Topology.
8. Dans la section VPN Domain (Domaine VPN), choisissez Manually defined (Défini manuellement), puis accédez au groupe simple vide que vous avez créé à l'étape 2 et sélectionnez-le. Choisissez OK.

> **Note**
>
> Vous pouvez conserver n'importe quel domaine VPN existant que vous avez configuré. Cependant, assurez-vous que les hôtes et les réseaux qui sont utilisés ou servis par la nouvelle connexion VPN ne sont pas déclarés dans ce domaine VPN, notamment si le domaine VPN est automatiquement dérivé.

9. Répétez ces étapes pour créer un second objet réseau, à l'aide des informations de la section `IPSec Tunnel #2` du fichier de configuration.

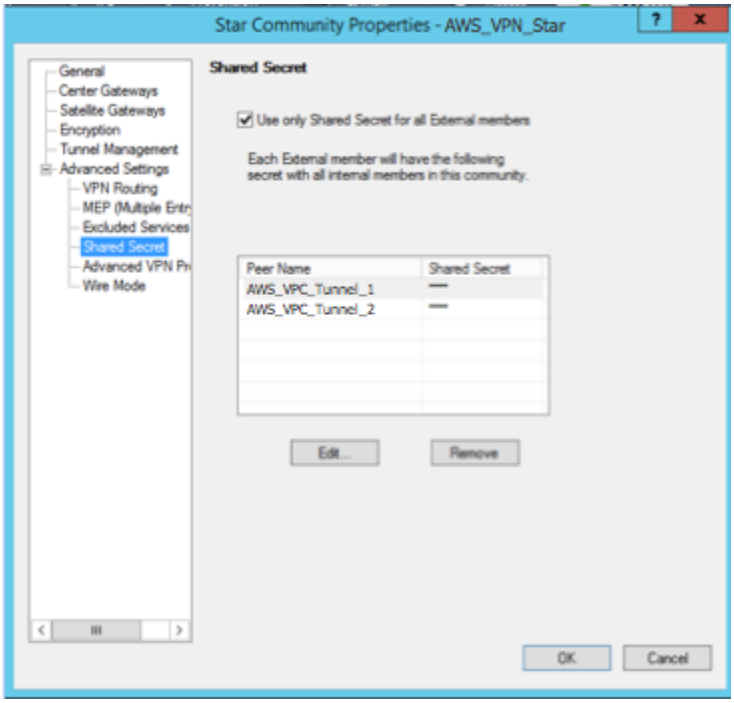
> **Note**
>
> Si vous utilisez des clusters, modifiez la topologie et définissez les interfaces comme interfaces de cluster. Utilisez les adresses IP spécifiées dans le fichier de configuration.

Pour créer et configurer la communauté VPN, l'IKE et IPsec les paramètres

Dans cette étape, vous créez une communauté VPN sur votre passerelle Check Point, à laquelle vous ajoutez les objets réseau (périphériques interopérables) de chaque tunnel. Vous configurez également l'échange de clés Internet (IKE) et IPsec les paramètres.

1. Dans les propriétés de votre passerelle, choisissez IPSecVPN dans le volet des catégories.
2. Choisissez Communities, New, Star Community.
3. Entrez un nom pour votre communauté (par exemple, `AWS_VPN_Star`), puis choisissez Center Gateways dans le volet des catégories.
4. Choisissez Add, puis ajoutez votre passerelle ou cluster à la liste des passerelles participantes.
5. Dans le volet des catégories, sélectionnez Satellite Gateways (Passerelles satellites), Add (Ajouter), puis ajoutez les périphériques interopérables que vous avez créés précédemment (`AWS_VPC_Tunnel_1` et `AWS_VPC_Tunnel_2`) à la liste des passerelles participantes.
6. Dans le volet des catégories, sélectionnez Encryption. Dans la section Méthode de chiffrement, sélectionnez IKEv1 uniquement. Dans la section Encryption Suite, choisissez Custom, Custom Encryption.
7. Dans la boîte de dialogue, configurez les propriétés de chiffrement comme suit, puis sélectionnez OK lorsque vous avez terminé :

   - Propriétés IKE Security Association (Phase 1) :
     - Perform key exchange encryption with : AES-128
     - Perform data integrity with : SHA-1
   - IPsec Propriétés de l'association de sécurité (phase 2) :
     - Effectuez le chiffrement IPsec des données avec : AES-128
     - Perform data integrity with : SHA-1
8. Dans le volet des catégories, sélectionnez Tunnel Management. Choisissez Set Permanent Tunnels, On all tunnels in the community. Dans la section VPN Tunnel Sharing, choisissez One VPN tunnel per Gateway pair.
9. Dans le volet des catégories, développez Advanced Settings, puis choisissez Shared Secret.
10. Sélectionnez le nom d'homologue du premier tunnel, choisissez Edit (Modifier) et entrez la clé prépartagée comme indiqué dans la section `IPSec Tunnel #1` du fichier de configuration.
11. Sélectionnez le nom d'homologue du second tunnel, choisissez Edit (Modifier) et entrez la clé prépartagée comme indiqué dans la section `IPSec Tunnel #2` du fichier de configuration.



12. Toujours dans la catégorie Advanced Settings (Paramètres avancés), choisissez Advanced VPN Properties (Propriétés de VPN avancées), configurez les propriétés comme suit et sélectionnez OK lorsque vous avez terminé :

    - IKE (Phase 1) :
        - Use Diffie-Hellman group (Utiliser le groupe Diffie-Hellman) : `Group 2`
        - Renegotiate IKE security associations every `480` minutes
    - IPsec (Phase 2) :
        - Choisissez Use Perfect Forward Secrecy
        - Use Diffie-Hellman group (Utiliser le groupe Diffie-Hellman) : `Group 2`
        - Renégociez les associations de IPsec sécurité toutes les secondes **`3600`**

Pour créer les règles de pare-feu

Dans cette étape, vous configurez une stratégie avec les règles de pare-feu et les règles de correspondance directionnelle qui autorisent les communications entre le VPC et le réseau local. Puis, vous installez la stratégie sur votre passerelle.

1. Dans le SmartDashboard, choisissez Propriétés globales pour votre passerelle. Dans le volet des catégories, développez VPN, puis choisissez Advanced.
2. Choisissez Enable VPN Directional Match in VPN Column et enregistrez vos modifications.

3. Dans le SmartDashboard, choisissez Firewall, puis créez une politique avec les règles suivantes :

   - Autoriser le sous-réseau VPC à communiquer avec le réseau local via les protocoles requis.
   - Autoriser le réseau local à communiquer avec le sous-réseau VPC via les protocoles requis.

4. Ouvrez le menu contextuel de la cellule de la colonne VPN, puis choisissez Edit Cell.
5. Dans la boîte de dialogue VPN Match Conditions, choisissez Match traffic in this direction only. Créez les règles de correspondance directionnelle suivantes en choisissant Add pour chaque règle, puis OK lorsque vous avez terminé :

   - `internal_clear` > Communauté VPN (la communauté VPN que vous avez créée plus tôt : par exemple, `AWS_VPN_Star`)
   - Communauté VPN > Communauté VPN
   - Communauté VPN > `internal_clear`

6. Dans le SmartDashboard, choisissez Policy, Install.
7. Dans la boîte de dialogue, sélectionnez votre passerelle, puis choisissez OK pour installer la stratégie.

Pour modifier la propriété tunnel_keepalive_method

Votre passerelle Check Point peut utiliser la détection d'homologue mort (DPD, Dead Peer Detection) pour savoir à quel moment une association IKE est arrêtée. Pour configurer DDP pour un tunnel permanent, le tunnel permanent doit être configuré dans la communauté AWS VPN (reportez-vous à l'étape 8).

Par défaut, la propriété `tunnel_keepalive_method` pour une passerelle VPN est définie sur `tunnel_test`. Vous devez modifier la valeur sur `dpd`. Chaque passerelle VPN de la communauté VPN qui nécessite une surveillance DPD doit être configurée avec la propriété `tunnel_keepalive_method`, notamment toute passerelle VPN tierce. Vous ne pouvez pas configurer différents mécanismes de surveillance pour la même passerelle.

Vous pouvez mettre à jour la `tunnel_keepalive_method` propriété à l'aide de l'DBedit outil Gui.

1. Ouvrez le point SmartDashboard de contrôle et choisissez Security Management Server, Domain Management Server.
2. Choisissez File, Database Revision Control... et créez un instantané de révision.
3. Fermez toutes les SmartConsole fenêtres, telles que le SmartDashboard SmartView Tracker et le SmartView Monitor.
4. Démarrez l'BDedit outil Gui. Pour plus d'informations, consultez l'article Check Point Database Tool sur le Centre de support Check Point.
5. Choisissez Security Management Server, Domain Management Server.
6. Dans le volet supérieur gauche, choisissez Table, Network Objects, network_objects.
7. Dans le volet supérieur droit, sélectionnez l'objet Security Gateway, Cluster approprié.
8. Appuyez sur CTRL+F, ou utilisez le menu Search pour rechercher ce qui suit : `tunnel_keepalive_method`.
9. Dans le volet inférieur, ouvrez le menu contextuel pour `tunnel_keepalive_method` et sélectionnez Edit... (Éditer...). Choisissez dpd, puis OK.
10. Répétez les étapes 7 à 9 pour chaque passerelle faisant partie de la communauté AWS VPN.
11. Sélectionnez File, Save As.
12. Fermez l'DBedit outil Gui.
13. Ouvrez le point SmartDashboard de contrôle et choisissez Security Management Server, Domain Management Server.
14. Installez la stratégie sur l'objet Security Gateway, Cluster approprié.

Pour plus d'informations, consultez l'article Nouvelles fonction VPN dans R77.10 sur le Centre de support Check Point.

Pour activer la restriction TCP MSS

La restriction TCP MSS réduit la taille de segment maximale des paquets TCP afin d'éviter la fragmentation des paquets.

1. Accédez au répertoire suivant : `C:\Program Files (x86)\CheckPoint\SmartConsole\R77.10\PROGRAM\`.
2. Ouvrez Check Point Database Tool en exécutant le fichier `GuiDBEdit.exe`.
3. Choisissez Table, Global Properties, properties.

4. Pour `fw_clamp_tcp_mss`, choisissez Edit. Remplacez la valeur par `true`, puis choisissez OK.

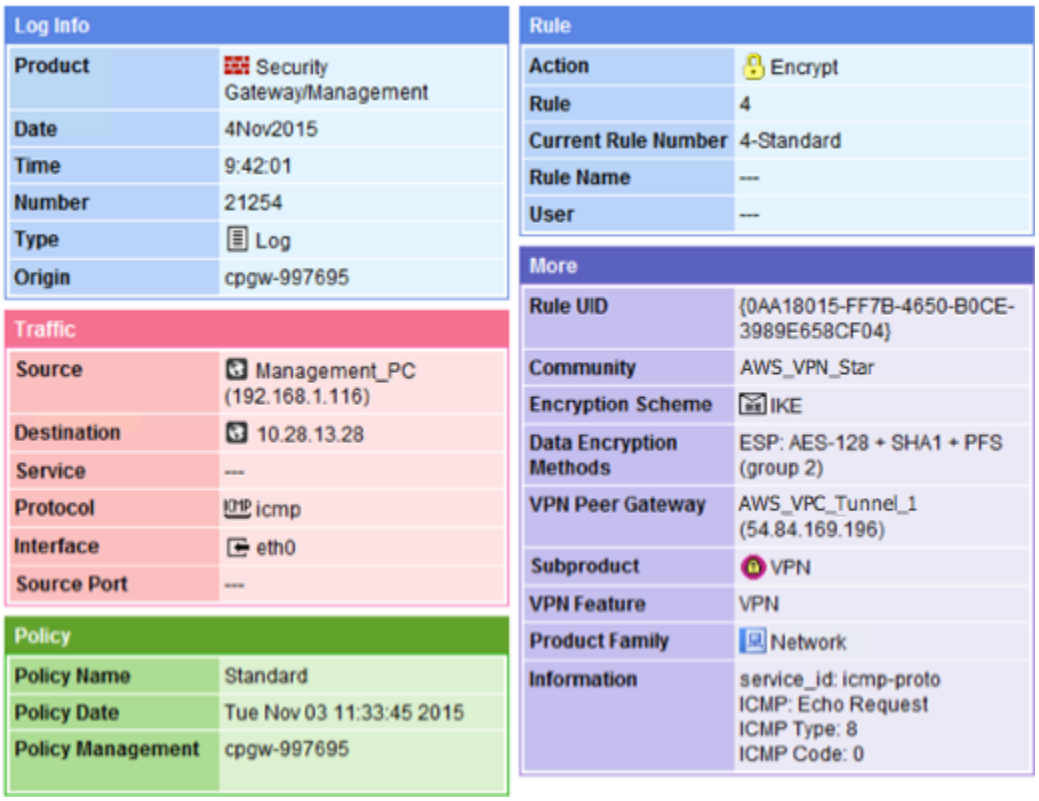
Pour vérifier l'état du tunnel

Vous pouvez vérifier l'état du tunnel en exécutant la commande suivante à partir de l'outil de ligne de commande en mode expert.

```
vpn tunnelutil
```

Dans les options qui s'affichent, choisissez 1 pour vérifier les associations IKE et 2 pour vérifier les IPsec associations.

Vous pouvez aussi utiliser le journal Check Point Smart Tracker Log pour vérifier que les paquets de la connexion sont chiffrés. Par exemple, le journal suivant indique qu'un paquet adressé au VPC a été envoyé via le tunnel 1 et qu'il a été chiffré.



SonicWALL

La procédure suivante montre comment configurer les tunnels VPN sur l'appareil SonicWALL à l'aide de l'interface de gestion SonicOS.

Pour configurer les tunnels

1. Ouvrez l'interface de gestion SonicOS SonicWALL.
2. Dans le volet de gauche, sélectionnez VPN, Settings. Sous VPN Policies, choisissez Add....
3. Dans la fenêtre de stratégie VPN de l'onglet General , renseignez les informations suivantes :
   - Type de stratégie : Choisissez Tunnel Interface.
   - Authentication Method : choisissez IKE using Preshared Secret.
   - Name : entrez un nom pour la stratégie VPN. Nous vous recommandons d'utiliser le nom de l'ID de VPN, tel que fourni dans le fichier de configuration.
   - IPsec Nom ou adresse de la passerelle principale : entrez l'adresse IP de la passerelle privée virtuelle telle que fournie dans le fichier de configuration (par exemple,`72.21.209.193`).
   - IPsec Nom ou adresse de la passerelle secondaire : conservez la valeur par défaut.
   - Shared Secret : entrez la clé pré-partagée, telle que fournie dans le fichier de configuration, puis entrez-la à nouveau dans Confirm Shared Secret.
   - ID IKE local : entrez l' IPv4 adresse de la passerelle client (l'appareil SonicWall).
   - ID IKE homologue : entrez l' IPv4 adresse de la passerelle privée virtuelle.
4. Dans l'onglet Network, renseignez les informations suivantes :
   - Sous Local Networks, choisissez Any address. Nous recommandons cette option afin d'éviter des problèmes de connectivité à partir de votre réseau local.
   - Sous Remote Networks, choisissez Choose a destination network from list. Créez un objet d'adresse avec le CIDR de votre VPC dans AWS.
5. Dans l'onglet Proposals (Propositions), renseignez les informations suivantes.
   - Sous IKE (Phase 1) Proposal, procédez comme suit :
     - Exchange : choisissez Main Mode.
     - DH Group (Groupe DH) : entrez une valeur pour le groupe Diffie-Hellman (par exemple, 2).
     - Encryption : choisissez AES-128 ou AES-256.
     - Authentification : Choisissez SHA1ou SHA256.
     - Life Time : entrez `28800`.
   - Sous IKE (Phase 2) Proposal, procédez comme suit :

- Protocol : choisissez ESP.
- Encryption : choisissez AES-128 ou AES-256.
- Authentification : Choisissez SHA1ou SHA256.
- Cochez la case Enable Perfect Forward Secrecy, puis choisissez le groupe Diffie-Hellman.
- Life Time : entrez `3600`.

> **Important**
>
> Si vous avez créé votre passerelle privée virtuelle avant octobre 2015, vous devez spécifier le groupe Diffie-Hellman 2, AES-128, et pour les deux phases. SHA1

6. Dans l'onglet Advanced, renseignez les informations suivantes :
   - Sélectionnez Enable Keep Alive.
   - Sélectionnez Enable Phase2 Dead Peer Detection et entrez les informations suivantes :
     - Pour Dead Peer Detection Interval, entrez `60` (c'est le minimum que l'appareil SonicWALL accepte).
     - Pour Failure Trigger Level, entrez `3`.
   - Pour VPN Policy bound to, sélectionnez Interface X1. C'est l'interface qui est généralement désignée pour les adresses IP publiques.
7. Choisissez OK. Sur la page Settings, la case Enable pour le tunnel doit être cochée par défaut. Un point vert indique que le tunnel fonctionne.

Appareils Cisco : informations supplémentaires

Certains modes Cisco ASAs ne prennent en charge que Active/Standby le mode. Lorsque vous utilisez ces Cisco ASAs, vous ne pouvez avoir qu'un seul tunnel actif à la fois. L'autre tunnel en veille devient actif si le premier tunnel devient inaccessible. Avec cette redondance, l'un des tunnels devrait toujours assurer la connexion à votre VPC.

Cisco ASAs à partir de la version 9.7.1 et du Active/Active mode de support ultérieur. Lorsque vous utilisez ces Cisco ASAs, les deux tunnels peuvent être actifs en même temps. Avec cette redondance, l'un des tunnels devrait toujours assurer la connexion à votre VPC.

Pour les périphériques Cisco, vous devez effectuer les opérations suivantes :

- Configurer l'interface externe.
- Vous assurer que le numéro de séquence de la stratégie ISAKMP du Crypto est unique.
- Vous assurer que le numéro de séquence de la stratégie de la liste Crypto est unique.
- Assurez-vous que le Crypto IPsec Transform Set et la Crypto ISAKMP Policy Sequence sont en harmonie avec tous IPsec les autres tunnels configurés sur l'appareil.
- Vous assurer que le numéro de supervision du SLA est unique.
- Configurer tous les routages internes qui acheminent le trafic entre le périphérique de passerelle client et votre réseau local.

Fichiers de configuration de routage dynamique téléchargeables pour AWS Site-to-Site VPN le dispositif de passerelle client

Pour télécharger un exemple de fichier de configuration avec des valeurs spécifiques à la configuration de votre connexion Site-to-Site VPN, utilisez la console Amazon VPC, la ligne de AWS commande ou l'API Amazon EC2. Pour de plus amples informations, veuillez consulter Étape 6 : Téléchargement du fichier de configuration.

Vous pouvez également télécharger des exemples de fichiers de configuration génériques pour le routage dynamique qui n'incluent pas de valeurs spécifiques à la configuration de votre connexion Site-to-Site VPN : dynamic-routing-examples.zip

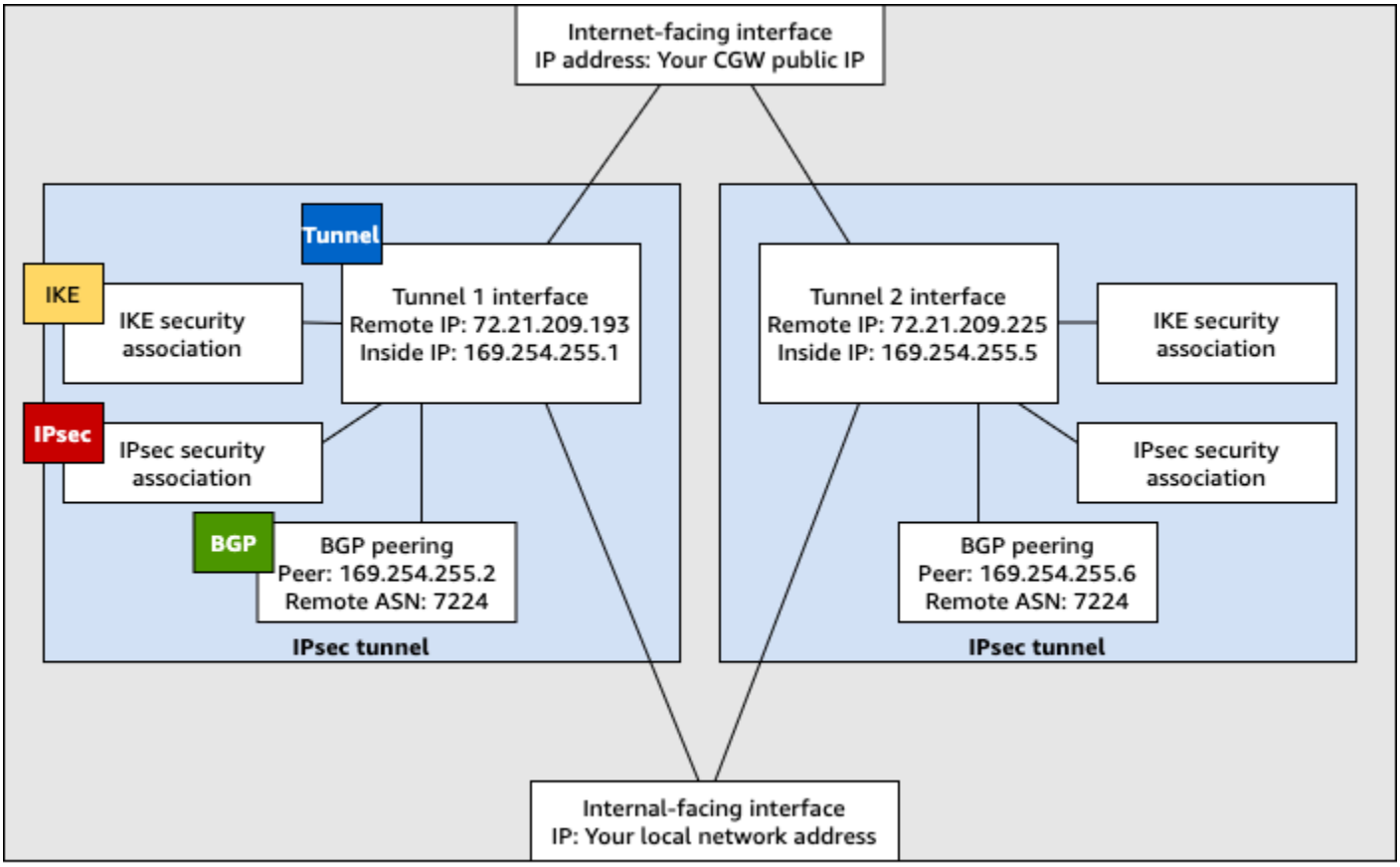
Les fichiers utilisent des valeurs d'espace réservé pour certains composants. Par exemple, ils utilisent :

- Des exemples de valeurs pour l'ID de connexion VPN, l'ID de passerelle client et l'ID de passerelle réseau privé virtuel
- Espaces réservés aux AWS points de terminaison d'adresses IP distants (*AWS_ENDPOINT_1*et) *AWS_ENDPOINT_2*
- Un espace réservé pour l'adresse IP de l'interface externe routable par Internet sur le dispositif de passerelle client () *your-cgw-ip-address*
- Un espace réservé pour la valeur de clé pré-partagée () pre-shared-key
- Des exemples de valeurs pour le tunnel à l'intérieur des adresses IP.
- Exemples de valeurs pour le paramètre MTU.

> **Note**
>
> Les paramètres MTU fournis dans les exemples de fichiers de configuration ne sont que des exemples. Veuillez vous référer à Les meilleures pratiques pour un AWS Site-to-Site VPN Appareil de passerelle client pour obtenir des informations sur la définition de la valeur MTU optimale pour votre situation.

En plus de fournir des valeurs d'espace réservé, les fichiers spécifient les exigences minimales pour une connexion Site-to-Site VPN de AES128, SHA1, et du groupe Diffie-Hellman 2 dans la plupart des AWS régions, et AES128 SHA2, et du groupe Diffie-Hellman 14 dans les régions. AWS GovCloud Ils spécifient également des clés prépartagées pour l'authentification. Vous devez modifier l'exemple de fichier de configuration pour tirer parti des algorithmes de sécurité supplémentaires, des groupes Diffie-Hellman, des certificats privés et du trafic. IPv6

Le diagramme suivant fournit une vue d'ensemble des différents composants configurés sur le périphérique de passerelle client. Il inclut des exemples de valeurs pour les adresses IP de l'interface tunnel.



Customer gateway device

Configuration du routage dynamique pour un dispositif de passerelle AWS Virtual Private Network client

Voici quelques exemples de procédures pour configurer un périphérique de passerelle client à l'aide de son interface utilisateur (si disponible).

Check Point

Voici les étapes à suivre pour configurer un appareil Check Point Security Gateway exécutant le R77.10 ou une version ultérieure, à l'aide du portail Web Gaia et de Check Point. SmartDashboard Pour de plus amples informations, veuillez consulter Amazon Web Services (AWS) VPN BGP sur le Centre de support Check Point.

Pour configurer l'interface du tunnel

La première étape consiste à créer les tunnels VPN et à fournir les adresses IP privées (internes) de la passerelle client et de la passerelle réseau privé virtuel pour chaque tunnel. Pour créer le premier tunnel, utilisez les informations fournies dans la section `IPSec Tunnel #1` du fichier

de configuration. Pour créer le second tunnel, utilisez les valeurs fournies dans la section `IPSec Tunnel #2` du fichier de configuration.

1. Connectez-vous à votre passerelle de sécurité via SSH. Si vous utilisez le shell autre que celui par défaut, choisissez clish en exécutant la commande suivante : `clish`
2. Définissez l'ASN de la passerelle client (l'ASN fourni lors de la création de la passerelle client AWS) en exécutant la commande suivante.

```
set as 65000
```

3. Créez l'interface de tunnel pour le premier tunnel, en utilisant les informations fournies dans la section `IPSec Tunnel #1` du fichier de configuration. Fournissez un nom unique pour votre tunnel, tel que `AWS_VPC_Tunnel_1`.

```
add vpn tunnel 1 type numbered local 169.254.44.234 remote 169.254.44.233
 peer AWS_VPC_Tunnel_1
set interface vpnt1 state on
set interface vpnt1 mtu 1436
```

4. Répétez ces commandes pour créer le second tunnel, à l'aide des informations fournies dans la section `IPSec Tunnel #2` du fichier de configuration. Fournissez un nom unique pour votre tunnel, tel que `AWS_VPC_Tunnel_2`.

```
add vpn tunnel 1 type numbered local 169.254.44.38 remote 169.254.44.37
 peer AWS_VPC_Tunnel_2
set interface vpnt2 state on
set interface vpnt2 mtu 1436
```

5. Définissez l'ASN de la passerelle réseau privé virtuel.

```
set bgp external remote-as 7224 on
```

6. Configurez le protocole BGP pour le premier tunnel, à l'aide des informations fournies dans la section `IPSec Tunnel #1` du fichier de configuration :

```
set bgp external remote-as 7224 peer 169.254.44.233 on
set bgp external remote-as 7224 peer 169.254.44.233 holdtime 30
set bgp external remote-as 7224 peer 169.254.44.233 keepalive 10
```

7. Configurez le protocole BGP pour le second tunnel, à l'aide des informations fournies dans la section `IPSec Tunnel #2` du fichier de configuration :

```
set bgp external remote-as 7224 peer 169.254.44.37 on
set bgp external remote-as 7224 peer 169.254.44.37 holdtime 30
set bgp external remote-as 7224 peer 169.254.44.37 keepalive 10
```

8. Enregistrez la configuration.

```
save config
```

Pour créer une stratégie BGP

Ensuite, créez une stratégie BGP qui autorise l'importation des acheminements publiés par AWS. Ensuite, configurez votre passerelle client pour publier ses acheminements locaux vers AWS.

1. Dans l'interface utilisateur Web de Gaia, sélectionnez Advanced Routing, Inbound Route Filters. Choisissez Add, puis sélectionnez Add BGP Policy (Based on AS).
2. Pour Add BGP Policy (Ajouter une stratégie BGP), sélectionnez une valeur comprise entre 512 et 1 024 dans le premier champ, puis saisissez l'ASN de la passerelle réseau privé virtuel dans le second champ (par exemple, `7224`).
3. Choisissez Enregistrer.

Pour publier les itinéraires locaux

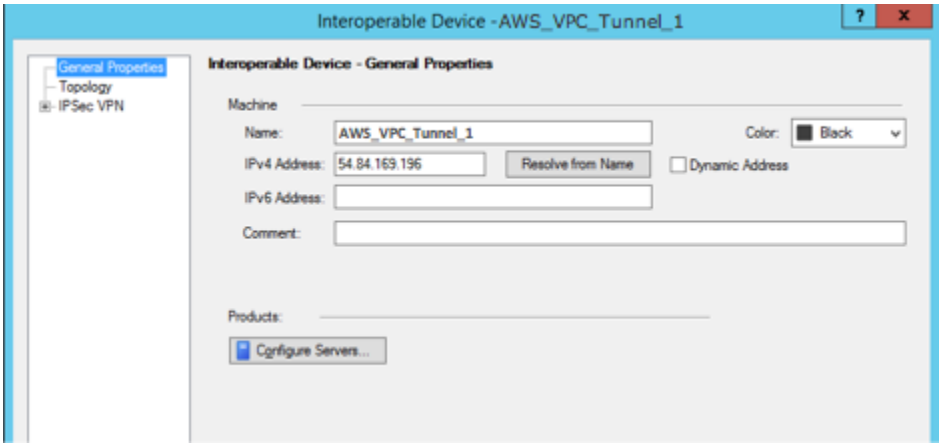
Les étapes suivantes concernent la répartition des itinéraires locaux d'interface. Vous pouvez également redistribuer les routes à partir de différentes sources (par exemple, les routes statiques ou celles obtenues via les protocoles de routage dynamique). Pour de plus amples informations, veuillez consulter le manuel Gaia Advanced Routing R77 Versions Administration Guide.

1. Dans l'interface utilisateur Web de Gaia, sélectionnez Advanced Routing, Routing Redistribution. Choisissez Add Redistribution From (Ajouter une redistribution à partir de) et sélectionnez Interface.
2. Pour To Protocol (Vers le protocole), sélectionnez l'ASN de la passerelle réseau privé virtuel (par exemple, `7224`).
3. Pour Interface, sélectionnez une interface interne. Choisissez Enregistrer.

Pour définir un nouvel objet réseau

Ensuite, créez un objet réseau pour chaque tunnel VPN, en spécifiant les adresses IP publiques (externes) de la passerelle réseau privé virtuel. Par la suite, vous ajoutez ces objets réseau en tant que passerelles satellite pour votre communauté VPN. Vous devez également créer un groupe vide comme espace réservé du domaine VPN.

1. Ouvrez le point de contrôle SmartDashboard.
2. Pour Groups, ouvrez le menu contextuel et choisissez Groups, Simple Group. Vous pouvez utiliser le même groupe pour chaque objet réseau.
3. Pour Network Objects, ouvrez le menu contextuel (clic droit) et choisissez New, Interoperable Device.
4. Pour Name (Nom), entrez le nom attribué à votre tunnel à l'étape 1 : `AWS_VPC_Tunnel_1` ou `AWS_VPC_Tunnel_2`, par exemple.
5. Pour IPv4 Adresse, entrez l'adresse IP externe de la passerelle privée virtuelle fournie dans le fichier de configuration, par exemple,`54.84.169.196`. Enregistrez vos paramètres et fermez la boîte de dialogue.



6. Dans le volet de gauche des catégories, sélectionnez Topology.
7. Dans la section VPN Domain (Domaine VPN), choisissez Manually defined (Défini manuellement), puis accédez au groupe simple vide que vous avez créé à l'étape 2 et sélectionnez-le. Choisissez OK.
8. Répétez ces étapes pour créer un second objet réseau, à l'aide des informations de la section `IPSec Tunnel #2` du fichier de configuration.
9. Accédez à votre objet réseau passerelle, ouvrez votre objet passerelle ou cluster, puis sélectionnez Topology.

10. Dans la section VPN Domain (Domaine VPN), choisissez Manually defined (Défini manuellement), puis accédez au groupe simple vide que vous avez créé à l'étape 2 et sélectionnez-le. Choisissez OK.

> **Note**
>
> Vous pouvez conserver n'importe quel domaine VPN existant que vous avez configuré. Cependant, assurez-vous que les hôtes et les réseaux qui sont utilisés ou servis par la nouvelle connexion VPN ne sont pas déclarés dans ce domaine VPN, notamment si le domaine VPN est automatiquement dérivé.

> **Note**
>
> Si vous utilisez des clusters, modifiez la topologie et définissez les interfaces comme interfaces de cluster. Utilisez les adresses IP spécifiées dans le fichier de configuration.

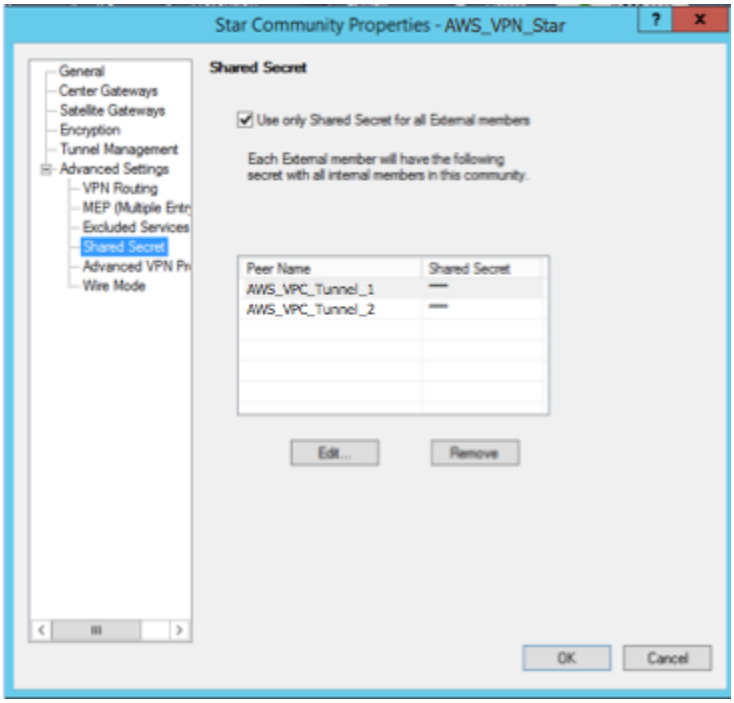
Pour créer et configurer la communauté VPN, l'IKE et IPsec les paramètres

Ensuite, créez une communauté VPN sur votre passerelle Check Point et ajoutez-y les objets réseau (périphériques interopérables) de chaque tunnel. Vous configurez également l'échange de clés Internet (IKE) et IPsec les paramètres.

1. Dans les propriétés de votre passerelle, choisissez IPSecVPN dans le volet des catégories.
2. Choisissez Communities, New, Star Community.
3. Entrez un nom pour votre communauté (par exemple, `AWS_VPN_Star`), puis choisissez Center Gateways dans le volet des catégories.
4. Choisissez Add, puis ajoutez votre passerelle ou cluster à la liste des passerelles participantes.
5. Dans le volet des catégories, sélectionnez Satellite Gateways (Passerelles satellites), Add (Ajouter), puis ajoutez les périphériques interopérables que vous avez créés précédemment (`AWS_VPC_Tunnel_1` et `AWS_VPC_Tunnel_2`) à la liste des passerelles participantes.
6. Dans le volet des catégories, sélectionnez Encryption. Dans la section Méthode de chiffrement, choisissez IKEv1 pour IPv4 et IKEv2 pour IPv6. Dans la section Encryption Suite, choisissez Custom, Custom Encryption.

> **Note**
>
> Vous devez sélectionner les options IKEv1 pour IPv4 et IKEv2 pour IPv6 pour les IKEv1 fonctionnalités.

7. Dans la boîte de dialogue, configurez les propriétés de chiffrement comme suit, puis sélectionnez OK lorsque vous avez terminé :
   - Propriétés IKE Security Association (Phase 1) :
     - Perform key exchange encryption with : AES-128
     - Perform data integrity with : SHA-1
   - IPsec Propriétés de l'association de sécurité (phase 2) :
     - Effectuez le chiffrement IPsec des données avec : AES-128
     - Perform data integrity with : SHA-1
8. Dans le volet des catégories, sélectionnez Tunnel Management. Choisissez Set Permanent Tunnels, On all tunnels in the community. Dans la section VPN Tunnel Sharing, choisissez One VPN tunnel per Gateway pair.
9. Dans le volet des catégories, développez Advanced Settings, puis choisissez Shared Secret.
10. Sélectionnez le nom d'homologue du premier tunnel, choisissez Edit (Modifier) et entrez la clé prépartagée comme indiqué dans la section `IPSec Tunnel #1` du fichier de configuration.
11. Sélectionnez le nom d'homologue du second tunnel, choisissez Edit (Modifier) et entrez la clé prépartagée comme indiqué dans la section `IPSec Tunnel #2` du fichier de configuration.



12. Toujours dans la catégorie Advanced Settings (Paramètres avancés), choisissez Advanced VPN Properties (Propriétés de VPN avancées), configurez les propriétés comme suit et sélectionnez OK lorsque vous avez terminé :

    - IKE (Phase 1) :
        - Use Diffie-Hellman group (Utiliser le groupe Diffie-Hellman) : `Group 2 (1024 bit)`
        - Renegotiate IKE security associations every `480` minutes
    - IPsec (Phase 2) :
        - Choisissez Use Perfect Forward Secrecy
        - Use Diffie-Hellman group (Utiliser le groupe Diffie-Hellman) : `Group 2 (1024 bit)`
        - Renégociez les associations de IPsec sécurité toutes les secondes **`3600`**

Pour créer les règles de pare-feu

Ensuite, configurez une stratégie avec les règles de pare-feu et les règles de correspondance directionnelle qui autorisent les communications entre le VPC et le réseau local. Puis, vous installez la stratégie sur votre passerelle.

1. Dans le SmartDashboard, choisissez Propriétés globales pour votre passerelle. Dans le volet des catégories, développez VPN, puis choisissez Advanced.
2. Choisissez Enable VPN Directional Match in VPN Column, puis OK.

3. Dans le SmartDashboard, choisissez Firewall, puis créez une politique avec les règles suivantes :

   - Autoriser le sous-réseau VPC à communiquer avec le réseau local via les protocoles requis.
   - Autoriser le réseau local à communiquer avec le sous-réseau VPC via les protocoles requis.
4. Ouvrez le menu contextuel de la cellule de la colonne VPN, puis choisissez Edit Cell.
5. Dans la boîte de dialogue VPN Match Conditions, choisissez Match traffic in this direction only. Créez les règles de correspondance directionnelle suivantes en choisissant Add (Ajouter) pour chaque règle, puis OK lorsque vous avez terminé :

   - `internal_clear` > Communauté VPN (la communauté VPN que vous avez créée plus tôt : par exemple, `AWS_VPN_Star`)
   - Communauté VPN > Communauté VPN
   - Communauté VPN > `internal_clear`
6. Dans le SmartDashboard, choisissez Policy, Install.
7. Dans la boîte de dialogue, sélectionnez votre passerelle, puis choisissez OK pour installer la stratégie.

Pour modifier la propriété tunnel_keepalive_method

Votre passerelle Check Point peut utiliser la détection d'homologue mort (DPD, Dead Peer Detection) pour savoir à quel moment une association IKE est arrêtée. Pour configurer DDP pour un tunnel permanent, le tunnel permanent doit être configuré dans la communauté AWS VPN.

Par défaut, la propriété `tunnel_keepalive_method` pour une passerelle VPN est définie sur `tunnel_test`. Vous devez modifier la valeur sur `dpd`. Chaque passerelle VPN de la communauté VPN qui nécessite une surveillance DPD doit être configurée avec la propriété `tunnel_keepalive_method`, notamment toute passerelle VPN tierce. Vous ne pouvez pas configurer différents mécanismes de surveillance pour la même passerelle.

Vous pouvez mettre à jour la `tunnel_keepalive_method` propriété à l'aide de l'DBedit outil Gui.

1. Ouvrez le point SmartDashboard de contrôle et choisissez Security Management Server, Domain Management Server.

2. Choisissez File, Database Revision Control... et créez un instantané de révision.
3. Fermez toutes les SmartConsole fenêtres, telles que le SmartDashboard SmartView Tracker et le SmartView Monitor.
4. Démarrez l'BDedit outil Gui. Pour plus d'informations, consultez l'article Check Point Database Tool sur le Centre de support Check Point.
5. Choisissez Security Management Server, Domain Management Server.
6. Dans le volet supérieur gauche, choisissez Table, Network Objects, network_objects.
7. Dans le volet supérieur droit, sélectionnez l'objet Security Gateway, Cluster approprié.
8. Appuyez sur CTRL+F, ou utilisez le menu Search pour rechercher ce qui suit : `tunnel_keepalive_method`.
9. Dans le volet inférieur, ouvrez le menu contextuel pour `tunnel_keepalive_method` et sélectionnez Edit.... Choisissez dpd, puis OK.
10. Répétez les étapes 7 à 9 pour chaque passerelle faisant partie de la communauté AWS VPN.
11. Sélectionnez File, Save As.
12. Fermez l'DBedit outil Gui.
13. Ouvrez le point SmartDashboard de contrôle et choisissez Security Management Server, Domain Management Server.
14. Installez la stratégie sur l'objet Security Gateway, Cluster approprié.

Pour plus d'informations, consultez l'article Nouvelles fonction VPN dans R77.10 sur le Centre de support Check Point.

Pour activer la restriction TCP MSS

La restriction TCP MSS réduit la taille de segment maximale des paquets TCP afin d'éviter la fragmentation des paquets.

1. Accédez au répertoire suivant : `C:\Program Files (x86)\CheckPoint\SmartConsole\R77.10\PROGRAM\`.
2. Ouvrez Check Point Database Tool en exécutant le fichier `GuiDBEdit.exe`.
3. Choisissez Table, Global Properties, properties.
4. Pour `fw_clamp_tcp_mss`, choisissez Edit. Remplacez la valeur par `true`, puis choisissez OK.

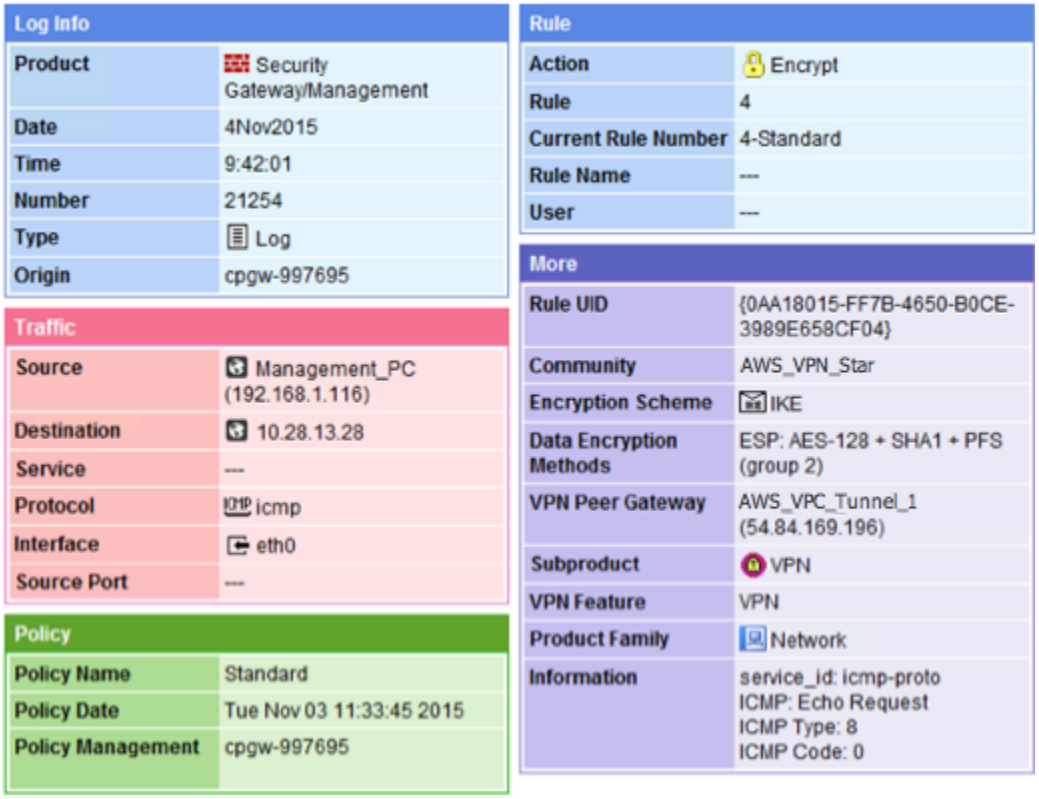
Pour vérifier l'état du tunnel

Vous pouvez vérifier l'état du tunnel en exécutant la commande suivante à partir de l'outil de ligne de commande en mode expert.

```
vpn tunnelutil
```

Dans les options qui s'affichent, choisissez 1 pour vérifier les associations IKE et 2 pour vérifier les IPsec associations.

Vous pouvez aussi utiliser le journal Check Point Smart Tracker Log pour vérifier que les paquets de la connexion sont chiffrés. Par exemple, le journal suivant indique qu'un paquet adressé au VPC a été envoyé via le tunnel 1 et qu'il a été chiffré.



SonicWALL

Vous pouvez configurer un appareil SonicWALL à l'aide de l'interface de gestion SonicOS. Pour plus d'informations sur la configuration des tunnels, consultez Configuration du routage statique pour un dispositif de passerelle AWS Site-to-Site VPN client.

Vous ne pouvez pas configurer BGP pour le dispositif à l'aide de l'interface de gestion. À la place, utilisez les instructions de ligne de commande fournies dans l'exemple de fichier de configuration, sous la section nommée BGP.

Appareils Cisco : informations supplémentaires

Certains modes Cisco ASAs ne prennent en charge que Active/Standby le mode. Lorsque vous utilisez ces Cisco ASAs, vous ne pouvez avoir qu'un seul tunnel actif à la fois. L'autre tunnel en veille devient actif si le premier tunnel devient inaccessible. Avec cette redondance, l'un des tunnels devrait toujours assurer la connexion à votre VPC.

Cisco ASAs à partir de la version 9.7.1 et du Active/Active mode de support ultérieur. Lorsque vous utilisez ces Cisco ASAs, les deux tunnels peuvent être actifs en même temps. Avec cette redondance, l'un des tunnels devrait toujours assurer la connexion à votre VPC.

Pour les périphériques Cisco, vous devez effectuer les opérations suivantes :

- Configurer l'interface externe.
- Vous assurer que le numéro de séquence de la stratégie ISAKMP du Crypto est unique.
- Vous assurer que le numéro de séquence de la stratégie de la liste Crypto est unique.
- Assurez-vous que le Crypto IPsec Transform Set et la Crypto ISAKMP Policy Sequence sont en harmonie avec tous IPsec les autres tunnels configurés sur l'appareil.
- Vous assurer que le numéro de supervision du SLA est unique.
- Configurer tous les routages internes qui acheminent le trafic entre le périphérique de passerelle client et votre réseau local.

Appareils Juniper : informations supplémentaires

Les informations suivantes s'appliquent aux exemples de fichiers de configuration pour les périphériques de passerelle client Juniper série J et SRX.

- L'interface extérieure est appelée*ge-0/0/0.0*.
- L'interface IDs du tunnel est appelée *st0.1* et*st0.2*.
- Vous assurer que vous identifiez la zone de sécurité pour l'interface de liaison montante (les informations de configuration utilisent la zone « untrust » par défaut).

- Vous assurer que vous identifiez la zone de sécurité pour l'interface interne (les informations de configuration utilisent la zone « trust » par défaut).

Configuration de Windows Server en tant que périphérique de passerelle AWS Site-to-Site VPN client

Vous pouvez configurer un serveur Windows Server en cours d'exécution en tant que passerelle client pour votre VPC. Utilisez la procédure suivante, que vous exécutiez Windows Server sur une instance EC2 dans un VPC ou sur votre propre serveur. Les procédures suivantes s'appliquent à Windows Server 2012 R2 et versions ultérieures.

Table des matières

Configuration de votre instance Windows

Si vous configurez Windows Server sur une instance EC2 que vous avez lancée à partir d'une AMI Windows, procédez comme suit :

- Désactivez la source/destination vérification pour l'instance :
  1. Ouvrez la console Amazon EC2 à l'adresse https://console.aws.amazon.com/ec2/.
  2. Sélectionnez votre instance Windows, puis Actions, Networking (Réseaux), Change Source/Destination Check (Modifier la vérification de source/destination). Sélectionnez Stop (Arrêter), puis Save (Enregistrer).
- Mettez à jour les paramètres de votre adaptateur pour pouvoir router le trafic depuis d'autres instances :
  1. Connectez-vous à votre instance Windows. Pour plus d'informations, consultez Connexion à votre instance Windows.

2. Ouvrez le Panneau de configuration, puis lancez le Gestionnaire de périphériques.
3. Développez le nœud Cartes réseau.
4. Sélectionnez la carte réseau (selon le type d'instance, il peut s'agir d'Amazon Elastic Network Adapter ou Intel 82599 Virtual Function), puis sélectionnez Action, Properties (Propriétés).
5. Dans l'onglet Avancé, désactivez les propriétés IPv4Checksum Offload, TCP Checksum Offload (IPv4) et UDP Checksum Offload (IPv4), puis choisissez OK.

- Allouez une adresse IP Elastic à votre compte et associez-la à l'instance. Pour plus d'informations, consultez la rubrique Adresses IP Elastic dans le Guide de l'utilisateur Amazon EC2. Prenez note de cette adresse : vous en aurez besoin lors de la création de la passerelle client.
- Assurez-vous que les règles du groupe de sécurité de l'instance autorisent le IPsec trafic sortant. Par défaut, un groupe de sécurité autorise tout le trafic sortant. Toutefois, si les règles sortantes du groupe de sécurité ont été modifiées par rapport à leur état d'origine, vous devez créer les règles de protocole personnalisées sortantes suivantes pour le IPsec trafic : protocole IP 50, protocole IP 51 et UDP 500.

Prenez note de la plage CIDR du réseau dans lequel se trouve votre instance Windows, par exemple `172.31.0.0/16`.

Étape 1: Créer une connexion VPN et configurer votre VPC

Pour créer une connexion VPN à partir de votre VPC, procédez comme suit :

1. Créez une passerelle réseau privé virtuel et attachez-la à votre VPC. Pour de plus amples informations, veuillez consulter Créer une passerelle réseau privé virtuel.
2. Créez une connexion VPN et une nouvelle passerelle client. Pour la passerelle client, spécifiez l'adresse IP publique de votre Windows Server. Pour la connexion VPN, sélectionnez le routage statique, puis saisissez la plage CIDR de votre réseau dans laquelle se trouve le Windows Server, par exemple `172.31.0.0/16`. Pour de plus amples informations, veuillez consulter Étape 5 : Création d'une connexion VPN.

Après avoir créé la connexion VPN, configurez le VPC pour activer la communication via la connexion VPN.

Pour configurer votre VPC

- Créez un sous-réseau privé dans votre VPC (si ce n'est déjà fait) pour lancer les instances qui communiqueront avec le Windows Server. Pour en savoir plus, consultez la section Création d'un sous-réseau dans votre VPC.

  > **Note**
  >
  > Un sous-réseau privé est un sous-réseau qui ne comporte pas de route vers une passerelle Internet. Le routage pour ce sous-réseau est décrit dans l'élément suivant.

- Mettez à jour vos tables de routage pour la connexion VPN :
  - Ajoutez une route à la table de routage de votre sous-réseau privé, en définissant la passerelle réseau privé virtuel comme cible et le réseau du Windows Server (plage CIDR) comme destination. Pour en savoir plus, consultez la section Ajout et suppression de routes d'une table de routage du guide de l'utilisateur Amazon VPC.
  - Activez la propagation de routes pour la passerelle réseau privé virtuel. Pour de plus amples informations, veuillez consulter (Passerelle réseau privé virtuel) Activer la propagation de route dans votre table de routage.
- Créez un groupe de sécurité pour vos instances, qui autorise la communication entre votre VPC et le réseau :
  - Ajoutez des règles autorisant l'accès SSH ou RDP entrant depuis votre réseau. Cela vous permet de vous connecter aux instances de votre VPC depuis votre réseau. Par exemple, pour autoriser les ordinateurs de votre réseau à accéder aux instances Linux dans votre VPC, créez une règle entrante avec le type SSH et la source définie sur la plage d'adresses CIDR de votre réseau (par exemple, `172.31.0.0/16`). Pour plus d'informations, consultez Groupes de sécurité pour votre VPC dans le Guide de l'utilisateur Amazon VPC.
  - Ajoutez une règle autorisant l'accès ICMP entrant depuis votre réseau. Cela vous permet de tester votre connexion VPN en effectuant un test ping de l'instance dans votre VPC à partir de votre Windows Server.

Étape 2 : Télécharger le fichier de configuration pour la connexion VPN

Vous pouvez utiliser la console Amazon VPC afin de télécharger un fichier de configuration Windows Server pour votre connexion VPN.

Pour télécharger le fichier de configuration :

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Site-to-Site VPN Connections.
3. Sélectionnez votre connexion VPN, puis choisissez Download Configuration (Télécharger la configuration).
4. Sélectionnez le fournisseur Microsoft, la plate-forme Windows Server et le logiciel 2012 R2. Choisissez Téléchargement. Vous pouvez ouvrir le fichier ou l'enregistrer.

Le fichier de configuration contient une section d'informations similaire à l'exemple suivant. Ces informations sont présentées deux fois, une fois pour chaque tunnel.

```
vgw-1a2b3c4d Tunnel1
-----------------------------------------------------------------
Local Tunnel Endpoint:       203.0.113.1
Remote Tunnel Endpoint:      203.83.222.237
Endpoint 1:                  [Your_Static_Route_IP_Prefix]
Endpoint 2:                  [Your_VPC_CIDR_Block]
Preshared key:               xCjNLsLoCmKsakwcdoR9yX6GsEXAMPLE
```

`Local Tunnel Endpoint`

Adresse IP que vous avez spécifiée pour la passerelle client lorsque vous avez créé la connexion VPN.

`Remote Tunnel Endpoint`

L'une des deux adresses IP de la passerelle privée virtuelle qui met fin à la connexion VPN du AWS côté de la connexion.

`Endpoint 1`

Préfixe IP que vous avez spécifié comme route statique lors de la création de la connexion VPN. Il s'agit des adresses IP de votre réseau qui sont autorisées à utiliser la connexion VPN pour accéder à votre VPC.

`Endpoint 2`

Plage d'adresses IP (bloc d'adresse CIDR) du VPC associé à la passerelle réseau privé virtuel (par exemple, 10.0.0.0/16).

`Preshared key`

La clé pré-partagée qui est utilisée pour établir la connexion IPsec VPN entre `Local Tunnel Endpoint` et`Remote Tunnel Endpoint`.

Nous vous conseillons de configurer les deux tunnels dans le cadre de la connexion VPN. Chaque tunnel se connecte à un concentrateur Site-to-Site VPN distinct du côté Amazon de la connexion VPN. Bien qu'un seul tunnel soit ouvert à la fois, le second tunnel s'établit automatiquement si le premier tunnel tombe en panne. Le fait de disposer de tunnels redondants garantit une disponibilité continue en cas de panne d'un appareil. Sachant qu'un seul tunnel est disponible à la fois, la console Amazon VPC indique qu'un tunnel est arrêté. Ce comportement étant attendu, aucune action de votre part n'est requise.

Lorsque deux tunnels sont configurés, en cas de panne d'un appareil AWS, votre connexion VPN bascule automatiquement vers le deuxième tunnel de la passerelle privée virtuelle en quelques minutes. Lorsque vous configurez votre passerelle client, vous devez configurer les deux tunnels.

> **Note**
>
> AWS Effectue de temps à autre une maintenance de routine sur la passerelle privée virtuelle. Il est possible que ces opérations désactivent l'un des deux tunnels de votre connexion VPN pendant une brève période. Votre connexion VPN bascule automatiquement vers le deuxième tunnel lors de ces opérations de maintenance.

Des informations supplémentaires concernant l'échange de clés Internet (IKE) et les associations de IPsec sécurité (SA) sont présentées dans le fichier de configuration téléchargé.

```
MainModeSecMethods:         DHGroup2-AES128-SHA1
MainModeKeyLifetime:        480min,0sess
QuickModeSecMethods:        ESP:SHA1-AES128+60min+100000kb
QuickModePFS:               DHGroup2
```

`MainModeSecMethods`

Algorithmes de chiffrement et d'authentification pour la SA IKE. Il s'agit des paramètres suggérés pour la connexion VPN et des paramètres par défaut pour les connexions IPsec VPN Windows Server.

`MainModeKeyLifetime`

Durée de vie de la clé de la SA IKE. Il s'agit du paramètre suggéré pour la connexion VPN et du paramètre par défaut pour les connexions IPsec VPN Windows Server.

`QuickModeSecMethods`

Les algorithmes de chiffrement et d'authentification pour la IPsec SA. Il s'agit des paramètres suggérés pour la connexion VPN et des paramètres par défaut pour les connexions IPsec VPN Windows Server.

`QuickModePFS`

Nous vous conseillons d'utiliser la clé principale Perfect Forward Secrecy (PFS) pour vos IPsec sessions.

Étape 3 : Configuration du serveur Windows

Avant de configurer le tunnel VPN, vous devez installer et configurer les services de routage et d'accès distant sur Windows Server. Ceci permet aux utilisateurs distants d'accéder aux ressources sur votre réseau.

Pour installer les services de routage et d'accès distant

1. Connectez-vous à votre Windows Server.
2. Accédez au menu Start et choisissez Server Manager.
3. Installez les services de routage et d'accès distant :
    a. Depuis le menu Gérer, choisissez Ajouter des rôles et fonctionnalités.
    b. Sur la page Avant de commencer, vérifiez si votre serveur respecte les conditions requises, puis choisissez Suivant.
    c. Choisissez Installation basée sur un rôle ou une fonctionnalité, puis Suivant.
    d. Sélectionnez Select a server from the server pool (Sélectionner un serveur du groupe de serveurs), puis votre Windows Server et Next (Suivant).
    e. Sélectionnez Services de stratégie et d'accès réseau dans la liste. Dans la boîte de dialogue qui s'affiche, choisissez Ajouter des fonctionnalités afin de confirmer les fonctions qui sont nécessaires pour ce rôle.
    f. Dans cette même liste, choisissez Remote Access (Accès distant), puis Next (Suivant).

g. Sur la page Sélectionner les fonctionnalités, choisissez Suivant.

h. Sur la page Services de stratégie et d'accès réseau, choisissez Suivant.

i. Sur la page Accès distant, choisissez Suivant. Sur la page suivante, sélectionnez DirectAccess et VPN (RAS). Dans la boîte de dialogue qui s'affiche, choisissez Ajouter des fonctionnalités afin de confirmer les fonctions qui sont nécessaires pour ce service de rôle. Dans cette même liste, sélectionnez Routage, puis choisissez Suivant.

j. Sur la page Rôle Serveur Web (IIS), choisissez Suivant. Conservez la sélection par défaut, puis choisissez Suivant.

k. Choisissez Installer. Une fois l'installation terminée, choisissez Fermer.

Pour configurer et activer le serveur de Routage et d'accès à distance :

1. Sur le tableau de bord, choisissez Notifications (icône de drapeau). Une tâche doit être effectuée avant de terminer la configuration de post-déploiement. Choisissez le lien Ouvrir l'Assistant Mise en route.
2. Choisissez Déployer VPN uniquement.
3. Dans la boîte de dialogue Routage et accès à distance, choisissez le nom de serveur, sélectionnez Action, puis Configurer et activer le routage et l'accès à distance.
4. Dans la section Assistant Installation d'un serveur Routage et accès distant, sur la première page, choisissez Suivant.
5. Sur la page Configuration, choisissez Configuration personnalisée, Suivant.
6. Choisissez LAN routing (Routage réseau), Next (Suivant), puis Finish (Terminer).
7. Lorsque vous y êtes invité par la boîte de dialogue Routage et accès distant, choisissez Démarrer le service.

Étape 4 : Configurer le tunnel VPN

Vous pouvez configurer le tunnel VPN en exécutant les scripts netsh inclus dans le fichier de configuration téléchargé ou à l'aide de l'interface utilisateur de Windows Server.

> **Important**
>
> Nous vous conseillons d'utiliser la clé principale Perfect Forward Secrecy (PFS) pour vos IPsec sessions. Si vous choisissez d'exécuter le script netsh, il inclut un paramètre

permettant d'activer PFS ()`qmpfs=dhgroup2`. Vous ne pouvez pas activer la clé PFS via l'interface utilisateur de Windows, vous devez l'activer à partir de la ligne de commande.

Options

- Option 1 : Exécuter le script netsh
- Option 2 : Utiliser l'interface utilisateur de Windows Server

Option 1 : Exécuter le script netsh

Copiez le script netsh dans le fichier de configuration téléchargé et remplacez les variables. Voici un exemple de script.

```
netsh advfirewall consec add rule Name="vgw-1a2b3c4d Tunnel 1" ^
Enable=Yes Profile=any Type=Static Mode=Tunnel ^
LocalTunnelEndpoint=Windows_Server_Private_IP_address ^
RemoteTunnelEndpoint=203.83.222.236 Endpoint1=Your_Static_Route_IP_Prefix ^
Endpoint2=Your_VPC_CIDR_Block Protocol=Any Action=RequireInClearOut ^
Auth1=ComputerPSK Auth1PSK=xCjNLsLoCmKsakwcdoR9yX6GsEXAMPLE ^
QMSecMethods=ESP:SHA1-AES128+60min+100000kb ^
ExemptIPsecProtectedConnections=No ApplyAuthz=No QMPFS=dhgroup2
```

Name : vous pouvez remplacer le nom proposé (`vgw-1a2b3c4d Tunnel 1`) par celui de votre choix.

LocalTunnelEndpoint: Entrez l'adresse IP privée du serveur Windows sur votre réseau.

Endpoint1 : bloc d'adresse CIDR de votre réseau sur lequel le Windows Server est situé (par exemple, `172.31.0.0/16`). Entourez cette valeur de guillemets doubles (").

Endpoint2 : bloc d'adresse CIDR de votre VPC ou d'un sous-réseau de votre VPC (par exemple, `10.0.0.0/16`). Entourez cette valeur de guillemets doubles (").

Exécutez le script mis à jour dans une fenêtre d'invite de commande sur votre Windows Server. (le caractère ^ vous permet de couper-coller le texte renvoyé à la ligne dans la ligne de commande). Pour configurer le deuxième tunnel VPN pour cette connexion VPN, répétez la procédure avec le deuxième script netsh du fichier de configuration.

Lorsque vous avez terminé, passez à la section Configurer le pare-feu Windows.

Pour plus d'informations sur les paramètres netsh, consultez la section Commandes Netsh AdvFirewall Consec de la Microsoft Library. TechNet

Option 2 : Utiliser l'interface utilisateur de Windows Server

Pour configurer le tunnel VPN, vous pouvez également utiliser l'interface utilisateur de Windows Server.

> **Important**
>
> Vous ne pouvez pas activer la fonction PFS (Perfect Forward Secrecy) de la clé principale via l'interface utilisateur de Windows Server. Vous devez activer PFS à partir de la ligne de commande, comme décrit à la section Activer la fonction PFS (Perfect Forward Secrecy) de la clé principale.

Tâches

- Configurer une règle de sécurité pour un tunnel VPN
- Valider la configuration des tunnels
- Activer la fonction PFS (Perfect Forward Secrecy) de la clé principale
- Configurer le pare-feu Windows

Configurer une règle de sécurité pour un tunnel VPN

Dans cette section, vous configurez une règle de sécurité sur votre Windows Server afin de créer un tunnel VPN.

Pour configurer une règle de sécurité pour un tunnel VPN :

1. Ouvrez Server Manager, sélectionnez Tools (Outils), puis Windows Defender Firewall with Advanced Security (Pare-feu Windows avec fonctions avancées de sécurité).
2. Sélectionnez Règles de sécurité de connexion, choisissez Action, puis Nouvelle règle.
3. Dans l'assistant Nouvelle règle de sécurité de connexion, sur la page Type de règle, choisissez Tunnel, puis Suivant.
4. Sur la page Type de tunnel, sous Quel type de tunnel voulez-vous créer ?, choisissez Configuration personnalisée. Sous Souhaitez-vous exempter les connexions IPsec protégées de

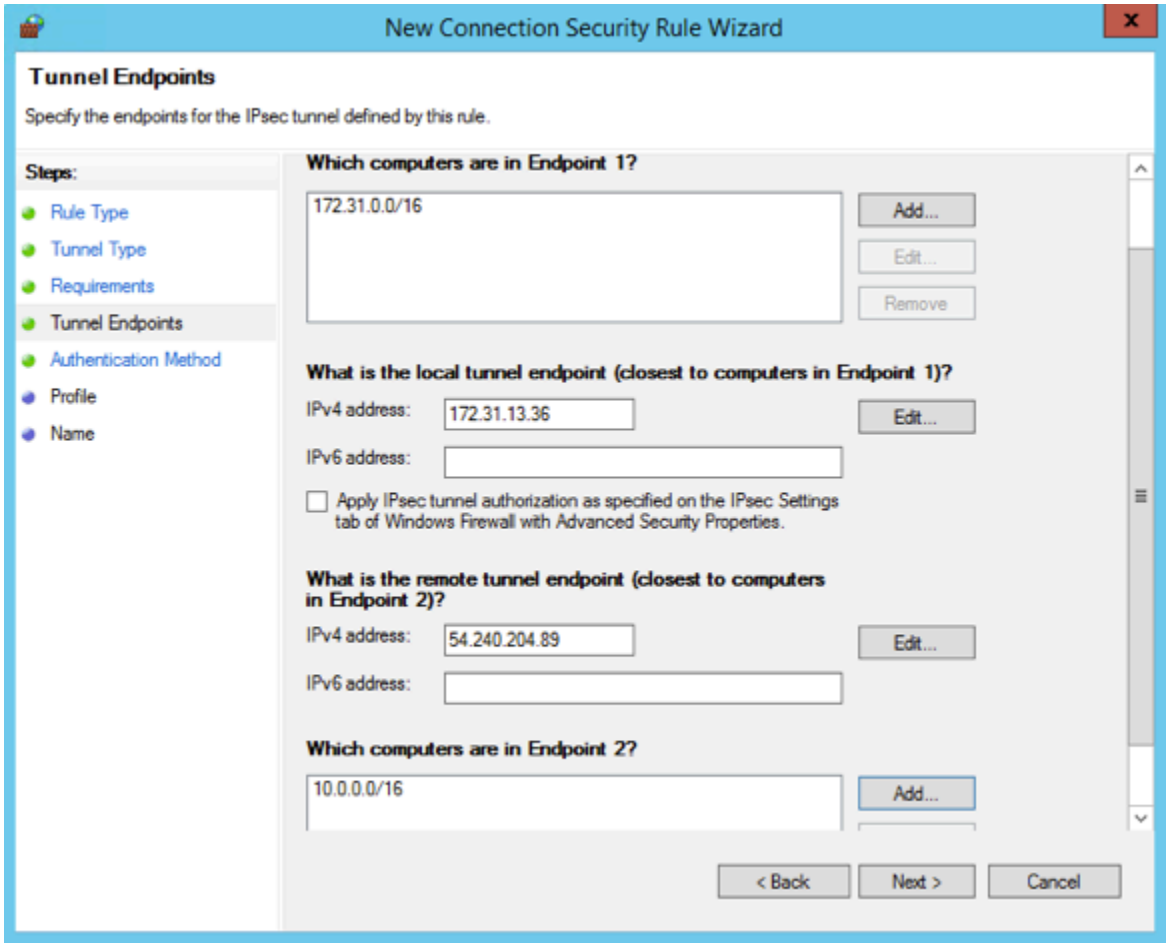
ce tunnel, laissez la valeur par défaut cochée (Non. Envoyez tout le trafic réseau correspondant à cette règle de sécurité de connexion (via le tunnel), puis choisissez Next.

5. Sur la page Exigences, choisissez Exiger l'authentification pour les connexions entrantes. N'établissez pas de tunnels pour les connexions sortantes, puis choisissez Next.
6. Sur la page Points de terminaison du tunnel, sous Quels ordinateurs se trouvent au point de terminaison 1 ?, choisissez Ajouter. Saisissez la plage CIDR de votre réseau (derrière votre périphérique de passerelle client Windows Server ; par exemple `172.31.0.0/16`), puis sélectionnez OK. La plage peut inclure l'adresse IP de votre passerelle client.
7. Sous Quel est le point de terminaison du tunnel local (le plus proche des ordinateurs du point de terminaison 1) ?, choisissez Modifier. Dans le champ d'IPv4 adresse, entrez l'adresse IP privée de votre serveur Windows, puis cliquez sur OK.
8. Sous Quel est le point de terminaison du tunnel distant (le plus proche des ordinateurs du point de terminaison 2) ?, choisissez Modifier. Dans le champ d'IPv4 adresse, entrez l'adresse IP de la passerelle privée virtuelle pour le tunnel 1 à partir du fichier de configuration (voir`Remote Tunnel Endpoint`), puis choisissez OK.

   > **Important**
   >
   > Si vous répétez cette procédure pour le tunnel 2, assurez-vous de sélectionner le point de terminaison pour le tunnel 2.

9. Sous Quels ordinateurs se trouvent au point de terminaison 2 ?, choisissez Ajouter. Dans le champ Cette adresse IP ou ce sous-réseau, entrez le bloc d'adresse CIDR de votre VPC, puis choisissez OK.

   > **Important**
   >
   > Vous devez faire défiler la boîte de dialogue jusqu'à la section Quels ordinateurs se trouvent au point de terminaison 2 ?. Ne choisissez pas Suivant avant d'avoir terminé cette étape, car vous ne pourriez pas vous connecter à votre serveur.



10. Assurez-vous que tous les paramètres que vous avez spécifiés sont corrects, puis choisissez Suivant.
11. Sur la page Authentication Method (Méthode d'authentification), sélectionnez Advanced (Avancé), puis choisissez Customize (Personnaliser).
12. Sous Premières méthodes d'authentification, choisissez Ajouter.
13. Sélectionnez Clé prépartagée, saisissez la valeur de la clé prépartagée provenant du fichier de configuration, puis cliquez sur OK.

> **Important**
>
> Si vous répétez cette procédure pour le tunnel 2, assurez-vous de sélectionner la clé pré partagée correspondante.

14. Assurez-vous que l'option La première authentification est facultative n'est pas sélectionnée, puis choisissez OK.

15. Choisissez Suivant.
16. Sur la page Profil, cochez les trois cases : Domaine, Privé et Public. Choisissez Suivant.
17. Sur la page Nom, entrez un nom pour votre règle de connexion ; par exemple, `VPN to Tunnel 1`, puis choisissez Terminer.

Répétez la procédure précédente, en spécifiant les données associées au tunnel 2 provenant du fichier de configuration.

Une fois l'opération terminée, vous disposez de deux tunnels configurés pour votre connexion VPN.

Valider la configuration des tunnels

Pour valider la configuration des tunnels :

1. Ouvrez Server Manager, choisissez Outils, sélectionnez Pare-feu Windows avec fonctions avancées de sécurité, puis sélectionnez Règles de sécurité de connexion.
2. Effectuez les vérifications suivantes pour les deux tunnels :

   - Activé est défini sur `Yes`.
   - Point de terminaison 1 est le bloc d'adresse CIDR pour votre réseau
   - Point de terminaison 2 est le bloc d'adresse CIDR pour votre VPC
   - Mode d'authentification est défini sur `Require inbound and clear outbound`.
   - Méthode d'authentification est défini sur `Custom`.
   - Port du point de terminaison 1 est défini sur `Any`.
   - Port du point de terminaison 2 est défini sur `Any`.
   - Protocole est défini sur `Any`
3. Sélectionnez la première règle et choisissez Propriétés.
4. Sous l'onglet Authentification sous Méthode, choisissez Personnaliser. Vérifiez que le champ Premières méthodes d'authentification contient la clé prépartagée correcte provenant de votre fichier de configuration pour le tunnel, puis choisissez OK.
5. Dans l'onglet Avancé, assurez-vous que les options Domaine, Privé et Public sont toutes sélectionnées.
6. Sous IPsec Tunneling, choisissez Personnaliser. Vérifiez les paramètres de IPsec tunneling suivants, puis cliquez sur OK et de nouveau sur OK pour fermer la boîte de dialogue.

   - L'option Utiliser le IPsec tunneling est sélectionnée.

- Le point de terminaison du tunnel local (le plus proche du point de terminaison 1) contient l'adresse IP de votre Windows Server. Si votre passerelle client est une instance EC2, il s'agit de l'adresse IP privée de cette dernière.
- Point de terminaison du tunnel distant (le plus proche du point de terminaison 2) contient l'adresse IP de la passerelle réseau privé virtuel pour ce tunnel.

7. Affichez les propriétés de votre second tunnel. Répétez les étapes 4 à 7 pour ce tunnel.

Activer la fonction PFS (Perfect Forward Secrecy) de la clé principale

Vous pouvez activer la fonction PFS de la clé principale à partir de la ligne de commande. Vous ne pouvez pas activer cette fonction à partir de l'interface utilisateur.

Pour activer la fonction PFS de la clé principale

1. Sur votre Windows Server, ouvrez une nouvelle fenêtre d'invite de commande.
2. Entrez la commande suivante, en remplaçant `rule_name` par le nom que vous avez attribué à la première règle de connexion.

```
netsh advfirewall consec set rule name="rule_name" new QMPFS=dhgroup2
 QMSecMethods=ESP:SHA1-AES128+60min+100000kb
```

3. Reprenez l'étape 2 pour le second tunnel, en remplaçant cette fois `rule_name` par le nom que vous avez attribué à la seconde règle de connexion.

Configurer le pare-feu Windows

Après avoir défini vos règles de sécurité sur votre serveur, configurez certains IPsec paramètres de base pour qu'ils fonctionnent avec la passerelle privée virtuelle.

Pour configurer le pare-feu Windows :

1. Ouvrez Server Manager, sélectionnez Tools (Outils), puis Windows Defender Firewall with Advanced Security (Pare-feu Windows avec fonctions avancées de sécurité) et Properties (Propriétés).
2. Dans l'onglet IPsec Paramètres, sous IPsecExemptions, vérifiez que l'option Exempter l'ICMP de IPsec est Non (valeur par défaut). Vérifiez que l'autorisation IPsec du tunnel est nulle.
3. Dans la section IPsec Paramètres par défaut, choisissez Personnaliser.

4. Sous Échange de clé (mode principal), sélectionnez Avancé, puis choisissez Personnaliser.
5. Dans Personnaliser les paramètres avancés d'échange de clés, sous Méthodes de sécurité, assurez-vous que les valeurs par défaut suivantes sont utilisées comme première entrée :

   - Intégrité : SHA-1
   - Chiffrement : AES-CBC 128
   - Algorithme d'échange de clés : Groupe Diffie-Hellman 2
   - Sous Durée de vie des clés, assurez-vous que Minutes est défini sur `480` et que Sessions est défini sur `0`.

   Ces paramètres correspondent aux entrées suivantes dans le fichier de configuration.

   ```
   MainModeSecMethods: DHGroup2-AES128-SHA1,DHGroup2-3DES-SHA1
   MainModeKeyLifetime: 480min,0sec
   ```

6. Sous Options d'échange de clés, sélectionnez Utiliser Diffie-Hellman pour une sécurité accrue, puis choisissez OK.
7. Sous Protection des données (mode rapide), sélectionnez Avancé, puis choisissez Personnaliser.
8. Sélectionnez Demander le chiffrement de toutes les règles de sécurité de connexion qui utilisent ces paramètres.
9. Sous Intégrité de données et chiffrement, conservez les valeurs par défaut:

   - Protocole : ESP
   - Intégrité : SHA-1
   - Chiffrement : AES-CBC 128
   - Durée de vie : 60 minutes

   Ces valeurs correspondent à l'entrée suivante du fichier de configuration.

   ```
   QuickModeSecMethods:
   ESP:SHA1-AES128+60min+100000kb
   ```

10. Cliquez sur OK pour revenir à la boîte de dialogue Personnaliser IPsec les paramètres, puis cliquez à nouveau sur OK pour enregistrer la configuration.

Étape 5 : Activer la détection de passerelle inactive

Ensuite, configurez TCP pour détecter quand une passerelle devient indisponible. Pour ce faire, vous pouvez modifier cette clé de registre : `HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters`. N'effectuez pas cette opération avant d'avoir terminé la procédure indiquée dans les sections précédentes. Une fois que vous avez modifié la clé de registre, vous devez redémarrer le serveur.

Pour activer la détection de passerelle inactive :

1. Depuis votre serveur Windows, lancez l'invite de commande ou une PowerShell session, puis entrez regedit pour démarrer l'éditeur de registre.
2. Développez HKEY_LOCAL_MACHINE, développez le SYSTÈME, étendez, étendez les services CurrentControlSet, étendez Tcpip, puis développez les paramètres.
3. Dans le menu Editer, sélectionnez Nouveau et sélectionnez Valeur DWORD 32 bits.
4. Saisissez le nom EnableDeadGWDetect.
5. Sélectionnez EnableDeadGWDetectet choisissez Modifier, Modifier.
6. Dans Données de la valeur, saisissez 1, puis choisissez OK.
7. Fermez l'Éditeur du Registre, puis redémarrez le serveur.

Pour plus d'informations, consultez EnableDeadGWDetectla Microsoft TechNet Library.

Étape 6 : Tester la connexion VPN

Pour vérifier si la connexion VPN fonctionne correctement, lancez une instance dans votre VPC et assurez-vous qu'elle n'est associée à aucune connexion Internet. Après avoir lancé l'instance, effectuez un test ping sur son adresse IP privée à partir de votre Windows Server. Le tunnel VPN intervient lorsque le trafic est généré à partir du périphérique de passerelle client. Par conséquent, la commande ping initie également la connexion VPN.

Pour savoir comment tester la connexion VPN, consultez Tester une AWS Site-to-Site VPN connexion.

Si la commande `ping` échoue, vérifiez les informations suivantes :

- Assurez-vous d'avoir configuré vos règles de groupe de sécurité pour autoriser le trafic ICMP vers l'instance dans votre VPC. Si votre serveur Windows est une instance EC2, assurez-vous

que les règles sortantes de son groupe de sécurité autorisent IPsec le trafic. Pour de plus amples informations, veuillez consulter Configuration de votre instance Windows.

- Assurez-vous que le système d'exploitation est configuré pour répondre à ICMP, sur l'instance faisant l'objet de votre test ping. Nous vous recommandons d'utiliser l'un des systèmes Amazon Linux AMIs.
- Si l'instance à laquelle vous envoyez un ping est une instance Windows, connectez-vous à l'instance et activez le trafic entrant ICMPv4 sur le pare-feu Windows.
- Assurez-vous d'avoir correctement configuré les tables de routage pour votre VPC ou votre sous-réseau. Pour de plus amples informations, veuillez consulter Étape 1: Créer une connexion VPN et configurer votre VPC.
- Si votre dispositif de passerelle client est une instance EC2, assurez-vous d'avoir désactivé la source/destination vérification de l'instance. Pour de plus amples informations, veuillez consulter Configuration de votre instance Windows.

Sur la page VPN Connections de la console Amazon VPC, sélectionnez votre connexion VPN. Le premier tunnel est à l'état « UP ». Le second tunnel doit être configuré, mais il ne sera utilisé que si le premier tunnel s'arrête. L'établissement des tunnels chiffrés peut prendre quelques instants.

Résolution des problèmes AWS Site-to-Site VPN Appareil de passerelle client

Lorsque vous résolvez des problèmes liés à votre dispositif de passerelle client, il est important d'adopter une approche structurée. Les deux premières rubriques de cette section fournissent des organigrammes généraux permettant de résoudre les problèmes liés à l'utilisation d'un périphérique configuré pour le routage dynamique (BGP activé) et d'un périphérique configuré pour le routage statique (sans BGP activé), respectivement. Vous trouverez ci-dessous des guides de dépannage spécifiques aux appareils pour les appareils de passerelle client Cisco, Juniper et Yamaha.

Outre les sujets abordés dans cette section, l'activation AWS Site-to-Site VPN journaux peut être très utile pour résoudre les problèmes de connectivité VPN. Pour les instructions générales de test, voir égalementTester une AWS Site-to-Site VPN connexion.

Rubriques

- Dépannage AWS Site-to-Site VPN connectivité lors de l'utilisation du protocole Border Gateway

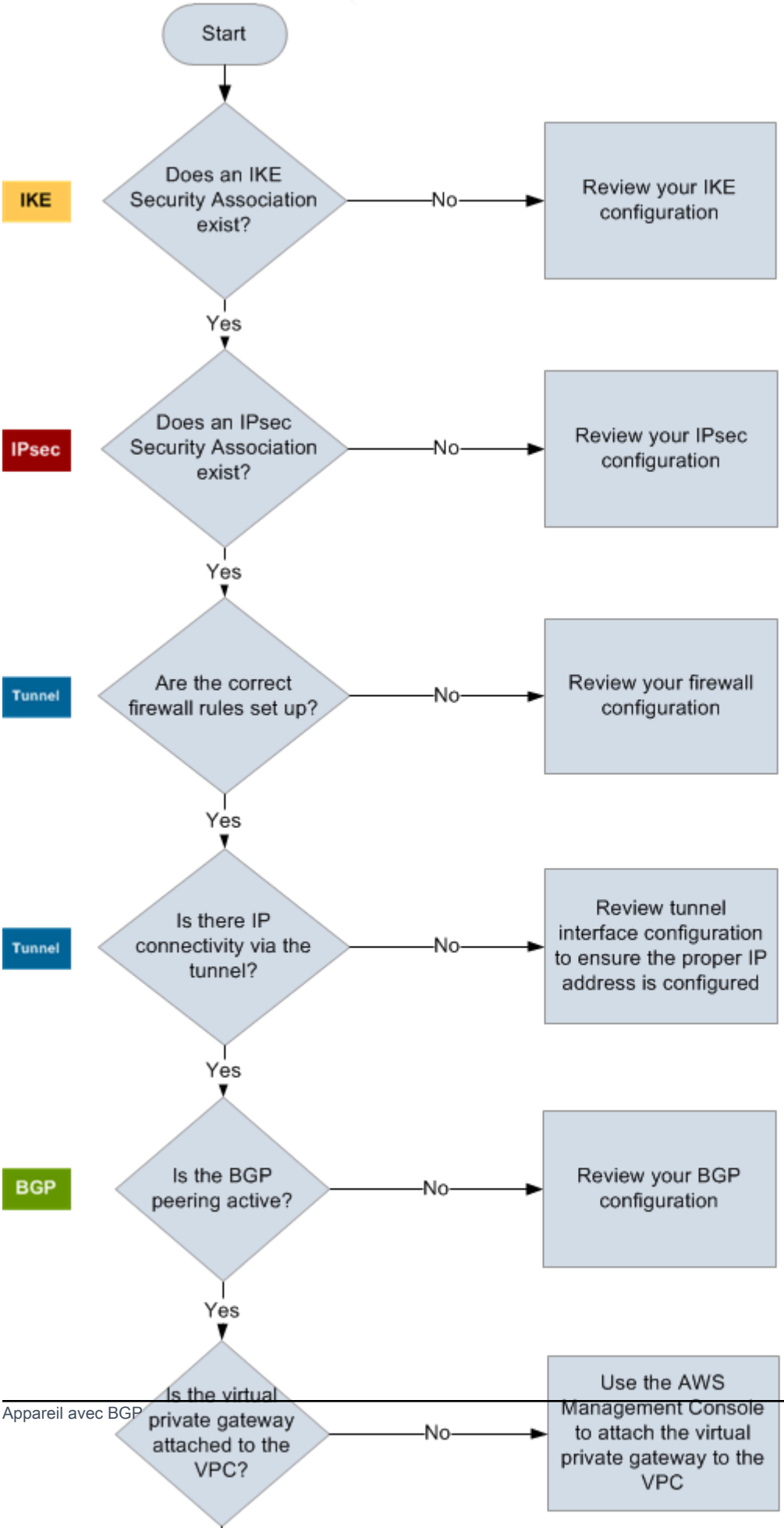
- Dépannage AWS Site-to-Site VPN connectivité sans Border Gateway Protocol
- Dépannage AWS Site-to-Site VPN connectivité avec un dispositif de passerelle client Cisco ASA
- Dépannage AWS Site-to-Site VPN connectivité avec un dispositif de passerelle client Cisco IOS
- Dépannage AWS Site-to-Site VPN connectivité avec un dispositif de passerelle client Cisco IOS sans le protocole Border Gateway
- Dépannage AWS Site-to-Site VPN connectivité avec un dispositif de passerelle client Juniper JunOS
- Dépannage AWS Site-to-Site VPN connectivité avec un dispositif de passerelle client Juniper ScreenOS
- Dépannage AWS Site-to-Site VPN connectivité avec un dispositif de passerelle client Yamaha

Ressources supplémentaires

- Forum Amazon VPC

Dépannage AWS Site-to-Site VPN connectivité lors de l'utilisation du protocole Border Gateway

Le schéma et le tableau suivants fournissent des instructions générales pour la résolution de problèmes sur un périphérique de passerelle client qui utilise le protocole BGP (Border Gateway Protocol). Nous vous recommandons également d'activer les fonctions de débogage de votre appareil. Consultez le fournisseur de votre périphérique de passerelle pour plus de détails.

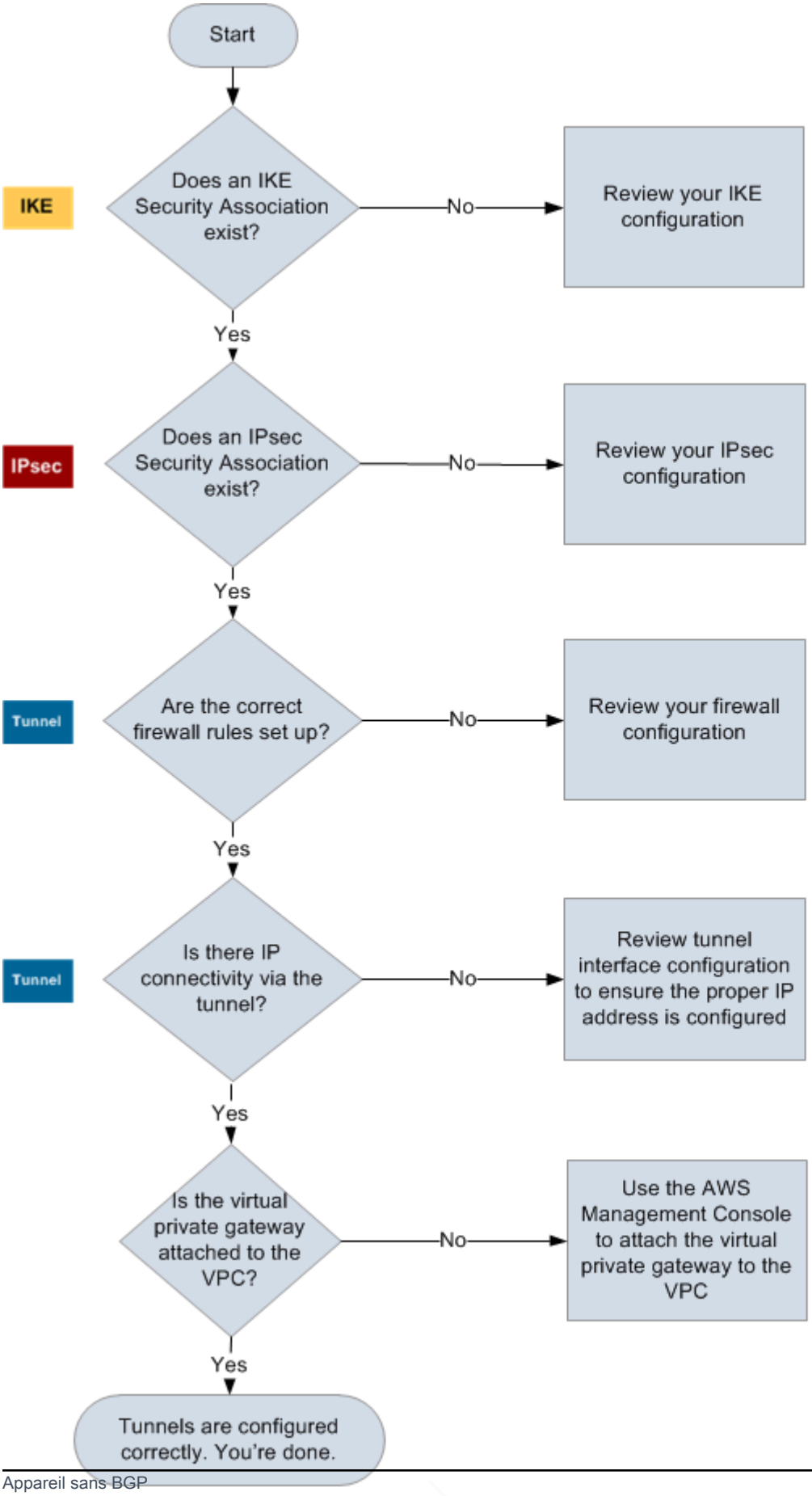

Start
IKE
Does an IKE Security Association exist?
No
Review your IKE configuration
Yes
IPsec
Does an IPsec Security Association exist?
No
Review your IPsec configuration
Yes
Tunnel
Are the correct firewall rules set up?
No
Review your firewall configuration
Yes
Tunnel
Is there IP connectivity via the tunnel?
No
Review tunnel interface configuration to ensure the proper IP address is configured
Yes
BGP
Is the BGP peering active?
No
Review your BGP configuration
Yes
Is the virtual private gateway attached to the VPC?
No
Use the AWS Management Console to attach the virtual private gateway to the VPC

IKE	Déterminez si une association de sécurité IKE existe. Une association de sécurité IKE est nécessaire pour échanger les clés utilisées pour établir l'association de sécurité IPsec. Si aucune association de sécurité IKE n'existe, passez en revue vos paramètres de configuration IKE. Vous devez configurer le chiffrement, l'authentification, la confidentialité persistante parfaite (perfect-forward-secrecy) et les paramètres de mode comme répertoriés dans le fichier de configuration. Si une association de sécurité IKE existe, passez à « IPsec ».
IPsec	Déterminez si une association de sécurité (SA) IPsec existe. Une SA IPSec est le tunnel lui-même. Interrogez votre périphérique de passerelle client pour déterminer si une SA IPSec est active. Assurez-vous de configurer le chiffrement, l'authentification, la confidentialité persistante parfaite (perfect-forward-secrecy) et les paramètres de mode comme répertoriés dans le fichier de configuration. Si aucune SA IPSec n'existe, vérifiez votre configuration IPSec. Si une SA IPSec existe, passez à « Tunnel ».
Tunnel	Vérifiez que les règles de pare-feu nécessaires sont configurées (pour une liste des règles, consultez Règles de pare-feu pour un AWS Site-to-Site VPN Appareil de passerelle client). Si c'est le cas, continuez. Déterminez s'il existe une connexion IP via le tunnel. Chaque côté du tunnel possède une adresse IP comme spécifié dans le fichier de configuration. L'adresse de la passerelle réseau privé virtuel est l'adresse utilisée comme l'adresse du voisin BGP. Depuis votre passerelle client, exécutez un test ping de cette adresse pour déterminer si le trafic IP est correctement chiffré et déchiffré. Si le test ping n'est pas réussi, passez en revue la configuration de votre interface de tunnel pour vérifier qu'une adresse IP correcte est configurée. Si le test ping est réussi, passez à « BGP ».

BGP	Déterminez si la session d'appairage BGP est active. Pour chaque tunnel, procédez de la façon suivante : • Sur votre passerelle client, déterminez si l'état du BGP est `Active` ou `Established` . Il peut se passer environ 30 secondes avant que l'appairage BGP devienne actif. • Assurez-vous que le dispositif de passerelle client annonce l'itinéraire par défaut (0.0.0). 0/0) vers la passerelle privée virtuelle. Si les tunnels ne sont pas dans cet état, passez en revue la configuration de votre BGP. Si l'appairage BGP est instauré, que vous recevez un préfixe et que vous publiez un préfixe, alors votre tunnel est configuré correctement. Assurez-vous que les deux tunnels sont dans cet état.

Dépannage AWS Site-to-Site VPN connectivité sans Border Gateway Protocol

Le schéma et le tableau suivants fournissent des instructions générales pour la résolution de problèmes sur un périphérique de passerelle client qui n'utilise pas de protocole BGP (Border Gateway Protocol). Nous vous recommandons également d'activer les fonctions de débogage de votre appareil. Consultez le fournisseur de votre périphérique de passerelle pour plus de détails.


Start
IKE
Does an IKE Security Association exist?
No
Review your IKE configuration
Yes
IPsec
Does an IPsec Security Association exist?
No
Review your IPsec configuration
Yes
Tunnel
Are the correct firewall rules set up?
No
Review your firewall configuration
Yes
Tunnel
Is there IP connectivity via the tunnel?
No
Review tunnel interface configuration to ensure the proper IP address is configured
Yes
Is the virtual private gateway attached to the VPC?
No
Use the AWS Management Console to attach the virtual private gateway to the VPC
Yes
Tunnels are configured correctly. You're done.

IKE	Déterminez si une association de sécurité IKE existe. Une association de sécurité IKE est nécessaire pour échanger les clés utilisées pour établir l'association de sécurité IPsec. Si aucune association de sécurité IKE n'existe, passez en revue vos paramètres de configuration IKE. Vous devez configurer le chiffrement, l'authentification, la confidentialité persistante parfaite (perfect-forward-secrecy) et les paramètres de mode comme répertoriés dans le fichier de configuration. Si une association de sécurité IKE existe, passez à « IPsec ».
IPsec	Déterminez si une association de sécurité (SA) IPsec existe. Une SA IPSec est le tunnel lui-même. Interrogez votre périphérique de passerelle client pour déterminer si une SA IPSec est active. Assurez-vous de configurer le chiffrement, l'authentification, la confidentialité persistante parfaite (perfect-forward-secrecy) et les paramètres de mode comme répertoriés dans le fichier de configuration. Si aucune SA IPSec n'existe, vérifiez votre configuration IPSec. Si une SA IPSec existe, passez à « Tunnel ».
Tunnel	Vérifiez que les règles de pare-feu nécessaires sont configurées (pour une liste des règles, consultez Règles de pare-feu pour un AWS Site-to-Site VPN Appareil de passerelle client). Si c'est le cas, continuez. Déterminez s'il existe une connexion IP via le tunnel. Chaque côté du tunnel possède une adresse IP comme spécifié dans le fichier de configuration. L'adresse de la passerelle réseau privé virtuel est l'adresse utilisée comme l'adresse du voisin BGP. Depuis votre passerelle client, exécutez un test ping de cette adresse pour déterminer si le trafic IP est correctement chiffré et déchiffré. Si le test ping n'est pas réussi, passez en revue la configuration de votre interface de tunnel pour vérifier qu'une adresse IP correcte est configurée. Si le ping réussit, passez à « Routes statiques ».

Routes statiques	Pour chaque tunnel, procédez de la façon suivante : • Vérifiez que vous avez ajouté une route statique au CIDR de votre VPC avec les tunnels comme prochain saut. • Vérifiez que vous avez ajouté une route statique dans la console Amazon VPC pour demander à la passerelle réseau privé virtuel de renvoyer le trafic vers vos réseaux internes. Si les tunnels ne sont pas dans cet état, passez en revue la configuration de votre périphérique. Assurez-vous que les deux tunnels sont dans cet état et vous avez terminé.

Dépannage AWS Site-to-Site VPN connectivité avec un dispositif de passerelle client Cisco ASA

Quand vous résolvez les problèmes de connexion d'une passerelle client Cisco, prenez en compte trois critères : IKE (Internet Key Exchange), IPsec (Internet Protocol Security) et le routage. Vous pouvez résoudre des problèmes dans ces domaines dans n'importe quel ordre mais nous vous recommandons de commencer avec l'IKE (en bas du stack réseau) et de remonter.

> **Important**
>
> Certains ASA Cisco ne prennent en charge que le Active/Standby mode. Lorsque vous utilisez ces systèmes Cisco ASA, vous ne pouvez avoir qu'un seul tunnel actif à la fois. L'autre tunnel en veille devient actif uniquement si le premier tunnel devient inaccessible. Le tunnel en veille peut générer l'erreur suivante dans vos fichiers journaux, qui peut être ignorée : `Rejecting IPSec tunnel: no matching crypto map entry for remote proxy 0.0.0.0/0.0.0.0/0/0 local proxy 0.0.0.0/0.0.0.0/0/0 on interface outside`.

IKE

Utilisez la commande suivante de l'. La réponse montre une passerelle client avec IKE configuré correctement.

```
ciscoasa# show crypto isakmp sa
```

```
   Active SA: 2
   Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 2

1   IKE Peer: AWS_ENDPOINT_1
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE
```

Vous devez voir une ou plusieurs lignes contenant une valeur `src` pour la passerelle à distance spécifiée dans les tunnels. La valeur de `state` doit être `MM_ACTIVE` et `status` doit être `ACTIVE`. L'absence d'une entrée, ou toute entrée dans un état différent, indique que l'IKE n'est pas correctement configuré.

Pour un dépannage plus approfondi, exécutez les commandes suivantes pour permettre la consignation des messages qui apportent des informations de diagnostic.

```
router# term mon
router# debug crypto isakmp
```

Pour désactiver le débogage, utilisez la commande suivante.

```
router# no debug crypto isakmp
```

IPsec

Utilisez la commande suivante de l'. La réponse montre une passerelle client avec IPsec configuré correctement.

```
ciscoasa# show crypto ipsec sa
```

```
interface: outside
    Crypto map tag: VPN_crypto_map_name, seq num: 2, local addr: 172.25.50.101

      access-list integ-ppe-loopback extended permit ip any vpc_subnet subnet_mask
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (vpc_subnet/subnet_mask/0/0)
      current_peer: integ-ppe1
```

```
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
    #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
    #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
    #send errors: 0, #recv errors: 0

    local crypto endpt.: 172.25.50.101, remote crypto endpt.: AWS_ENDPOINT_1

    path mtu 1500, ipsec overhead 74, media mtu 1500
    current outbound spi: 6D9F8D3B
    current inbound spi : 48B456A6

  inbound esp sas:
    spi: 0x48B456A6 (1219778214)
       transform: esp-aes esp-sha-hmac no compression
       in use settings ={L2L, Tunnel, PFS Group 2, }
       slot: 0, conn_id: 4710400, crypto-map: VPN_cry_map_1
       sa timing: remaining key lifetime (kB/sec): (4374000/3593)
       IV size: 16 bytes
       replay detection support: Y
       Anti replay bitmap:
        0x00000000 0x00000001
  outbound esp sas:
    spi: 0x6D9F8D3B (1839172923)
       transform: esp-aes esp-sha-hmac no compression
       in use settings ={L2L, Tunnel, PFS Group 2, }
       slot: 0, conn_id: 4710400, crypto-map: VPN_cry_map_1
       sa timing: remaining key lifetime (kB/sec): (4374000/3593)
       IV size: 16 bytes
       replay detection support: Y
       Anti replay bitmap:
       0x00000000 0x00000001
```

Pour chaque interface du tunnel, vous devez voir `inbound esp sas` et `outbound esp sas`. Ceci suppose qu'une SA (Security Association, association de sécurité) est répertoriée (par exemple, `spi: 0x48B456A6`), et qu'IPsec est correctement configuré.

Dans Cisco ASA, IPsec n'apparaît qu'après l'envoi d'un trafic intéressant (trafic qui doit être chiffré). Pour qu'IPsec demeure toujours actif, nous vous recommandons de configurer un moniteur SLA. Le moniteur SLA continue d'envoyer le trafic intéressant, tout en gardant IPsec actif.

Vous pouvez aussi utiliser la commande ping suivante pour forcer votre IPsec à démarrer les négociations et remonter.

```
ping ec2_instance_ip_address
```

```
Pinging ec2_instance_ip_address with 32 bytes of data:

Reply from ec2_instance_ip_address: bytes=32 time<1ms TTL=128
Reply from ec2_instance_ip_address: bytes=32 time<1ms TTL=128
Reply from ec2_instance_ip_address: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.4:
Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),

Approximate round trip times in milliseconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Pour un dépannage plus approfondi, exécutez les commandes suivantes pour activer le débogage.

```
router# debug crypto ipsec
```

Pour désactiver le débogage, utilisez la commande suivante.

```
router# no debug crypto ipsec
```

Routage

Effectuez un test ping sur l'autre entrée du tunnel. Si cela fonctionne, votre IPsec doit être établi. Si cela ne fonctionne pas, vérifiez vos listes d'accès et consultez la section IPsec précédente.

Si vous ne pouvez pas atteindre vos instances, vérifiez les points suivants :

1. Vérifiez que la liste d'accès est configurée pour autoriser le trafic associé à la carte de chiffrement.

   Vous pouvez le faire à l'aide de la commande suivante.

   ```
   ciscoasa# show run crypto
   ```

   ```
   crypto ipsec transform-set transform-amzn esp-aes esp-sha-hmac
   ```

```
crypto map VPN_crypto_map_name 1 match address access-list-name
crypto map VPN_crypto_map_name 1 set pfs
crypto map VPN_crypto_map_name 1 set peer AWS_ENDPOINT_1 AWS_ENDPOINT_2
crypto map VPN_crypto_map_name 1 set transform-set transform-amzn
crypto map VPN_crypto_map_name 1 set security-association lifetime seconds 3600
```

2. Vérifiez la liste d'accès à l'aide de la commande suivante.

```
ciscoasa# show run access-list access-list-name
```

```
access-list access-list-name extended permit ip any vpc_subnet subnet_mask
```

3. Vérifiez que la liste d'accès est correcte. L'exemple de liste d'accès suivant autorise tout le trafic interne vers le sous-réseau VPC 10.0.0. 0/16.

```
access-list access-list-name extended permit ip any 10.0.0.0 255.255.0.0
```

4. Exécutez un traceroute depuis le périphérique Cisco ASA pour voir s'il atteint les routeurs Amazon (par exemple,*AWS_ENDPOINT_1*/). *AWS_ENDPOINT_2*

   S'il atteint le routeur Amazon, vérifiez les routes statiques que vous avez ajoutées à la console Amazon VPC, ainsi que les groupes de sécurité des instances spécifiques.

5. Pour un dépannage plus approfondi, passez en revue la configuration.

Faites rebondir l'interface du tunnel

Si le tunnel semble ouvert mais que le trafic ne circule pas correctement, le fait de rebondir (désactiver et réactiver) l'interface du tunnel peut souvent résoudre les problèmes de connectivité. Pour faire rebondir l'interface du tunnel sur un Cisco ASA :

1. Exécutez les commandes suivantes :

```
ciscoasa# conf t
ciscoasa(config)# interface tunnel X  (where X is your tunnel ID)
ciscoasa(config-if)# shutdown
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# end
```

   Vous pouvez également utiliser une commande d'une seule ligne :

```
ciscoasa# conf t ; interface tunnel X ; shutdown ; no shutdown ; end
```

2. Après avoir fait rebondir l'interface, vérifiez si la connexion VPN a été rétablie et si le trafic circule désormais correctement.

Dépannage AWS Site-to-Site VPN connectivité avec un dispositif de passerelle client Cisco IOS

Quand vous résolvez les problèmes de connexion d'une passerelle client Cisco, prenez en compte quatre critères : IKE, IPsec, le tunnel et le protocole BGP. Vous pouvez résoudre des problèmes dans ces domaines dans n'importe quel ordre mais nous vous recommandons de commencer avec l'IKE (en bas du stack réseau) et de remonter.

IKE

Utilisez la commande suivante de l'. La réponse montre une passerelle client avec IKE configuré correctement.

```
router# show crypto isakmp sa
```

```
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
192.168.37.160  72.21.209.193   QM_IDLE           2001    0 ACTIVE
192.168.37.160  72.21.209.225   QM_IDLE           2002    0 ACTIVE
```

Vous devez voir une ou plusieurs lignes contenant une valeur `src` pour la passerelle à distance spécifiée dans les tunnels. `state` doit être `QM_IDLE` et `status` doit être `ACTIVE`. L'absence d'une entrée, ou toute entrée dans un état différent, indique qu'IKE n'est pas correctement configuré.

Pour un dépannage plus approfondi, exécutez les commandes suivantes pour permettre la consignation des messages qui apportent des informations de diagnostic.

```
router# term mon
router# debug crypto isakmp
```

Pour désactiver le débogage, utilisez la commande suivante.

```
router# no debug crypto isakmp
```

IPsec

Utilisez la commande suivante de l'. La réponse montre une passerelle client avec IPsec configuré correctement.

```
router# show crypto ipsec sa
```

```
interface: Tunnel1
    Crypto map tag: Tunnel1-head-0, local addr 192.168.37.160

    protected vrf: (none)
    local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
    remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
    current_peer 72.21.209.225 port 500
     PERMIT, flags={origin_is_acl,}
     #pkts encaps: 149, #pkts encrypt: 149, #pkts digest: 149
     #pkts decaps: 146, #pkts decrypt: 146, #pkts verify: 146
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 0, #pkts compr. failed: 0
     #pkts not decompressed: 0, #pkts decompress failed: 0
     #send errors 0, #recv errors 0

     local crypto endpt.: 174.78.144.73, remote crypto endpt.: 72.21.209.225
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0
     current outbound spi: 0xB8357C22(3090512930)

     inbound esp sas:
      spi: 0x6ADB173(112046451)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 1, flow_id: Motorola SEC 2.0:1, crypto map: Tunnel1-head-0
       sa timing: remaining key lifetime (k/sec): (4467148/3189)
       IV size: 16 bytes
       replay detection support: Y  replay window size: 128
       Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:
```

```
      outbound esp sas:
       spi: 0xB8357C22(3090512930)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2, flow_id: Motorola SEC 2.0:2, crypto map: Tunnel1-head-0
        sa timing: remaining key lifetime (k/sec): (4467148/3189)
        IV size: 16 bytes
        replay detection support: Y  replay window size: 128
        Status: ACTIVE

      outbound ah sas:

      outbound pcp sas:

interface: Tunnel2
      Crypto map tag: Tunnel2-head-0, local addr 174.78.144.73

      protected vrf: (none)
      local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      current_peer 72.21.209.193 port 500
       PERMIT, flags={origin_is_acl,}
      #pkts encaps: 26, #pkts encrypt: 26, #pkts digest: 26
      #pkts decaps: 24, #pkts decrypt: 24, #pkts verify: 24
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts compr. failed: 0
      #pkts not decompressed: 0, #pkts decompress failed: 0
      #send errors 0, #recv errors 0

      local crypto endpt.: 174.78.144.73, remote crypto endpt.: 72.21.209.193
      path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0
      current outbound spi: 0xF59A3FF6(4120526838)

      inbound esp sas:
       spi: 0xB6720137(3060924727)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 3, flow_id: Motorola SEC 2.0:3, crypto map: Tunnel2-head-0
        sa timing: remaining key lifetime (k/sec): (4387273/3492)
        IV size: 16 bytes
        replay detection support: Y  replay window size: 128
        Status: ACTIVE

      inbound ah sas:
```

```
    inbound pcp sas:

    outbound esp sas:
     spi: 0xF59A3FF6(4120526838)
      transform: esp-aes esp-sha-hmac ,
      in use settings ={Tunnel, }
      conn id: 4, flow_id: Motorola SEC 2.0:4, crypto map: Tunnel2-head-0
      sa timing: remaining key lifetime (k/sec): (4387273/3492)
      IV size: 16 bytes
      replay detection support: Y  replay window size: 128
      Status: ACTIVE

    outbound ah sas:

    outbound pcp sas:
```

Pour chaque interface du tunnel, vous devez voir `inbound esp sas` et `outbound esp sas`. En supposant qu'une SA est répertoriée (`spi: 0xF95D2F3C` par exemple) et que `Status` a pour valeur `ACTIVE`, l'IPsec est correctement configuré.

Pour un dépannage plus approfondi, exécutez les commandes suivantes pour activer le débogage.

```
router# debug crypto ipsec
```

Utilisez la commande suivante pour désactiver le débogage.

```
router# no debug crypto ipsec
```

Tunnel

Tout d'abord, vérifiez que les règles de pare-feu nécessaires sont instaurées. Pour de plus amples informations, veuillez consulter Règles de pare-feu pour un AWS Site-to-Site VPN Appareil de passerelle client.

Si vos règles de pare-feu sont correctement configurées, alors continuez le dépannage avec la commande suivante.

```
router# show interfaces tun1
```

```
Tunnel1 is up, line protocol is up
```

```
  Hardware is Tunnel
  Internet address is 169.254.255.2/30
  MTU 17867 bytes, BW 100 Kbit/sec, DLY 50000 usec,
    reliability 255/255, txload 2/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 174.78.144.73, destination 72.21.209.225
  Tunnel protocol/transport IPSEC/IP
  Tunnel TTL 255
  Tunnel transport MTU 1427 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPSec (profile "ipsec-vpn-92df3bfb-0")
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 1 packets/sec
  5 minute output rate 1000 bits/sec, 1 packets/sec
    407 packets input, 30010 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
```

Assurez-vous que le `line protocol` est opérationnel. Vérifiez que l'adresse IP source du tunnel, l'interface source et la destination correspondent respectivement à la configuration du tunnel pour l'adresse IP externe de la passerelle client, pour l'interface et pour l'adresse IP externe de la passerelle réseau privé virtuel. Assurez-vous que `Tunnel protection via IPSec` est présent. Assurez-vous d'exécuter la commande sur les deux interfaces du tunnel. Pour résoudre les éventuels problèmes, vérifiez la configuration et les connexions physiques à votre passerelle client.

Utilisez également la commande suivante, en remplaçant `169.254.255.1` par l'adresse IP interne de votre passerelle réseau privé virtuel.

```
router# ping 169.254.255.1 df-bit size 1410
```

```
Type escape sequence to abort.
Sending 5, 1410-byte ICMP Echos to 169.254.255.1, timeout is 2 seconds:
Packet sent with the DF bit set
!!!!!
```

Vous devez voir 5 points d'exclamation.

Pour un dépannage plus approfondi, passez en revue la configuration.

BGP

Utilisez la commande suivante de l'.

```
router# show ip bgp summary
```

```
BGP router identifier 192.168.37.160, local AS number 65000
BGP table version is 8, main routing table version 8
2 network entries using 312 bytes of memory
2 path entries using 136 bytes of memory
3/1 BGP path/bestpath attribute entries using 444 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 1 (at peak 2) using 32 bytes of memory
BGP using 948 total bytes of memory
BGP activity 4/1 prefixes, 4/1 paths, scan interval 15 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
169.254.255.1   4  7224     363     323        8    0    0 00:54:21        1
169.254.255.5   4  7224     364     323        8    0    0 00:00:24        1
```

Les deux voisins doivent être répertoriés. Pour chacun d'entre eux, vous devez voir la valeur 1 pour `State/PfxRcd`.

Si le peering BGP est activé, vérifiez que votre dispositif de passerelle client annonce l'itinéraire par défaut (0.0.0). 0/0) vers le VPC.

```
router# show bgp all neighbors 169.254.255.1 advertised-routes
```

```
For address family: IPv4 Unicast
BGP table version is 3, local router ID is 174.78.144.73
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
     r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Originating default network 0.0.0.0

Network             Next Hop            Metric   LocPrf Weight Path
*> 10.120.0.0/16    169.254.255.1          100        0   7224    i
```

```
Total number of prefixes 1
```

En outre, assurez-vous de recevoir le préfixe correspondant à votre VPC depuis la passerelle réseau privé virtuel.

```
router# show ip route bgp
```

```
 10.0.0.0/16 is subnetted, 1 subnets
B       10.255.0.0 [20/0] via 169.254.255.1, 00:00:20
```

Pour un dépannage plus approfondi, passez en revue la configuration.

Dépannage AWS Site-to-Site VPN connectivité avec un dispositif de passerelle client Cisco IOS sans le protocole Border Gateway

Quand vous résolvez les problèmes de connexion d'une passerelle client Cisco, prenez en compte trois critères : IKE (Internet Key Exchange), IPsec (Internet Protocol Security) et le tunnel. Vous pouvez résoudre des problèmes dans ces domaines dans n'importe quel ordre mais nous vous recommandons de commencer avec l'IKE (en bas du stack réseau) et de remonter.

IKE

Utilisez la commande suivante de l'. La réponse montre une passerelle client avec IKE configuré correctement.

```
router# show crypto isakmp sa
```

```
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
174.78.144.73 205.251.233.121 QM_IDLE           2001    0 ACTIVE
174.78.144.73 205.251.233.122 QM_IDLE           2002    0 ACTIVE
```

Vous devez voir une ou plusieurs lignes contenant une valeur `src` pour la passerelle à distance spécifiée dans les tunnels. `state` doit être `QM_IDLE` et `status` doit être `ACTIVE`. L'absence d'une entrée, ou toute entrée dans un état différent, indique que l'IKE n'est pas correctement configuré.

Pour un dépannage plus approfondi, exécutez les commandes suivantes pour permettre la consignation des messages qui apportent des informations de diagnostic.

```
router# term mon
router# debug crypto isakmp
```

Pour désactiver le débogage, utilisez la commande suivante.

```
router# no debug crypto isakmp
```

IPsec

Utilisez la commande suivante de l'. La réponse montre une passerelle client avec IPsec configuré correctement.

```
router# show crypto ipsec sa
```

```
interface: Tunnel1
    Crypto map tag: Tunnel1-head-0, local addr 174.78.144.73

    protected vrf: (none)
    local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
    remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
    current_peer 72.21.209.225 port 500
     PERMIT, flags={origin_is_acl,}
     #pkts encaps: 149, #pkts encrypt: 149, #pkts digest: 149
     #pkts decaps: 146, #pkts decrypt: 146, #pkts verify: 146
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 0, #pkts compr. failed: 0
     #pkts not decompressed: 0, #pkts decompress failed: 0
     #send errors 0, #recv errors 0

     local crypto endpt.: 174.78.144.73, remote crypto endpt.:205.251.233.121
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0
     current outbound spi: 0xB8357C22(3090512930)

     inbound esp sas:
      spi: 0x6ADB173(112046451)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 1, flow_id: Motorola SEC 2.0:1, crypto map: Tunnel1-head-0
       sa timing: remaining key lifetime (k/sec): (4467148/3189)
       IV size: 16 bytes
       replay detection support: Y  replay window size: 128
```

```
        Status: ACTIVE

      inbound ah sas:

      inbound pcp sas:

      outbound esp sas:
       spi: 0xB8357C22(3090512930)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2, flow_id: Motorola SEC 2.0:2, crypto map: Tunnel1-head-0
        sa timing: remaining key lifetime (k/sec): (4467148/3189)
        IV size: 16 bytes
        replay detection support: Y  replay window size: 128
        Status: ACTIVE

      outbound ah sas:

      outbound pcp sas:

interface: Tunnel2
      Crypto map tag: Tunnel2-head-0, local addr 205.251.233.122

      protected vrf: (none)
      local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      current_peer 72.21.209.193 port 500
       PERMIT, flags={origin_is_acl,}
      #pkts encaps: 26, #pkts encrypt: 26, #pkts digest: 26
      #pkts decaps: 24, #pkts decrypt: 24, #pkts verify: 24
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts compr. failed: 0
      #pkts not decompressed: 0, #pkts decompress failed: 0
      #send errors 0, #recv errors 0

      local crypto endpt.: 174.78.144.73, remote crypto endpt.:205.251.233.122
      path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0
      current outbound spi: 0xF59A3FF6(4120526838)

      inbound esp sas:
       spi: 0xB6720137(3060924727)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 3, flow_id: Motorola SEC 2.0:3, crypto map: Tunnel2-head-0
```

```
        sa timing: remaining key lifetime (k/sec): (4387273/3492)
        IV size: 16 bytes
        replay detection support: Y  replay window size: 128
        Status: ACTIVE

      inbound ah sas:

      inbound pcp sas:

      outbound esp sas:
       spi: 0xF59A3FF6(4120526838)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 4, flow_id: Motorola SEC 2.0:4, crypto map: Tunnel2-head-0
        sa timing: remaining key lifetime (k/sec): (4387273/3492)
        IV size: 16 bytes
        replay detection support: Y  replay window size: 128
        Status: ACTIVE

      outbound ah sas:

      outbound pcp sas:
```

Pour chaque interface du tunnel, vous devez voir un `esp sas` entrant et un `esp sas` sortant. Cela suppose qu'une SA est répertoriée (par exemple, `spi: 0x48B456A6`), que le statut est `ACTIVE` et qu'IPsec est correctement configuré.

Pour un dépannage plus approfondi, exécutez les commandes suivantes pour activer le débogage.

```
router# debug crypto ipsec
```

Pour désactiver le débogage, utilisez la commande suivante.

```
router# no debug crypto ipsec
```

Tunnel

Tout d'abord, vérifiez que les règles de pare-feu nécessaires sont instaurées. Pour de plus amples informations, veuillez consulter Règles de pare-feu pour un AWS Site-to-Site VPN Appareil de passerelle client.

Si vos règles de pare-feu sont correctement configurées, alors continuez le dépannage avec la commande suivante.

```
router# show interfaces tun1
```

```
Tunnel1 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 169.254.249.18/30
  MTU 17867 bytes, BW 100 Kbit/sec, DLY 50000 usec,
    reliability 255/255, txload 2/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 174.78.144.73, destination 205.251.233.121
  Tunnel protocol/transport IPSEC/IP
  Tunnel TTL 255
  Tunnel transport MTU 1427 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPSec (profile "ipsec-vpn-92df3bfb-0")
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 1 packets/sec
  5 minute output rate 1000 bits/sec, 1 packets/sec
    407 packets input, 30010 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
```

Assurez-vous que le protocole de ligne est opérationnel. Vérifiez que l'adresse IP source du tunnel, l'interface source et la destination correspondent respectivement à la configuration du tunnel pour l'adresse IP externe de la passerelle client, pour l'interface et pour l'adresse IP externe de la passerelle réseau privé virtuel. Assurez-vous que `Tunnel protection through IPSec` est présent. Assurez-vous d'exécuter la commande sur les deux interfaces du tunnel. Pour résoudre les éventuels problèmes, vérifiez la configuration et les connexions physiques à votre passerelle client.

Vous pouvez également utiliser la commande suivante, en remplaçant `169.254.249.18` par l'adresse IP interne de votre passerelle réseau privé virtuel.

```
router# ping 169.254.249.18 df-bit size 1410
```

```
Type escape sequence to abort.
Sending 5, 1410-byte ICMP Echos to 169.254.249.18, timeout is 2 seconds:
Packet sent with the DF bit set
!!!!!
```

Vous devez voir 5 points d'exclamation.

Routage

Pour voir votre table de routage statique, utilisez la commande suivante.

```
router# sh ip route static
```

```
     1.0.0.0/8 is variably subnetted
S       10.0.0.0/16 is directly connected, Tunnel1
is directly connected, Tunnel2
```

Vous devez voir que la route statique existe pour le CIDR du VPC via deux tunnels. Si elle n'existe pas, ajoutez les routes statiques comme suit:

```
router# ip route 10.0.0.0 255.255.0.0 Tunnel1 track 100
router# ip route 10.0.0.0 255.255.0.0 Tunnel2 track 200
```

Vérification du moniteur SLA

```
router# show ip sla statistics 100
```

```
IPSLAs Latest Operation Statistics

IPSLA operation id: 100
        Latest RTT: 128 milliseconds
Latest operation start time: *18:08:02.155 UTC Wed Jul  15 2012
Latest operation return code: OK
Number of successes: 3
Number of failures: 0
Operation time to live: Forever
```

```
router# show ip sla statistics 200
```

```
IPSLAs Latest Operation Statistics

IPSLA operation id: 200
        Latest RTT: 128 milliseconds
Latest operation start time: *18:08:02.155 UTC Wed Jul  15 2012
Latest operation return code: OK
Number of successes: 3
Number of failures: 0
Operation time to live: Forever
```

La valeur de `Number of successes` indique si le moniteur SLA a bien été configuré.

Pour un dépannage plus approfondi, passez en revue la configuration.

Dépannage AWS Site-to-Site VPN connectivité avec un dispositif de passerelle client Juniper JunOS

Quand vous résolvez les problèmes de connexion d'une passerelle client Juniper, prenez en compte quatre critères : IKE, IPsec, le tunnel et le protocole BGP. Vous pouvez résoudre des problèmes dans ces domaines dans n'importe quel ordre mais nous vous recommandons de commencer avec l'IKE (en bas du stack réseau) et de remonter.

IKE

Utilisez la commande suivante de l'. La réponse montre une passerelle client avec IKE configuré correctement.

```
user@router> show security ike security-associations
```

```
Index   Remote Address  State  Initiator cookie  Responder cookie  Mode
4       72.21.209.225   UP     c4cd953602568b74  0d6d194993328b02  Main
3       72.21.209.193   UP     b8c8fb7dc68d9173  ca7cb0abaedeb4bb  Main
```

Vous devez voir une ou plusieurs lignes contenant une adresse à distance de la passerelle à distance spécifiée dans les tunnels. `State` doit être `UP`. L'absence d'une entrée, ou toute entrée dans un état différent (comme `DOWN`), indique qu'IKE n'est pas correctement configuré.

Pour un dépannage plus approfondi, autorisez les options de suivi IKE, comme recommandé dans l'exemple de fichier de configuration. Exécutez ensuite la commande suivante pour imprimer différents messages de débogage sur l'écran.

```
user@router> monitor start kmd
```

Depuis un hôte externe, vous pouvez récupérer le fichier journal complet avec la commande suivante.

```
scp username@router.hostname:/var/log/kmd
```

IPsec

Utilisez la commande suivante de l'. La réponse montre une passerelle client avec IPsec configuré correctement.

```
user@router> show security ipsec security-associations
```

```
Total active tunnels: 2
ID      Gateway         Port  Algorithm        SPI      Life:sec/kb Mon vsys
<131073 72.21.209.225  500   ESP:aes-128/sha1 df27aae4 326/ unlim   -   0
>131073 72.21.209.225  500   ESP:aes-128/sha1 5de29aa1 326/ unlim   -   0
<131074 72.21.209.193  500   ESP:aes-128/sha1 dd16c453 300/ unlim   -   0
>131074 72.21.209.193  500   ESP:aes-128/sha1 c1e0eb29 300/ unlim   -   0
```

Vous devez notamment voir au moins deux lignes par adresse de passerelle (correspondant à la passerelle à distance). Notez les carets au début de chaque ligne (**< >**) qui indiquent la direction du trafic pour une entrée en particulier. Le résultat comporte des lignes séparées pour le trafic entrant (« **<** », trafic de la passerelle réseau privé virtuel vers la passerelle client) et le trafic sortant (« **>** »).

Pour un dépannage plus approfondi, autorisez les options de suivi IKE (pour plus d'informations, consultez la section précédente sur l'IKE).

Tunnel

Tout d'abord, vérifiez que les règles de pare-feu nécessaires sont instaurées. Pour obtenir la liste des règles, consultez Règles de pare-feu pour un AWS Site-to-Site VPN Appareil de passerelle client.

Si vos règles de pare-feu sont correctement configurées, alors continuez le dépannage avec la commande suivante.

```
user@router> show interfaces st0.1
```

```
Logical interface st0.1 (Index 70) (SNMP ifIndex 126)
   Flags: Point-To-Point SNMP-Traps Encapsulation: Secure-Tunnel
   Input packets : 8719
   Output packets: 41841
   Security: Zone: Trust
   Allowed host-inbound traffic : bgp ping ssh traceroute
   Protocol inet, MTU: 9192
     Flags: None
     Addresses, Flags: Is-Preferred Is-Primary
     Destination: 169.254.255.0/30, Local: 169.254.255.2
```

Assurez-vous que la `Security: Zone` est correcte, et que l'adresse `Local` correspond à l'adresse interne du tunnel de la passerelle client.

Ensuite, utilisez la commande suivante, en remplaçant `169.254.255.1` par l'adresse IP interne de votre passerelle réseau privé virtuel. Vos résultats doivent ressembler à la réponse présentée ici.

```
user@router> ping 169.254.255.1 size 1382 do-not-fragment
```

```
PING 169.254.255.1 (169.254.255.1): 1410 data bytes
64 bytes from 169.254.255.1: icmp_seq=0 ttl=64 time=71.080 ms
64 bytes from 169.254.255.1: icmp_seq=1 ttl=64 time=70.585 ms
```

Pour un dépannage plus approfondi, passez en revue la configuration.

BGP

Exécutez la commande suivante.

```
user@router> show bgp summary
```

```
Groups: 1 Peers: 2 Down peers: 0
Table          Tot Paths  Act Paths Suppressed    History Damp State    Pending
inet.0                 2          1          0          0          0          0
Peer                     AS      InPkt     OutPkt    OutQ   Flaps Last Up/Dwn State|
#Active/Received/Accepted/Damped...
169.254.255.1          7224          9         10       0       0        1:00 1/1/1/0
            0/0/0/0
169.254.255.5          7224          8          9       0       0          56 0/1/1/0
            0/0/0/0
```

Pour un dépannage plus approfondi, utilisez la commande suivante, en remplaçant `169.254.255.1` par l'adresse IP interne de votre passerelle réseau privé virtuel.

```
user@router> show bgp neighbor 169.254.255.1
```

```
Peer: 169.254.255.1+179 AS 7224 Local: 169.254.255.2+57175 AS 65000
  Type: External    State: Established    Flags: <ImportEval Sync>
  Last State: OpenConfirm   Last Event: RecvKeepAlive
  Last Error: None
  Export: [ EXPORT-DEFAULT ]
  Options: <Preference HoldTime PeerAS LocalAS Refresh>
  Holdtime: 30 Preference: 170 Local AS: 65000 Local System AS: 0
  Number of flaps: 0
  Peer ID: 169.254.255.1    Local ID: 10.50.0.10       Active Holdtime: 30
  Keepalive Interval: 10         Peer index: 0
  BFD: disabled, down
  Local Interface: st0.1
  NLRI for restart configured on peer: inet-unicast
  NLRI advertised by peer: inet-unicast
  NLRI for this session: inet-unicast
  Peer supports Refresh capability (2)
  Restart time configured on the peer: 120
  Stale routes from peer are kept for: 300
  Restart time requested by this peer: 120
  NLRI that peer supports restart for: inet-unicast
  NLRI that restart is negotiated for: inet-unicast
  NLRI of received end-of-rib markers: inet-unicast
  NLRI of all end-of-rib markers sent: inet-unicast
  Peer supports 4 byte AS extension (peer-as 7224)
  Table inet.0 Bit: 10000
    RIB State: BGP restart is complete
    Send state: in sync
    Active prefixes:              1
    Received prefixes:            1
    Accepted prefixes:            1
    Suppressed due to damping:    0
    Advertised prefixes:          1
Last traffic (seconds): Received 4    Sent 8    Checked 4
Input messages:  Total 24     Updates 2       Refreshes 0     Octets 505
Output messages: Total 26     Updates 1       Refreshes 0     Octets 582
Output Queue[0]: 0
```

Ici, vous devez voir `Received prefixes` et `Advertised prefixes` avec la valeur 1 pour chacun de ces champs. Ils doivent se trouver dans la section `Table inet.0`.

Si `State` n'est pas `Established`, vérifiez `Last State` et `Last Error` pour plus de détails sur ce que vous devez faire pour corriger le problème.

Si le peering BGP est activé, vérifiez que votre dispositif de passerelle client annonce l'itinéraire par défaut (0.0.0). 0/0) vers le VPC.

```
user@router> show route advertising-protocol bgp 169.254.255.1
```

```
inet.0: 10 destinations, 11 routes (10 active, 0 holddown, 0 hidden)
  Prefix                  Nexthop              MED     Lclpref    AS path
* 0.0.0.0/0               Self                                    I
```

En outre, assurez-vous de recevoir le préfixe correspondant à votre VPC depuis la passerelle réseau privé virtuel.

```
user@router> show route receive-protocol bgp 169.254.255.1
```

```
inet.0: 10 destinations, 11 routes (10 active, 0 holddown, 0 hidden)
  Prefix                  Nexthop              MED     Lclpref    AS path
* 10.110.0.0/16           169.254.255.1        100                7224 I
```

Dépannage AWS Site-to-Site VPN connectivité avec un dispositif de passerelle client Juniper ScreenOS

Lorsque vous dépannez la connectivité d'un dispositif de passerelle ScreenOS-based client Juniper, tenez compte de quatre éléments : IKE, IPsec, tunnel et BGP. Vous pouvez résoudre des problèmes dans ces domaines dans n'importe quel ordre mais nous vous recommandons de commencer avec l'IKE (en bas du stack réseau) et de remonter.

IKE et IPsec

Utilisez la commande suivante de l'. La réponse montre une passerelle client avec IKE configuré correctement.

```
ssg5-serial-> get sa
```

```
total configured sa: 2
HEX ID    Gateway         Port Algorithm     SPI      Life:sec kb Sta   PID vsys
00000002<   72.21.209.225  500 esp:a128/sha1 80041ca4  3385 unlim A/-    -1 0
00000002>   72.21.209.225  500 esp:a128/sha1 8cdd274a  3385 unlim A/-    -1 0
00000001<   72.21.209.193  500 esp:a128/sha1 ecf0bec7  3580 unlim A/-    -1 0
00000001>   72.21.209.193  500 esp:a128/sha1 14bf7894  3580 unlim A/-    -1 0
```

Vous devez voir une ou plusieurs lignes contenant une adresse à distance de la passerelle à distance spécifiée dans les tunnels. La valeur de `Sta` doit être `A/-`, et `SPI` doit être un nombre hexadécimal autre que `00000000`. Des entrées dans un état différent indiquent que l'IKE n'est pas correctement configuré.

Pour un dépannage plus approfondi, autorisez les options de suivi IKE, comme recommandé dans l'exemple de fichier de configuration.

Tunnel

Tout d'abord, vérifiez que les règles de pare-feu nécessaires sont instaurées. Pour obtenir la liste des règles, consultez Règles de pare-feu pour un AWS Site-to-Site VPN Appareil de passerelle client.

Si vos règles de pare-feu sont correctement configurées, alors continuez le dépannage avec la commande suivante.

```
ssg5-serial-> get interface tunnel.1
```

```
  Interface tunnel.1:
  description tunnel.1
  number 20, if_info 1768, if_index 1, mode route
  link ready
  vsys Root, zone Trust, vr trust-vr
  admin mtu 1500, operating mtu 1500, default mtu 1500
  *ip 169.254.255.2/30
  *manage ip 169.254.255.2
  route-deny disable
  bound vpn:
    IPSEC-1

  Next-Hop Tunnel Binding table
  Flag Status Next-Hop(IP)    tunnel-id  VPN

  pmtu-v4 disabled
```

```
  ping disabled, telnet disabled, SSH disabled, SNMP disabled
  web disabled, ident-reset disabled, SSL disabled

  OSPF disabled  BGP enabled  RIP disabled  RIPng disabled  mtrace disabled
  PIM: not configured  IGMP not configured
  NHRP disabled
  bandwidth: physical 0kbps, configured egress [gbw 0kbps mbw 0kbps]
             configured ingress mbw 0kbps, current bw 0kbps
             total allocated gbw 0kbps
```

Assurez-vous de voir `link:ready` et que l'adresse `IP` correspond à l'adresse interne du tunnel de la passerelle client.

Ensuite, utilisez la commande suivante, en remplaçant `169.254.255.1` par l'adresse IP interne de votre passerelle réseau privé virtuel. Vos résultats doivent ressembler à la réponse présentée ici.

```
ssg5-serial-> ping 169.254.255.1
```

```
Type escape sequence to abort

Sending 5, 100-byte ICMP Echos to 169.254.255.1, timeout is 1 seconds
!!!!!
Success Rate is 100 percent (5/5), round-trip time min/avg/max=32/32/33 ms
```

Pour un dépannage plus approfondi, passez en revue la configuration.

BGP

Exécutez la commande suivante.

```
ssg5-serial-> get vrouter trust-vr protocol bgp neighbor
```

```
Peer AS Remote IP       Local IP          Wt Status   State     ConnID Up/Down
------------------------------------------------------------------------------
   7224 169.254.255.1   169.254.255.2    100 Enabled  ESTABLISH     10 00:01:01
   7224 169.254.255.5   169.254.255.6    100 Enabled  ESTABLISH     11 00:00:59
```

L'état des deux homologues BGP doit être `ESTABLISH`, ce qui signifie que la connexion BGP à la passerelle réseau privé virtuel est active.

Pour un dépannage plus approfondi, utilisez la commande suivante, en remplaçant `169.254.255.1` par l'adresse IP interne de votre passerelle réseau privé virtuel.

```
ssg5-serial-> get vr trust-vr prot bgp neigh 169.254.255.1
```

```
peer: 169.254.255.1,  remote AS: 7224, admin status: enable
type: EBGP, multihop: 0(disable), MED: node default(0)
connection state: ESTABLISH, connection id: 18 retry interval: node default(120s), cur
 retry time 15s
configured hold time: node default(90s), configured keepalive: node default(30s)
configured adv-interval: default(30s)
designated local IP: n/a
local IP address/port: 169.254.255.2/13946, remote IP address/port: 169.254.255.1/179
router ID of peer: 169.254.255.1, remote AS: 7224
negotiated hold time: 30s, negotiated keepalive interval: 10s
route map in name: , route map out name:
weight: 100 (default)
self as next hop: disable
send default route to peer: disable
ignore default route from peer: disable
send community path attribute: no
reflector client: no
Neighbor Capabilities:
  Route refresh: advertised and received
  Address family IPv4 Unicast:  advertised and received
force reconnect is disable
total messages to peer: 106, from peer: 106
update messages to peer: 6, from peer: 4
Tx queue length 0, Tx queue HWM: 1
route-refresh messages to peer: 0, from peer: 0
last reset 00:05:33 ago, due to BGP send Notification(Hold Timer Expired)(code 4 :
 subcode 0)
number of total successful connections: 4
connected: 2 minutes 6 seconds
Elapsed time since last update: 2 minutes 6 seconds
```

Si le peering BGP est activé, vérifiez que votre dispositif de passerelle client annonce l'itinéraire par défaut (0.0.0). 0/0) vers le VPC. Cette commande s'applique au ScreenOS 6.2.0 et version plus récente.

```
ssg5-serial-> get vr trust-vr protocol bgp  rib neighbor 169.254.255.1 advertised
```

```
i: IBGP route, e: EBGP route, >: best route, *: valid route
               Prefix         Nexthop    Wt  Pref   Med Orig    AS-Path
-------------------------------------------------------------------------------
>i          0.0.0.0/0         0.0.0.0 32768   100     0  IGP
Total IPv4 routes advertised: 1
```

En outre, assurez-vous de recevoir le préfixe correspondant à votre VPC depuis la passerelle réseau privé virtuel. Cette commande s'applique au ScreenOS 6.2.0 et version plus récente.

```
ssg5-serial-> get vr trust-vr protocol bgp  rib neighbor 169.254.255.1 received
```

```
i: IBGP route, e: EBGP route, >: best route, *: valid route
               Prefix         Nexthop    Wt  Pref   Med Orig    AS-Path
-------------------------------------------------------------------------------
>e*     10.0.0.0/16   169.254.255.1   100   100   100  IGP   7224
Total IPv4 routes received: 1
```

Dépannage AWS Site-to-Site VPN connectivité avec un dispositif de passerelle client Yamaha

Quand vous résolvez les problèmes de connexion d'une passerelle client Yamaha, prenez en compte quatre critères : IKE, IPsec, le tunnel et le protocole BGP. Vous pouvez résoudre des problèmes dans ces domaines dans n'importe quel ordre mais nous vous recommandons de commencer avec l'IKE (en bas du stack réseau) et de remonter.

> **Note**
>
> Le`proxy ID` paramètre utilisé dans la phase 2 d'IKE est désactivé par défaut sur le routeur Yamaha. Cela peut entraîner des problèmes de connexion au Site-to-Site VPN. Si le n'`proxy ID`est pas configuré sur votre routeur, veuillez consulter le fichier d'exemple de configuration AWS fourni pour que Yamaha le configure correctement.

IKE

Exécutez la commande suivante. La réponse montre une passerelle client avec IKE configuré correctement.

```
# show ipsec sa gateway 1
```

```
sgw  flags local-id                      remote-id        # of sa
-------------------------------------------------------------------------
1    U K   YOUR_LOCAL_NETWORK_ADDRESS     72.21.209.225    i:2 s:1 r:1
```

Vous devez voir une ligne contenant une valeur de `remote-id` pour la passerelle à distance spécifiée dans les tunnels. Vous pouvez répertorier toutes les associations de sécurité (SA) en omettant le numéro du tunnel.

Pour un dépannage plus approfondi, exécutez les commandes suivantes pour permettre la consignation des messages de niveau DEBUG qui apportent des informations de diagnostic.

```
# syslog debug on
# ipsec ike log message-info payload-info key-info
```

Pour annuler les éléments enregistrés, utilisez la commande suivante.

```
# no ipsec ike log
# no syslog debug on
```

IPsec

Exécutez la commande suivante. La réponse montre une passerelle client avec IPsec configuré correctement.

```
# show ipsec sa gateway 1 detail
```

```
SA[1] Duration: 10675s
Local ID: YOUR_LOCAL_NETWORK_ADDRESS
Remote ID: 72.21.209.225
Protocol: IKE
Algorithm: AES-CBC, SHA-1, MODP 1024bit

SPI: 6b ce fd 8a d5 30 9b 02 0c f3 87 52 4a 87 6e 77
Key: ** ** ** ** **  (confidential)   ** ** ** ** **
-------------------------------------------------
SA[2] Duration: 1719s
```

```
Local ID: YOUR_LOCAL_NETWORK_ADDRESS
Remote ID: 72.21.209.225
Direction: send
Protocol: ESP (Mode: tunnel)
Algorithm: AES-CBC (for Auth.: HMAC-SHA)
SPI: a6 67 47 47
Key: ** ** ** ** **  (confidential)   ** ** ** ** **
-----------------------------------------------------
SA[3] Duration: 1719s
Local ID: YOUR_LOCAL_NETWORK_ADDRESS
Remote ID: 72.21.209.225
Direction: receive
Protocol: ESP (Mode: tunnel)
Algorithm: AES-CBC (for Auth.: HMAC-SHA)
SPI: 6b 98 69 2b
Key: ** ** ** ** **  (confidential)   ** ** ** ** **
-----------------------------------------------------
SA[4] Duration: 10681s
Local ID: YOUR_LOCAL_NETWORK_ADDRESS
Remote ID: 72.21.209.225
Protocol: IKE
Algorithm: AES-CBC, SHA-1, MODP 1024bit
SPI: e8 45 55 38 90 45 3f 67 a8 74 ca 71 ba bb 75 ee
Key: ** ** ** ** **  (confidential)   ** ** ** ** **
-----------------------------------------------------
```

Pour chaque interface du tunnel, vous devez voir `receive sas` et `send sas`.

Pour un dépannage plus approfondi, exécutez les commandes suivantes pour activer le débogage.

```
# syslog debug on
# ipsec ike log message-info payload-info key-info
```

Utilisez la commande suivante pour désactiver le débogage.

```
# no ipsec ike log
# no syslog debug on
```

Tunnel

Tout d'abord, vérifiez que les règles de pare-feu nécessaires sont instaurées. Pour obtenir la liste des règles, consultez Règles de pare-feu pour un AWS Site-to-Site VPN Appareil de passerelle client.

Si vos règles de pare-feu sont correctement configurées, alors continuez le dépannage avec la commande suivante.

```
# show status tunnel 1
```

```
TUNNEL[1]:
Description:
  Interface type: IPsec
  Current status is Online.
  from 2011/08/15 18:19:45.
  5 hours 7 minutes 58 seconds  connection.
  Received:    (IPv4) 3933 packets [244941 octets]
               (IPv6) 0 packet [0 octet]
  Transmitted: (IPv4) 3933 packets [241407 octets]
               (IPv6) 0 packet [0 octet]
```

Assurez-vous que la valeur de `current status` est en ligne et que `Interface type` est IPsec. Assurez-vous d'exécuter la commande sur les deux interfaces du tunnel. Pour résoudre tout problème se présentant ici, passez en revue la configuration.

BGP

Exécutez la commande suivante.

```
# show status bgp neighbor
```

```
BGP neighbor is 169.254.255.1, remote AS 7224, local AS 65000, external link
  BGP version 0, remote router ID 0.0.0.0
  BGP state = Active
  Last read 00:00:00, hold time is 0, keepalive interval is 0 seconds
  Received 0 messages, 0 notifications, 0 in queue
  Sent 0 messages, 0 notifications, 0 in queue
  Connection established 0; dropped 0
  Last reset never
Local host: unspecified
Foreign host: 169.254.255.1, Foreign port: 0

BGP neighbor is 169.254.255.5, remote AS 7224, local AS 65000, external link
  BGP version 0, remote router ID 0.0.0.0
  BGP state = Active
  Last read 00:00:00, hold time is 0, keepalive interval is 0 seconds
```

```
  Received 0 messages, 0 notifications, 0 in queue
  Sent 0 messages, 0 notifications, 0 in queue
  Connection established 0; dropped 0
  Last reset never
Local host: unspecified
Foreign host: 169.254.255.5, Foreign port:
```

Les deux voisins doivent être répertoriés. Pour chacun d'entre eux, vous devez voir la valeur `Active` pour BGP `state`.

Si le peering BGP est activé, vérifiez que votre dispositif de passerelle client annonce l'itinéraire par défaut (0.0.0). 0/0) vers le VPC.

```
# show status bgp neighbor 169.254.255.1 advertised-routes
```

```
Total routes: 1
*: valid route
  Network            Next Hop        Metric LocPrf Path
* default            0.0.0.0              0        IGP
```

En outre, assurez-vous de recevoir le préfixe correspondant à votre VPC depuis la passerelle réseau privé virtuel.

```
# show ip route
```

```
Destination         Gateway          Interface       Kind  Additional Info.
default             ***.***.***.***   LAN3(DHCP)    static
10.0.0.0/16         169.254.255.1    TUNNEL[1]       BGP  path=10124
```

Intégration avec AWS Site-to-Site VPN et eero

AWS Site-to-Site VPN a collaboré avec eero pour permettre aux entreprises d'établir de manière simple et pratique une connectivité sécurisée entre leurs sites distants et AWS en quelques clics.

Cette solution exploite les points d' WiFi accès et les passerelles réseau d'eero pour fournir une connectivité locale. À l'aide des appareils de passerelle et du Site-to-Site VPN d'eero, les clients peuvent établir automatiquement une connectivité VPN pour accéder à leurs applications hébergées sur AWS, telles que les passerelles de paiement pour les systèmes de point de vente, en quelques

clics. Cela permet aux clients de faire évoluer facilement et plus rapidement la connectivité de leurs sites distants sur des centaines de sites et élimine le besoin d'un technicien sur site ayant une expertise en réseau pour configurer la connectivité. Cette solution convient aux entreprises distribuées comptant jusqu'à 500 bureaux distants, chaque bureau pouvant accueillir jusqu'à 100 utilisateurs.

Pour en savoir plus sur cette intégration, y compris le guide de configuration détaillé, consultez la documentation eero.

> **Note**
>
> Aucune modification n'est apportée aux fonctionnalités du Site-to-Site VPN AWS dans le cadre de cette intégration.

Considérations :

- Disponible uniquement pour les connexions VPN connectées à un Transit Gateway ou à un Cloud WAN. Non pris en charge pour les pièces jointes de Virtual Private Gateway.
- Les tunnels 5 Gbit/s ne sont pas pris en charge.
- Site-to-Site Le concentrateur VPN n'est pas pris en charge.
- Site-to-Site Les quotas VPN ne changent pas avec cette intégration.

Travaillez avec AWS Site-to-Site VPN

Vous pouvez utiliser les ressources Site-to-Site VPN à l'aide de la console Amazon VPC ou du.AWS CLI

Rubriques

Création et gestion de AWS Site-to-Site VPN concentrateurs

Site-to-SiteLes concentrateurs VPN vous permettent d'agréger et de gérer plusieurs connexions VPN à partir de sites distants, offrant ainsi une gestion centralisée.

Après avoir créé vos concentrateurs Site-to-Site VPN, vous pouvez les consulter et les gérer depuis la page principale des concentrateurs Site-to-Site VPN de la console Amazon VPC. Ce tableau de bord affiche tous les concentrateurs VPN actifs qui gèrent les connexions sécurisées entre AWS et vos sites distants.

Rubriques

Création d'un AWS Site-to-Site VPN concentrateur

Créez un concentrateur à l'aide de la console Amazon VPC, APIs du, ou du. AWS CLI Avant de créer un concentrateur, vous devez d'abord avoir créé une passerelle de transit à associer au concentrateur. Pour plus d'informations sur la création de passerelles de transit, consultez Create a transit gateway dans le guide Amazon AWS VPC Transit Gateway.

Créez un concentrateur Site-to-Site VPN à l'aide de la console

Pour créer un concentrateur Site-to-Site VPN à l'aide de la console AWS de gestion, procédez comme suit :

Pour créer un concentrateur Site-to-Site VPN à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Site-to-Site VPN Concentrators.
3. Choisissez Create Site-to-Site VPN Concentrator.
4. (Facultatif) Dans le champ Name tag, saisissez le nom de votre concentrateur Site-to-Site VPN.
5. Pour Transit gateway, sélectionnez une passerelle de transit existante.
6. (Facultatif) Ajoutez des balises pour identifier et organiser votre concentrateur Site-to-Site VPN.
    a. Sélectionnez Ajouter une nouvelle balise.
    b. Pour Clé, entrez une clé de balise (par exemple,**`Name`**).
    c. Pour Valeur, entrez une valeur de balise (par exemple,**`Production-VPN-Concentrator`**).
    d. Répétez les étapes précédentes pour ajouter des balises supplémentaires si nécessaire.
7. Choisissez Create Site-to-Site VPN Concentrator.

Après sa création, le concentrateur Site-to-Site VPN sera dans un `pending` état pendant son provisionnement. Une fois prêt, l'état passe à `available` et vous pouvez commencer à créer des connexions VPN utilisant le concentrateur Site-to-Site VPN.

Créez un concentrateur Site-to-Site VPN à l'aide de la CLI

Avant de créer un concentrateur Site-to-Site VPN à l'aide de la CLI, assurez-vous de disposer des éléments suivants :

- Un Transit Gateway existant dans votre AWS compte
- Autorisations IAM appropriées pour créer des concentrateurs Site-to-Site VPN
- L'ID du Transit Gateway auquel vous souhaitez associer le Concentrator

L'exemple suivant crée un concentrateur Site-to-Site VPN pour la passerelle de transit spécifiée :

```
aws ec2 create-vpn-concentrator --transit-gateway-id tgw-123456789
```

Ce qui suit montre une réponse réussie :

```
{
    "VpnConcentrator": {
        "VpnConcentratorId": "vcn-0123456789abcdef0",
        "State": "pending",
        "TransitGatewayId": "tgw-123456789",
        "CreationTime": "2025-09-29T17:26:31.000Z",
        "Tags": []
    }
}
```

Créez un concentrateur Site-to-Site VPN à l'aide de l'API

Vous pouvez créer un concentrateur Site-to-Site VPN à l'aide de l' CreateVpnConcentrators API.

L'API accepte les paramètres clés suivants :

`TransitGatewayId`

L'ID du Transit Gateway auquel connecter le concentrateur Site-to-Site VPN.

`TagSpecification`

Tags à attribuer au concentrateur Site-to-Site VPN pour l'organisation des ressources et la facturation.

L'exemple suivant montre comment créer un concentrateur Site-to-Site VPN connecté à un Transit Gateway :

```
POST / HTTP/1.1
```

```
Host: ec2.us-east-1.amazonaws.com
Content-Type: application/x-www-form-urlencoded
Authorization: AWS4-HMAC-SHA256 Credential=...

Action=CreateVpnConcentrator
&Version=2016-11-15
&TransitGatewayId=tgw-0123456789abcdef0
&TagSpecification.1.ResourceType=vpn-concentrator
&TagSpecification.1.Tag.1.Key=Name
&TagSpecification.1.Tag.1.Value=MyVpnConcentrator
```

Une fois la création réussie, l'API renvoie des informations sur le concentrateur Site-to-Site VPN nouvellement créé :

```
<?xml version="1.0" encoding="UTF-8"?>
<CreateVpnConcentratorResponse xmlns="http://ec2.amazonaws.com/doc/2016-11-15/">
    <requestId>12345678-1234-1234-1234-123456789012</requestId>
    <vpnConcentrator>
        <vpnConcentratorId>vcn-0123456789abcdef0</vpnConcentratorId>
        <state>pending</state>
        <transitGatewayId>tgw-0123456789abcdef0</transitGatewayId>
        <creationTime>2024-01-15T10:30:00.000Z</creationTime>
        <tagSet>
            <item>
                <key>Name</key>
                <value>MyVpnConcentrator</value>
            </item>
        </tagSet>
    </vpnConcentrator>
</CreateVpnConcentratorResponse>
```

Gérer les tags du AWS Site-to-Site VPN Concentrator

Les tags sont des paires clé-valeur qui vous aident à organiser et à gérer vos concentrateurs Site-to-Site VPN. Vous pouvez utiliser des balises pour classer les concentrateurs Site-to-Site VPN par objectif, environnement, centre de coûts ou tout autre critère pertinent pour votre organisation.

Gérer les tags à l'aide de la console

Vous pouvez ajouter ou supprimer des balises pour un concentrateur Site-to-Site VPN à l'aide de la console AWS de gestion.

Pour ajouter des balises à un concentrateur Site-to-Site VPN

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Site-to-Site VPN Concentrators.
3. Sélectionnez le concentrateur Site-to-Site VPN que vous souhaitez baliser.
4. Sélectionnez l'onglet Tags (Identifications).
5. Choisissez Gérer les balises.
6. Choisissez Add new tag (Ajouter une nouvelle balise).
7. Pour Clé, entrez une clé de balise (par exemple,**`Environment`**).
8. Pour Valeur, entrez une valeur de balise (par exemple,**`Production`**).
9. Sélectionnez Enregistrer les modifications.

Pour supprimer des tags d'un concentrateur Site-to-Site VPN

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Site-to-Site VPN Concentrators.
3. Sélectionnez le concentrateur Site-to-Site VPN dont vous souhaitez supprimer les tags.
4. Sélectionnez l'onglet Tags (Identifications).
5. Choisissez Gérer les balises.
6. Pour chaque étiquette que vous souhaitez supprimer, choisissez Supprimer.
7. Sélectionnez Enregistrer les modifications.

Gérer les balises à l'aide de la CLI

Vous pouvez ajouter, modifier ou supprimer des balises à l'aide du AWS CLI.

Ajout de balises

L'exemple suivant ajoute des balises à un concentrateur Site-to-Site VPN :

```
aws ec2 create-tags --resources vcn-0123456789abcdef0 --tags
 Key=Environment,Value=Production Key=Team,Value=NetworkOps
```

Cette commande ne renvoie aucun résultat en cas de réussite.

Affichage des balises

L'exemple suivant décrit les balises d'un concentrateur Site-to-Site VPN :

```
aws ec2 describe-tags --filters "Name=resource-id,Values=vcn-0123456789abcdef0"
```

La réponse suivante est renvoyée :

```
{
    "Tags": [
        {
            "Key": "Environment",
            "ResourceId": "vcn-0123456789abcdef0",
            "ResourceType": "vpn-concentrator",
            "Value": "Production"
        },
        {
            "Key": "Team",
            "ResourceId": "vcn-0123456789abcdef0",
            "ResourceType": "vpn-concentrator",
            "Value": "NetworkOps"
        }
    ]
}
```

Suppression de balises

L'exemple suivant supprime les balises d'un concentrateur Site-to-Site VPN :

```
aws ec2 delete-tags --resources vcn-0123456789abcdef0 --tags Key=Environment Key=Team
```

Cette commande ne renvoie aucun résultat en cas de réussite.

Gérez les tags à l'aide de l'API

Vous pouvez gérer par programmation les balises Site-to-Site VPN Concentrator à l'aide des opérations d'API Amazon EC2 .

CreateTags

Utilisez l'`CreateTags`opération pour ajouter ou mettre à jour des balises :

```
POST / HTTP/1.1
Host: ec2.region.amazonaws.com
```

```
Content-Type: application/x-www-form-urlencoded

Action=CreateTags
&ResourceId.1=vcn-0123456789abcdef0
&Tag.1.Key=Environment
&Tag.1.Value=Production
&Tag.2.Key=Team
&Tag.2.Value=NetworkOps
&Version=2016-11-15
```

La réponse suivante est renvoyée :

```
<?xml version="1.0" encoding="UTF-8"?>
<CreateTagsResponse xmlns="http://ec2.amazonaws.com/doc/2016-11-15/">
    <requestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</requestId>
    <return>true</return>
</CreateTagsResponse>
```

DescribeTags

Utilisez l'`DescribeTags`opération pour récupérer les tags :

```
POST / HTTP/1.1
Host: ec2.region.amazonaws.com
Content-Type: application/x-www-form-urlencoded

Action=DescribeTags
&Filter.1.Name=resource-id
&Filter.1.Value.1=vcn-0123456789abcdef0
&Version=2016-11-15
```

La réponse suivante est renvoyée :

```
<?xml version="1.0" encoding="UTF-8"?>
<DescribeTagsResponse xmlns="http://ec2.amazonaws.com/doc/2016-11-15/">
    <requestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</requestId>
    <tagSet>
        <item>
            <resourceId>vcn-0123456789abcdef0</resourceId>
            <resourceType>vpn-concentrator</resourceType>
            <key>Environment</key>
            <value>Production</value>
        </item>
```

```
        <item>
            <resourceId>vcn-0123456789abcdef0</resourceId>
            <resourceType>vpn-concentrator</resourceType>
            <key>Team</key>
            <value>NetworkOps</value>
        </item>
    </tagSet>
</DescribeTagsResponse>
```

DeleteTags

Utilisez l'`DeleteTags`opération pour supprimer les tags :

```
POST / HTTP/1.1
Host: ec2.region.amazonaws.com
Content-Type: application/x-www-form-urlencoded

Action=DeleteTags
&ResourceId.1=vcn-0123456789abcdef0
&Tag.1.Key=Environment
&Tag.2.Key=Team
&Version=2016-11-15
```

La réponse suivante est renvoyée :

```
<?xml version="1.0" encoding="UTF-8"?>
<DeleteTagsResponse xmlns="http://ec2.amazonaws.com/doc/2016-11-15/">
    <requestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</requestId>
    <return>true</return>
</DeleteTagsResponse>
```

Supprimer un AWS Site-to-Site VPN concentrateur

Lorsque vous n'avez plus besoin d'un concentrateur Site-to-Site VPN, vous pouvez le supprimer pour ne plus encourir de frais. La suppression d'un concentrateur Site-to-Site VPN le supprime définitivement ainsi que toutes les configurations associées.

Conditions préalables

Avant de supprimer un concentrateur Site-to-Site VPN, assurez-vous de ce qui suit :

- Toutes les connexions VPN associées au concentrateur Site-to-Site VPN sont supprimées.

- Vous disposez des autorisations nécessaires pour supprimer les concentrateurs Site-to-Site VPN (`ec2:DeleteVpnConcentrator`).

Supprimer un concentrateur Site-to-Site VPN à l'aide de la console

Pour supprimer un concentrateur Site-to-Site VPN

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Concentrators de site à site.
3. Sélectionnez le concentrateur Site-to-Site VPN que vous souhaitez supprimer.
4. Choisissez Actions, puis choisissez Supprimer le concentrateur Site-to-Site VPN.
5. Dans la boîte de dialogue de confirmation, tapez **`delete`** pour confirmer la suppression.
6. Sélectionnez Delete (Supprimer).

Supprimer un concentrateur Site-to-Site VPN à l'aide de la CLI

Utilisez la `delete-vpn-concentrator` commande pour supprimer un concentrateur Site-to-Site VPN. Vous `vpn-concentrator-id` en aurez besoin pour le supprimer.

L'exemple suivant supprime un concentrateur Site-to-Site VPN :

```
aws ec2 delete-vpn-concentrator --vpn-concentrator-id vcn-0123456789abcdef0
```

La réponse suivante est renvoyée :

```
{
    "VpnConcentrator": {
        "VpnConcentratorId": "vcn-0123456789abcdef0",
        "State": "deleting",
        "Message": "The Site-to-Site VPN Concentrator vcn-0123456789abcdef0 is being
 deleted and will be removed from your account."
    }
}
```

Supprimer un concentrateur Site-to-Site VPN à l'aide de l'API

Utilisez cette `DeleteVpnConcentrator` opération pour supprimer un concentrateur Site-to-Site VPN. Vous `VpnConcentratorId` en aurez besoin pour le supprimer.

L'exemple suivant supprime un concentrateur Site-to-Site VPN :

```
POST / HTTP/1.1
Host: ec2.region.amazonaws.com
Content-Type: application/x-www-form-urlencoded

Action=DeleteVpnConcentrator
&VpnConcentratorId=vcn-0123456789abcdef0
&Version=2016-11-15
```

La réponse suivante est renvoyée :

```
<?xml version="1.0" encoding="UTF-8"?>
<DeleteVpnConcentratorResponse xmlns="http://ec2.amazonaws.com/doc/2016-11-15/">
    <requestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</requestId>
    <vpnConcentrator>
        <vpnConcentratorId>vcn-0123456789abcdef0</vpnConcentratorId>
        <state>deleting</state>
        <message>The Site-to-Site VPN Concentrator vcn-0123456789abcdef0 is being
 deleted and will be removed from your account.</message>
    </vpnConcentrator>
</DeleteVpnConcentratorResponse>
```

Création d'une AWS Site-to-Site VPN connexion

Vous pouvez créer des connexions Site-to-Site VPN qui se connectent à des passerelles de transit ou à des réseaux mondiaux Cloud WAN. Les deux types de pièces jointes prennent en charge les IPv6 protocoles IPv4 et peuvent éventuellement utiliser des concentrateurs Site-to-Site VPN pour connecter plusieurs sites distants de manière rentable.

Création d'une connexion VPN à l'aide de la console

Pour créer une connexion VPN à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Connexions Site-to-Site VPN.
3. Choisissez Create VPN connection (Créer une connexion VPN).
4. (Facultatif) Pour Identification de nom, saisissez un nom pour la connexion. Une identification est alors créée avec la clé `Name` et la valeur que vous spécifiez.

5. Pour le type de passerelle cible, choisissez l'une des options suivantes :

   - Passerelle privée virtuelle : créez une nouvelle connexion VPN de passerelle privée virtuelle en choisissant une passerelle privée virtuelle existante.
   - Passerelle de transit : créez une nouvelle connexion VPN de passerelle de transit en choisissant une passerelle de transit existante. Pour plus d'informations sur la création d'une passerelle de transit, consultez Passerelles de transit dans Passerelles de transit Amazon VPC.
   - Site-to-Site Concentrateur VPN - Créez une nouvelle connexion au concentrateur Site-to-Site VPN en utilisant un concentrateur Site-to-Site VPN existant ou en créant un nouveau. Sélectionnez l'une des méthodes suivantes :
     - Existant : créez une nouvelle connexion Site-to-Site VPN au concentrateur VPN à l'aide d'un concentrateur existant.
     - Nouveau - Entrez un nom facultatif pour le concentrateur Site-to-Site VPN, puis choisissez la passerelle de transit à associer à celui-ci.
   - Non associée : créez une connexion VPN indépendante qui pourra ensuite être associée à Cloud WAN via la console ou l'API Network Manager. Pour plus d'informations sur les pièces jointes VPN et le Cloud WAN, consultez la section Pièces jointes Site-to-site VPN dans le AWS Cloud WAN dans le Guide de l'utilisateur du AWS Cloud WAN.

6. Pour Passerelle client, effectuez l'une des actions suivantes :

   - Pour utiliser une passerelle client existante, choisissez Existing, puis choisissez l'ID de passerelle client.
   - Pour créer une nouvelle passerelle client, choisissez Nouveau, puis procédez comme suit :
     - Pour l'adresse IP, entrez une adresse statique IPv4ou une IPv6adresse.
     - (Facultatif) Pour l'ARN du certificat, choisissez l'ARN de votre certificat privé (si vous utilisez l'authentification basée sur les certificats).
     - Dans Version du moteur de cache, saisissez le numéro d'ASN (Autonomous System Number) BGP (Border Gateway Protocol) de votre passerelle client. Pour de plus amples informations, veuillez consulter Options de passerelle client.

7. Pour les options de routage, choisissez Dynamic (nécessite BGP) ou Static.

> **Note**
>
> Les connexions VPN Cloud WAN et les connexions VPN utilisant des concentrateurs ne prennent en charge que le routage BGP. Le routage statique n'est pas pris en charge pour ces types de connexion.

8. Pour le stockage de clés pré-partagé, choisissez Standard ou Secrets Manager. La sélection par défaut est Standard. Pour plus d'informations sur l'utilisation de AWS Secrets Manager, consultez Sécurité.
9. Pour la version Tunnel inside IP, choisissez IPv4ou IPv6.
10. (Facultatif) Pour Activer l'accélération, cochez la case pour activer l'accélération. Pour de plus amples informations, veuillez consulter Connexions VPN accélérées.

    Si vous activez l'accélération, nous créons deux accélérateurs qui sont utilisés par votre connexion VPN. Des frais supplémentaires s'appliquent.
11. (Facultatif) En fonction de la version de tunnel IP que vous avez choisie, effectuez l'une des opérations suivantes :

    - IPv4 — Pour le CIDR IPv4 du réseau local, spécifiez la plage d'adresses IPv4 CIDR du côté de la passerelle client (sur site) autorisée à communiquer via les tunnels VPN. Pour le IPv4 réseau distant CIDR, choisissez la plage d'adresses CIDR du AWS côté autorisé à communiquer via des tunnels VPN. La valeur par défaut pour les deux champs est`0.0.0.0/0`.
    - IPv6 — Pour le CIDR IPv6 du réseau local, spécifiez la plage d'adresses IPv6 CIDR du côté de la passerelle client (sur site) autorisée à communiquer via les tunnels VPN. Pour le IPv6 réseau distant CIDR, choisissez la plage d'adresses CIDR du AWS côté autorisé à communiquer via des tunnels VPN. La valeur par défaut pour les deux champs est `::/0`
12. Pour le type d'adresse IP externe, choisissez l'une des options suivantes :

    - Public IPv4 - (par défaut) Utilise les IPv4 adresses du tunnel extérieur IPs.
    - Privé IPv4 - Utilisez une IPv4 adresse privée pour une utilisation sur des réseaux privés.
    - IPv6- Utilisez IPv6 les adresses du tunnel extérieur IPs. Cette option nécessite que votre dispositif de passerelle client prenne en charge l' IPv6adressage.

> **Note**
>
> Si vous sélectionnez IPv6le type d'adresse IP externe, vous devez créer une passerelle client avec une IPv6 adresse

13. (Facultatif) Pour les options du tunnel 1, vous pouvez spécifier les informations suivantes pour chaque tunnel :
    - Un bloc IPv4 CIDR de taille /30 issu de la `169.254.0.0/16` plage des adresses du tunnel IPv4 intérieur.
    - Si vous avez spécifié IPv6pour la version IP du tunnel intérieur, un bloc d'adresse IPv6 CIDR /126 dans la `fd00::/8` plage des adresses du tunnel IPv6 intérieur.
    - La clé pré-partagée (PSK) IKE. Les versions suivantes sont prises en charge : IKEv1 ou IKEv2.
    - Pour modifier les options avancées de votre tunnel, choisissez Modifier les options du tunnel. Pour de plus amples informations, veuillez consulter Options de tunnel VPN.
    - (Facultatif) Choisissez Activer pour que le journal d'activité du tunnel capture les messages du journal d' IPsec activité et les messages du protocole DDP.
    - (Facultatif) Choisissez Activer pour le cycle de vie des terminaux du tunnel afin de contrôler le calendrier des remplacements des terminaux. Pour plus d'informations sur le cycle de vie des points de terminaison du tunnel, consultezCycle de vie des points de terminaison de tunnel.
14. (Facultatif) Choisissez les options du tunnel 2 et suivez les étapes précédentes pour configurer un deuxième tunnel.
15. Choisissez Create VPN connection (Créer une connexion VPN).

Création d'une connexion à une passerelle de AWS Site-to-Site VPN transit à l'aide de la CLI ou de l'API

Créez une connexion VPN à Transit Gateway à l'aide de la CLI

Utilisez la create-vpn-connectioncommande et spécifiez l'ID de passerelle de transit pour l'`--transit-gateway-id`option.

L'exemple suivant illustre la création d'une connexion VPN avec un tunnel IPv6 externe IPs et un tunnel IPv6 interne IPs :

```
aws ec2 create-vpn-connection \
--type ipsec.1 \
--transit-gateway-id tgw-12312312312312312 \
--customer-gateway-id cgw-001122334455aabbc \
--options
 OutsideIPAddressType=Ipv6,TunnelInsideIpVersion=ipv6,TunnelOptions=[{StartupAction=start},
{StartupAction=start}]
```

Exemple de réponse :

```
{
    "VpnConnection": {
        "VpnConnectionId": "vpn-0abcdef1234567890",
        "State": "pending",
        "CustomerGatewayId": "cgw-001122334455aabbc",
        "Type": "ipsec.1",
        "TransitGatewayId": "tgw-12312312312312312",
        "Category": "VPN",
        "Routes": [],
        "Options": {
            "StaticRoutesOnly": false,
            "OutsideIPAddressType": "Ipv6",
            "TunnelInsideIpVersion": "ipv6"
        }
    }
}
```

Créez une connexion VPN à Transit Gateway à l'aide de l'API

Vous pouvez créer une connexion VPN à l'aide de l'API Amazon EC2. Cette section fournit des exemples de messages de demande et de réponse pour créer une connexion VPN de passerelle de transit à l'aide de l'API.

Conditions préalables

Avant de créer une connexion VPN à l'aide de l'API, assurez-vous d'avoir :

- Une passerelle de transport en commun créée et disponible

- Une passerelle client configurée avec les détails de votre appareil sur site

L'exemple suivant montre comment créer une connexion VPN à l'aide de l'action `CreateVpnConnection` API :

```
POST / HTTP/1.1
Host: ec2.us-east-1.amazonaws.com
Content-Type: application/x-www-form-urlencoded

Action=CreateVpnConnection
&Type=ipsec.1
&TransitGatewayId=tgw-12345678901234567
&CustomerGatewayId=cgw-12345678901234567
&Options.StaticRoutesOnly=false
&Version=2016-11-15
```

Cet exemple crée une connexion VPN avec routage dynamique (BGP) entre la passerelle de transit spécifiée et la passerelle client.

Une réponse API réussie renvoie les détails de la connexion VPN :

```
<?xml version="1.0" encoding="UTF-8"?>
<CreateVpnConnectionResponse xmlns="http://ec2.amazonaws.com/doc/2016-11-15/">
    <requestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</requestId>
    <vpnConnection>
        <vpnConnectionId>vpn-1a2b3c4d5e6f78901</vpnConnectionId>
        <state>pending</state>
        <customerGatewayId>cgw-12345678901234567</customerGatewayId>
        <type>ipsec.1</type>
        <transitGatewayId>tgw-12345678901234567</transitGatewayId>
        <category>VPN</category>
        <options>
            <staticRoutesOnly>false</staticRoutesOnly>
        </options>
    </vpnConnection>
</CreateVpnConnectionResponse>
```

La réponse inclut l'ID de connexion VPN, l'état actuel et les détails de configuration. La connexion sera initialement dans un état « en attente » pendant qu'AWS approvisionne les tunnels VPN.

Créez une connexion AWS Site-to-Site VPN Cloud WAN à l'aide de la CLI ou de l'API

Vous pouvez créer des connexions Site-to-Site VPN entre votre réseau local et votre réseau WAN dans AWS le cloud en suivant la procédure ci-dessous. Pour plus d'informations, consultez la section Pièces jointes Site-to-site VPN dans AWS le Cloud WAN dans le Guide de l'utilisateur du AWS Cloud WAN.

Créez une connexion VPN au Cloud WAN à l'aide de la CLI

Utilisez la create-vpn-connectioncommande pour créer une connexion VPN qui sera ultérieurement connectée à un réseau mondial Cloud WAN. Cela crée une connexion VPN indépendante qui peut ensuite être associée au Cloud WAN via la console ou l'API Network Manager.

Conditions préalables

Avant de créer une connexion VPN Cloud WAN, assurez-vous de disposer des éléments suivants :

- `customer-gateway-id`- Une ressource de passerelle client existante (`cgw-xxxxxxxxx`) qui représente votre appareil VPN sur site.
- Réseau mondial Cloud WAN - Un réseau mondial Cloud WAN doit être créé et configuré avec des segments de réseau appropriés.
- Configuration BGP - Les connexions VPN Cloud WAN nécessitent un routage BGP ; le routage statique n'est pas pris en charge. Vous devez définir `StaticRoutesOnly=false` dans le paramètre options

Cette commande crée une connexion VPN sans spécifier de passerelle cible. La connexion sera isolée et pourra ensuite être associée à votre réseau mondial Cloud WAN via la console ou l'API Network Manager. L'`StaticRoutesOnly=false`option active le routage BGP, qui est obligatoire pour les pièces jointes au VPN Cloud WAN, car le routage statique n'est pas pris en charge.

L'exemple suivant crée une connexion VPN indépendante pour Cloud WAN :

```
aws ec2 create-vpn-connection \
            --type ipsec.1 \
            --customer-gateway-id cgw-0123456789abcdef0 \
            --options StaticRoutesOnly=false
```

La réponse renvoie ce qui suit :

```
{
            "VpnConnection": {
            "VpnConnectionId": "vpn-0abcdef1234567890",
            "State": "pending",
            "CustomerGatewayId": "cgw-0123456789abcdef0",
            "Type": "ipsec.1",
            "Category": "VPN",
            "Routes": [],
            "Options": {
            "StaticRoutesOnly": false
            }
            }
            }
```

Après avoir créé la connexion VPN, vous pouvez l'associer à votre réseau mondial Cloud WAN à l'aide de la console Network Manager ou de l'appel `create-site-to-site-vpn-attachment` d'API.

Créez une connexion VPN Cloud WAN à l'aide de l'API

Vous pouvez utiliser l'API EC2 pour créer une connexion VPN pour l'intégration du Cloud WAN. Cela implique de passer un appel d'`CreateVpnConnection`API qui crée une connexion VPN indépendante, qui peut ensuite être associée à votre réseau mondial Cloud WAN.

La demande d'API crée une connexion VPN sans spécifier de passerelle cible, la laissant dans un état non connecté prêt à être intégré au Cloud WAN. La connexion utilise le routage BGP, qui est requis pour les pièces jointes au VPN Cloud WAN.

L'exemple suivant montre la requête HTTP pour créer une connexion VPN Cloud WAN :

```
POST / HTTP/1.1
            Host: ec2.us-east-1.amazonaws.com
            Content-Type: application/x-www-form-urlencoded
            Authorization: AWS4-HMAC-SHA256 Credential=...

            Action=CreateVpnConnection
            &Type=ipsec.1
            &CustomerGatewayId=cgw-0123456789abcdef0
            &Options.StaticRoutesOnly=false
            &Version=2016-11-15
```

L'API renvoie une réponse réussie contenant les détails de la connexion VPN. La connexion sera dans un `pending` état initial lors de AWS l'approvisionnement des tunnels VPN, moment auquel le statut passe à`available`.

```
<?xml version="1.0" encoding="UTF-8"?>
            <CreateVpnConnectionResponse xmlns="http://ec2.amazonaws.com/
doc/2016-11-15/">
            <requestId>12345678-1234-1234-1234-123456789012</requestId>
            <vpnConnection>
            <vpnConnectionId>vpn-0abcdef1234567890</vpnConnectionId>
            <state>pending</state>
            <customerGatewayId>cgw-0123456789abcdef0</customerGatewayId>
            <type>ipsec.1</type>
            <category>VPN</category>
            <options>
            <staticRoutesOnly>false</staticRoutesOnly>
            </options>
            <vgwTelemetry/>
            <routes/>
            </vpnConnection>
            </CreateVpnConnectionResponse>
```

Détails de la réponse

La réponse de l'API fournit les informations clés suivantes :

- vpnConnectionId- L'identifiant unique de votre connexion VPN (par exemple,`vpn-0abcdef1234567890`) que vous utiliserez pour l'associer au Cloud WAN
- état - Initialement « en attente » pendant qu'AWS approvisionne les tunnels VPN, puis passe à « disponible » lorsqu'il est prêt à être rattaché
- catégorie - Affiche « VPN » indiquant qu'il s'agit d'une connexion VPN non connectée adaptée à l'intégration Cloud WAN
- staticRoutesOnly- Réglez sur « false » pour activer le routage BGP, qui est requis pour les pièces jointes au VPN Cloud WAN

Une fois que la connexion VPN atteint l'état « disponible », vous pouvez l'associer à votre réseau mondial Cloud WAN à l'aide de l'`CreateSiteToSiteVpnAttachment`API Network Manager ou de la console AWS.

Création d'une connexion au AWS Site-to-Site VPN concentrateur à l'aide de la CLI ou de l'API

Créez une connexion Site-to-Site VPN Concentrator à l'aide de la CLI

Après avoir créé un concentrateur Site-to-Site VPN, vous devez établir des connexions VPN individuelles entre vos sites distants et le concentrateur Site-to-Site VPN. Chaque site distant nécessite sa propre connexion VPN qui fait référence à l'ID du concentrateur Site-to-Site VPN. Cela permet à plusieurs sites distants de partager la même infrastructure de concentrateur Site-to-Site VPN tout en maintenant des tunnels sécurisés séparés pour chaque site.

Pour établir une connexion VPN à l'aide d'un concentrateur Site-to-Site VPN, spécifiez le concentrateur Site-to-Site VPN au lieu de la passerelle de transit lors de la création de la connexion VPN. L'exemple suivant crée une connexion VPN à l'aide d'un concentrateur Site-to-Site VPN :

```
aws ec2 create-vpn-connection \
--type ipsec.1 \
--customer-gateway-id cgw-123456789 \
--vpn-concentrator-id vcn-0123456789abcdef0
```

Une réponse réussie renvoie ce qui suit :

```
{
    "VpnConnection": {
        "VpnConnectionId": "vpn-0abcdef1234567890",
        "State": "pending",
        "CustomerGatewayId": "cgw-123456789",
        "Type": "ipsec.1",
        "VpnConcentratorId": "vcn-0123456789abcdef0",
        "Category": "VPN",
        "Routes": [],
        "Options": {
            "StaticRoutesOnly": false
        }
    }
}
```

Créez une connexion Site-to-Site VPN Concentrator à l'aide de l'API

Vous pouvez créer une connexion VPN qui utilise un concentrateur Site-to-Site VPN à l'aide de l'API Amazon EC2. Cette section fournit des exemples de messages de demande et de réponse pour créer une connexion VPN avec un concentrateur Site-to-Site VPN.

Avant de créer une connexion VPN avec un concentrateur Site-to-Site VPN à l'aide de l'API, assurez-vous d'avoir :

- Un concentrateur Site-to-Site VPN créé et disponible
- Une passerelle client configurée pour votre site distant
- Configuration réseau autorisant IPsec le trafic entre votre site et AWS

L'exemple suivant montre comment créer une connexion VPN à l'aide d'un concentrateur Site-to-Site VPN avec l'action `CreateVpnConnection` API :

```
POST / HTTP/1.1
Host: ec2.us-east-1.amazonaws.com
Content-Type: application/x-www-form-urlencoded

Action=CreateVpnConnection
&Type=ipsec.1
&VpnConcentratorId=vcn-0123456789abcdef0
&CustomerGatewayId=cgw-12345678901234567
&Options.StaticRoutesOnly=false
&Version=2016-11-15
```

Cet exemple crée une connexion VPN entre le concentrateur Site-to-Site VPN spécifié et la passerelle client. Le concentrateur Site-to-Site VPN agit en tant que point de terminaison AWS secondaire, permettant à plusieurs sites distants de se connecter via un hub centralisé.

Une réponse API réussie renvoie les détails de la connexion VPN avec les informations du concentrateur Site-to-Site VPN :

```
<?xml version="1.0" encoding="UTF-8"?>
<CreateVpnConnectionResponse xmlns="http://ec2.amazonaws.com/doc/2016-11-15/">
    <requestId>8b73d60f-458f-5gc5-a442-7f9fEXAMPLE</requestId>
    <vpnConnection>
```

```
        <vpnConnectionId>vpn-9z8y7x6w5v4u32109</vpnConnectionId>
        <state>pending</state>
        <customerGatewayId>cgw-12345678901234567</customerGatewayId>
        <type>ipsec.1</type>
        <vpnConcentratorId>vcn-0123456789abcdef0</vpnConcentratorId>
        <category>VPN</category>
        <options>
            <staticRoutesOnly>false</staticRoutesOnly>
        </options>
    </vpnConnection>
</CreateVpnConnectionResponse>
```

La réponse inclut l'identifiant de connexion VPN et fait référence à l'identifiant du concentrateur Site-to-Site VPN au lieu d'un identifiant de passerelle de transit. Cette connexion permet à votre site distant de communiquer avec d'autres sites connectés au même concentrateur Site-to-Site VPN, ce qui permet d'activer les hub-and-spoke topologies réseau.

Afficher les AWS Site-to-Site VPN connexions

Afficher les connexions VPN à l'aide de la console

Vous pouvez consulter vos connexions VPN et leurs détails à l'aide de l'AWS Management Console. Cela fournit une interface visuelle pour surveiller l'état de la connexion, l'état du tunnel et les détails de configuration.

Pour afficher les connexions VPN à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Site-to-Site VPN Connections.
3. Sélectionnez votre connexion VPN pour afficher des informations détaillées, notamment :

    - État et statut de la connexion
    - Détails du tunnel et état de santé
    - Informations sur l'itinéraire
    - Paramètres de configuration

La console affiche des informations d'état en temps réel et vous permet de surveiller la connectivité des tunnels, de consulter les tables de routage et d'accéder aux détails de configuration pour le dépannage.

Afficher les connexions VPN à l'aide de la CLI

Utilisez la CLI AWS pour interroger et récupérer des informations détaillées sur vos connexions VPN par programmation. Cette méthode permet l'automatisation, la création de scripts et l'intégration aux outils de surveillance.

Pour interroger toutes les connexions VPN de votre compte AWS et de votre région actuels, exécutez la `describe-vpn-connections` commande sans paramètres. Toutefois, si vous souhaitez consulter les détails d'une connexion VPN en particulier, vous devez connaître l'identifiant de connexion VPN.

Pour obtenir des informations détaillées sur une connexion VPN spécifique, spécifiez l'ID de connexion en tant que paramètre. L'exemple suivant montre une demande visant à afficher les détails d'une connexion VPN spécifique.

```
aws ec2 describe-vpn-connections --vpn-connection-ids vpn-1234567890abcdef0
```

La réponse inclut des informations complètes sur la connexion VPN, notamment les options de tunnel, les détails du routage et l'état actuel.

- `State`- L'état actuel de la connexion VPN
- `TunnelOptions`- Configuration et état de chaque tunnel
- `OutsideIpAddress`- Les adresses IP publiques des tunnels VPN
- `Routes`- Informations de routage pour la connexion

Exemple d'extrait de réponse montrant les principaux détails de connexion :

```
{
    "VpnConnections": [
        {
            "VpnConnectionId": "vpn-1234567890abcdef0",
            "State": "available",
            "CustomerGatewayId": "cgw-1234567890abcdef0",
            "Type": "ipsec.1",
            "Options": {
                "StaticRoutesOnly": false,
                "TunnelOptions": [
```

```
                    {
                        "OutsideIpAddress": "203.0.113.12",
                        "TunnelInsideCidr": "169.254.10.0/30",
                        "PreSharedKey": "example_key_1234567890abcdef0",
                        "Phase1LifetimeSeconds": 28800,
                        "Phase2LifetimeSeconds": 3600
                    },
                    {
                        "OutsideIpAddress": "203.0.113.34",
                        "TunnelInsideCidr": "169.254.11.0/30",
                        "PreSharedKey": "example_key_0987654321fedcba0",
                        "Phase1LifetimeSeconds": 28800,
                        "Phase2LifetimeSeconds": 3600
                    }
                ]
            }
        }
    ]
}
```

Afficher les connexions VPN à l'aide de l'API

Passez des appels d'API directs au EC2 service Amazon pour récupérer les informations de connexion VPN. Cette approche offre une flexibilité maximale pour les applications personnalisées et les intégrations programmatiques.

L'action `DescribeVpnConnections` API interroge et renvoie des informations détaillées sur une ou plusieurs connexions VPN. Vous pouvez appliquer des filtres par ID de connexion, par état ou par d'autres attributs pour affiner vos résultats.

L'exemple suivant montre un exemple de demande visant à fournir des informations sur une connexion VPN unique.

```
POST / HTTP/1.1
Host: ec2.us-east-1.amazonaws.com
Content-Type: application/x-www-form-urlencoded
Authorization: AWS4-HMAC-SHA256 Credential=AKIAIOSFODNN7EXAMPLE/20230101/us-east-1/ec2/
aws4_request, SignedHeaders=host;x-amz-date, Signature=example_signature

Action=DescribeVpnConnections
&VpnConnectionId.1=vpn-1234567890abcdef0
```

```
&Version=2016-11-15
```

La réponse renvoie des informations sur cette connexion VPN.

```
<?xml version="1.0" encoding="UTF-8"?>
<DescribeVpnConnectionsResponse xmlns="http://ec2.amazonaws.com/doc/2016-11-15/">
    <requestId>12345678-1234-1234-1234-123456789012</requestId>
    <vpnConnectionSet>
        <item>
            <vpnConnectionId>vpn-1234567890abcdef0</vpnConnectionId>
            <state>available</state>
            <customerGatewayId>cgw-1234567890abcdef0</customerGatewayId>
            <type>ipsec.1</type>
            <options>
                <staticRoutesOnly>false</staticRoutesOnly>
                <tunnelOptionSet>
                    <item>
                        <outsideIpAddress>203.0.113.12</outsideIpAddress>
                        <tunnelInsideCidr>169.254.10.0/30</tunnelInsideCidr>
                        <preSharedKey>example_key_1234567890abcdef0</preSharedKey>
                    </item>
                    <item>
                        <outsideIpAddress>203.0.113.34</outsideIpAddress>
                        <tunnelInsideCidr>169.254.11.0/30</tunnelInsideCidr>
                        <preSharedKey>example_key_0987654321fedcba0</preSharedKey>
                    </item>
                </tunnelOptionSet>
            </options>
        </item>
    </vpnConnectionSet>
</DescribeVpnConnectionsResponse>
```

Tester une AWS Site-to-Site VPN connexion

Après avoir créé la AWS Site-to-Site VPN connexion et configuré la passerelle client, vous pouvez lancer une instance et tester la connexion en envoyant un ping à l'instance.

Avant de commencer, veillez à exécuter les actions suivantes :

- Utilisez une AMI répondant aux requêtes ping. Nous vous recommandons d'utiliser l'un des systèmes Amazon Linux AMIs.
- Configurez tous les groupes de sécurité ou toutes les listes ACL réseau de votre VPC qui filtrent le trafic vers l'instance pour autoriser le trafic ICMP entrant et sortant. Cela permet à l'instance de recevoir des demandes `ping`.
- Si vous utilisez des instances exécutant Windows Server, connectez-vous à l'instance et activez le trafic entrant ICMPv4 sur le pare-feu Windows afin d'envoyer un ping à l'instance.
- (Routage statique) Assurez-vous que le périphérique de passerelle client a une route statique vers votre VPC et que votre connexion VPN a une route statique afin que le trafic puisse revenir à votre périphérique de passerelle client.
- (Routage dynamique) Assurez-vous que l'état du BGP sur votre périphérique de passerelle client est établi. Environ 30 secondes s'écoulent avant que la session d'appairage BGP soit établie. Assurez-vous que les routes sont publiées correctement avec le BGP et apparaissent dans la table de routage du sous-réseau afin que le trafic puisse revenir à votre passerelle client. Assurez-vous que les deux tunnels sont configurés avec le routage BGP.
- Assurez-vous que vous avez configuré le routage dans vos tables de routage de sous-réseau pour la connexion VPN.

Pour tester la connectivité

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Sur le tableau de bord, choisissez Lancer une instance.
3. (Facultatif) Pour Nom, saisissez un nom descriptif pour votre instance.
4. Pour Images d'applications et de systèmes d'exploitation (Amazon Machine Image), choisissez Démarrage rapide, puis choisissez le système d'exploitation de votre instance.
5. Pour Nom de la paire de clés, choisissez une paire de clés existante ou créez-en une.
6. Pour Paramètres réseau, choisissez Sélectionner un groupe de sécurité existant, puis sélectionnez le groupe de sécurité que vous avez configuré.
7. Dans le panneau Summary (Récapitulatif), sélectionnez Launch instance (Lancer l'instance).
8. Après l'exécution de l'instance, obtenez son adresse IP privée (par exemple, 10.0.0.4). La EC2 console Amazon affiche l'adresse dans le cadre des détails de l'instance.
9. Depuis un ordinateur dans votre réseau qui se trouver derrière la périphérique de passerelle client, utilisez la commande ping avec l'adresse IP privée de l'instance.

```
ping 10.0.0.4
```

Une réponse positive ressemble à ceci :

```
Pinging 10.0.0.4 with 32 bytes of data:

Reply from 10.0.0.4: bytes=32 time<1ms TTL=128
Reply from 10.0.0.4: bytes=32 time<1ms TTL=128
Reply from 10.0.0.4: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.4:
Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),

Approximate round trip times in milliseconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Pour tester le basculement de tunnel, vous pouvez désactiver temporairement un des tunnels sur votre appareil de passerelle client et répéter cette étape. Vous ne pouvez pas désactiver un tunnel côté AWS de la connexion VPN.

10. Pour tester la connexion depuis AWS votre réseau local, vous pouvez utiliser SSH ou RDP pour vous connecter à votre instance depuis votre réseau. Vous pouvez ensuite exécuter la commande `ping` avec l'adresse IP privée d'un autre ordinateur de votre réseau, pour vérifier que les deux côtés de la connexion peuvent lancer et recevoir des demandes.

    Pour plus d'informations sur la connexion à une instance Linux, consultez Connect to your Linux instance dans le guide de EC2 l'utilisateur Amazon. Pour plus d'informations sur la façon de se connecter à une instance Windows, consultez Connect to your Windows User Guide dans le guide de EC2 l'utilisateur Amazon.

Supprimer une AWS Site-to-Site VPN connexion et une passerelle

Si vous n'avez plus besoin d'une AWS Site-to-Site VPN connexion, vous pouvez la supprimer. Lorsque vous supprimez une connexion Site-to-Site VPN, nous ne supprimons pas la passerelle client ou la passerelle privée virtuelle associée à la connexion Site-to-Site VPN. Si vous n'avez plus besoin de la passerelle client et de la passerelle réseau privé virtuel, vous pouvez les supprimer.

> **Warning**
>
> Si vous supprimez votre connexion Site-to-Site VPN puis en créez une nouvelle, vous devez télécharger un nouveau fichier de configuration et reconfigurer le dispositif de passerelle client.

Tâches

- Supprimer une AWS Site-to-Site VPN connexion
- Supprimer une passerelle AWS Site-to-Site VPN client
- Détachez et supprimez une passerelle privée virtuelle dans AWS Site-to-Site VPN

Supprimer une AWS Site-to-Site VPN connexion

Une fois que vous avez supprimé votre connexion Site-to-Site VPN, elle reste visible pendant un court moment avec l'état de`deleted`, puis l'entrée est automatiquement supprimée.

Pour supprimer une connexion VPN avec la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Connexions Site-to-Site VPN.
3. Sélectionnez la connexion VPN, puis choisissez Actions, Supprimer une connexion VPN.
4. Lorsque vous êtes invité à confirmer, entrez **`delete`**, puis choisissez Delete (Supprimer).

Pour supprimer une connexion VPN à l'aide de la ligne de commande ou de l'API

- DeleteVpnConnection(API Amazon EC2 Query)
- delete-vpn-connection (AWS CLI)
- Remove-EC2VpnConnection (AWS Tools for Windows PowerShell)

Supprimer une passerelle AWS Site-to-Site VPN client

Si vous n'avez plus besoin d'une passerelle client, vous pouvez la supprimer. Vous ne pouvez pas supprimer une passerelle client utilisée dans une connexion Site-to-Site VPN.

Pour supprimer une passerelle client avec la console

1. Dans le volet de navigation, choisissez Passerelles client.
2. Sélectionnez la passerelle client, puis choisissez Actions, Supprimer la passerelle client.
3. Lorsque vous êtes invité à confirmer, entrez **`delete`**, puis choisissez Delete (Supprimer).

Pour supprimer une passerelle client à l'aide de la ligne de commande ou de l'API

- DeleteCustomerGateway(API Amazon EC2 Query)
- delete-customer-gateway (AWS CLI)
- Remove-EC2CustomerGateway (AWS Tools for Windows PowerShell)

Détachez et supprimez une passerelle privée virtuelle dans AWS Site-to-Site VPN

Si vous n'avez plus besoin d'une passerelle privée virtuelle pour votre VPC, vous pouvez la détacher du VPC.

Pour détacher une passerelle réseau privé virtuel avec la console

1. Dans le volet de navigation, choisissez Passerelles réseau privé virtuel.
2. Sélectionnez la passerelle réseau privé virtuel, puis choisissez Actions, Détacher du VPC.
3. Choisissez Détacher une passerelle réseau privé virtuel.

Si vous n'avez plus besoin d'une passerelle réseau privé virtuel détachée, vous pouvez la supprimer. Vous ne pouvez pas supprimer une passerelle réseau privé virtuel qui est toujours attachée à un VPC. Après avoir supprimé votre passerelle réseau privé virtuel, elle reste visible pendant un court moment avec un état de `deleted`, puis l'entrée est automatiquement supprimée.

Pour supprimer une passerelle réseau privé virtuel avec la console

1. Dans le volet de navigation, choisissez Passerelles réseau privé virtuel.
2. Sélectionnez la passerelle réseau privé virtuel, puis choisissez Actions, Supprimer une passerelle réseau privé virtuel.
3. Lorsque vous êtes invité à confirmer, entrez **`delete`**, puis choisissez Delete (Supprimer).

Pour détacher une passerelle réseau privé virtuel à l'aide de la ligne de commande ou de l'API

- DetachVpnGateway(API Amazon EC2 Query)
- detach-vpn-gateway (AWS CLI)
- Dismount-EC2VpnGateway (AWS Tools for Windows PowerShell)

Pour supprimer une passerelle réseau privé virtuel à l'aide de la ligne de commande ou de l'API

- DeleteVpnGateway(API Amazon EC2 Query)
- delete-vpn-gateway (AWS CLI)
- Remove-EC2VpnGateway (AWS Tools for Windows PowerShell)

Modifier la passerelle cible d'une AWS Site-to-Site VPN connexion

Vous pouvez modifier la passerelle cible d'une AWS Site-to-Site VPN connexion. Les options de migration suivantes sont disponibles :

- Une passerelle réseau privé virtuel existante vers une passerelle de transit
- Une passerelle réseau privé virtuel vers une autre passerelle réseau privé virtuel
- Une passerelle de transit existante vers une autre passerelle de transit
- Une passerelle de transit existante vers une passerelle réseau privé virtuel

Après avoir modifié la passerelle cible, votre connexion Site-to-Site VPN sera temporairement indisponible pendant une brève période pendant que nous fournissons les nouveaux points de terminaison.

Les tâches suivantes vous aident à procéder à la migration vers une nouvelle passerelle.

Tâches

- Étape 1 : Créer la nouvelle passerelle cible
- Étape 2 : Suppression de vos routes statiques (conditionnel)
- Étape 3 : Migration vers une nouvelle passerelle
- Étape 4 : Mise à jour des tables de routage de VPC
- Étape 5 : Mettre à jour le routage (conditionnel) de la passerelle cible
- Étape 6 : Mise à jour de l'ASN de la passerelle client (conditionnel)

Étape 1 : Créer la nouvelle passerelle cible

Avant de procéder à la migration vers la nouvelle passerelle cible, vous devez configurer cette dernière. Pour plus d'informations sur l'ajout d'une passerelle réseau privé virtuel, consultez the section called "Créer une passerelle réseau privé virtuel". Pour plus d'informations sur l'ajout d'une passerelle de transit, consultez Créer une passerelle de transit dans Passerelles de transit Amazon VPC.

Si la nouvelle passerelle cible est une passerelle de transit, attachez-la VPCs à la passerelle de transit. Pour plus d'informations sur les attachements de VPC, consultez Réseaux de transit par passerelle vers un VPC dans Passerelles de transit Amazon VPC.

Lorsque vous modifiez la cible d'une passerelle réseau privé virtuel vers une passerelle de transit, vous pouvez éventuellement définir l'ASN de la passerelle de transit pour qu'il ait la même valeur que l'ASN de la passerelle réseau privé virtuel. Si vous choisissez d'avoir un ASN différent, vous devez définir l'ASN sur votre périphérique de passerelle client sur l'ASN de la passerelle de transit. Pour de plus amples informations, veuillez consulter the section called "Étape 6 : Mise à jour de l'ASN de la passerelle client (conditionnel)".

Étape 2 : Suppression de vos routes statiques (conditionnel)

Cette étape est obligatoire lorsque vous procédez à une migration depuis une passerelle réseau privé virtuel avec des routes statiques vers une passerelle de transit.

Vous devez supprimer les routes statiques avant de procéder à la migration vers la nouvelle passerelle.

> **Tip**
>
> Gardez une copie de la route statique avant de la supprimer. Vous devrez rajouter ces routes à la passerelle de transit lorsque la migration de la connexion VPN sera terminée.

Pour supprimer un itinéraire dans une table d'itinéraires

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Tables de routage, puis sélectionnez la table de routage.
3. Dans l'onglet Routes, choisissez Edit routes (Modifier les routes).

4. Choisissez Supprimer pour la route statique menant à la passerelle réseau privé virtuel.
5. Sélectionnez Enregistrer les modifications.

Étape 3 : Migration vers une nouvelle passerelle

Pour modifier la passerelle cible

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Connexions Site-to-Site VPN.
3. Sélectionnez la connexion VPN, puis choisissez Actions, Modifier la connexion VPN.
4. Pour Type de cible, choisissez le type de passerelle.
   a. Si la nouvelle passerelle cible est une passerelle privée virtuelle, choisissez Passerelle VPN.
   b. Si la nouvelle passerelle cible est une passerelle de transit, choisissez Passerelle de transit.
5. Sélectionnez Enregistrer les modifications.

Pour modifier une connexion Site-to-Site VPN à l'aide de la ligne de commande ou de l'API

- ModifyVpnConnection(API de requête Amazon EC2)
- modify-vpn-connection (AWS CLI)

Étape 4 : Mise à jour des tables de routage de VPC

Après la migration vers la nouvelle passerelle, il se peut que vous ayez besoin de modifier votre table de routage de VPC. Pour plus d'informations, consultez Tables de routage dans le Guide de l'utilisateur Amazon VPC.

Le tableau suivant fournit des informations sur les mises à jour de la table de routage VPC à effectuer après avoir modifié la cible de la passerelle VPN.

Passerelle existante	Nouvelle passerelle	Modification de table de routage de VPC
Passerelle réseau privé virtuel avec routes propagées	Passerelle de transit	Ajoutez une route qui contient l'ID de la passerelle de transit.

Passerelle existante	Nouvelle passerelle	Modification de table de routage de VPC
Passerelle réseau privé virtuel avec routes propagées	Passerelle réseau privé virtuel avec routes propagées	Aucune action n'est requise.
Passerelle réseau privé virtuel avec routes propagées	Passerelle réseau privé virtuel avec routes statiques	Ajoutez une entrée qui contient l'ID de la passerelle réseau privé virtuel.
Passerelle réseau privé virtuel avec routes statiques	Passerelle de transit	Mettez à jour la route qui contient l'ID de la passerelle réseau privé virtuel avec l'ID de la passerelle de transit.
Passerelle réseau privé virtuel avec routes statiques	Passerelle réseau privé virtuel avec routes statiques	Mettez à jour la route qui contient l'ID de la passerell e réseau privé virtuel avec l'ID de la nouvelle passerelle réseau privé virtuel.
Passerelle réseau privé virtuel avec routes statiques	Passerelle réseau privé virtuel avec routes propagées	Supprimez la route qui contient l'ID de la passerelle réseau privé virtuel.
Passerelle de transit	Passerelle réseau privé virtuel avec routes statiques	Mettez à jour la route qui contient l'ID de la passerell e de transit avec l'ID de la passerelle réseau privé virtuel.
Passerelle de transit	Passerelle réseau privé virtuel avec routes propagées	Supprimez la route qui contient l'ID de la passerelle de transit.
Passerelle de transit	Passerelle de transit	Mettez à jour la route qui contient l'ID de la passerell e de transit avec l'ID de la nouvelle passerelle de transit.

Étape 5 : Mettre à jour le routage (conditionnel) de la passerelle cible

Lorsque la nouvelle passerelle est une passerelle de transit, modifiez la table de routage de la passerelle de transit pour autoriser le trafic entre le VPC et le Site-to-Site VPN. Pour plus d'informations, consultez Tables de routage de passerelle de transit dans Passerelle de transit Amazon VPC.

Si vous avez supprimé les routes statiques de VPN, vous devez ajouter les routes statiques à la table de routage de passerelle de transit.

Contrairement à une passerelle réseau privé virtuel, une passerelle de transit définit la même valeur pour le discriminateur à sorties multiples (MED, multi-exit discriminator) sur tous les tunnels d'un attachement VPN. Si vous migrez d'une passerelle réseau privé virtuel vers une passerelle de transit et que vous vous êtes appuyé sur la valeur MED pour la sélection des tunnels, nous vous recommandons d'apporter des modifications de routage pour éviter les problèmes de connexion. Par exemple, vous pouvez annoncer des acheminements plus spécifiques sur votre passerelle de transit. Pour de plus amples informations, veuillez consulter Tables de routage et priorité des AWS Site-to-Site VPN itinéraires.

Étape 6 : Mise à jour de l'ASN de la passerelle client (conditionnel)

Lorsque la nouvelle passerelle a un ASN différent de l'ancienne passerelle, vous devez mettre à jour l'ASN sur votre périphérique de passerelle client pour qu'il pointe vers le nouvel ASN. Pour plus d'informations, consultez Options de passerelle client pour votre AWS Site-to-Site VPN connexion.

Modify AWS Site-to-Site VPN options de connexion

Vous pouvez modifier les options de connexion de votre connexion Site-to-Site VPN. Vous pouvez modifier les options suivantes :

- Les plages CIDR IPv4 côté local (passerelle client) et côté distant (AWS) de la connexion VPN qui peuvent communiquer via les tunnels VPN. La valeur par défaut est `0.0.0.0/0` pour les deux plages.
- Les plages CIDR IPv6 côté local (passerelle client) et côté distant (AWS) de la connexion VPN qui peuvent communiquer via les tunnels VPN. La valeur par défaut est `::/0` pour les deux plages.
- La bande passante du tunnel pour la connexion VPN. `standard`prend en charge jusqu'à 1,25 Gbit/s par tunnel, tandis que `large` prend en charge jusqu'à 5 Gbit/s par tunnel. Une large bande

passante n'est disponible que pour les connexions VPN connectées à une passerelle de transit ou au Cloud WAN. Pour de plus amples informations, veuillez consulter Tunnels à large bande passante.

Lorsque vous modifiez les options de connexion VPN, les adresses IP des points de terminaison VPN situés sur le AWS côté ne changent pas et les options du tunnel ne changent pas. Votre connexion VPN sera temporairement indisponible pour une courte période lors de la mise à jour de la connexion VPN.

Pour modifier les options de connexion VPN à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Connexions Site-to-Site VPN.
3. Sélectionnez votre connexion VPN, puis choisissez Actions, Modifier les options de connexion VPN.
4. Saisissez de nouvelles plages d'adresses CIDR en fonction des besoins.
5. Sélectionnez Enregistrer les modifications.

Pour modifier les options de connexion VPN à l'aide de la ligne de commande ou de l'API

- modify-vpn-connection-options (AWS CLI)
- ModifyVpnConnectionOptions(API de requête Amazon EC2)

Modifier la bande passante du tunnel

Vous pouvez modifier la bande passante du tunnel des connexions VPN existantes, en basculant entre `standard` (jusqu'à 1,25 Gbit/s par tunnel) et `large` (jusqu'à 5 Gbit/s par tunnel) sans recréer les connexions VPN. Cela vous permet d'effectuer une modification sur place pour augmenter ou diminuer la bande passante de votre tunnel en fonction de vos besoins.

La possibilité de modifier la bande passante du tunnel est disponible dans les options suivantes Régions AWS :

- Afrique (Le Cap)
- Asie-Pacifique (Hong Kong)
- Asie-Pacifique (Hyderabad)

- Asie-Pacifique (Jakarta)
- Asie-Pacifique (Malaisie)
- Asie-Pacifique (Mumbai)
- Asie-Pacifique (Nouvelle Zélande)
- Asie-Pacifique (Osaka)
- Asie-Pacifique (Séoul)
- Asie-Pacifique (Sydney)
- Asie-Pacifique (Taipei)
- Asie-Pacifique (Thaïlande)
- Asie-Pacifique (Tokyo)
- Europe (Francfort)
- Europe (Londres)
- Europe (Paris)
- Europe (Espagne)
- Europe (Stockholm)
- Mexique (Centre)
- Amérique du Sud (São Paulo)
- USA Est (Virginie du Nord)
- USA Est (Ohio)
- USA Ouest (Californie du Nord)
- AWS GovCloud (US-West)

Dans les régions où la modification de la bande passante du tunnel n'est pas prise en charge, vous devez d'abord supprimer la connexion VPN, puis créer une nouvelle connexion VPN et définir la bande passante du tunnel sur Large.

Modifier les options AWS Site-to-Site VPN du tunnel

Vous pouvez modifier les options de tunnel pour les tunnels VPN de votre connexion Site-to-Site VPN. Vous pouvez modifier un seul tunnel VPN à la fois.

> **Important**
>
> Lorsque vous modifiez un tunnel VPN, la connexion au tunnel est interrompue pendant plusieurs minutes. Pensez à tenir compte des temps d'arrêt prévus.

Pour modifier les options du tunnel VPN à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Connexions Site-to-Site VPN.
3. Sélectionnez la connexion Site-to-Site VPN, puis choisissez Actions, Modifier les options du tunnel VPN.
4. Pour Adresse IP externe du tunnel VPN, choisissez l'adresse IP du point de terminaison du tunnel VPN.
5. Choisissez les valeurs des options du tunnel ou saisissez-en de nouvelles si nécessaire. Pour plus d'informations sur les options de tunnel, consultezOptions de tunnel VPN.

   > **Note**
   >
   > Certaines options de tunnel comportent plusieurs valeurs par défaut. Cliquez pour supprimer toute valeur par défaut. Cette valeur par défaut est ensuite supprimée de l'option tunnel.

6. Sélectionnez Enregistrer les modifications.

Pour modifier les options du tunnel VPN à l'aide de la ligne de commande ou de l'API

- (AWS CLI) describe-vpn-connectionsÀ utiliser pour afficher les options de tunnel actuelles et modify-vpn-tunnel-optionspour modifier les options de tunnel.
- (Amazon EC2 Query API) DescribeVpnConnectionsÀ utiliser pour afficher les options de tunnel actuelles et ModifyVpnTunnelOptionspour modifier les options de tunnel.

Modifier les itinéraires statiques pour une AWS Site-to-Site VPN connexion

Pour une connexion Site-to-Site VPN sur une passerelle privée virtuelle configurée pour le routage statique, vous pouvez ajouter ou supprimer des routes statiques de votre configuration VPN.

Pour ajouter ou supprimer une route statique à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Connexions Site-to-Site VPN.
3. Sélectionnez la connexion VPN.
4. Choisissez Modifier des routes statiques.
5. Ajoutez ou supprimez des routes en fonction des besoins.
6. Sélectionnez Enregistrer les modifications.
7. Si vous n'avez pas autorisé la propagation du routage pour votre table de routage, vous devez manuellement mettre à jour les routes dans votre table de routage afin de tenir compte des préfixes IP statiques mis à jour dans votre connexion VPN. Pour de plus amples informations, veuillez consulter (Passerelle réseau privé virtuel) Activer la propagation de route dans votre table de routage.
8. Pour une connexion VPN sur une passerelle de transit, vous devez ajouter, modifier ou supprimer les routes statiques dans la table de routage de la passerelle de transit. Pour plus d'informations, consultez Tables de routage de passerelle de transit dans Passerelle de transit Amazon VPC.

Pour ajouter une route statique à l'aide de la ligne de commande ou d'une API

- CreateVpnConnectionRoute(API Amazon EC2 Query)
- create-vpn-connection-route (AWS CLI)
- New-EC2VpnConnectionRoute (AWS Tools for Windows PowerShell)

Pour supprimer une route statique à l'aide de la ligne de commande ou d'une API

- DeleteVpnConnectionRoute(API Amazon EC2 Query)
- delete-vpn-connection-route (AWS CLI)

- Remove-EC2VpnConnectionRoute (AWS Tools for Windows PowerShell)

Modifier la passerelle client pour une AWS Site-to-Site VPN connexion

Vous pouvez modifier la passerelle client de votre connexion Site-to-Site VPN à l'aide de la console Amazon VPC ou d'un outil de ligne de commande.

Après avoir modifié la passerelle client, votre connexion VPN est indisponible pendant une courte période, le temps que nous mettions en service les nouveaux points de terminaison.

Pour modifier la passerelle client à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Connexions Site-to-Site VPN.
3. Sélectionnez la connexion VPN.
4. Choisissez Actions, Modifier la connexion VPN.
5. Pour Type de cible, choisissez Passerelle client.
6. Pour Passerelle client cible, choisissez la nouvelle passerelle client.
7. Sélectionnez Enregistrer les modifications.

Pour modifier la passerelle client à l'aide de la ligne de commande ou de l'API

- ModifyVpnConnection(API Amazon EC2 Query)
- modify-vpn-connection (AWS CLI)

Remplacer les informations d'identification compromises pour une AWS Site-to-Site VPN connexion

Si vous pensez que les informations d'identification du tunnel pour votre connexion Site-to-Site VPN ont été compromises, vous pouvez modifier la clé pré-partagée IKE ou le certificat ACM. La méthode que vous utilisez dépend de l'option d'authentification utilisée pour vos tunnels VPN. Pour de plus amples informations, veuillez consulter AWS Site-to-Site VPN options d'authentification du tunnel.

Changer la clé pré-partagée IKE

Vous pouvez modifier les options de tunnel pour la connexion VPN et spécifier une nouvelle clé pré-partagée IKE pour chaque tunnel. Pour de plus amples informations, veuillez consulter Modifier les options AWS Site-to-Site VPN du tunnel.

Vous pouvez également supprimer la connexion VPN. Pour de plus amples informations, veuillez consulter Supprimer une connexion VPN et une passerelle. Vous n'avez pas besoin de supprimer le VPC ni la passerelle réseau privé virtuel. Créez ensuite une connexion VPN en utilisant la même passerelle réseau privé virtuel, puis configurez les nouvelles clés sur votre appareil de passerelle client. Vous pouvez spécifier vos propres clés pré-partagées pour les tunnels ou laisser AWS générer de nouvelles clés pré-partagées pour vous. Pour en savoir plus, consultez Création d'une connexion VPN. Les adresses interne et externe du tunnel peuvent changer lorsque vous recréez la connexion VPN.

Pour modifier le certificat du AWS côté du point de terminaison du tunnel

Effectuez une rotation du certificat. Pour de plus amples informations, veuillez consulter Rotation des certificats des points de terminaison du tunnel VPN.

Pour modifier le certificat sur le périphérique de passerelle client

1. Créez un nouveau certificat. Pour en savoir plus, consultez Émission et gestion de certificats dans le Guide de l'utilisateur AWS Certificate Manager .
2. Ajoutez le certificat au périphérique de passerelle client.

Rotation des certificats de terminaison AWS Site-to-Site VPN du tunnel

Vous pouvez faire pivoter les certificats sur les points de terminaison du tunnel situés sur le AWS côté à l'aide de la console Amazon VPC. Lorsque le certificat d'un point de terminaison du tunnel est sur le point d'expirer, il fait AWS automatiquement pivoter le certificat en utilisant le rôle lié au service. Pour de plus amples informations, veuillez consulter the section called “Service-linked rôles”.

Pour faire pivoter le certificat de point de terminaison du tunnel Site-to-Site VPN à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Connexions Site-to-Site VPN.
3. Sélectionnez la connexion Site-to-Site VPN, puis choisissez Actions, Modifier le certificat du tunnel VPN.

4. Sélectionnez le point de terminaison du tunnel.
5. Choisissez Enregistrer.

Pour faire pivoter le certificat de point de terminaison du tunnel Site-to-Site VPN à l'aide du AWS CLI

Utilisez la commande modify-vpn-tunnel-certificate.

IP privée AWS Site-to-Site VPN avec Direct Connect

Avec un VPN IP privé, vous pouvez déployer IPsec un VPN par-dessus Direct Connect, crypter le trafic entre votre réseau local et ce AWS, sans utiliser d'adresses IP publiques ou d'équipements VPN tiers supplémentaires.

L'un des principaux cas d'utilisation du VPN IP privéDirect Connect consiste à aider les clients des secteurs de la finance, de la santé et du secteur fédéral à atteindre leurs objectifs réglementaires et de conformité. Le VPN IP privéDirect Connect garantit que le trafic entre les réseaux locaux AWS et sur site est à la fois sécurisé et privé, ce qui permet aux clients de se conformer à leurs obligations réglementaires et de sécurité.

Avantages du VPN d'IP privée

- Gestion et opérations réseau simplifiées : sans VPN IP privé, les clients doivent déployer un VPN et des routeurs tiers pour implémenter le privé VPNs sur Direct Connect les réseaux. Avec la capacité VPN d'IP privée, les clients n'ont pas besoin de déployer et de gérer leur propre infrastructure VPN. Cela permet de simplifier les opérations réseau et de réduire les coûts.
- Position de sécurité améliorée : Auparavant, les clients devaient utiliser une interface Direct Connect virtuelle publique (VIF) pour chiffrer le trafic Direct Connect, ce qui nécessitait des adresses IP publiques pour les points de terminaison VPN. Le recours au public IPs augmente la probabilité d'attaques externes (DOS), ce qui oblige les clients à déployer des équipements de sécurité supplémentaires pour protéger le réseau. En outre, un VIF public ouvre l'accès entre tous les services AWS publics et les réseaux locaux des clients, augmentant ainsi la gravité du risque. La fonctionnalité VPN IP privée permet le chiffrement via le Direct Connect transit VIFs (au lieu du chiffrement public VIFs), associé à la possibilité de configurer le mode privé IPs. Cela fournit une connectivité end-to-end privée en plus du chiffrement, améliorant ainsi la posture de sécurité globale.

- Échelle d'itinéraire plus élevée : les connexions VPN IP privées offrent des limites de routes plus élevées (5 000 routes sortantes et 1 000 routes entrantes) par rapport aux connexions Direct Connect seules, qui sont actuellement limitées à 200 routes sortantes et 100 routes entrantes.

Comment fonctionne le VPN d'IP privée

Site-to-SiteLe VPN IP privé fonctionne via une interface virtuelle de Direct Connect transit (VIF). Il utilise une Direct Connect passerelle et une passerelle de transit pour interconnecter vos réseaux locaux avec.AWS VPCs Une connexion VPN IP privée possède des points de terminaison sur la passerelle de transit sur le AWS côté, et sur le dispositif de passerelle de votre client sur site. Vous devez attribuer des adresses IP privées à la fois à la passerelle de transit et à l'extrémité du dispositif de passerelle client des IPsec tunnels. Vous pouvez utiliser des adresses IP privées issues de l'une RFC1918 ou de plusieurs plages RFC6598 d' IPv4 adresses privées.

Vous attachez une connexion VPN d'IP privée à une passerelle de transit. Vous acheminez ensuite le trafic entre le rattachement VPN et tout réseau VPCs (ou autre) également connecté à la passerelle de transit. Pour ce faire, vous associez une table de routage à l'attachement de VPN. Dans le sens inverse, vous pouvez acheminer le trafic VPCs de votre attachement VPN IP privé à l'aide des tables de routage associées au VPCs.

La table de routage associée à la pièce jointe VPN peut être identique ou différente de celle associée à la Direct Connect pièce jointe sous-jacente. Cela vous permet d'acheminer le trafic chiffré et non chiffré simultanément entre votre réseau VPCs et votre réseau sur site.

Pour plus de détails sur le chemin de trafic quittant le VPN, consultez la section Politiques de routage de l'interface virtuelle privée et de l'interface virtuelle de transit dans le guide de Direct Connect l'utilisateur.

Conditions préalables

Le tableau suivant décrit les conditions préalables à la création d'un VPN IP privé via Direct Connect.

Élément	Étapes	Informations
Préparez la passerelle de transit pour le Site-to-Site VPN.	Créez la passerelle de transit à l'aide de la console Amazon Virtual Private Cloud(VPC), de	Une passerelle de transit est un hub de transit réseau que vous pouvez utiliser pour interconnecter vos réseaux

Élément	Étapes	Informations
	la ligne de commande ou de l'API. Consultez la section Passerelles de transit dans le guide des passerelles de transit Amazon VPC.	VPCs et ceux sur site. Vous pouvez créer une nouvelle passerelle de transit ou utiliser une passerelle existante pour la connexion VPN d'IP privée. Lorsque vous créez la passerelle de transit ou que vous modifiez une passerelle de transit existante, vous spécifiez un bloc CIDR d'IP privée pour la connexion. **Note** Lorsque vous spécifiez le bloc CIDR de la passerelle de transit à associer à votre VPN d'IP privée, assurez-vous que le bloc CIDR ne chevauche aucune adresse IP pour les autres attachements réseau de la passerelle de transit. Si des blocs CIDR IP se chevauchent, cela peut entraîner des problèmes de configuration avec votre appareil de passerelle client.

Élément	Étapes	Informations
Créez la Direct Connect passerelle pour le Site-to-Site VPN.	Créez la passerelle Direct Connect à l'aide de la console Direct Connect, de la ligne de commande ou de l'API. Reportez-vous à la section Création d'une passerelle AWS Direct Connect dans le guide de Direct Connect l'utilisateur.	Une passerelle Direct Connect vous permet de connecter des interfaces virtuelles (VIFs) dans plusieurs AWS régions. Cette passerelle est utilisée pour se connecter à votre VIF.
Créez l'association de passerelle de transit pour le Site-to-Site VPN.	Créez l'association entre la passerelle Direct Connect et la passerelle de transit à l'aide de la console Direct Connect, de la ligne de commande ou de l'API. Voir Associer ou dissocier Direct Connect une passerelle de transit dans le guide de l'Direct Connect utilisateur.	Après avoir créé la Direct Connect passerelle, créez une association de passerelle de transit pour la Direct Connect passerelle. Spécifiez le CIDR d'IP privée pour la passerelle de transit identifiée précédemment dans la liste des préfixes autorisés.

Tâches

- Créez une adresse IP privée AWS Site-to-Site VPN sur Direct Connect

Créez une adresse IP privée AWS Site-to-Site VPN sur Direct Connect

Pour créer un VPN IP privé, Direct Connect procédez comme suit. Avant de créer le VPN IP privé via Direct Connect, vous devez d'abord vous assurer qu'une passerelle de transit et une passerelle Direct Connect sont créées. Après avoir créé les deux passerelles, vous devez créer une association entre les deux. Ces prérequis sont décrits dans le tableau suivant. Une fois que vous avez créé et associé les deux passerelles, vous créerez une passerelle client VPN et une connexion à l'aide de cette association.

Conditions préalables

Le tableau suivant décrit les conditions préalables à la création d'un VPN IP privé via Direct Connect.

Élément	Étapes	Informations
Préparez la passerelle de transit pour le Site-to-Site VPN.	Créez la passerelle de transit à l'aide de la console Amazon Virtual Private Cloud (VPC), de la ligne de commande ou de l'API. Consultez la section Passerelles de transit dans le guide des passerelles de transit Amazon VPC.	Une passerelle de transit est un hub de transit réseau que vous pouvez utiliser pour interconnecter vos réseaux VPCs et ceux sur site. Vous pouvez créer une nouvelle passerelle de transit ou utiliser une passerelle existante pour la connexion VPN d'IP privée. Lorsque vous créez la passerelle de transit ou que vous modifiez une passerelle de transit existante, vous spécifiez un bloc CIDR d'IP privée pour la connexion. **Note** Lorsque vous spécifiez le bloc CIDR de la passerelle de transit à associer à votre VPN d'IP privée, assurez-vous que le bloc CIDR ne chevauche aucune adresse IP pour les autres attachements réseau de la passerelle de transit. Si des blocs CIDR IP se chevauchent,

Élément	Étapes	Informations
		cela peut entraîner des problèmes de configuration avec votre appareil de passerelle client.
Créez la Direct Connect passerelle pour le Site-to-Site VPN.	Créez la passerelle Direct Connect à l'aide de la console Direct Connect, de la ligne de commande ou de l'API. Reportez-vous à la section Création d'une passerelle AWS Direct Connect dans le guide de Direct Connect l'utilisateur.	Une passerelle Direct Connect vous permet de connecter des interfaces virtuelles (VIFs) dans plusieurs AWS régions. Cette passerelle est utilisée pour se connecter à votre VIF.
Créez l'association de passerelle de transit pour le Site-to-Site VPN.	Créez l'association entre la passerelle Direct Connect et la passerelle de transit à l'aide de la console Direct Connect, de la ligne de commande ou de l'API. Voir Associer ou dissocier Direct Connect une passerelle de transit dans le guide de l'Direct Connect utilisateur.	Après avoir créé la Direct Connect passerelle, créez une association de passerelle de transit pour la Direct Connect passerelle. Spécifiez le CIDR d'IP privée pour la passerelle de transit identifiée précédemment dans la liste des préfixes autorisés.

Création de la passerelle client et de la connexion pour le Site-to-Site VPN

Une passerelle client est une ressource que vous créez dans AWS. Elle représente l'appareil de passerelle client dans votre réseau sur site. Lorsque vous créez une passerelle client, vous fournissez des informations sur votre appareil à AWS. Pour en savoir plus, consultez Passerelle client.

Pour créer une passerelle client avec la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Passerelles client.
3. Choisissez Créer la passerelle client.
4. (Facultatif) Pour Name tag (Étiquette de nom), entrez un nom pour votre passerelle client. Une identification est alors créée avec la clé `Name` et la valeur que vous spécifiez.
5. Dans BGP ASN (Version du moteur de cache), saisissez le numéro d'ASN (Autonomous System Number) BGP (Border Gateway Protocol) de votre passerelle client.
6. Pour Adresse IP, entrez l'adresse IP privée de votre appareil de passerelle client.

   > **Important**
   >
   > Lors de la configuration de l'adresse IP AWS privée AWS Site-to-Site VPN, vous devez spécifier vos propres adresses IP de point de terminaison de tunnel à l'aide des adresses RFC 1918. N'utilisez pas les adresses point-to-point IP pour le peering eBGP entre le routeur de votre passerelle client et le Direct Connect point de terminaison. AWS recommande d'utiliser une interface de boucle ou une interface LAN sur le routeur de votre passerelle client comme adresse source ou de destination plutôt que des point-to-point connexions.
   >
   > Pour plus d'informations sur la RFC 1918, consultez la section Allocation d'adresses pour les réseaux Internet privés.

7. (Facultatif) PourDevice (Appareil) Entrez un nom pour l'appareil qui héberge cette passerelle client.
8. Choisissez Créer la passerelle client.
9. Dans le volet de navigation, sélectionnez Connexions Site-to-Site VPN.
10. Choisissez Create VPN connection (Créer une connexion VPN).
11. (Facultatif) Dans le champ Name tag, saisissez le nom de votre connexion Site-to-Site VPN. Une identification est alors créée avec la clé `Name` et la valeur que vous spécifiez.
12. Pour Target gateway type (Type de passerelle cible), choisissez Transit gateway (Passerelle de transit). Ensuite, choisissez la passerelle de transit que vous avez identifiée précédemment.
13. Pour Customer gateway (Passerelle client), sélectionnez Existing (Existante). Sélectionnez ensuite la passerelle client que vous avez créée précédemment.

14. Sélectionnez une des options de routage en fonction de la prise en charge ou non de Border Gateway Protocol (BGP) par votre périphérique de passerelle client :

    - Si votre périphérique de passerelle client prend en charge BGP, choisissez Dynamique (nécessite BGP).
    - Si votre périphérique de passerelle client ne prend pas en charge BGP, choisissez Statique.
15. Pour la version Tunnel inside IP, spécifiez si les tunnels VPN prennent en charge le IPv6 trafic IPv4 ou le trafic.
16. (Facultatif) Si vous avez spécifié IPv4la version Tunnel inside IP, vous pouvez éventuellement spécifier les plages IPv4 CIDR pour la passerelle client et AWS les côtés autorisés à communiquer via les tunnels VPN. La valeur par défaut est `0.0.0.0/0`.

    Si vous avez spécifié IPv6la version Tunnel inside IP, vous pouvez éventuellement spécifier les plages IPv6 CIDR pour la passerelle client et AWS les côtés autorisés à communiquer via les tunnels VPN. La valeur par défaut pour les deux plages est `::/0`.
17. Pour le type d'adresse IP externe, choisissez PrivateIpv4.
18. Pour l'ID de pièce jointe de transport, choisissez la pièce jointe de passerelle de transit pour la Direct Connect passerelle appropriée.
19. Choisissez Create VPN connection (Créer une connexion VPN).

> **Note**
>
> L'option Enable acceleration (Activer l'accélération) n'est pas applicable aux connexions VPN sur Direct Connect.

Pour créer une passerelle client à l'aide de la ligne de commande ou de l'API

- CreateCustomerGateway(API de requête Amazon EC2)
- create-customer-gateway (AWS CLI)

Sécurité dans AWS Site-to-Site VPN

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez de centres de données et d'architectures réseau conçus pour répondre aux exigences des organisations les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit ceci comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud : AWS est responsable de la protection de l'infrastructure qui exécute AWS les services dans le AWS Cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Third-party les auditeurs testent et vérifient régulièrement l'efficacité de notre sécurité dans le AWS cadre des programmes de . Pour en savoir plus sur les programmes de conformité qui s'appliquent au AWS Site-to-Site VPN, consultez la section AWS Services concernés par le programme de conformité .
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris de la sensibilité de vos données, des exigences de votre entreprise, ainsi que de la législation et de la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation d' Site-to-Site un VPN. Les rubriques suivantes vous montrent comment configurer Site-to-Site un VPN pour atteindre vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser vos ressources Site-to-Site VPN.

Table des matières

Amélioré AWS Site-to-Site VPN fonctionnalités de sécurité à l'aide de Secrets Manager

La fonction Security Rebase d'AWS Site-to-Site VPN fournit des fonctionnalités de sécurité améliorées qui vous offrent un meilleur contrôle et une meilleure visibilité sur vos connexions VPN. L'une des principales améliorations réside dans la possibilité de stocker les clés pré-partagées (PSK) dans le service Site-to-Site VPN AWS Secrets Manager plutôt que directement dans celui-ci, ce qui permet une meilleure gestion des secrets et le respect des meilleures pratiques de sécurité. La fonctionnalité inclut également une `GetActiveVpnTunnelStatus` API qui fournit une visibilité en temps réel sur les paramètres de sécurité utilisés dans les tunnels VPN actifs, y compris les algorithmes de chiffrement, les algorithmes d'intégrité et les Diffie-Hellman groupes pour les deux phases IKE. En outre, vous pouvez désormais générer des configurations de sécurité recommandées qui imposent l'utilisation de protocoles modernes en excluant les options existantes telles que IKEv1. Ces améliorations sont particulièrement utiles si votre organisation doit maintenir des normes de sécurité strictes, nécessite des pistes d'audit détaillées de vos configurations VPN ou souhaite s'assurer que vos connexions VPN utilisent les protocoles les plus sécurisés disponibles.

Table des matières

Modifiez la clé pré-partagée de Secrets Manager dans AWS Site-to-Site VPN

Si votre tunnel n'est pas accessible dans Secrets Manager, vous pouvez modifier la clé pré-partagée pour ce tunnel.

> **Note**
>
> - Lorsque vous modifiez la clé pré-partagée, assurez-vous de disposer des autorisations IAM nécessaires pour le service Secrets Manager.
> - Après avoir modifié la clé pré-partagée d'un tunnel VPN, la connectivité est interrompue pendant plusieurs minutes. Assurez-vous de planifier les temps d'arrêt prévus.

Pour modifier la clé pré-partagée de Secrets Manager pour un tunnel VPN

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Connexions Site-to-Site VPN.
3. Sélectionnez la connexion Site-to-Site VPN, puis choisissez Actions, Modifier les options du tunnel VPN.
4. Pour Adresse IP externe du tunnel VPN, choisissez l'adresse IP du point de terminaison du tunnel VPN.
5. Dans la section Nouvelle clé pré-partagée, choisissez une nouvelle clé pré-partagée.

> **Note**
>
> Cette option n'est disponible que pour les clés stockées dans Secrets Manager.

6. Sélectionnez Enregistrer les modifications.
7. Répétez ces étapes pour tout autre tunnel.

Modifiez le mode de stockage des clés pré-partagées dans AWS Site-to-Site VPN

Modifiez le mode de stockage des clés pré-partagées pour un tunnel VPN existant.

> **Note**
>
> - Lorsque vous changez de mode de stockage, assurez-vous de disposer des autorisations IAM nécessaires pour les services Site-to-Site VPN et Secrets Manager.
> - Après avoir modifié le mode de stockage d'un tunnel VPN, la connectivité est interrompue pendant plusieurs minutes. Assurez-vous de planifier les temps d'arrêt prévus.

Pour modifier le mode de stockage des clés pré-partagées

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Connexions Site-to-Site VPN.
3. Sélectionnez la connexion Site-to-Site VPN, puis choisissez Actions, Modifier les options du tunnel VPN.

4. Pour Adresse IP externe du tunnel VPN, choisissez l'adresse IP du point de terminaison du tunnel VPN.
5. Dans la Pre-shared section Stockage des clés, choisissez l'un des types de stockage de clés pré-partagés suivants.
   - Standard : la clé pré-partagée est stockée directement dans le service Site-to-Site VPN.
   - Gestionnaire de secrets — La clé pré-partagée est stockée à l'aide AWS Secrets Manager de. Pour plus d'informations sur Secrets Manager, consultezFonctionnalités de sécurité améliorées à l'aide de Secrets Manager.
6. Sélectionnez Enregistrer les modifications.

Lorsque vous passez du mode de stockage de Secrets Manager à Standard :

- La clé pré-partagée est supprimée de Secrets Manager et déplacée vers le service Site-to-Site VPN.
- L'entrée du tunnel est supprimée du secret du Gestionnaire des secrets.

Lorsque vous passez du mode de stockage Standard au mode Secrets Manager :

- La clé pré-partagée est supprimée du Site-to-Site service VPN
- Un nouveau secret Secrets Manager est créé, s'il n'en existe pas déjà un.
- La nouvelle clé pré-partagée est stockée dans Secrets Manager.

Protection des données dans AWS Site-to-Site VPN

Le modèle de responsabilité AWS https://aws.amazon.com/compliance/shared-responsibility-model/ s'applique à la protection des données dans le AWS Site-to-Site VPN. Comme décrit dans ce modèle, AWS est responsable de la protection de l'infrastructure mondiale qui gère tous les AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez la FAQ sur la confidentialité des données et les conditions légales de la région . Pour plus d'informations sur la protection des données en Europe, consultez le Centre du règlement général sur la protection des données (RGPD).

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec AWS IAM Identity Center ou Gestion des identités et des accès AWS (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- SSL/TLS À utiliser pour communiquer avec AWS les ressources. Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation des activités des utilisateurs avec AWS CloudTrail. Pour plus d'informations sur l'utilisation des CloudTrail sentiers pour enregistrer AWS des activités, consultez la section Utilisation des CloudTrail sentiers dans le Guide de AWS CloudTrail l'utilisateur.
- Utilisez des solutions de AWS cryptage, ainsi que tous les contrôles de sécurité par défaut qui s'y trouvent Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-3 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour plus d'informations sur les points de terminaison FIPS disponibles, consultez Norme FIPS (Federal Information Processing Standard) 140-3.

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Nom. Cela inclut lorsque vous travaillez avec Site-to-Site un VPN ou autre à Services AWS l'aide de la console, de l'API ou des AWS kits de développement logiciel. AWS CLI Toutes les données que vous entrez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à ce serveur.

Confidentialité du trafic inter-réseau

Une connexion Site-to-Site VPN connecte en privé votre VPC à votre réseau local. Les données transférées entre votre VPC et votre réseau empruntent une connexion VPN chiffrée pour maintenir la confidentialité et l'intégrité des données en transit. Amazon prend en charge les connexions VPN

utilisant l'Internet Protocol Security (IPsec). IPsec est une suite de protocoles de sécurisation des communications IP par l'authentification et le chiffrement de chaque paquet IP d'un flux de données.

Chaque connexion Site-to-Site VPN se compose de deux tunnels VPN IPsec cryptés qui relient AWS votre réseau à votre réseau. Le trafic de chaque tunnel peut être chiffré avec AES128 ou AES256 et utiliser Diffie-Hellman des groupes pour l'échange de clés, garantissant ainsi une confidentialité avancée parfaite. AWS s'authentifie à l'aide des fonctions de hachage SHA1 ou SHA2.

Les instances de votre VPC ne nécessitent pas d'adresse IP publique pour se connecter aux ressources situées de l'autre côté de votre connexion Site-to-Site VPN. Les instances peuvent acheminer leur trafic Internet via la connexion Site-to-Site VPN vers votre réseau local. Elles peuvent ensuite accéder à Internet via vos points de trafic sortant existants, et vos dispositifs de sécurité et de surveillance réseau.

Pour plus d'informations, consultez les rubriques suivantes :

- Options de tunnel pour votre AWS Site-to-Site VPN connexion : fournit des informations sur les options IPSec et IKE (Internet Key Exchange) disponibles pour chaque tunnel.
- AWS Site-to-Site VPN options d'authentification du tunnel : fournit des informations sur les options d'authentification pour vos points de terminaison de tunnel VPN.
- Exigences relatives à un AWS Site-to-Site VPN Appareil de passerelle client : fournit des informations sur la configuration requise pour le périphérique de passerelle client de votre côté de la connexion VPN.
- Communication sécurisée entre les AWS Site-to-Site VPN connexions à l'aide d'un VPN CloudHub: Si vous disposez de plusieurs connexions Site-to-Site VPN, vous pouvez assurer une communication sécurisée entre vos sites locaux à l'aide du AWS VPN CloudHub.

Gestion des identités et des accès pour AWS Site-to-Site VPN

Gestion des identités et des accès AWS (IAM) permet à un Service AWS administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Les administrateurs IAM contrôlent qui peut être authentifié (connecté) et autorisé (possède des autorisations) à utiliser les ressources Site-to-Site VPN. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

- Public ciblé

- Authentification par des identités
- Gestion de l'accès à l'aide de politiques
- Comment ? AWS Site-to-Site Le VPN fonctionne avec IAM
- Identity-based exemples de politiques pour AWS Site-to-Site VPN
- Résolution des problèmes AWS Site-to-Site Identité et accès au VPN
- AWS politiques gérées pour les Site-to-Site VPN
- Utilisation de rôles liés à un service pour un VPN Site-to-Site

Public ciblé

La façon dont vous utilisez Gestion des identités et des accès AWS (IAM) varie en fonction de votre rôle :

- Utilisateur du service : demandez des autorisations à votre administrateur si vous ne pouvez pas accéder aux fonctionnalités (voir Résolution des problèmes AWS Site-to-Site Identité et accès au VPN)
- Administrateur du service : déterminez l'accès des utilisateurs et soumettez les demandes d'autorisation (voir Comment ? AWS Site-to-Site Le VPN fonctionne avec IAM)
- Administrateur IAM : rédigez des politiques pour gérer l'accès (voir Identity-based exemples de politiques pour AWS Site-to-Site VPN)

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identité. Vous devez être authentifié en tant qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

Vous pouvez vous connecter en tant qu'identité fédérée à l'aide d'informations d'identification provenant d'une source d'identité telle que AWS IAM Identity Center (IAM Identity Center), de l'authentification unique ou d'informations d'identification. Google/Facebook Pour plus d'informations sur la connexion, consultez Connexion à votre Compte AWS dans le Guide de l'utilisateur Connexion à AWS .

Pour l'accès par programmation, AWS fournit un SDK et une interface de ligne de commande pour signer les demandes de manière cryptographique. Pour plus d'informations, consultez Signature AWS Version 4 pour les demandes d'API dans le Guide de l'utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez avec une seule identité de connexion appelée utilisateur Compte AWS root qui dispose d'un accès complet à toutes Services AWS les ressources. Il est vivement déconseillé d'utiliser l'utilisateur racine pour vos tâches quotidiennes. Pour les tâches qui requièrent des informations d'identification de l'utilisateur racine, consultez Tâches qui requièrent les informations d'identification de l'utilisateur racine dans le Guide de l'utilisateur IAM.

Identité fédérée

Il est recommandé d'obliger les utilisateurs humains à utiliser la fédération avec un fournisseur d'identité pour accéder à l' Services AWS aide d'informations d'identification temporaires.

Une identité fédérée est un utilisateur de votre annuaire d'entreprise, de votre fournisseur d'identité Web ou Directory Service qui accède à l' Services AWS aide d'informations d'identification provenant d'une source d'identité. Les identités fédérées assument des rôles qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Pour plus d'informations, consultez Qu'est-ce que IAM Identity Center ? dans le Guide de l'utilisateur AWS IAM Identity Center .

Utilisateurs et groupes IAM

Un utilisateur IAM est une identité qui dispose d'autorisations spécifiques pour une seule personne ou application. Nous vous recommandons d'utiliser ces informations d'identification temporaires au lieu des utilisateurs IAM avec des informations d'identification à long terme. Pour plus d'informations, voir Exiger des utilisateurs humains qu'ils utilisent la fédération avec un fournisseur d'identité pour accéder à AWS l'aide d'informations d'identification temporaires dans le Guide de l'utilisateur IAM.

Les groupes IAM spécifient une collection d'utilisateurs IAM et permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Pour plus d'informations, consultez Cas d'utilisation pour les utilisateurs IAM dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une identité dotée d'autorisations spécifiques qui fournit des informations d'identification temporaires. Vous pouvez assumer un rôle en passant d'un rôle utilisateur à un rôle IAM (console) ou en appelant une opération AWS CLI ou AWS API. Pour plus d'informations, consultez Méthodes pour endosser un rôle dans le Guide de l'utilisateur IAM.

Les rôles IAM sont utiles pour l'accès des utilisateurs fédérés, les autorisations temporaires des utilisateurs IAM, les accès intercompte, les accès entre services et les applications exécutées sur Amazon EC2. Pour plus d'informations, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Gestion de l'accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique définit les autorisations lorsqu'elles sont associées à une identité ou à une ressource. AWS évalue ces politiques lorsqu'un directeur fait une demande. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations les documents de politique JSON, consultez Vue d'ensemble des politiques JSON dans le Guide de l'utilisateur IAM.

À l'aide de politiques, les administrateurs précisent qui a accès à quoi en définissant quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Un administrateur IAM crée des politiques IAM et les ajoute aux rôles, que les utilisateurs peuvent ensuite assumer. Les politiques IAM définissent les autorisations quelle que soit la méthode que vous utilisez pour exécuter l'opération.

Identity-based politiques

Identity-based les politiques sont des documents de politique d'autorisations JSON que vous associez à une identité (utilisateur, groupe ou rôle). Ces politiques contrôlent les actions que peuvent exécuter ces identités, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Définition d'autorisations IAM personnalisées avec des politiques gérées par le client dans le Guide de l'utilisateur IAM.

Identity-based les politiques peuvent être des politiques en ligne (intégrées directement dans une identité unique) ou des politiques gérées (politiques autonomes associées à plusieurs identités). Pour découvrir comment choisir entre des politiques gérées et en ligne, consultez Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

Resource-based politiques

Resource-based les politiques sont des documents de stratégie JSON que vous joignez à une ressource. Les exemples incluent les politiques de confiance de rôle IAM et les stratégies de

compartiment Amazon S3. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Vous devez spécifier un principal dans une politique basée sur les ressources.

Resource-based les politiques sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser les politiques AWS gérées par IAM dans une stratégie basée sur les ressources.

Autres types de politique

AWS prend en charge des types de politiques supplémentaires qui peuvent définir les autorisations maximales accordées par les types de politiques les plus courants :

- Limites d'autorisations : une limite des autorisations définit le nombre maximum d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM. Pour plus d'informations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.
- Politiques de contrôle des services (SCP) : spécifient les autorisations maximales pour une organisation ou une unité organisationnelle dans AWS Organizations. Pour plus d'informations, consultez Politiques de contrôle de service dans le Guide de l'utilisateur AWS Organizations .
- Politiques de contrôle des ressources (RCP) : définissent les autorisations maximales disponibles pour les ressources de votre organisation. Pour plus d'informations, consultez Politiques de contrôle des ressources (RCP) dans le Guide de l'utilisateur AWS Organizations .
- Politiques de session : politiques avancées que vous passez en tant que paramètre lorsque vous créez par programmation une session temporaire pour un rôle ou un utilisateur fédéré. Pour plus d'informations, consultez Politiques de session dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section Logique d'évaluation des politiques dans le guide de l'utilisateur IAM.

Comment ? AWS Site-to-Site Le VPN fonctionne avec IAM

Avant d'utiliser IAM pour gérer l'accès au Site-to-Site VPN, découvrez quelles fonctionnalités IAM peuvent être utilisées avec Site-to-Site le VPN.

Fonctionnalités IAM que vous pouvez utiliser avec AWS Site-to-Site VPN

Fonctionnalité IAM	Site-to-Site Prise en charge des VPN
Identity-based politiques	Oui
Resource-based politiques	Non
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition de politique (spécifiques au service)	Oui
ACL	Non
ABAC (étiquettes dans les politiques)	Non
Informations d'identification temporaires	Oui
Autorisations de principal	Oui
Rôles de service	Oui
Service-linked rôles	Oui

Pour obtenir une vue d'ensemble de la façon dont le Site-to-Site VPN et les autres AWS services fonctionnent avec la plupart des fonctionnalités IAM, consultez la section AWS Services qui fonctionnent avec IAM dans le Guide de l'utilisateur IAM.

Identity-based politiques relatives aux Site-to-Site VPN

Prend en charge les politiques basées sur l'identité : oui

Identity-based les politiques sont des documents de politique d'autorisations JSON que vous pouvez joindre à une identité, telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Définition d'autorisations IAM personnalisées avec des politiques gérées par le client dans le Guide de l'utilisateur IAM.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Pour découvrir tous les éléments que vous utilisez dans une politique JSON, consultez Références des éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

Identity-based exemples de politiques pour les Site-to-Site VPN

Pour consulter des exemples de politiques basées sur l'identité des Site-to-Site VPN, consultez. Identity-based exemples de politiques pour AWS Site-to-Site VPN

Resource-based politiques au sein du Site-to-Site VPN

Prend en charge les politiques basées sur les ressources : non

Resource-based les politiques sont des documents de stratégie JSON que vous joignez à une ressource. Par exemple, les politiques de confiance de rôle IAM et les politiques de compartiment Amazon S3 sont des politiques basées sur les ressources. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Pour permettre un accès intercompte, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une politique basée sur les ressources. Pour plus d'informations, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Actions politiques pour le Site-to-Site VPN

Prend en charge les actions de politique : oui

Les administrateurs peuvent utiliser des politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Intégration d'actions dans une politique afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour consulter la liste des actions Site-to-Site VPN, consultez la section Actions définies par le AWS Site-to-Site VPN dans la référence d'autorisation de service.

Les actions de politique dans le Site-to-Site VPN utilisent le préfixe suivant avant l'action :

```
ec2
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules.

```
"Action": [
      "ec2:action1",
      "ec2:action2"
         ]
```

Pour consulter des exemples de politiques basées sur l'identité des Site-to-Site VPN, consultez. Identity-based exemples de politiques pour AWS Site-to-Site VPN

Ressources politiques pour les Site-to-Site VPN

Prend en charge les ressources de politique : oui

Les administrateurs peuvent utiliser des politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

```
"Resource": "*"
```

Pour consulter la liste des types de ressources Site-to-Site VPN et de leurs ARN, consultez la section Ressources définies par le AWS Site-to-Site VPN dans la référence d'autorisation de service. Pour savoir avec quelles actions vous pouvez spécifier l'ARN de chaque ressource, consultez la section Actions définies par AWS Site-to-Site un VPN.

Pour consulter des exemples de politiques basées sur l'identité des Site-to-Site VPN, consultez. Identity-based exemples de politiques pour AWS Site-to-Site VPN

Clés de condition de politique pour le Site-to-Site VPN

Prend en charge les clés de condition de politique spécifiques au service : oui

Les administrateurs peuvent utiliser des politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Condition` indique à quel moment les instructions s'exécutent en fonction de critères définis. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande. Pour voir toutes les clés de condition AWS globales, consultez les clés contextuelles de conditions AWS globales dans le guide de l'utilisateur IAM.

Pour consulter la liste des clés de condition Site-to-Site VPN, consultez la section Clés de condition pour le AWS Site-to-Site VPN dans la référence d'autorisation de service. Pour savoir avec quelles actions et quelles ressources vous pouvez utiliser une clé de condition, consultez la section Actions définies par AWS Site-to-Site un VPN.

Pour consulter des exemples de politiques basées sur l'identité des Site-to-Site VPN, consultez. Identity-based exemples de politiques pour AWS Site-to-Site VPN

ACL dans un VPN Site-to-Site

Prend en charge les ACL : non

Les listes de contrôle d'accès (ACL) vérifie quels principaux (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

ABAC avec VPN Site-to-Site

Prise en charge d'ABAC (balises dans les politiques) : non

Attribute-based le contrôle d'accès (ABAC) est une stratégie d'autorisation qui définit les autorisations en fonction d'attributs appelés balises. Vous pouvez associer des balises aux entités et AWS ressources IAM, puis concevoir des politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à celle de la ressource.

Pour contrôler l'accès basé sur des étiquettes, vous devez fournir les informations d'étiquette dans l'élément de condition d'une politique utilisant les clés de condition `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`.

Si un service prend en charge les trois clés de condition pour tous les types de ressources, alors la valeur pour ce service est Oui. Si un service prend en charge les trois clés de condition pour certains types de ressources uniquement, la valeur est Partielle.

Pour plus d'informations sur ABAC, consultez Définition d'autorisations avec l'autorisation ABAC dans le Guide de l'utilisateur IAM. Pour accéder à un didacticiel décrivant les étapes de configuration de l'ABAC, consultez Utilisation du contrôle d'accès par attributs (ABAC) dans le Guide de l'utilisateur IAM.

Utiliser des informations d'identification temporaires avec Site-to-Site un VPN

Prend en charge les informations d'identification temporaires : oui

Les informations d'identification temporaires fournissent un accès de courte durée aux AWS ressources et sont automatiquement créées lorsque vous utilisez la fédération ou que vous changez de rôle. AWS recommande de générer dynamiquement des informations d'identification temporaires au lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez Informations d'identification de sécurité temporaires dans IAM et Services AWS compatibles avec IAM dans le Guide de l'utilisateur IAM.

Cross-service autorisations principales pour le Site-to-Site VPN

Prend en charge les sessions d'accès direct (FAS) : oui

Les sessions d'accès direct (FAS) utilisent les autorisations du principal appelant et Service AWS, combinées Service AWS à la demande d'envoi de demandes aux services en aval. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez la section Sessions de transmission d'accès.

Rôles de service pour le Site-to-Site VPN

Prend en charge les rôles de service : oui

Un rôle de service est un rôle IAM qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer un rôle de service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.

> **Warning**
>
> La modification des autorisations pour un rôle de service peut interrompre la fonctionnalité Site-to-Site VPN. Modifiez les rôles de service uniquement lorsque le Site-to-Site VPN fournit des instructions à cet effet.

Service-linked rôles pour le Site-to-Site VPN

Prend en charge les rôles liés à un service : oui

Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut assumer le rôle d'effectuer une action en votre nom. Service-linked les rôles apparaissent dans votre compte Compte AWS et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

Pour plus d'informations sur la création ou la gestion des rôles liés à un service, consultez Services AWS qui fonctionnent avec IAM. Recherchez un service dans le tableau qui inclut un `Yes` dans la colonne des Service-linked rôles. Choisissez le lien Oui pour consulter la documentation du rôle lié à ce service.

Identity-based exemples de politiques pour AWS Site-to-Site VPN

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier des ressources Site-to-Site VPN. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM.

Pour apprendre à créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de politique JSON, consultez Création de politiques IAM (console) dans le Guide de l'utilisateur IAM.

Pour plus de détails sur les actions et les types de ressources définis par le Site-to-Site VPN, y compris le format des ARN pour chacun des types de ressources, consultez la section Actions, ressources et clés de condition pour le AWS Site-to-Site VPN dans la référence d'autorisation de service.

Rubriques

- Bonnes pratiques en matière de politiques
- Utilisation de la console Site-to-Site VPN
- Décrire des connexions Site-to-Site VPN spécifiques

- Créez et décrivez les ressources nécessaires pour AWS Site-to-Site VPN connexion

Bonnes pratiques en matière de politiques

Identity-based les politiques déterminent si quelqu'un peut créer des ressources Site-to-Site VPN sur votre compte, y accéder ou les supprimer. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations avec le moindre privilège — Pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par le AWS client qui sont spécifiques à vos cas d'utilisation. Pour plus d'informations, consultez politiques gérées par AWS ou politiques gérées par AWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.
- Accordez les autorisations de moindre privilège : lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l'exécution d'une seule tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation d'IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.
- Utilisez des conditions dans les politiques IAM pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un outil spécifique Service AWS, tel que CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez l'Analyseur d'accès IAM pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : l'Analyseur d'accès IAM valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez Validation de politiques avec IAM Access Analyzer dans le Guide de l'utilisateur IAM.

- Exiger une authentification multifacteur (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root Compte AWS, activez l'authentification multifacteur pour renforcer la sécurité. Pour exiger la MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Sécurisation de l'accès aux API avec MFA dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les bonnes pratiques dans IAM, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.

Utilisation de la console Site-to-Site VPN

Pour accéder à la console AWS Site-to-Site VPN, vous devez disposer d'un ensemble minimum d'autorisations. Ces autorisations doivent vous permettre de répertorier et d'afficher les détails des ressources Site-to-Site VPN de votre Compte AWS. Si vous créez une politique basée sur l'identité qui est plus restrictive que l'ensemble minimum d'autorisations requis, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs ou rôles) tributaires de cette politique.

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement l'API AWS CLI ou l' AWS API. Autorisez plutôt l'accès à uniquement aux actions qui correspondent à l'opération d'API qu'ils tentent d'effectuer.

Pour vous assurer que les utilisateurs et les rôles peuvent toujours utiliser la console Site-to-Site VPN, associez également le Site-to-Site VPN `AmazonVPCFullAccess` ou la politique `AmazonVPCReadOnlyAccess` AWS gérée aux entités. Pour plus d'informations, consultez Ajout d'autorisations à un utilisateur dans le Guide de l'utilisateur IAM.

Décrire des connexions Site-to-Site VPN spécifiques

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "ec2:DescribeVpnConnections"
         ],
         "Resource": ["*"]
```

```
      }
   ]
}
```

Créez et décrivez les ressources nécessaires pour AWS Site-to-Site VPN connexion

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
         "ec2:DescribeVpnConnections",
         "ec2:DescribeVpnGateways",
         "ec2:DescribeCustomerGateways",
         "ec2:CreateCustomerGateway",
         "ec2:CreateVpnGateway",
         "ec2:CreateVpnConnection"
         ],
         "Resource": [
            "*"
         ]
      },
   {
         "Effect": "Allow",
         "Action": "iam:CreateServiceLinkedRole",
         "Resource": "arn:aws:iam::*:role/aws-service-role/s2svpn.amazonaws.com/
AWSServiceRoleForVPCS2SVPNInternal",
         "Condition": {
            "StringLike": {
               "iam:AWSServiceName":"s2svpn.amazonaws.com"
            }
         }
      }
   ]
}
```

Résolution des problèmes AWS Site-to-Site Identité et accès au VPN

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec Site-to-Site un VPN et IAM.

Rubriques

Je ne suis pas autorisé à effectuer une action dans un Site-to-Site VPN

Si vous recevez une erreur qui indique que vous n'êtes pas autorisé à effectuer une action, vos politiques doivent être mises à jour afin de vous permettre d'effectuer l'action.

L'exemple d'erreur suivant se produit quand l'utilisateur IAM `mateojackson` tente d'utiliser la console pour afficher des informations détaillées sur une ressource *`my-example-widget`* fictive, mais ne dispose pas des autorisations `ec2:`*`GetWidget`* fictives.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 ec2:GetWidget on resource: my-example-widget
```

Dans ce cas, la politique qui s'applique à l'utilisateur `mateojackson` doit être mise à jour pour autoriser l'accès à la ressource *`my-example-widget`* à l'aide de l'action `ec2:`*`GetWidget`*.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je ne suis pas autorisé à effectuer iam : PassRole

Si vous recevez un message d'erreur indiquant que vous n'êtes pas autorisé à effectuer l'`iam:PassRole`action, vos politiques doivent être mises à jour pour vous permettre de transmettre un rôle au Site-to-Site VPN.

Certains vous Services AWS permettent de transmettre un rôle existant à ce service au lieu de créer un nouveau rôle de service ou un rôle lié à un service. Pour ce faire, vous devez disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un utilisateur IAM nommé `marymajor` essaie d'utiliser la console pour effectuer une action dans le Site-to-Site VPN. Toutefois, l'action nécessite que le service ait des autorisations accordées par un rôle de service. Mary n'est pas autorisée à transmettre le rôle au service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dans ce cas, les politiques de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je souhaite autoriser des personnes extérieures à mon Compte AWS pour accéder à mes ressources Site-to-Site VPN

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACL), vous pouvez utiliser ces politiques pour donner l'accès à vos ressources.

Pour plus d'informations, consultez les éléments suivants :

- Pour savoir si le Site-to-Site VPN prend en charge ces fonctionnalités, consultezComment ? AWS Site-to-Site Le VPN fonctionne avec IAM.
- Pour savoir comment donner accès à vos ressources par l'intermédiaire de celles Comptes AWS que vous possédez, consultez la section Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS qui vous appartient dans le Guide de l'utilisateur IAM.
- Pour savoir comment donner accès à vos ressources à des tiers Comptes AWS, consultez la section Fournir un accès à des ressources Comptes AWS détenues par des tiers dans le Guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez Fournir un accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le Guide de l'utilisateur IAM.

- Pour en savoir plus sur la différence entre l'utilisation des rôles et des politiques basées sur les ressources pour l'accès intercompte, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

AWS politiques gérées pour les Site-to-Site VPN

Pour ajouter des autorisations aux utilisateurs, aux groupes et aux rôles, il est plus facile d'utiliser des politiques AWS gérées que de rédiger vous-même des politiques. Il faut du temps et de l'expertise pour créer des politiques gérées par le client IAM qui ne fournissent à votre équipe que les autorisations dont elle a besoin. Pour démarrer rapidement, vous pouvez utiliser nos politiques AWS gérées. Ces politiques couvrent les cas d'utilisation courants et sont disponibles sur votre AWS compte. Pour plus d'informations sur les politiques AWS gérées, consultez les politiques AWS gérées dans le Guide de l'utilisateur IAM.

AWS les services maintiennent et mettent à jour les politiques AWS gérées. Vous ne pouvez pas modifier les autorisations dans les politiques AWS gérées. Les services ajoutent occasionnellement des autorisations à une politique gérée par AWS pour prendre en charge de nouvelles fonctionnalités. Ce type de mise à jour affecte toutes les identités (utilisateurs, groupes et rôles) auxquelles la politique est attachée. Les services sont très susceptibles de mettre à jour une politique gérée par AWS quand une nouvelle fonctionnalité est lancée ou quand de nouvelles opérations sont disponibles. Les services ne suppriment pas les autorisations d'une politique AWS gérée, de sorte que les mises à jour des politiques n'interrompront pas vos autorisations existantes.

En outre, AWS prend en charge les politiques gérées pour les fonctions qui couvrent plusieurs services. Par exemple, la politique `ReadOnlyAccess` AWS gérée fournit un accès en lecture seule à tous les AWS services et ressources. Lorsqu'un service lance une nouvelle fonctionnalité, AWS ajoute des autorisations en lecture seule pour les nouvelles opérations et ressources. Pour obtenir la liste des politiques de fonctions professionnelles et leurs descriptions, consultez la page politiques gérées par AWS pour les fonctions de tâche dans le Guide de l'utilisateur IAM.

AWS stratégie gérée : AWSVPCS2SVpnServiceRolePolicy

Vous pouvez associer la politique `AWSVPCS2SVpnServiceRolePolicy` à vos identités IAM. Cette politique permet au Site-to-Site VPN de gérer un AWS Secrets Manager secret au sein du Site-to-Site VPN. Pour de plus amples informations, veuillez consulter the section called "Utilisation des rôles liés à un service".

Pour voir les autorisations de cette stratégie, consultez AWSVPCS2SVpnServiceRolePolicy dans le AWS Guide de référence des stratégies gérées par.

Site-to-Site Mises à jour du VPN pour AWS stratégies gérées

Consultez les détails des mises à jour des politiques AWS gérées pour les Site-to-Site VPN depuis que ce service a commencé à suivre ces changements en mai 2025.

Modifier	Description	Date
AWSVPCS2SVpnServiceRolePolicy- Politique mise à jour.	De nouvelles autorisations ont été ajoutées à la politique permettant au Site-to-Site VPN de gérer le secret AWS Secrets Manager `s2svpn` géré de la connexion VPN.	14 mai 2025

Utilisation de rôles liés à un service pour un VPN Site-to-Site

AWS Site-to-Site Le VPN utilise des Gestion des identités et des accès AWS rôles liés aux services (IAM). Un rôle lié à un service est un type unique de rôle IAM directement lié au VPN. Site-to-Site Service-linked les rôles sont prédéfinis par le Site-to-Site VPN et incluent toutes les autorisations dont le service a besoin pour appeler d'autres AWS services en votre nom.

Un rôle lié à un service facilite la configuration du Site-to-Site VPN car vous n'avez pas à ajouter manuellement les autorisations nécessaires. Site-to-Site Le VPN définit les autorisations de ses rôles liés aux services et, sauf indication contraire, seul le Site-to-Site VPN peut assumer ses rôles. Les autorisations définies comprennent la politique de confiance et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

Vous pouvez supprimer un rôle lié à un service uniquement après la suppression préalable de ses ressources connexes. Cela protège les ressources de votre Site-to-Site VPN car vous ne pouvez pas supprimer par inadvertance l'autorisation d'accéder à ces ressources.

Service-linked autorisations de rôle pour le Site-to-Site VPN

Site-to-Site Le VPN utilise le rôle lié à un service nommé « AWSServiceRoleForVPCS2SVPN Autoriser le Site-to-Site VPN à créer et à gérer des ressources liées à vos connexions VPN ».

Le rôle AWSServiceRoleForVPCS2SVPN lié à un service fait confiance au service suivant pour assumer le rôle :

- `s2svpn.amazonaws.com`

Ce rôle lié à un service utilise la politique gérée AWSVPCS2SVpnServiceRolePolicy pour effectuer les actions suivantes sur les ressources spécifiées :

- Lorsque vous utilisez l'authentification par certificat pour votre connexion VPN, AWS Site-to-Site VPN exporte les AWS Certificate Manager certificats du tunnel VPN pour les utiliser sur les points de terminaison du tunnel VPN.
- Lorsque vous utilisez l'authentification par certificat pour votre connexion VPN, AWS Site-to-Site VPN gère le renouvellement des AWS Certificate Manager certificats du tunnel VPN.
- Lorsque vous utilisez un stockage de clés SecretsManager pré-partagé pour votre connexion VPN, AWS Site-to-Site VPN gère le secret géré AWS Secrets Manager s2svpn de la connexion VPN.

Pour voir les autorisations de cette stratégie, consultez AWSVPCS2SVpnServiceRolePolicy dans le AWS Guide de référence des stratégies gérées par.

Création d'un rôle lié à un service pour le VPN Site-to-Site

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous créez une passerelle client avec un certificat privé ACM associé dans l'API Console de gestion AWS, l'API ou l' AWS API AWS CLI, le Site-to-Site VPN crée le rôle lié au service pour vous.

Si vous supprimez ce rôle lié à un service et que vous avez ensuite besoin de le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte. Lorsque vous créez une passerelle client avec un certificat privé ACM associé, le Site-to-Site VPN crée à nouveau le rôle lié au service pour vous.

Modifier un rôle lié à un service pour un VPN Site-to-Site

Site-to-Site Le VPN ne vous permet pas de modifier le rôle AWSServiceRoleForVPCS2SVPN lié au service. Après avoir créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence à ce rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour plus d'informations, consultez la section Modification d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Supprimer un rôle lié à un service pour un VPN Site-to-Site

Si vous n'avez plus besoin d'utiliser une fonctionnalité ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, vous n'avez aucune entité inutilisée qui n'est pas surveillée ou gérée activement. Cependant, vous devez nettoyer les ressources de votre rôle lié à un service avant de pouvoir les supprimer manuellement.

> **Note**
>
> Si le service Site-to-Site VPN utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression risque d'échouer. Si cela se produit, patientez quelques minutes et réessayez.

Pour supprimer les ressources Site-to-Site VPN utilisées par AWSServiceRoleForVPCS2SVPN

Vous ne pouvez supprimer ce rôle lié à un service qu'après avoir supprimé toutes les passerelles client qui ont un certificat privé ACM associé. Cela garantit que vous ne pouvez pas supprimer par inadvertance l'autorisation d'accéder à vos certificats ACM utilisés par Site-to-Site les connexions VPN.

Pour supprimer manuellement le rôle lié à un service à l'aide d'IAM

Utilisez la console IAM AWS CLI, l'API ou l' AWS API pour supprimer le rôle lié au AWSServiceRoleForVPCS2SVPN service. Pour plus d'informations, consultez la section Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Résilience dans AWS Site-to-Site VPN

L'infrastructure AWS mondiale est construite autour des AWS régions et des zones de disponibilité. AWS Les régions fournissent plusieurs zones de disponibilité physiquement séparées et isolées, qui

sont connectées à un réseau à faible latence, haut débit et hautement redondant. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone à l'autre sans interruption. Les zones de disponibilité sont davantage disponibles, tolérantes aux pannes et ont une plus grande capacité de mise à l'échelle que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour plus d'informations sur AWS les régions et les zones de disponibilité, consultez la section Infrastructure AWS globale.

Outre l'infrastructure AWS mondiale, le Site-to-Site VPN propose des fonctionnalités qui vous aident à répondre à vos besoins en matière de résilience et de sauvegarde des données.

Deux tunnels par connexion VPN

Une connexion Site-to-Site VPN se compose de deux tunnels, chacun se terminant dans une zone de disponibilité différente, afin de fournir une disponibilité accrue à votre VPC. En cas de panne de l'appareil AWS, votre connexion VPN bascule automatiquement vers le deuxième tunnel afin que votre accès ne soit pas interrompu. De temps à autre, effectue AWS également une maintenance de routine de votre connexion VPN, ce qui peut désactiver brièvement l'un des deux tunnels de votre connexion VPN. Pour de plus amples informations, veuillez consulter AWS Site-to-Site VPN remplacement des extrémités des tunnels. Lorsque vous configurez votre passerelle client, il est donc important de configurer les deux tunnels.

Redondance

Pour vous protéger contre une perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une deuxième connexion Site-to-Site VPN. Pour plus d'informations, consultez la documentation suivante :

- Redondant AWS Site-to-Site VPN connexions pour basculement
- Amazon Virtual Private Cloud Connectivity Options
- Création d'une infrastructure Multi-VPC AWS réseau évolutive et sécurisée

Sécurité de l'infrastructure dans AWS Site-to-Site VPN

En tant que service géré, le AWS Site-to-Site VPN est protégé par la sécurité du réseau AWS mondial. Pour plus d'informations sur les services AWS de sécurité et la manière de AWS protéger l'infrastructure, consultez AWS Cloud Security. Pour concevoir votre AWS environnement en utilisant

les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section Protection de l'infrastructure dans Security Pillar AWS Well-Architected Framework.

Vous utilisez des appels d'API AWS publiés pour accéder au Site-to-Site VPN via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Protocole TLS (Transport Layer Security). Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Suites de chiffrement avec une confidentialité directe parfaite (PFS) telles que DHE (Ephemeral) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Diffie-Hellman La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

Surveillance et AWS Site-to-Site VPN connexion

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité et des performances de votre AWS Site-to-Site VPN connexion. Vous devez recueillir les données de surveillance de toutes les parties de votre solution de telle sorte que vous puissiez déboguer plus facilement un éventuelle défaillance multipoint. Avant de commencer à surveiller votre connexion Site-to-Site VPN, vous devez toutefois créer un plan de surveillance qui inclut les réponses aux questions suivantes :

- Quels sont les objectifs de la surveillance ?
- Quelles sont les ressources à surveiller ?
- À quelle fréquence les ressources doivent-elles être surveillées ?
- Quels outils de surveillance utiliser ?
- Qui exécute les tâches de supervision ?
- Qui doit être informé en cas de problème ?

L'étape suivante consiste à établir une référence de performances normales d'un VPN dans votre environnement, en mesurant la performance à divers moments et dans diverses conditions de charge. Lorsque vous surveillez votre VPN, conservez les données d'historique de surveillance afin de pouvoir les comparer aux données de performances actuelles, d'identifier les modèles de performances normales et les anomalies de performances, et de concevoir des méthodes pour résoudre les problèmes.

Pour établir une référence, vous devez superviser les éléments suivants :

- L'état de vos tunnels VPN
- Données entrant dans le tunnel
- Données sortant du tunnel

Rubriques

Outils de surveillance

AWS fournit différents outils que vous pouvez utiliser pour surveiller une connexion Site-to-Site VPN. Vous pouvez configurer certains outils pour qu'ils effectuent la supervision automatiquement, tandis que d'autres nécessitent une intervention manuelle. Nous vous recommandons d'automatiser le plus possible les tâches de supervision.

Outils de surveillance automatique

Vous pouvez utiliser les outils de surveillance automatique suivants pour surveiller une connexion Site-to-Site VPN et signaler tout problème :

- Amazon CloudWatch Alarms : surveillez une seule métrique sur une période que vous spécifiez et effectuez une ou plusieurs actions en fonction de la valeur de la métrique par rapport à un seuil donné sur un certain nombre de périodes. L'action est une notification envoyée à une rubrique Amazon SNS. CloudWatch les alarmes n'appellent pas d'actions simplement parce qu'elles se trouvent dans un état particulier ; l'état doit avoir changé et être maintenu pendant un certain nombre de périodes. Pour de plus amples informations, veuillez consulter Surveillez AWS Site-to-Site VPN les tunnels à l'aide d'Amazon CloudWatch.
- AWS CloudTrail Surveillance des journaux : partagez les fichiers journaux entre les comptes, surveillez les fichiers CloudTrail CloudWatch journaux en temps réel en les envoyant à Logs, écrivez des applications de traitement des journaux en Java et vérifiez que vos fichiers journaux n'ont pas changé après leur livraison par CloudTrail. Pour plus d'informations, consultez les sections Utilisation des appels d'API de journalisation AWS CloudTrail dans le manuel de référence des API Amazon EC2 et Utilisation de fichiers CloudTrail journaux dans le guide de l'AWS CloudTrail utilisateur.
- AWS Health événements — Recevez des alertes et des notifications relatives aux modifications de l'état de santé de vos tunnels Site-to-Site VPN, aux recommandations de configuration des meilleures pratiques ou à l'approche des limites de dimensionnement. Utilisez les événements du Personal Health Dashboard pour déclencher des basculements automatisés, réduire les délais de dépannage ou optimiser les connexions pour une haute disponibilité. Pour de plus amples informations, veuillez consulter AWS Health et AWS Site-to-Site VPN événements.

Outils de surveillance manuelle

Un autre élément important de la surveillance d'une connexion Site-to-Site VPN consiste à surveiller manuellement les éléments non couverts par les CloudWatch alarmes. Les tableaux de bord

Amazon VPC et CloudWatch console fournissent une at-a-glance vue d'ensemble de l'état de votre environnement. AWS

> **Note**
>
> Dans la console Amazon VPC, les paramètres d'état du tunnel Site-to-Site VPN, tels que « Status » et « Dernière modification de statut », peuvent ne pas refléter des changements d'état transitoires ou des battements de tunnel momentanés. Il est recommandé d'utiliser des CloudWatch métriques et des journaux pour les mises à jour détaillées des modifications de l'état des tunnels.

- Le tableau de bord Amazon VPC affiche les éléments suivants :
  - Intégrité du service par région
  - Site-to-Site Connexions VPN
  - État du tunnel VPN (dans le volet de navigation, choisissez Connexions Site-to-Site VPN, sélectionnez une connexion Site-to-Site VPN, puis choisissez Détails du tunnel)
- La page d' CloudWatch accueil indique :
  - Alarmes et statuts en cours
  - Graphiques des alarmes et des ressources
  - Statut d'intégrité du service

  En outre, vous pouvez CloudWatch effectuer les opérations suivantes :
  - Créer des tableaux de bord personnalisés pour surveiller les services de votre choix
  - Représenter graphiquement les données de métriques pour résoudre les problèmes et découvrir les tendances
  - Recherchez et parcourez tous les indicateurs de vos AWS ressources
  - Créer et modifier des alarmes pour être informé des problèmes

AWS Site-to-Site VPN journaux

AWS Site-to-Site VPN les journaux vous offrent une meilleure visibilité sur vos déploiements Site-to-Site VPN. Grâce à cette fonctionnalité, vous avez accès aux journaux de connexion Site-to-Site VPN qui fournissent des informations sur l'établissement du tunnel de sécurité IP (IPsec), les négociations

relatives à l'échange de clés Internet (IKE), les messages du protocole de détection des pairs morts (DDP), l'état du protocole Border Gateway (BGP) et les mises à jour du routage.

Site-to-Site Les journaux VPN peuvent être publiés sur Amazon CloudWatch Logs. Cette fonctionnalité fournit aux clients un moyen unique et cohérent d'accéder aux journaux détaillés de toutes leurs connexions Site-to-Site VPN et de les analyser.

Rubriques

Avantages des journaux Site-to-Site VPN

- Résolution des problèmes VPN simplifiés : les journaux Site-to-Site VPN vous aident à identifier les incohérences de configuration entre AWS le dispositif de passerelle de votre client et à résoudre les problèmes de connectivité VPN initiaux. Les connexions VPN peuvent échouer par intermittence au fil du temps en raison de paramètres mal configurés (tels que des délais d'expiration mal réglés), des problèmes peuvent se produire dans les réseaux de transport sous-jacents (comme la météo Internet), ou des modifications de routage/défaillances de chemin peuvent interrompre la connectivité au VPN. Cette fonctionnalité vous permet de diagnostiquer avec précision la cause des défaillances de connexion intermittentes et d'affiner la configuration du tunnel de bas niveau pour assurer la fiabilité du fonctionnement.
- AWS Site-to-Site VPN Visibilité centralisée : les journaux Site-to-Site VPN peuvent fournir des journaux d'activité du tunnel et de routage BGP pour tous les types de connexions Site-to-Site VPN. Cette fonctionnalité fournit aux clients un moyen unique et cohérent d'accéder aux journaux détaillés de toutes leurs connexions Site-to-Site VPN et de les analyser.
- Sécurité et conformité : les journaux Site-to-Site VPN peuvent être envoyés à Amazon CloudWatch Logs pour une analyse rétrospective de l'état et de l'activité de la connexion VPN au fil du temps. Cela peut vous aider à respecter les exigences réglementaires et de conformité.

Politique relative CloudWatch aux ressources et restrictions relatives à la taille d'Amazon Logs

CloudWatch Les politiques relatives aux ressources des journaux sont limitées à 5 120 caractères. Lorsque CloudWatch Logs détecte qu'une politique approche cette limite de taille, elle active automatiquement les groupes de journaux commençant par`/aws/vendedlogs/`. Lorsque vous activez la journalisation, le Site-to-Site VPN doit mettre à jour votre politique de ressources de CloudWatch journaux avec le groupe de journaux que vous spécifiez. Pour éviter d'atteindre la limite de taille de la politique des CloudWatch journaux, préfixez les noms de vos groupes de journaux par`/aws/vendedlogs/`.

Site-to-Site Contenu du journal VPN

Les informations suivantes sont incluses dans le journal d'activité du tunnel Site-to-Site VPN. Le nom du fichier journal utilise les VpnConnection identifiants ID et TunnelOutsideIPAddress.

Champ	Description
VpnLogCreationTimestamp (`event_timestamp`)	Horodatage de création du journal au format epoch time.
VpnLogCreationTimestampReadable (`timestamp`)	Horodatage de création du journal au format temporel lisible par l'homme.
Tunnel DPDEnabled (`dpd_enabled`)	Statut d'activation du protocole Dead Peer Detection (True/False).
CGWNATTDetectionÉtat du tunnel (`nat_t_detected`)	Détection de NAT-T sur l'appareil de passerelle client (True/False).
IKEPhase1État du tunnel (`ike_phase1_state`)	État du protocole IKE en phase 1 (Established | Rekeying | Negotiating | Down).
IKEPhase2État du tunnel (`ike_phase2_state`)	État du protocole IKE en phase 2 (Established | Rekeying | Negotiating | Down).
VpnLogDetail (`details`)	Messages détaillés pour IPsec les protocoles IKE et DDP.

Les informations suivantes sont incluses dans le journal BGP du tunnel Site-to-Site VPN. Le nom du fichier journal utilise les VpnConnection identifiants ID et TunnelOutsideIPAddress.

Champ	Description
identifiant_ressource	Un identifiant unique pour identifier le tunnel et la connexion VPN à laquelle le journal est associé.
event_timestamp	Horodatage de création du journal au format epoch time.
timestamp	Horodatage de création du journal au format temporel lisible par l'homme.
type	Type d'événement du journal BGP (BGPStatus | RouteStatus).
status	mise à jour du statut pour un type spécifiqu e d'événement de journal (BGPStatus: UP | DOWN) (RouteStatus: ANNONCÉ {l'itinér aire a été annoncé par le pair} | MIS À JOUR : {l'itinéraire existant a été mis à jour par le pair} | RETIRÉ : {l'itinéraire a été retiré par le pair}).
message	Fournit des informations supplémentaires sur l'événement et le statut du journal. Ce champ vous aidera à comprendre pourquoi les BGPStatus attributs de route échangés dans le RouteStatus message sont en panne.

Table des matières

- Messages d'état de l'itinéraire

IKEv1 Messages d'erreur

Message	Explication
Le pair ne répond pas – Déclarer le pair mort	Le pair n'a pas répondu aux messages DDP, ce qui a imposé une action de temporisation de DDP.
AWS le déchiffrement de la charge utile du tunnel a échoué en raison d'une clé pré-partagée non valide	La même clé pré-partagée doit être configurée sur les deux pairs IKE.
Aucune proposition correspondante n'a été trouvée par AWS	Les attributs proposés pour la phase 1 (chiffrement, hachage et groupe DH) ne sont pas pris en charge par le point de terminaison VPN AWS, 3DES par exemple.
Aucune proposition correspondante trouvée. Notifier avec « Aucune proposition choisie »	Le message d'erreur No Proposal Chosen est échangé entre pairs pour indiquer que la configuration correcte Proposals/Policies doit être configurée pour la phase 2 sur les homologues IKE.
AWS tunnel a reçu DELETE pour la phase 2 SA avec SPI : xxxx	CGW a envoyé le message Delete_SA pour la phase 2.
AWS le tunnel a reçu la commande DELETE pour IKE_SA de la part de CGW	CGW a envoyé le message Delete_SA pour la phase 1.

IKEv2 Messages d'erreur

Message	Explication
AWS le délai imparti au tunnel DDP a expiré après les retransmissions de {retry_count}	Le pair n'a pas répondu aux messages DDP, ce qui a imposé une action de temporisation de DDP.
AWS le tunnel a reçu la commande DELETE pour IKE_SA de la part de CGW	Peer a envoyé le message Delete_SA pour Parent/IKE_SA.
AWS tunnel a reçu DELETE pour la phase 2 SA avec SPI : xxxx	Peer a envoyé le message Delete_SA pour CHILD_SA.
AWS le tunnel a détecté une collision (CHILD_REKEY) en tant que CHILD_DELETE	CGW a envoyé le message Delete_SA pour la SA active, dont la clé est en cours de changement.
AWS le SA redondant du tunnel (CHILD_SA) est supprimé en raison d'une collision détectée	En raison d'une collision, si des redondants SAs sont générés, les pairs fermeront le SA redondant après avoir fait correspondre les valeurs de nonce conformément à la RFC.
AWS la phase 2 du tunnel n'a pas pu être établie tout en maintenant la phase 1	Le pair n'a pas pu établir CHILD_SA en raison d'une erreur de négociation, par exemple d'une proposition incorrecte.
AWS : sélecteur de trafic : TS_UNACCE PTABLE : reçu du répondeur	Le pair a proposé un Selectors/Encryption domaine de trafic incorrect. Les pairs doivent être configurés de manière identique et correcte CIDRs.
AWS le tunnel envoie AUTHENTICATION_FAI LED comme réponse	Le pair ne peut pas authentifier le pair en vérifiant le contenu du message IKE_AUTH
AWS le tunnel a détecté une incompatibilité de clé pré-partagée avec cgw : xxxx	La même clé pré-partagée doit être configurée sur les deux pairs IKE.

Message	Explication
AWS délai d'expiration du tunnel : suppression de la phase 1 non établie IKE_SA avec cgw : xxxx	La suppression de IKE_SA à moitié ouvert en tant que pair n'a pas donné lieu à des négociations
Aucune proposition correspondante trouvée. Notifier avec « Aucune proposition choisie »	Le message d'erreur « Aucune proposition choisie » est échangé entre les pairs pour informer que des propositions correctes doivent être configurées sur les pairs IKE.
Aucune proposition correspondante n'a été trouvée par AWS	Les attributs proposés pour la phase 1 ou la phase 2 (chiffrement, hachage et groupe DH) ne sont pas pris en charge par le point de terminaison AWS VPN, `3DES` par exemple.

IKEv2 Messages de négociation

Message	Explication
AWS demande traitée par tunnel (id=xxx) pour CREATE_CHILD_SA	AWS a reçu la demande CREATE_CHILD_SA de CGW.
AWS le tunnel envoie une réponse (id=xxx) pour CREATE_CHILD_SA	AWS envoie une réponse CREATE_CHILD_SA à CGW.
AWS le tunnel envoie une demande (id=xxx) pour CREATE_CHILD_SA	AWS envoie une demande CREATE_CHILD_SA à CGW.
AWS réponse traitée par tunnel (id=xxx) pour CREATE_CHILD_SA	AWS a reçu une réponse CREATE_CHILD_SA de CGW.

Messages d'état BGP

Les messages d'état BGP contiennent des informations relatives aux transitions d'état des sessions BGP, aux avertissements relatifs aux limites de préfixes, aux violations des limites, aux notifications

de session BGP, aux messages BGP OPEN et aux mises à jour d'attributs pour un voisin BGP pour une session BGP donnée.

Message	État du BGP	Explication
L'état de la session BGP du pair AWS est passé de Idle à Connect with neighbor {ip : xxx}	VERS LE BAS	L'état de la connexion BGP côté AWS a été mis à jour pour devenir Connect.
L'état de la session BGP du pair côté AWS est passé de Connect à OpenSent with neighbor {ip : xxx}	VERS LE BAS	L'état de la connexion BGP du côté AWS a été mis à jour à OpenSent.
L'état de la session BGP du pair côté AWS est passé de OpenSent à OpenConfirm avec voisin {ip : xxx}	VERS LE BAS	L'état de la connexion BGP du côté AWS a été mis à jour à OpenConfirm.
L'état de la session BGP du pair côté AWS est passé de OpenConfirm à Établi avec le voisin {ip : xxx}	EN HAUT	L'état de la connexion BGP du côté AWS a été mis à jour à Established.
L'état de la session BGP du pair AWS est passé de Établi à Inactif avec le voisin {ip : xxx}	VERS LE BAS	L'état de la connexion BGP côté AWS a été mis à jour à Idle.
L'état de la session BGP du pair côté AWS est passé de Connect à Active with neighbor {ip : xxx}	VERS LE BAS	L'état de connexion BGP du côté AWS est passé de Connect à Active. Vérifiez la disponibilité du port TCP 179 sur CGW si la session BGP est bloquée dans l'état Connect.

Message	État du BGP	Explication
Un homologue côté AWS signale un avertissement relatif à la limite maximale de préfixes : {prefixes (count) : xxx} préfixes reçus du voisin {ip : xxx}, la limite est {limit (numeric) : xxx}	EN HAUT	Le côté AWS génère régulièrement un message de journal lorsque le nombre de préfixes reçus du CGW approche de la limite autorisée.
Le pair AWS a détecté que la limite maximale de préfixes était dépassée. Il a reçu {prefixes (count) : xxx} préfixes du voisin {ip : xxx}, la limite est {limit (numeric) : xxx}	VERS LE BAS	Le côté AWS génère un message de journal lorsque le nombre de préfixes reçus du CGW a dépassé la limite autorisée.
Le pair côté AWS a envoyé une notification 6/1 (cessation/ nombre maximum de préfixes atteints) au voisin {ip : xxx}	VERS LE BAS	La partie AWS a envoyé une notification à l'homolog ue BGP CGW pour indiquer que la session BGP avait été interrompue en raison d'une violation de la limite de préfixe.
Le pair côté AWS a reçu une notification 6/1 (cessation/ nombre maximum de préfixes atteints) du voisin {ip : xxx}	VERS LE BAS	La partie AWS a reçu une notification de l'homologue CGW indiquant que la session BGP avait été interrompue en raison d'une violation de la limite de préfixe.
Le pair côté AWS a envoyé une notification 6/2 (cessatio n/arrêt administratif) au voisin {ip : xxx}	VERS LE BAS	La partie AWS a envoyé une notification à l'homolog ue BGP CGW pour indiquer que la session BGP avait été interrompue.

Message	État du BGP	Explication
Le pair côté AWS a reçu une notification 6/2 (cessation/arrêt administratif) du voisin {ip : xxx}	VERS LE BAS	La partie AWS a reçu une notification de l'homologue CGW indiquant que la session BGP avait été interrompue.
Le pair côté AWS a envoyé une notification 6/3 (Cease/Pe er Unconfigured) au voisin {ip : xxx}	VERS LE BAS	La partie AWS a envoyé une notification à l'homologue CGW pour indiquer que celui-ci n'est pas configuré ou qu'il a été retiré de la configuration.
Le pair côté AWS a reçu une notification 6/3 (cessation/ homologue non configuré) du voisin {ip : xxx}	VERS LE BAS	La partie AWS a reçu une notification de l'homologue CGW indiquant que celui-ci n'est pas configuré ou qu'il a été retiré de la configuration.
Le pair côté AWS a envoyé une notification 6/4 (cessation/ réinitialisation administrative) au voisin {ip : xxx}	VERS LE BAS	La partie AWS a envoyé une notification à l'homologue BGP CGW pour indiquer que la session BGP avait été réinitial isée.
Le pair côté AWS a reçu une notification 6/4 (cessation/ réinitialisation administrative) du voisin {ip : xxx}	VERS LE BAS	La partie AWS a reçu une notification de l'homologue CGW indiquant que la session BGP avait été réinitialisée.
Le pair côté AWS a envoyé une notification 6/5 (cessatio n/connexion rejetée) au voisin {ip : xxx}	VERS LE BAS	La partie AWS a envoyé une notification à l'homologue BGP CGW pour indiquer que la session BGP avait été rejetée.

Message	État du BGP	Explication
Le pair côté AWS a reçu une notification 6/5 (cessation/ connexion rejetée) du voisin {ip : xxx}	VERS LE BAS	La partie AWS a reçu une notification de l'homologue CGW indiquant que la session BGP avait été rejetée.
Le pair côté AWS a envoyé une notification 6/6 (cessation/ autre modification de configura tion) au voisin {ip : xxx}	VERS LE BAS	La partie AWS a envoyé une notification à l'homologue BGP CGW pour indiquer qu'un changement de configuration de session BGP avait eu lieu.
Le pair côté AWS a reçu une notification 6/6 (cessation/ autre modification de configura tion) du voisin {ip : xxx}	VERS LE BAS	La partie AWS a reçu une notification de l'homolog ue CGW indiquant qu'un changement de configuration de session BGP a eu lieu.
Le pair côté AWS a envoyé une notification 6/7 (résolution des collisions de cessation/de connexion) au voisin {ip : xxx}	VERS LE BAS	La partie AWS a envoyé une notification à l'homolog ue CGW pour résoudre une collision de connexion lorsque les deux homologues tentent d'établir une connexion simultanément.
Le pair côté AWS a reçu une notification 6/7 (résolution des collisions de cessation/de connexion) du voisin {ip : xxx}	VERS LE BAS	La partie AWS a reçu une notification de l'homologue CGW indiquant la résolution d'une collision de connexion lorsque les deux homologues tentent d'établir une connexion simultanément.

Message	État du BGP	Explication
Un pair côté AWS a envoyé une notification d'expiration du délai d'attente au voisin {ip : xxx}	VERS LE BAS	Le délai de blocage du BGP a expiré et une notification a été envoyée par AWS au CGW.
Un pair côté AWS a détecté un message OPEN incorrect provenant du voisin {ip : xxx} - remote AS is {asn : xxx}, attendu {asn : xxx}	VERS LE BAS	Le côté AWS a détecté qu'un message OPEN erroné avait été reçu de l'homologue CGW, ce qui indique une incompati bilité de configuration.
Le pair côté AWS a reçu un message OUVERT du voisin {ip : xxx} - version 4, AS {asn : xxx}, holdtime {holdtime (seconds) : xxx}, router-id {id : xxx}}	VERS LE BAS	La partie AWS a reçu un message d'ouverture BGP pour lancer une session BGP avec l'homologue CGW.
Le pair côté AWS a envoyé un message OUVERT au voisin {ip : xxx} - version 4, AS {asn : xxx}, holdtime {holdtime (seconds) : xxx}, router-id {id : xxx}	VERS LE BAS	L'homologue CGW a envoyé un message d'ouverture BGP pour lancer une session BGP avec l'homologue BGP côté AWS.
L'homologue côté AWS établit une connexion (via Connect) avec le voisin {ip : xxx}	VERS LE BAS	Le côté AWS tente de se connecter au voisin BGP CGW.
Le pair côté AWS a envoyé un End-of-RIB message au voisin {ip : xxx}	EN HAUT	Le côté AWS a fini de transmettre les itinéraires au CGW après l'établissement de la session BGP.

Message	État du BGP	Explication
Le pair côté AWS a reçu une mise à jour avec les attributs du voisin {ip : xxx} - AS path : {aspath (list) : xxx xxx xxx}	EN HAUT	Le côté AWS a reçu une mise à jour de l'attribut de session BGP de la part du voisin.

Messages d'état de l'itinéraire

Contrairement aux messages d'état BGP, les messages d'état de route contiennent des données sur les attributs BGP d'un préfixe donné, tels que le chemin AS, les préférences locales, le discriminateur à sorties multiples (MED), l'adresse IP du prochain saut et le poids. Un message d'état de l'itinéraire ne contiendra un champ de détails qu'en cas d'erreur concernant un itinéraire ANNONCÉ, MIS À JOUR ou RETIRÉ. Les exemples suivants en sont les suivants :

Message	Explication
REFUSÉ car : as-path contient notre propre AS	Les messages de mise à jour BGP pour un nouveau préfixe provenant de CGW ont été refusés par AWS en raison de la route contenant le propre AS du pair côté AWS.
REFUSÉ pour cause de : prochain saut non connecté	AWS a rejeté une annonce de route BGP pour le préfixe émise par le CGW en raison d'un échec de validation du prochain saut non connecté. Assurez-vous que l'itinéraire est accessible du côté de la CGW.

Exemple de format de journal pour les journaux Tunnel BGP


```
{
    "resource_id": "vpn-1234abcd_1.2.3.4",
    "event_timestamp": 1762580429641,
    "timestamp": "2025-11-08 05:40:29.641Z",
    "type": "BGPStatus",
    "status": "UP",
```

```
    "message": {
        "details": "AWS-side peer BGP session state has changed from OpenConfirm to
 Established with neighbor 169.254.50.85"
    }
}

{
    "resource_id": "vpn-1234abcd_1.2.3.4",
    "event_timestamp": 1762579573243,
    "timestamp": "2025-11-08 05:26:13.243Z",
    "type": "RouteStatus",
    "status": "UPDATED",
    "message": {
        "prefix": "172.31.0.0/16",
        "asPath": "64512",
        "localPref": 100,
        "med": 100,
        "nextHopIp": "169.254.50.85",
        "weight": 32768,
        "details": "DENIED due to: as-path contains our own AS"
    }
}
```

Exigences IAM pour publier dans Logs CloudWatch

Pour que la fonctionnalité de journalisation fonctionne correctement, la politique IAM attachée au principal IAM utilisée pour configurer la fonctionnalité doit inclure au minimum les autorisations suivantes. Vous trouverez également plus de détails dans la section Activation de la journalisation à partir de certains AWS services du guide de l'utilisateur Amazon CloudWatch Logs.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Action": [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
```

```
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries"
      ],
      "Resource": [
        "*"
      ],
      "Effect": "Allow",
      "Sid": "S2SVPNLogging"
    },
    {
      "Sid": "S2SVPNLoggingCWL",
      "Action": [
        "logs:PutResourcePolicy",
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups"
      ],
      "Resource": [
        "*"
      ],
      "Effect": "Allow"
    }
  ]
}
```

Afficher la configuration AWS Site-to-Site VPN des journaux

Consultez le journal d'activité d'une connexion Site-to-Site VPN. Vous pouvez voir ici des détails sur la configuration de tels algorithmes de chiffrement ou sur l'activation des journaux VPN par tunnel. Vous pouvez également consulter l'état du tunnel. Cela vous permet de mieux suivre les problèmes ou les conflits que vous pourriez rencontrer avec une connexion VPN.

Pour afficher les paramètres de journalisation de tunnel en cours

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Connexions Site-to-Site VPN.
3. Sélectionnez la connexion VPN que vous souhaitez afficher dans la liste Connexions VPN.
4. Cliquez sur l'onglet Détails du tunnel.
5. Développez les sections Tunnel 1 options (Options du tunnel 1) et Tunnel 2 options (Options du tunnel 2) pour afficher tous les détails de configuration du tunnel.

6. Vous pouvez consulter l'état actuel de la fonctionnalité de journal du tunnel VPN et le groupe de CloudWatch journaux actuellement configuré (le cas échéant) sous le groupe de journaux pour le CloudWatch journal du tunnel VPN et le format de sortie du journal sous Format de sortie pour le journal du VPN du tunnel.
7. Vous pouvez consulter l'état actuel de la fonctionnalité de journal BGP du tunnel, le groupe de CloudWatch journaux actuellement configuré (le cas échéant) sous le groupe de journaux pour le CloudWatch journal du tunnel VPN et le format de sortie du journal sous Format de sortie pour le journal BGP du tunnel.

Pour afficher les paramètres actuels de journalisation du tunnel sur une connexion Site-to-Site VPN à l'aide de la ligne de AWS commande ou de l'API

- DescribeVpnConnections(API de requête Amazon EC2)
- describe-vpn-connections (AWS CLI)

Activer AWS Site-to-Site VPN les journaux

Activez les journaux Site-to-Site VPN pour enregistrer l'activité du VPN, telle que l'état du tunnel et d'autres détails. Vous pouvez activer la connexion à une nouvelle connexion ou modifier une connexion existante pour démarrer l'activité de journalisation. Si vous souhaitez désactiver la journalisation d'une connexion, consultezDésactiver les journaux Site-to-Site VPN.

> **Note**
>
> Lorsque vous activez les journaux Site-to-Site VPN pour un tunnel de connexion VPN existant, votre connectivité via ce tunnel peut être interrompue pendant plusieurs minutes. Cependant, chaque connexion VPN propose deux tunnels pour assurer la haute disponibilité, de sorte que vous pouvez activer la journalisation sur un tunnel à la fois tout en maintenant la connectivité sur le tunnel qui n'est pas modifié. Pour de plus amples informations, veuillez consulter AWS Site-to-Site VPN remplacement des extrémités des tunnels.

Pour activer la journalisation VPN lors de la création d'une nouvelle connexion Site-to-Site VPN

Suivez la procédure Étape 5 : Création d'une connexion VPN. Au cours de l'étape 9 Options de tunnel, vous pouvez spécifier toutes les options que vous souhaitez utiliser pour les deux tunnels,

y compris les options de journalisation du VPN. Pour plus d'informations sur ces options, consultez Options de tunnel pour votre AWS Site-to-Site VPN connexion.

Pour activer la journalisation par tunnel sur une nouvelle connexion Site-to-Site VPN à l'aide de la ligne de AWS commande ou de l'API

- CreateVpnConnection(API de requête Amazon EC2)
- create-vpn-connection (AWS CLI)

Pour activer la journalisation de l'activité du tunnel sur une connexion Site-to-Site VPN existante

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Connexions Site-to-Site VPN.
3. Sélectionnez la connexion VPN que vous souhaitez modifier dans la liste Connexions VPN.
4. Sélectionnez Actions, Modify VPN tunnel options (Modifier les options de tunnel VPN).
5. Sélectionnez le tunnel que vous souhaitez modifier en choisissant l'adresse IP appropriée dans la liste VPN tunnel outside IP address (Adresse IP extérieure du tunnel VPN).
6. Sous Tunnel activity log (Journal d'activité du tunnel), sélectionnez Enable (Activer).
7. Sous Groupe de CloudWatch journaux Amazon, sélectionnez le groupe de CloudWatch journaux Amazon dans lequel vous souhaitez que les journaux soient envoyés.
8. (Facultatif) Sous Output format (Format de sortie), choisissez le format souhaité pour la sortie du journal, à savoir json ou text.
9. Sélectionnez Save changes (Enregistrer les modifications).
10. (Facultatif) Répétez les étapes 4 à 9 pour l'autre tunnel si vous le souhaitez.

Pour activer la journalisation BGP par tunnel sur une connexion Site-to-Site VPN existante

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Connexions Site-to-Site VPN.
3. Sélectionnez la connexion VPN que vous souhaitez modifier dans la liste Connexions VPN.
4. Sélectionnez Actions, Modify VPN tunnel options (Modifier les options de tunnel VPN).
5. Sélectionnez le tunnel que vous souhaitez modifier en choisissant l'adresse IP appropriée dans la liste VPN tunnel outside IP address (Adresse IP extérieure du tunnel VPN).
6. Sous Journal BGP du tunnel, sélectionnez Activer.

7. Sous Groupe de CloudWatch journaux Amazon, sélectionnez le groupe de CloudWatch journaux Amazon dans lequel vous souhaitez que les journaux soient envoyés.
8. (Facultatif) Sous Output format (Format de sortie), choisissez le format souhaité pour la sortie du journal, à savoir json ou text.
9. Sélectionnez Save changes (Enregistrer les modifications).
10. (Facultatif) Répétez les étapes 4 à 9 pour l'autre tunnel si vous le souhaitez.

Pour activer la journalisation par tunnel sur une connexion Site-to-Site VPN existante à l'aide de la ligne de AWS commande ou de l'API

- ModifyVpnTunnelOptions(API de requête Amazon EC2)
- modify-vpn-tunnel-options (AWS CLI)

Désactiver AWS Site-to-Site VPN les journaux

Désactivez la connexion VPN sur une connexion si vous ne souhaitez plus suivre aucune activité sur cette connexion. Cette action désactive uniquement la journalisation et n'affecte rien d'autre pour cette connexion. Pour activer ou réactiver la connexion à une connexion, consultezActiver les journaux Site-to-Site VPN.

Pour désactiver la journalisation de l'activité du tunnel sur une connexion Site-to-Site VPN

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Site-to-Site VPN Connections.
3. Sélectionnez la connexion VPN que vous souhaitez modifier dans la liste Connexions VPN.
4. Sélectionnez Actions, Modify VPN tunnel options (Modifier les options de tunnel VPN).
5. Sélectionnez le tunnel que vous souhaitez modifier en choisissant l'adresse IP appropriée dans la liste VPN tunnel outside IP address (Adresse IP extérieure du tunnel VPN).
6. Sous Tunnel activity log (Journal d'activité du tunnel), décochez Enable (Activer).
7. Sélectionnez Save changes (Enregistrer les modifications).
8. (Facultatif) Répétez les étapes 4 à 7 pour l'autre tunnel si vous le souhaitez.

Pour désactiver la journalisation BGP par tunnel sur une connexion Site-to-Site VPN

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.

2. Dans le volet de navigation, choisissez Site-to-Site VPN Connections.
3. Sélectionnez la connexion VPN que vous souhaitez modifier dans la liste Connexions VPN.
4. Sélectionnez Actions, Modify VPN tunnel options (Modifier les options de tunnel VPN).
5. Sélectionnez le tunnel que vous souhaitez modifier en choisissant l'adresse IP appropriée dans la liste VPN tunnel outside IP address (Adresse IP extérieure du tunnel VPN).
6. Dans le journal BGP du tunnel, désactivez Activer.
7. Sélectionnez Save changes (Enregistrer les modifications).
8. (Facultatif) Répétez les étapes 4 à 7 pour l'autre tunnel si vous le souhaitez.

Pour désactiver la journalisation par tunnel sur une connexion Site-to-Site VPN à l'aide de la ligne de AWS commande ou de l'API

- ModifyVpnTunnelOptions(API de requête Amazon EC2)
- modify-vpn-tunnel-options (AWS CLI)

Surveillez AWS Site-to-Site VPN les tunnels à l'aide d'Amazon CloudWatch

Vous pouvez surveiller les tunnels VPN à l'aide CloudWatch d'un système qui collecte et traite les données brutes du service VPN en indicateurs lisibles en temps quasi réel. Ces statistiques sont enregistrées pour une durée de 15 mois et, par conséquent, vous pouvez accéder aux informations historiques et acquérir un meilleur point de vue de la façon dont votre service ou application web s'exécute. Les données métriques du VPN sont automatiquement envoyées CloudWatch dès qu'elles sont disponibles.

Pour plus d'informations, consultez le guide de CloudWatch l'utilisateur Amazon.

Table des matières

Métriques et dimensions VPN

Les CloudWatch statistiques suivantes sont disponibles pour vos connexions Site-to-Site VPN.

Métrique	Description
`TunnelState`	État des tunnels. Pour une valeur statique VPNs, 0 indique DOWN et 1 indique UP. Pour le BGP VPNs, 1 indique ESTABLISHED et 0 est utilisé pour tous les autres états. Pour les deux types de VPNs, les valeurs comprises entre 0 et 1 indiquent qu'au moins un tunnel n'est pas activé. Unités : valeur fractionnelle comprise entre 0 et 1
`TunnelDataIn` †	Les octets reçus du AWS côté de la connexion via le tunnel VPN depuis une passerelle client. Chaque point de données de métriques représente le nombre d'octets reçus après le point de données précédent. Utilisez la statistique Somme pour afficher le nombre total d'octets reçus pendant la période. Cette métrique comptabilise les données après déchiffrement. Unités : octets
`TunnelDataOut` †	Les octets envoyés depuis le AWS côté de la connexion via le tunnel VPN vers la passerelle client. Chaque point de données de métriques représente le nombre d'octets envoyés après le point de données précédent. Utilisez la statistique Somme pour afficher le nombre total d'octets envoyés pendant la période.

Métrique	Description
	Cette métrique comptabilise les données avant chiffrement. Unités : octets
`ConcentratorBandwidthUsage`	L'utilisation de la bande passante pour une connexion au concentrateur Site-to-Site VPN. Cette métrique est disponible pour les connexions VPN qui utilisent un concentra teur Site-to-Site VPN. Utilisez la statistique moyenne pour afficher l'utilisation moyenne de la bande passante au cours de la période. Unités : bits par seconde

† Ces métriques peuvent signaler l'utilisation du réseau même lorsque le tunnel est hors service. Cela est dû aux contrôles de statut périodiques effectués sur le tunnel et aux requêtes ARP et BGP en arrière-plan.

Pour filtrer les données de métriques, utilisez les dimensions suivantes.

Dimension	Description
`VpnId`	Filtre les données métriques en fonction de l'ID de connexion Site-to-Site VPN.
`TunnelIpAddress`	Permet de filtrer les données en fonction de l'adresse IP du tunnel de la passerelle réseau privé virtuel.

Afficher les statistiques Amazon CloudWatch Logs pour AWS Site-to-Site VPN

Lorsque vous créez une connexion Site-to-Site VPN, le service VPN envoie les statistiques relatives à votre connexion VPN CloudWatch dès qu'elles sont disponibles. Vous pouvez consulter les métriques de votre connexion VPN comme suit.

Pour afficher les métriques à l'aide de la CloudWatch console

Les métriques sont d'abord regroupées par espace de noms de service, puis par les différentes combinaisons de dimension au sein de chaque espace de noms.

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans le panneau de navigation, sélectionnez Métriques.
3. Sous All metrics, choisissez l'espace de nom de métrique VPN.
4. Sélectionnez la dimension métrique pour afficher les métriques, par exemple, les métriques du tunnel VPN.

> **Note**
>
> L'espace de noms VPN n'apparaîtra dans la CloudWatch console qu'après la création d'une connexion Site-to-Site VPN dans la AWS région que vous consultez.

Pour consulter les statistiques à l'aide du AWS CLI

À partir d'une invite de commande, utilisez la commande suivante :

```
aws cloudwatch list-metrics --namespace "AWS/VPN"
```

Créez des CloudWatch alarmes Amazon pour surveiller AWS Site-to-Site VPN les tunnels

Vous pouvez créer une CloudWatch alarme qui envoie un message Amazon SNS lorsque l'alarme change d'état. Une alarme surveille une seule métrique sur une durée définie et envoie une notification à une rubrique Amazon SNS en fonction de la valeur de la métrique par rapport à un seuil donné sur un certain nombre de durées.

Par exemple, vous pouvez créer une alarme qui surveille l'état d'un tunnel VPN unique, puis qui envoie une notification lorsque l'état du tunnel est DOWN pendant 3 périodes de 15 minutes consécutives.

Pour créer une alarme pour l'état d'un tunnel unique

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.

2. Dans le panneau de navigation, développez Alarmes, puis choisissez Toutes les alarmes.
3. Choisissez Créer une alarme, puis Sélectionner une métrique.
4. Choisissez VPN, puis Métriques de tunnel VPN.
5. Sélectionnez l'adresse IP du tunnel souhaité, sur la même ligne que la TunnelStatemétrique. Choisissez Select metric (Sélectionner une métrique).
6. Pour chaque fois que TunnelState c'est... , sélectionnez Inférieur, puis entrez « 1 » dans le champ de saisie situé sous... .
7. Sous Configuration supplémentaire, définissez Points de données pour le déclenchement d'alarme sur « 3 sur 3 ».
8. Choisissez Suivant.
9. Sous Envoyer une notification à la rubrique SNS suivante, sélectionnez une liste de notifications existante ou créez-en une.
10. Choisissez Suivant.
11. Saisissez un nom pour votre alarme. Choisissez Suivant.
12. Vérifiez les paramètres de votre alarme, puis choisissez Create alarm (Créer une alarme).

Vous pouvez créer une alarme qui surveille l'état de la connexion Site-to-Site VPN. Par exemple, vous pouvez créer une alarme qui envoie une notification lorsque l'état d'un ou des deux tunnels est DOWN (arrêt) pendant une période de 5 minutes consécutives.

Pour créer une alarme concernant l'état de la connexion Site-to-Site VPN

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans le panneau de navigation, développez Alarmes, puis choisissez Toutes les alarmes.
3. Choisissez Créer une alarme, puis Sélectionner une métrique.
4. Choisissez VPN, puis choisissez VPN Connection Metrics (Métriques de connexion VPN).
5. Sélectionnez votre connexion Site-to-Site VPN et la TunnelStatemétrique. Choisissez Sélectionner une métrique.
6. Pour Statistic (Statistiques), spécifiez Maximum.

   Sinon, si vous avez configuré votre connexion Site-to-Site VPN de manière à ce que les deux tunnels soient actifs, vous pouvez spécifier une statistique Minimum pour envoyer une notification lorsqu'au moins un tunnel est en panne.

7. Pour Whenever (Chaque fois), choisissez Lower/Equal (Inférieur à/Égal à) (<=) et entrez 0 (ou 0,5 quand un tunnel au moins est arrêté). Choisissez Suivant.
8. Sous Select an SNS topic (Sélectionner une rubrique SNS), sélectionnez une liste de notifications existante ou choisissez New list (Nouvelle liste). Choisissez Suivant.
9. Saisissez un nom et une description pour votre alarme. Choisissez Suivant.
10. Vérifiez les paramètres de votre alarme, puis choisissez Create alarm (Créer une alarme).

Vous pouvez aussi créer des alarmes qui surveille la quantité de trafic entrant dans le tunnel VPN ou en sortant. Par exemple, l'alarme suivante surveille la quantité de trafic entrant dans le tunnel VPN à partir de votre réseau et envoie une notification lorsque le nombre d'octets atteint un seuil de 5 000 000 pendant une période de 15 minutes.

Pour créer une alarme pour votre trafic réseau entrant

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans le panneau de navigation, développez Alarmes, puis choisissez Toutes les alarmes.
3. Choisissez Créer une alarme, puis Sélectionner une métrique.
4. Choisissez VPN, puis choisissez VPN Tunnel Metrics (Métriques de tunnel VPN).
5. Sélectionnez l'adresse IP du tunnel VPN et la TunnelDataInmétrique. Choisissez Sélectionner une métrique.
6. Pour Statistic (Statistiques), spécifiez Sum (Somme).
7. Pour Period (Période), sélectionnez 15 minutes.
8. Pour Whenever (Chaque fois), choisissez Greater/Equal (Supérieur à/Égal à) (>=) et entrez 5000000. Choisissez Suivant.
9. Sous Select an SNS topic (Sélectionner une rubrique SNS), sélectionnez une liste de notifications existante ou choisissez New list (Nouvelle liste). Choisissez Suivant.
10. Saisissez un nom et une description pour votre alarme. Choisissez Suivant.
11. Vérifiez les paramètres de votre alarme, puis choisissez Create alarm (Créer une alarme).

Par exemple, l'alarme suivante surveille la quantité de trafic entrant dans le tunnel VPN à partir de votre réseau et envoie une notification lorsque le nombre d'octets atteint un seuil de 1 000 000 pendant une période de 15 minutes.

Pour créer une alarme pour votre trafic réseau sortant

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans le panneau de navigation, développez Alarmes, puis choisissez Toutes les alarmes.
3. Choisissez Créer une alarme, puis Sélectionner une métrique.
4. Choisissez VPN, puis choisissez VPN Tunnel Metrics (Métriques de tunnel VPN).
5. Sélectionnez l'adresse IP du tunnel VPN et la TunnelDataOutmétrique. Choisissez Sélectionner une métrique.
6. Pour Statistic (Statistiques), spécifiez Sum (Somme).
7. Pour Period (Période), sélectionnez 15 minutes.
8. Pour Whenever (Chaque fois), choisissez Lower/Equal (Inférieur à/Égal à) (<=) et entrez `1000000`. Choisissez Suivant.
9. Sous Select an SNS topic (Sélectionner une rubrique SNS), sélectionnez une liste de notifications existante ou choisissez New list (Nouvelle liste). Choisissez Suivant.
10. Saisissez un nom et une description pour votre alarme. Choisissez Suivant.
11. Vérifiez les paramètres de votre alarme, puis choisissez Create alarm (Créer une alarme).

Pour d'autres exemples de création d'alarmes, consultez la section Création d' CloudWatch alarmes Amazon dans le guide de CloudWatch l'utilisateur Amazon.

AWS Health et AWS Site-to-Site VPN événements

AWS Site-to-Site VPN envoie automatiquement des notifications au Tableau de bord Health. Ce tableau de bord ne nécessite aucune configuration et est prêt à être utilisé par les AWS utilisateurs authentifiés. Vous pouvez configurer plusieurs actions en réponse aux notifications d'événements via le Tableau de bord Health.

Tableau de bord Health fournit les types de notifications suivants pour vos connexions VPN :

- Notifications de remplacement des points de terminaison du tunnel
- Notifications de VPN à tunnel unique

Notifications de remplacement des points de terminaison du tunnel

Vous recevez une notification de remplacement du point de terminaison du tunnel Tableau de bord Health lorsque l'un ou les deux points de terminaison du tunnel VPN de votre connexion VPN sont remplacés. Un point de terminaison du tunnel est remplacé lorsque AWS effectue des mises à jour de tunnel ou lorsque vous modifiez votre connexion VPN. Pour de plus amples informations, veuillez consulter AWS Site-to-Site VPN remplacement des extrémités des tunnels.

Lorsque le remplacement d'un point de terminaison du tunnel est terminé, AWS envoie la notification de remplacement du point de terminaison du tunnel par le biais d'un Tableau de bord Health événement.

Notifications de VPN à tunnel unique

Une connexion Site-to-Site VPN se compose de deux tunnels de redondance. Nous vous recommandons fortement de configurer les deux tunnels pour une haute disponibilité. Si votre connexion VPN a un tunnel actif mais que l'autre est à l'arrêt pendant plus d'une heure par jour, vous recevez une notification de tunnel unique VPN mensuelle via un événement Tableau de bord Health . Cet événement est mis à jour quotidiennement pour tenir compte de toute nouvelle connexion VPN détectée comme un tunnel unique et des notifications sont envoyées chaque semaine. Un nouvel événement est créé chaque mois, qui efface toutes les connexions VPN qui ne sont plus détectées comme étant un tunnel unique.

AWS Site-to-Site VPN quotas

Votre AWS compte possède les quotas suivants, anciennement appelés limites, liés au Site-to-Site VPN. Sauf indication contraire, chaque quota est spécifique à une région. Vous pouvez demander des augmentations pour certains quotas, et d'autres quotas ne peuvent pas être augmentés.

Pour demander une augmentation de quota pour un quota ajustable, choisissez Yes (Oui) dans la colonne Adjustable (Ajustable). Pour de plus amples informations, veuillez consulter Demande d'augmentation de quota dans le Guide de l'utilisateur Service Quotas.

Site-to-Site Ressources VPN

Name	Par défaut	Ajustable
Passerelles client par région	50	Oui
Passerelles réseau privé virtuel par région	5	Oui
Site-to-Site Connexions VPN par région	50	Oui
Site-to-Site Connexions VPN par passerelle privée virtuelle	10	Oui
Connexions Site-to-Site VPN accélérées par région	10	Oui
Connexions Site-to-Site VPN non associées par région	10	Oui
Connexions par tunnel à large bande passante par région	50	Oui
Site-to-Site Concentrateurs VPN par région	50	Oui
Site-to-Site Concentrateurs VPN pour Transit Gateway ou Cloud WAN	5	Oui
Sites distants par concentrateur Site-to-Site VPN	100	Oui

> **Note**
>
> Les connexions accélérées et non associées sont prises en compte dans le quota total de connexions Site-to-Site VPN par région.

Vous pouvez attacher une passerelle réseau privé virtuel à un VPC à la fois. Pour connecter la même connexion Site-to-Site VPN à plusieurs VPCs, nous vous recommandons d'utiliser plutôt une passerelle de transit. Pour plus d'informations, consultez Passerelles de transit dans Passerelles de transit Amazon VPC.

Site-to-Site Les connexions VPN sur une passerelle de transit sont soumises à la limite totale de pièces jointes de la passerelle de transit. Pour plus d'informations, consultez Quotas de passerelle Transit Gateway.

Routes

Les sources d'acheminement annoncées incluent les acheminements VPC, les autres acheminements VPN et les acheminements provenant d'interfaces virtuelles Direct Connect. Les routes annoncées proviennent de la table de routage associée à l'attachement VPN.

> **Note**
>
> Si vous utilisez une passerelle réseau privé virtuel et que la propagation de routage est activée sur la table de routage de votre VPC, des routes dynamiques et statiques sont automatiquement ajoutées à votre connexion VPN, dans la limite de la table de routage du VPC. Pour plus de détails, consultez Quotas Amazon VPC dans le Guide de l'utilisateur Amazon VPC.

Name	Par défaut	Ajustable
Itinéraires dynamiques annoncés depuis un dispositif de passerelle client vers une connexion Site-to-Site VPN sur une passerelle privée virtuelle	100	Non

Name	Par défaut	Ajustable
Itinéraires annoncés à partir d'une connexion Site-to-Site VPN sur une passerelle privée virtuelle vers un dispositif de passerelle client	1 000	Non
Itinéraires dynamiques annoncés depuis un dispositif de passerelle client vers une connexion Site-to-Site VPN sur une passerelle de transit	1 000	Non
Itinéraires annoncés à partir d'une connexion Site-to-Site VPN sur une passerelle de transit vers un dispositif de passerelle client	5 000	Non
Routes statiques entre un dispositif de passerelle client et une connexion Site-to-Site VPN sur une passerelle privée virtuelle	100	Non

Bande passante et débit

De nombreux facteurs peuvent affecter la bande passante obtenue par le biais d'une connexion Site-to-Site VPN, notamment, mais sans s'y limiter : la taille des paquets, la composition du trafic (TCP/UDP), les politiques de mise en forme ou de limitation sur les réseaux intermédiaires, la météo Internet et les exigences spécifiques des applications.

Name	Par défaut	Ajustable
Bande passante maximale par tunnel VPN Concentrator	Jusqu'à 100 Mbits/s	Non
Nombre maximal de paquets par seconde (PPS) par tunnel VPN Concentrator	Jusqu'à 10 000	Non
Bande passante maximale par tunnel VPN standard	Jusqu'à 1,25 Gbit/s	Non

Name	Par défaut	Ajustable
Nombre maximal de paquets par seconde (PPS) par tunnel VPN standard	Jusqu'à 140 000	Non
Bande passante maximale par tunnel VPN à large bande passante	Jusqu'à 5 Gbit/s	Non
Nombre maximal de paquets par seconde (PPS) par tunnel VPN à large bande passante	Jusqu'à 400 000	Non

Pour les connexions Site-to-Site VPN sur une passerelle de transit, vous pouvez utiliser l'ECMP pour obtenir une bande passante VPN plus élevée en agrégeant plusieurs tunnels VPN. Pour utiliser l'ECMP, la connexion VPN doit être configurée pour le routage dynamique. L'ECMP n'est pas pris en charge sur les connexions VPN qui utilisent le routage statique. Pour plus d'informations, consultez Passerelles de transit.

> **Note**
>
> IPv6 VPNs supportent les mêmes limites de débit (Gbit/s et PPS), de MTU et de route que. IPv4 VPNs Il n'y a aucune différence de performance entre IPv4 les connexions IPv6 VPN.

Unité de transmission maximale (MTU)

Site-to-Site Le VPN prend en charge une unité de transmission maximale (MTU) de 1446 octets et une taille de segment maximale (MSS) correspondante de 1406 octets. Cependant, certains algorithmes qui utilisent des en-têtes TCP plus grands peuvent réduire efficacement cette valeur maximale. Pour éviter la fragmentation, nous vous recommandons de définir la MTU et la MSS en fonction des algorithmes sélectionnés. Pour plus de détails sur la MTU, la MSS et les valeurs optimales, consultez Les meilleures pratiques pour un AWS Site-to-Site VPN Appareil de passerelle client.

Les trames jumbo ne sont pas prises en charge. Pour plus d'informations, consultez la section Cadres Jumbo dans le guide de EC2 l'utilisateur Amazon.

Une connexion Site-to-Site VPN ne prend pas en charge Path MTU Discovery.

Les limites du MTU s'appliquent à la fois aux connexions IPv6 VPN IPv4 et aux connexions VPN.

Ressources de quotas supplémentaires

Pour connaître les quotas liés aux passerelles de transit, en particulier le nombre d'attachements sur une passerelle de transit, consultez Quotas pour vos passerelles de transit dans le Guide des passerelles de transit Amazon VPC.

Pour obtenir des quotas VPC supplémentaires, consultez Quotas Amazon VPC dans le Guide de l'utilisateur Amazon VPC.

Historique des documents pour le guide de l'utilisateur du Site-to-Site VPN

Le tableau suivant décrit les mises à jour du guide de AWS Site-to-Site VPN l'utilisateur.

Modification	Description	Date
Site-to-Site Concentrateurs VPN	Site-to-Site Les concentrateurs VPN fournissent un hub centralisé pour gérer plusieurs connexions VPN avec une évolutivité améliorée et une architecture réseau simplifiée.	15 novembre 2025
Site-to-Site Support VPN pour les tunnels à large bande passante	Site-to-Site Le VPN prend désormais en charge une large bande passante de tunnel, permettant ainsi une passerelle de transit et des connexions VPN Cloud WAN avec un débit allant jusqu'à 5 Gbit/s.	25 septembre 2025
IPv6 support du AWS Site-to-Site VPN pour le tunnel extérieur IPs	Site-to-Site Le VPN prend désormais en charge les IPv6 adresses du tunnel extérieur IPs sur les connexions VPN Transit Gateway et Cloud WAN. Cela permet une IPv6 migration complète avec IPv6 des adresses pour le tunnel extérieur IPs et le paquet interne IPs (IPv6-in-IPv6), ainsi que pour le tunnel IPv6 externe IPs avec le paquet IPv4 interne IPs (IPv4-in-IPv6).	1er juillet 2025

Mise à jour de la politique AWSVPCS2 SVpn ServiceRolePolicy AWS gérée	Ajout de nouvelles autorisations à la politique AWS gérée permettant au Site-to-Site VPN de gérer le secret AWS Secrets Manager géré de la connexion VPN.	27 mai 2025
Options de stockage de clés pré-partagées mises à jour	Site-to-Site Le VPN prend désormais en AWS Secrets Manager charge le stockage d'une clé pré-partagée.	27 mai 2025
Informations sur Classic VPN supprimées	Les informations sur Classic VPN ont été supprimées du guide.	19 janvier 2023
Exemples de messages de journaux VPN	Exemples de journaux ajoutés pour les connexions Site-to-Site VPN.	9 décembre 2022

Utilitaire de téléchargement de configuration mis à jour	Site-to-Site Les clients VPN peuvent générer des modèles de configuration pour les appareils Customer Gateway (CGW) compatibles, ce qui facilite la création de connexions VPN avec.AWS Cette mise à jour ajoute la prise en charge des paramètre s Internet Key Exchange version 2 (IKEv2) pour de nombreux appareils CGW populaires et inclut deux nouveaux APIs : GetVpnCon nectionDeviceTypes et GetVpnConnectionDe viceSampleConfiguration.	21 septembre 2021
Notifications de connexion VPN	Site-to-Site Le VPN envoie automatiquement des notifications concernant votre connexion VPN au Tableau de bord Health.	29 octobre 2020
Lancement du tunnel VPN	Vous pouvez configurer vos tunnels VPN de manière àAWS ce qu'ils apparaissent.	27 août 2020
Modifier les options de connexion VPN	Vous pouvez modifier les options de connexion de votre connexion Site-to-Site VPN.	27 août 2020
Algorithmes de sécurité supplémentaires	Vous pouvez appliquer des algorithmes de sécurité supplémentaires à vos tunnels VPN.	14 août 2020

IPv6 soutien	Vos tunnels VPN peuvent prendre en charge le IPv6 trafic à l'intérieur des tunnels.	12 août 2020
AWS Site-to-Site VPN Guides de fusion	Cette version fusionne le contenu du guide de l'adminis trateur AWS Site-to-Site VPN réseau dans ce guide.	31 mars 2020
AWS Site-to-Site VPN Connexions accélérées	Vous pouvez activer l'accélér ation pour votre AWS Site-to-S ite VPN connexion.	3 décembre 2019
Modifier les options AWS Site-to-Site VPN du tunnel	Vous pouvez modifier les options d'un tunnel VPN dans une AWS Site-to-Site VPN connexion. Vous pouvez également configurer d'autres options de tunnel.	29 août 2019
Autorité de certification privée AWS support de certificats privés	Vous pouvez utiliser un certificat privéAutorité de certification privée AWS pour authentifier votre VPN.	15 août 2019
Guide de l'utilisateur du nouveau Site-to-Site VPN	Cette version sépare le contenu AWS Site-to-S ite VPN(précédemment connu sous le nom de AWS Managed VPN) du guide de l'utilisateur Amazon VPC.	18 décembre 2018
Modification de la passerelle cible	Vous pouvez modifier la passerelle de AWS Site-to-Site VPN connexion cible.	18 décembre 2018

ASN personnalisé	Lorsque vous créez une passerelle réseau privé virtuel, vous pouvez spécifier le numéro d'ASN (Autonomous System Number) privé pour le côté Amazon de la passerelle.	10 octobre 2017
Options de tunnel VPN	Vous pouvez spécifier des blocs d'adresse CIDR de tunnel internes et des clés pré-partagées personnalisées pour vos tunnels VPN.	3 octobre 2017
Métriques VPN	Vous pouvez consulter CloudWatch les statistiques de vos connexions VPN.	15 mai 2017
Améliorations VPN	Une connexion VPN prend désormais en charge la fonction de chiffrement AES 256 bits, la fonction de hachage SHA-256, la traversée NAT et d'autres groupes Diffie-Hellman supplémentaires pendant la Phase 1 et la Phase 2 d'une connexion. En outre, vous pouvez maintenant utiliser la même adresse IP de passerelle client pour chaque connexion VPN qui utilise le même périphérique de passerelle client.	28 octobre 2015

Connexions VPN utilisant une configuration de routage statique	Vous pouvez créer des connexions IPsec VPN vers Amazon VPC à l'aide de configurations de routage statiques. Auparavant, les connexions VPN impliquaient l'utilisation du protocole BGP (Border Gateway Protocol). Nous prenons désormais en charge les deux types de connexion et vous pouvez maintenant établir des connexions depuis des appareils qui ne prennent pas en charge BGP, notamment Cisco ASA et Microsoft Windows Server 2008 R2.	13 septembre 2012
Propagation automatique du routage	Vous pouvez désormais configurer la propagation automatique des routes depuis votre VPN et AWS Direct Connect des liens vers vos tables de routage VPC.	13 septembre 2012
Site-to-Site VPN CloudHub et connexions VPN redondantes	Vous pouvez communiquer en toute sécurité entre deux sites avec ou sans un VPC. Vous pouvez utiliser des connexions VPN redondantes afin de permettre une connexion tolérante aux pannes à votre VPC.	29 septembre 2011

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.