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 AWS Site-to-Site VPN ?

Par défaut, les instances que vous lancez sur un Amazon VPC ne peuvent pas communiquer avec votre propre réseau (distant). Vous pouvez activer l'accès à votre réseau distant à partir de votre VPC en créant une connexion AWS Site-to-Site VPN (Site-to-Site VPN) et en configurant le routage pour transmettre le trafic via la 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 sur site. Site-to-Site VPN prend en charge les connexions VPN utilisant l'Internet Protocol Security (IPsec).

Table des matières

Concepts

Voici les concepts clés de Site-to-Site VPN :

- Connexion VPN : connexion sécurisée entre votre équipement sur site et vos VPC.
- 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 : ressource AWS qui fournit des informations à AWS sur votre périphérique de passerelle client.
- Périphérique de passerelle client : périphérique physique ou application logicielle de votre côté de la connexion Site-to-Site VPN.
- Passerelle cible : terme générique pour le point de terminaison VPN du côté Amazon de la connexion Site-to-Site VPN.
- Passerelle réseau privé virtuel : il s'agit du point de terminaison VPN du côté Amazon de votre connexion Site-to-Site VPN qui peut être connecté à un seul VPC.

- Passerelle de transit : hub de transit qui peut être utilisé pour interconnecter plusieurs VPC et réseaux sur site, et comme point de terminaison VPN pour le côté Amazon de la connexion Site-to-Site VPN.

Fonctions de Site-to-Site VPN

Les fonctions suivantes sont prises en charge par les connexions AWS Site-to-Site VPN :

- Internet Key Exchange version 2 (IKEv2)
- NAT Traversal
- ASN sur 4 octets dans la plage de 1 à 2147483647 pour la configuration de Virtual Private Gateway (VGW). Pour plus d'informations, consultez Options de passerelle client pour votre connexion Site-to-Site VPN.
- ASN sur 2 octets pour Customer Gateway (CGW) dans la plage de 1 à 65535. Pour plus d'informations, consultez Options de passerelle client pour votre connexion Site-to-Site VPN.
- Métriques CloudWatch
- 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 AWS Private Certificate Authority
- Prise en charge du trafic IPv6 pour les connexions VPN sur une passerelle de transit

Limites de Site-to-Site VPN

Une connexion Site-to-Site VPN présente les limites suivantes.

- Le trafic IPv6 n'est pas pris en charge pour les connexions VPN sur une passerelle réseau privé virtuel.
- Une connexion AWS VPN ne prend pas en charge la détection de la MTU du chemin.

De plus, tenez compte des points suivants lorsque vous utilisez Site-to-Site VPN.

- Lors de la connexion de vos VPC à un réseau local commun, nous vous recommandons d'utiliser des blocs CIDR non superposés pour vos réseaux.

Utilisation de Site-to-Site VPN

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

- AWS Management Console : 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 une large gamme de services AWS, notamment Amazon VPC, et est prise en charge sur Windows, macOS et Linux. Pour de plus amples informations, veuillez consulter AWS Command Line Interface.
- Kits SDK AWS : fournissent des API propres au langage et se chargent de nombreux détails de connexion, tels que le calcul des signatures, la gestion des nouvelles tentatives de demande et la gestion des erreurs. Pour plus d'informations, consultez Kits SDK AWS.
- 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 la Référence d'API Amazon EC2.

Tarification

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

Le transfert de données depuis Amazon EC2 vers l'Internet vous est facturé. Pour plus d'informations, consultez Transfert de données sur la page Tarification à la demande d'Amazon EC2.

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 PricingAWS Global Accelerator (Tarification).

Fonctionnement d'AWS Site-to-Site VPN

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

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

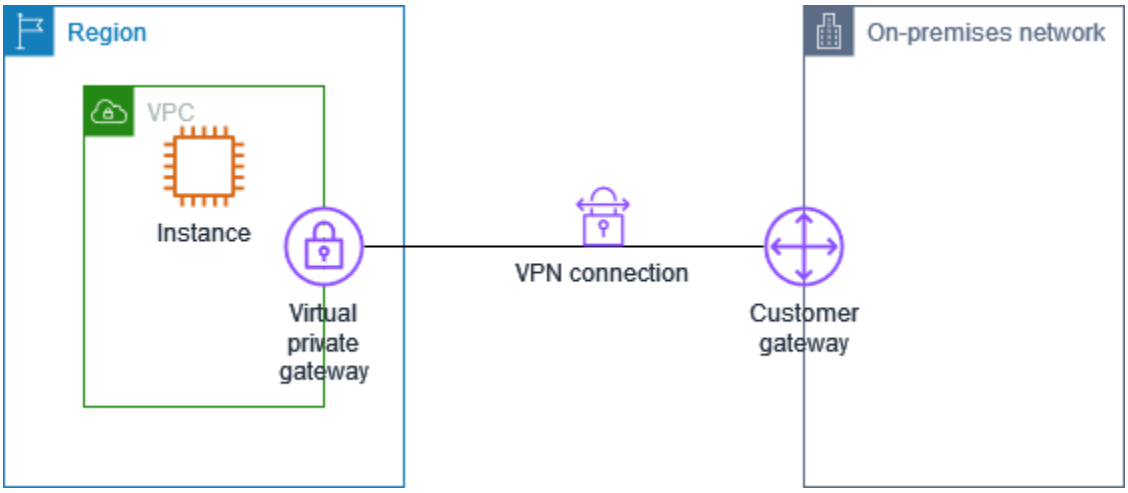
La connexion VPN offre deux tunnels VPN entre une passerelle réseau privé virtuel ou une passerelle de transit du côté d'AWS et une passerelle client du côté sur site.

Pour plus d'informations sur les quotas de Site-to-Site VPN, consultez Quotas de Site-to-Site VPN.

Passerelle réseau privé virtuel

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



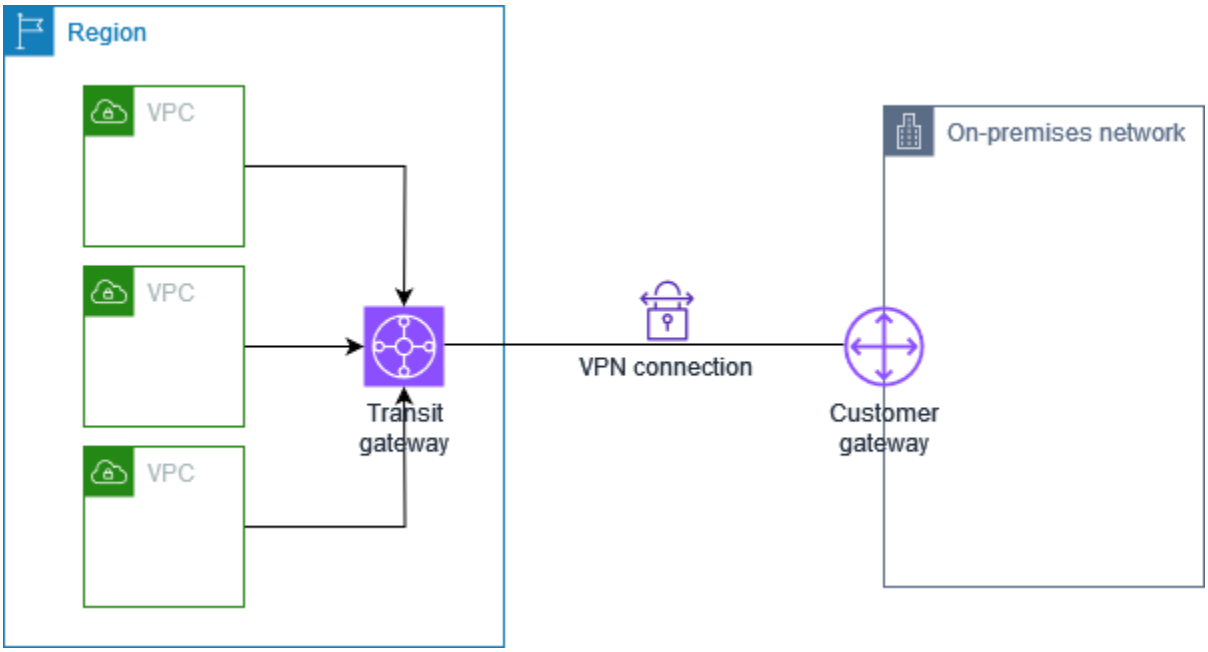
Lorsque vous créez une passerelle réseau privé virtuel, vous pouvez spécifier le numéro d'ASN (Autonomous System Number) privé pour le côté Amazon de la passerelle. Si vous ne spécifiez pas d'ASN, la passerelle réseau privé virtuel est créée avec l'ASN par défaut (64512). Une fois la

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).

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 qu'attachement 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 soit le trafic IPv4, soit le trafic IPv6 à l'intérieur des tunnels VPN. Pour de plus amples informations, veuillez consulter Trafic IPv4 et IPv6.

Vous pouvez modifier la passerelle cible d'une connexion Site-to-Site VPN d'une passerelle réseau privé virtuel vers une passerelle de transit. Pour plus d'informations, consultez the section called "Modification de la passerelle cible d'une connexion VPN".

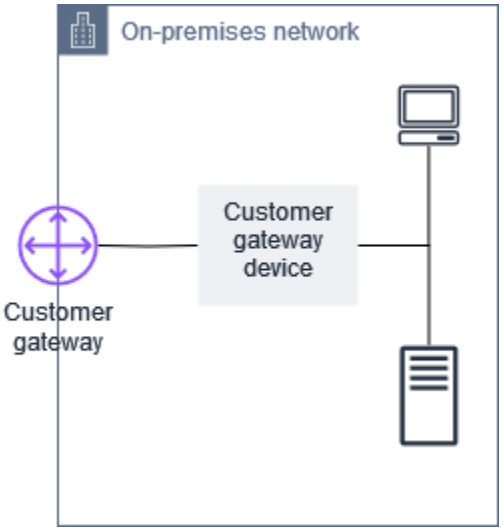
Périphérique de passerelle client

Un périphérique de passerelle client est un périphérique physique ou une application logicielle de votre côté de la connexion Site-to-Site VPN. Vous configurez le périphérique pour qu'il fonctionne avec la connexion Site-to-Site VPN. Pour plus d'informations, consultez Votre périphérique de passerelle client.

Par défaut, votre périphérique de passerelle client doit activer les tunnels de 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 de manière à spécifier que AWS doit lancer le processus de négociation IKE à la place. Pour plus d'informations, consultez Options d'initiation du tunnel Site-to-Site VPN.

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”.

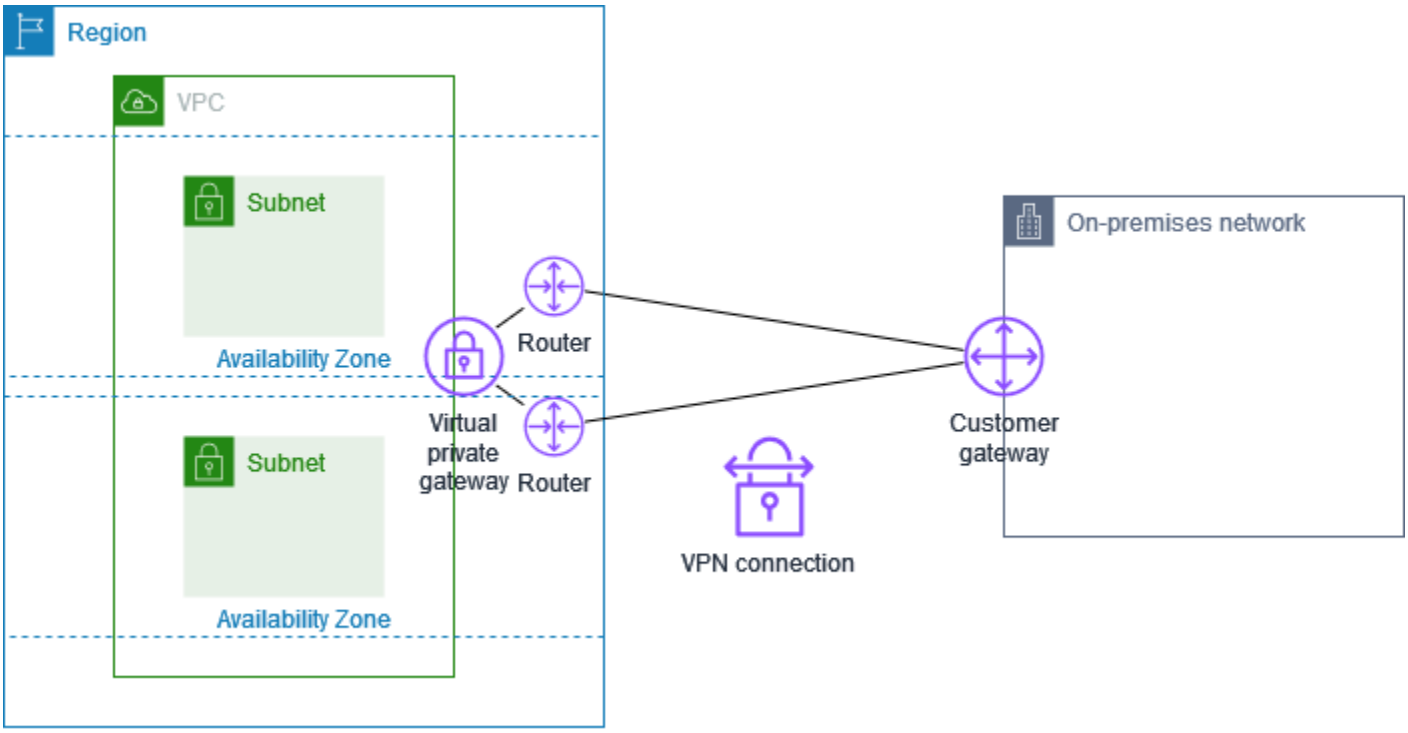


Pour utiliser Amazon VPC avec une connexion Site-to-Site VPN, vous ou votre administrateur réseau devez également configurer le périphérique ou l'application de passerelle client dans un réseau distant. Lorsque vous créez la connexion Site-to-Site VPN, nous vous fournissons les informations de configuration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

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

Vous utilisez une connexion Site-to-Site VPN pour connecter votre réseau distant à un VPC. Chaque connexion Site-to-Site VPN a deux tunnels, chacun utilisant une adresse IP publique unique. Il est important de configurer deux tunnels pour la redondance. Quand un tunnel devient indisponible (par exemple, à des fins de 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 en provenance du réseau sur site vers AWS utilise les deux tunnels. Le trafic en provenance d'AWS vers le réseau sur site préfère l'un des tunnels, mais il peut basculer automatiquement vers l'autre tunnel en cas de panne du côté d'AWS.



Lorsque vous créez une connexion Site-to-Site VPN, vous téléchargez un fichier de configuration spécifique à votre périphérique de passerelle client qui contient les informations nécessaires à la configuration du périphérique, notamment pour chacun des tunnels. Si vous le souhaitez, vous pouvez spécifier vous-même certaines options de tunnel lorsque vous créez la connexion Site-to-Site VPN. Sinon, AWS fournit des valeurs par défaut.

> **Note**
>
> Les points de terminaison du tunnel VPN de site à site évaluent les propositions de votre passerelle client en commençant par la valeur configurée la plus basse dans la liste ci-dessous, quel que soit l'ordre de proposition de la passerelle client. Vous pouvez utiliser la commande `modify-vpn-connection-options` pour restreindre la liste des options que les points de terminaison AWS accepteront. Pour plus d'informations, consultez modify-vpn-connection-options dans Amazon EC2 Command Line Reference (Référence de ligne de commande Amazon EC2).

Voici les options de tunnel que vous pouvez configurer.

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'attente DPD de 40 secondes signifie que le point de terminaison VPN considère que le pair est perdu 30 secondes après le premier keep-alive en échec. 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 Options d'initiation du tunnel Site-to-Site VPN.

Par défaut: `Clear`

Options de journalisation de VPN

Les journaux Site-to-Site VPN vous permettent d'accéder aux détails de l'établissement d'un tunnel IP Security (IPsec), des négociations IKE (Internet Key Exchange) et des messages de protocole DPD (Dead Peer Detection).

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.

Valeur 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 d'adresse CIDR doit être unique sur l'ensemble des connexions Site-to-Site VPN qui utilisent la même passerelle réseau privé virtuel.

> **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. Procéder avec précaution lors de la réutilisation du même bloc d'adresse 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`.

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

d'adresse CIDR doit être unique sur l'ensemble des connexions Site-to-Site VPN qui utilisent la même passerelle de transit.

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

CIDR de réseau IPv4 local

(Connexion VPN IPv4 uniquement) Plage CIDR IPv4 côté passerelle client (sur site) autorisée à communiquer via les tunnels VPN.

Par défaut : 0.0.0.0/0

CIDR réseau IPv4 distant

(Connexion VPN IPv4 uniquement) Plage CIDR IPv4 côté AWS autorisée à communiquer via les tunnels VPN.

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) Plage CIDR IPv6 côté AWS autorisée à communiquer via les tunnels VPN.

Par défaut : ::/0

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

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.

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

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

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.

Valeur 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.

Valeur 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.

Valeur 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.

Valeur 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.

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

Durée de vie phase 1

> **Note**
>
> AWS relance des chiffrements avec les valeurs de synchronisation définies dans les champs de durée de vie Phase 1 et 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 relance des chiffrements avec les valeurs de synchronisation définies dans les champs de durée de vie Phase 1 et 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)

Clé pré-partagée (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 de la phase 1 et de la phase 2, au cours de laquelle le côté AWS de la connexion VPN effectue un changement de 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 valeurs suivantes :

- `Start` : AWS lance la négociation IKE pour activer 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 Options d'initiation du tunnel Site-to-Site VPN.

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 Contrôle du cycle de vie des points de terminaison de tunnel.

Par défaut: `Off`

Vous pouvez spécifier les options de tunnel lorsque vous créez une connexion Site-to-Site VPN ou 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

- Modification des options de tunnel Site-to-Site VPN

Options d'authentification du tunnel Site-to-Site VPN

Vous pouvez utiliser des clés prépartagées ou des certificats pour authentifier vos points de terminaison de tunnel Site-to-Site VPN.

Clés prépartagées

La clé prépartagée est l'option d'authentification par défaut.

Une clé prépartagée est une option de tunnel Site-to-Site VPN que vous pouvez spécifier lorsque vous créez un tunnel Site-to-Site VPN.

Une clé prépartagée est une chaîne que vous entrez lorsque vous configurez votre périphérique de passerelle client. Si vous ne spécifiez pas de chaîne, nous générons automatiquement une chaîne pour vous. Pour plus d'informations, consultez Votre périphérique de passerelle client.

Certificat privé de AWS Private Certificate Authority

Si vous ne souhaitez pas utiliser de clés prépartagées, vous pouvez utiliser un certificat privé provenant de AWS Private Certificate Authority pour authentifier votre VPN.

Vous devez créer un certificat privé à partir d'une autorité de certification subordonnée à l'aide d' AWS Private Certificate Authority (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 AWS Private Certificate Authority .

Vous devez créer un rôle lié à un service pour générer et utiliser le certificat pour le côté AWS du point de terminaison du tunnel VPN site à site. Pour plus d'informations, consultez the section called "Rôles liés à un service".

Après avoir généré le certificat privé, vous spécifiez le certificat lorsque vous créez la passerelle client, puis vous l'appliquez à votre périphérique de passerelle client.

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.

Options d'initiation du tunnel Site-to-Site VPN

Par défaut, votre périphérique de passerelle client doit activer les tunnels de 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 l'autre des options (ou les deux) pour l'un ou l'autre des tunnels (ou les deux) dans votre connexion VPN site à site. 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 dispositif de passerelle client est nécessaire. 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 plus d'informations, consultez Modification de la passerelle client pour une connexion VPN site à site.
- L'initiation IKE (action de démarrage) depuis le AWS côté de la connexion VPN n'est prise en charge que pour IKEv2.

- 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 périphérique de passerelle client se trouve derrière un pare-feu ou un autre périphérique utilisant NAT (Network Address Translation), il doit avoir une identité (IDR) configurée. Pour plus d'informations sur une IDr, consulter 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 pendant une période (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 : Modification des options de tunnel Site-to-Site VPN

Remplacements de points de terminaison de tunnel Site-to-Site VPN

Votre connexion Site-to-Site VPN se compose de deux tunnels VPN pour la redondance. Parfois, un ou les deux points de terminaison du tunnel VPN est remplacé lorsque AWS effectue des mises à jour de 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

- Contrôle du cycle de vie des points de terminaison de 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 à vos points de terminaison de 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 de 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.

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 des remplacements des points de terminaison et peut contribuer à minimiser les interruptions de connectivité lors des remplacements des points de terminaison de tunnel gérés par AWS. Grâce à cette fonction, vous pouvez choisir d'accepter les mises à jour gérées par AWS pour les points de terminaison de 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, AWS peut appliquer immédiatement des mises à jour critiques aux points de terminaison de tunnel, même si la fonction de contrôle du cycle de vie des points de terminaison de 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 notifications AWS Health concernant les prochains remplacements de points de terminaison de tunnel.
- Le statut de la maintenance en attente, ainsi que les horodatages de la Maintenance appliquée automatiquement après et de la Dernière maintenance appliquée, peuvent être consultés dans la AWS Management Console ou à l'aide de la commande d'AWS CLI get-vpn-tunnel-replacement-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 les mises à jour avant la date de Maintenance appliquée automatiquement après, AWS remplacera automatiquement le point de terminaison de tunnel peu de temps après, dans le cadre du cycle de mise à jour de maintenance normal.

Activer le contrôle du cycle de vie des points de terminaison de tunnel

Vous pouvez activer cette fonction à l'aide de la AWS Management Console ou de l'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 points de terminaison de tunnel avec la AWS Management Console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation de gauche, choisissez Connexions VPN site à site.
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. Choisissez Enregistrer les modifications.

Pour activer le contrôle du cycle de vie des points de terminaison de tunnel avec la AWS CLI

Utilisez la commande modify-vpn-tunnel-options pour activer le contrôle du cycle de vie des points de terminaison de 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 points de terminaison de tunnel lors de la création d'une connexion VPN avec la AWS Management 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 (Connexions Site-to-Site VPN).
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 points de terminaison de tunnel lors de la création d'une connexion VPN avec la AWS CLI

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

Vérifier si le contrôle du cycle de vie des points de terminaison de tunnel est activé

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

Pour vérifier si le contrôle du cycle de vie des points de terminaison de tunnel est activé avec la AWS Management Console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation de gauche, choisissez Connexions VPN site à site.
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 de tunnel est activé avec la AWS CLI

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

Vérifier les mises à jour disponibles

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 AWS Management Console ou l'interface de ligne de commande.

Pour vérifier les mises à jour disponibles avec la AWS Management Console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation de gauche, choisissez Connexions VPN site à site.
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 avec la AWS CLI

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

Accepter une mise à jour de maintenance

Lorsqu'une mise à jour de maintenance est disponible, vous pouvez l'accepter à l'aide de la AWS Management Console ou de l'interface de ligne de commande.

Pour accepter une mise à jour de maintenance disponible avec la AWS Management Console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation de gauche, choisissez Connexions VPN site à site.
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 avec la AWS CLI

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

Désactiver le contrôle du cycle de vie des points de terminaison de tunnel

Si vous ne souhaitez plus utiliser la fonction de contrôle du cycle de vie des points de terminaison de tunnel, vous pouvez la désactiver à l'aide de la AWS Management Console ou de l'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 fonction sans utiliser l'option Ignorer le remplacement du tunnel, mais AWS déploiera automatiquement les mises à jour de maintenance en attente disponibles en lançant immédiatement le remplacement du point de terminaison de tunnel.

Pour désactiver le contrôle du cycle de vie des points de terminaison de tunnel avec la AWS Management Console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation de gauche, choisissez Connexions VPN site à site.
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. Choisissez Enregistrer les modifications.

Pour désactiver le contrôle du cycle de vie des points de terminaison de tunnel avec la AWS CLI

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

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

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	Un ASN compris entre 1 et 4 294 967 295 est pris en charge. Vous pouvez utiliser un numéro

Élément	Description
(Border Gateway Protocol) de la passerelle client.	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 65 000. Pour en savoir plus sur le routage, consultez Options de routage Site-to-Site VPN.
(Facultatif) L'adresse IP de l'interface externe du périphérique de passerelle client.	L'adresse IP doit être statique. Si votre passerelle client se trouve derrière un appareil exécutant une traduction d'adresse réseau (NAT), utilisez l'adresse IP de cet appareil 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 points de terminaison. AWS Site-to-Site VPN Pour plus d'informations, consultez Règles de pare-feu. Une adresse IP n'est pas requise lorsque vous utilisez un certificat privé AWS Private Certificate Authority 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 la configurer pour qu'elle utilise des certificats privés AWS Private Certificate Authority 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 AWS Private Certificate Authority, 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 AWS Private Certificate Authority .
Appareil (Facultatif).	Nom de l'appareil de passerelle client associé à cette passerelle client.

Connexions Site-to-Site VPN accélérées

Vous pouvez activer l'accélération pour votre connexion Site-to-Site VPN. Une connexion VPN Site-to-site accélérée (connexion VPN accélérée) permet d'acheminer le trafic de votre réseau local AWS Global Accelerator vers l'emplacement AWS périphérique le plus proche de votre dispositif de 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 des API.

Pour plus d'informations sur les AWS régions qui prennent en charge les connexions VPN accélérées, consultez les FAQ sur le VPN AWS accéléré de site à site.

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

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 attachées à une passerelle de transit. Les passerelles réseau privé virtuel ne prennent pas en charge les connexions VPN accélérées.
- Une connexion VPN accélérée de site à site ne peut pas être utilisée avec une AWS Direct Connect interface virtuelle publique.

- Vous ne pouvez pas activer ou désactiver l'accélération d'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. Ensuite, configurez votre périphérique de passerelle client pour utiliser 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.
- Les connexions VPN de site à site 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.

Options de routage Site-to-Site VPN

Lorsque vous créez une connexion Site-to-Site VPN, vous devez procéder comme suit :

- 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

- Trafic IPv4 et IPv6

Routage statique et dynamique

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

Si vous utilisez un périphérique qui prend en charge les annonces BGP, vous n'avez pas besoin de spécifier de routes statiques vers la connexion Site-to-Site VPN puisque le périphérique utilise BGP pour publier ses routes vers la passerelle réseau privé virtuel. 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 périphérique de passerelle client pour acheminer le trafic de votre réseau sur site 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 Votre périphérique de passerelle client.

Tables de routage et priorité de route VPN

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 acheminements propagés à partir d'une connexion Site-to-Site VPN ou d'une connexion AWS Direct Connect chevauchent l'acheminement local de votre VPC, l'acheminement local est privilégié, même si les acheminements reproduits sont plus spécifiques.
- Si les acheminement propagés à partir d'une connexion Site-to-Site VPN ou d'une connexion AWS Direct Connect ont le même bloc d'adresse CIDR de destination que d'autres acheminements statiques existants (la correspondance du préfixe le plus long ne peut pas s'appliquer), la priorité est accordée aux acheminements statiques dont les cibles sont une passerelle Internet, une passerelle réseau privé virtuel, une interface réseau, un ID d'instance, une connexion d'appairage de VPC, une passerelle NAT, une passerelle de transit ou un point de terminaison d'un 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 réseau privé virtuel ne prennent pas en charge le trafic IPv6.

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 VPN sur

les passerelles réseau privé virtuel et les 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 :

- Acheminements propagés BGP depuis une connexion AWS Direct Connect
- Routes statiques ajoutées manuellement pour une connexion Site-to-Site VPN
- Routes propagées BGP à partir d'une connexion Site-to-Site VPN
- Pour les préfixes qui correspondent lorsque chaque connexion Site-to-Site VPN utilise BGP, le chemin d'AS est comparé et le préfixe comportant le chemin d'AS le plus court est privilégié.

> **Note**
>
> AWS recommande fortement d'utiliser des périphériques de passerelle client qui prennent en charge l'acheminement 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 chemins d'AS ont la même longueur et si le premier AS dans AS_SEQUENCE est le même sur plusieurs chemins, les attributs MED (multi-exit discriminators) 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 d'évacuation 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 VPN sur les passerelles réseau privé virtuel et les passerelles de transit.

Pour une passerelle réseau privé virtuel, un tunnel à travers toutes les connexions Site-to-Site VPN de la passerelle sera sélectionné. Pour utiliser plusieurs tunnels, nous vous recommandons d'explorer Equal Cost Multipath (ECMP), 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. ECMP n'est pas pris en charge pour les connexions Site-to-Site VPN sur une passerelle réseau privé virtuel.

Pour les connexions Site-to-Site VPN qui utilisent 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 de trafic ou des métriques.

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

Une connexion Site-to-Site VPN est composée de deux tunnels VPN entre un périphérique de passerelle client et une passerelle réseau privé virtuel ou une passerelle de transit. Nous vous recommandons de configurer les deux tunnels pour la redondance. De temps en temps, AWS effectue également des opérations de maintenance habituelles 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).

Trafic IPv4 et IPv6

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

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

Les règles suivantes s'appliquent :

- Les adresses IPv6 ne sont prises en charge que pour les adresses IP internes des tunnels VPN. Les adresses IP externes du tunnel des points de terminaison AWS sont des adresses IPv4, et l'adresse IP publique de votre passerelle client doit être une adresse IPv4.
- Les connexions Site-to-Site VPN sur une passerelle réseau privé virtuel ne prennent pas en charge IPv6.
- Vous ne pouvez pas activer la prise en charge IPv6 pour une connexion Site-to-Site VPN existante.
- Une connexion Site-to-Site VPN ne peut pas prendre en charge le trafic IPv4 et IPv6.

Pour plus d'informations sur la création d'une connexion VPN, consultez Étape 5 : Création d'une connexion VPN.

Commencer avec AWS Site-to-Site VPN

Pour configurer une AWS Site-to-Site VPN connexion, procédez comme suit. Pendant la création, vous devrez spécifier une passerelle réseau privé virtuel, une passerelle de transit ou l'option « Non associée » 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

- Prérequis
- 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, consultezCréation d'une pièce jointe VPN pour AWS Cloud WAN.
- Pour créer une connexion VPN sur une passerelle de transit, consultez Création d'un attachement de VPN de passerelle de transit.

Prérequis

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 AWS Private Certificate Authority pour authentifier votre VPN Pour plus d'informations, consultez 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 plus d'informations, consultez Options de tunnel pour votre connexion Site-to-Site VPN.

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 plus d'informations, consultez 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. AWS Private Certificate Authority 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 AWS Private Certificate Authority .

> **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. (Facultatif) Pour IP address (Adresse IP), entrez l'adresse IP statique routable sur Internet pour votre périphérique 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.
7. (Facultatif) Si vous souhaitez utiliser un certificat privé, pour ARN du certificat, choisissez l'Amazon Resource Name (ARN) du certificat privé.

8. (Facultatif) Pour Appareil, saisissez un nom pour l'appareil de passerelle client associé à cette passerelle client.
9. Choisissez Créer la passerelle client.

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

- CreateCustomerPasserelle (API de requête Amazon EC2)
- create-customer-gateway (AWS CLI)
- 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. Pour VPC disponibles, choisissez votre VPC, puis Attacher au VPC.

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

- CreateVpnPasserelle (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

- AttachVpnPasserelle (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 de route pour que votre table de routage propage automatiquement les routes 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, choisissez Connexions VPN site à site.
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 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. Pour Préfixes IP statiques, spécifiez chaque préfixe IP pour le réseau privé de votre connexion VPN.

7. Si votre type de passerelle cible est la passerelle de transit, pour Version des adresses IP internes du tunnel, indiquez si les tunnels VPN prennent en charge le trafic IPv4 ou IPv6. Le trafic IPv6 n'est pris en charge que pour les connexions VPN sur une passerelle de transit.
8. Si vous avez spécifié IPv4 pour la version Tunnel inside IP, vous pouvez éventuellement spécifier les plages d'adresses CIDR IPv4 pour la passerelle client et AWS les côtés autorisés à communiquer via les tunnels VPN. L'argument par défaut est `0.0.0.0/0`.

   Si vous avez spécifié IPv6 pour la version Tunnel inside IP, vous pouvez éventuellement spécifier les plages d'adresses CIDR IPv6 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`.
9. Pour le type d'adresse IP externe, conservez l'option par défaut, PublicIpv4.
10. (Facultatif) Pour Options de tunnel, vous pouvez spécifier les informations suivantes pour chaque tunnel :

    - Bloc d'adresses CIDR de taille /30 IPv4 de la plage `169.254.0.0/16` pour les adresses IPv4 internes du tunnel.
    - Si vous avez spécifié IPv6 pour Version des adresses IP internes du tunnel, un bloc d'adresses CIDR /126 IPv6 de la plage `fd00::/8` pour les adresses IPv6 internes du tunnel.
    - La clé pré-partagée (PSK) IKE. Les versions suivantes sont prises en charge : IKEv1 et IKEv2.
    - Pour modifier les options avancées de votre tunnel, choisissez Modifier les options du tunnel. Pour plus d'informations, consultez Options de tunnel VPN.
11. 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

- CreateVpnConnexion (API de requête Amazon EC2)
- create-vpn-connection (AWS CLI)
- 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 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 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. Pour obtenir la liste des fichiers de configuration avec prise en charge d'IKEv2, consultez Votre périphérique de passerelle client.

Autorisations

Pour charger correctement l'écran de configuration du téléchargement depuis le AWS Management Console, vous devez vous assurer que votre rôle ou utilisateur IAM est autorisé à utiliser les API `GetVpnConnectionDeviceTypes` Amazon EC2 suivantes : 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, choisissez Connexions VPN site à site.
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-sample-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 plus d'informations, voir Votre périphérique de passerelle client.

Architectures Site-to-Site VPN

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

- the section called "Connexions VPN uniques et multiples"
- the section called "Connexions VPN redondantes"
- the section called "AWS VPN CloudHub"

Exemples d'une connexion VPN site à site unique et de plusieurs connexions VPN

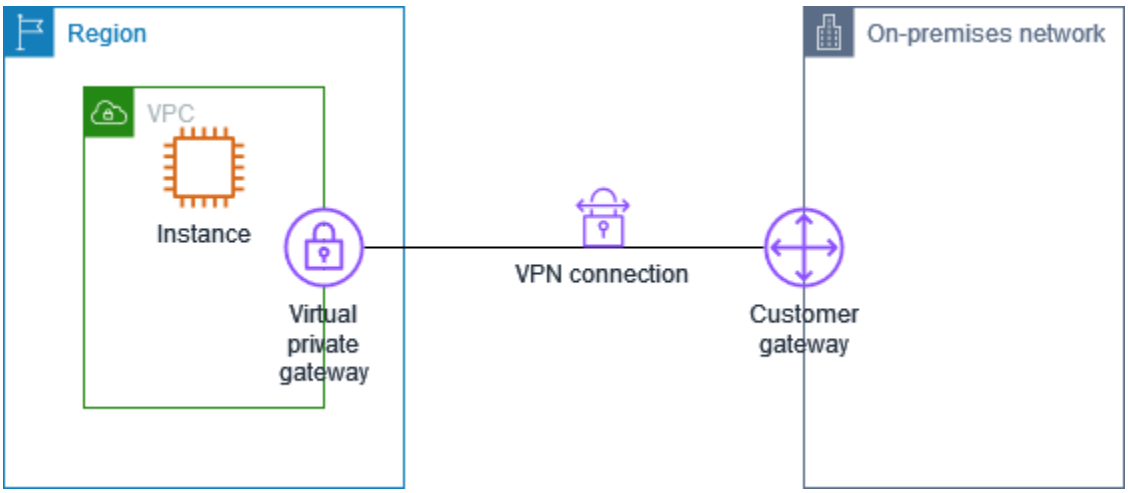
Les schémas suivants illustrent des connexions Site-to-Site VPN simples et multiples.

Exemples

- Connexion Site-to-Site VPN simple
- Connexion Site-to-Site VPN simple avec passerelle de transit
- Connexions Site-to-Site VPN multiples
- Connexions Site-to-Site VPN multiples avec une passerelle de transit
- Connexion de site à site VPN avec AWS Direct Connect.
- Connexion de site à site VPN d'IP privée avec AWS Direct Connect.

Connexion Site-to-Site VPN simple

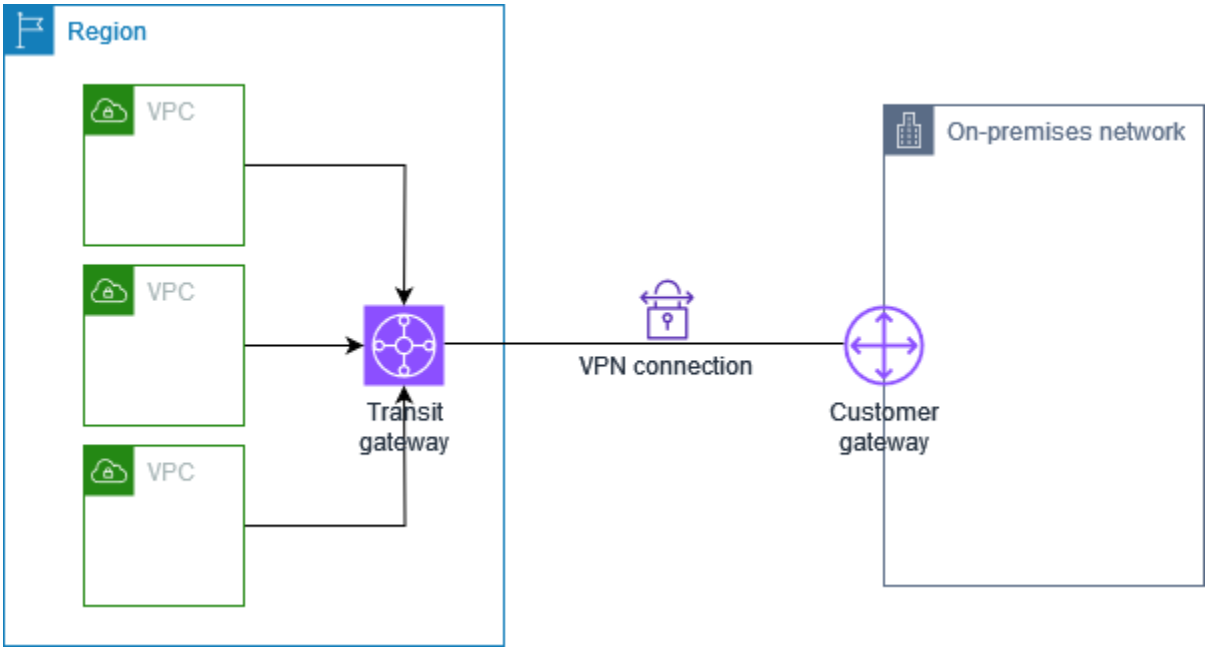
Le VPC a une passerelle réseau privé virtuel attachée et votre réseau sur site (distant) comprend un périphérique de passerelle client que vous devez configurer pour activer la connexion VPN. Vous devez mettre à jour les tables de routage de VPC afin que le trafic de votre VPC lié à votre réseau soit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



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

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

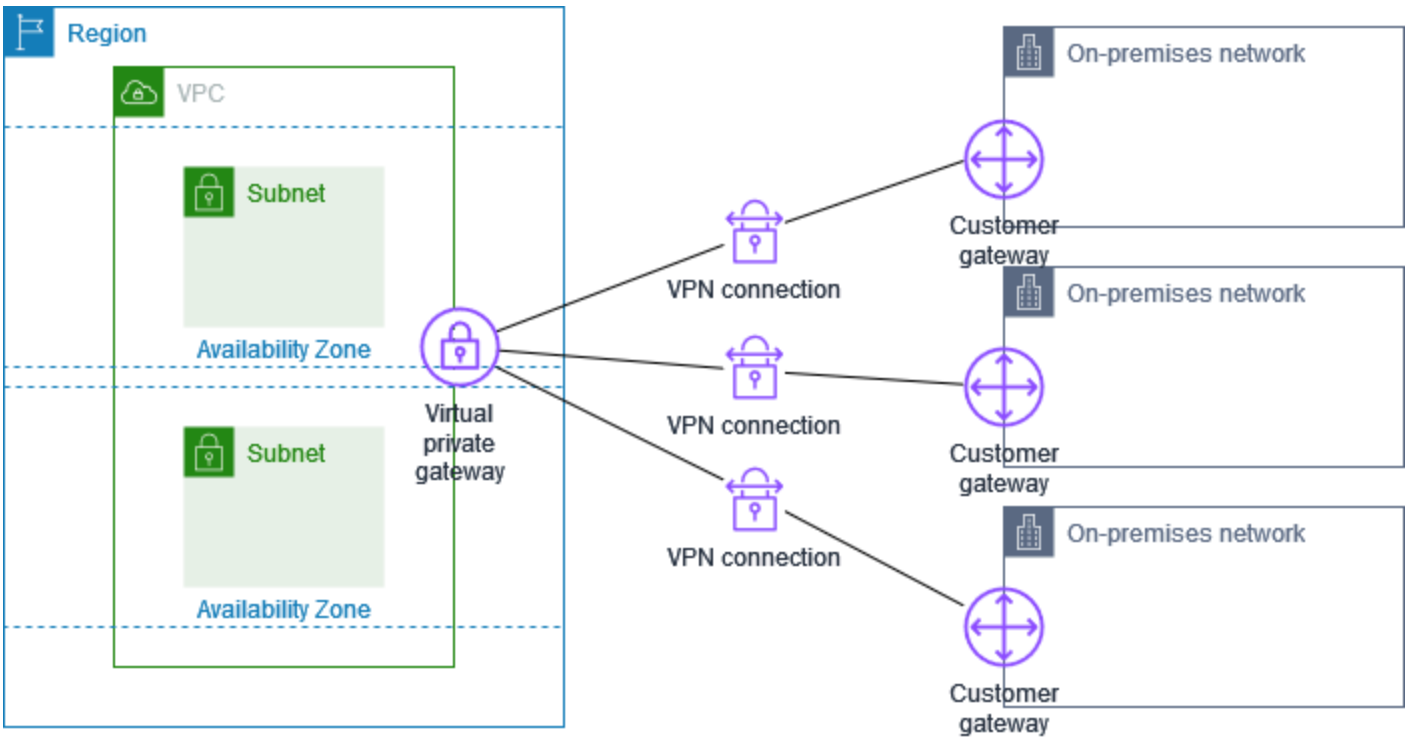
Le VPC a une passerelle de transit attachée et votre réseau sur site (distant) comprend un périphérique de passerelle client que vous devez configurer pour permettre la connexion VPN. Vous devez mettre à jour les tables de routage de VPC afin que le trafic de votre VPC lié à votre réseau soit acheminé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



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

Connexions Site-to-Site VPN multiples

Le VPC dispose d'une passerelle réseau privé virtuel attachée et vous disposez de plusieurs connexions Site-to-Site VPN vers plusieurs emplacements 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.

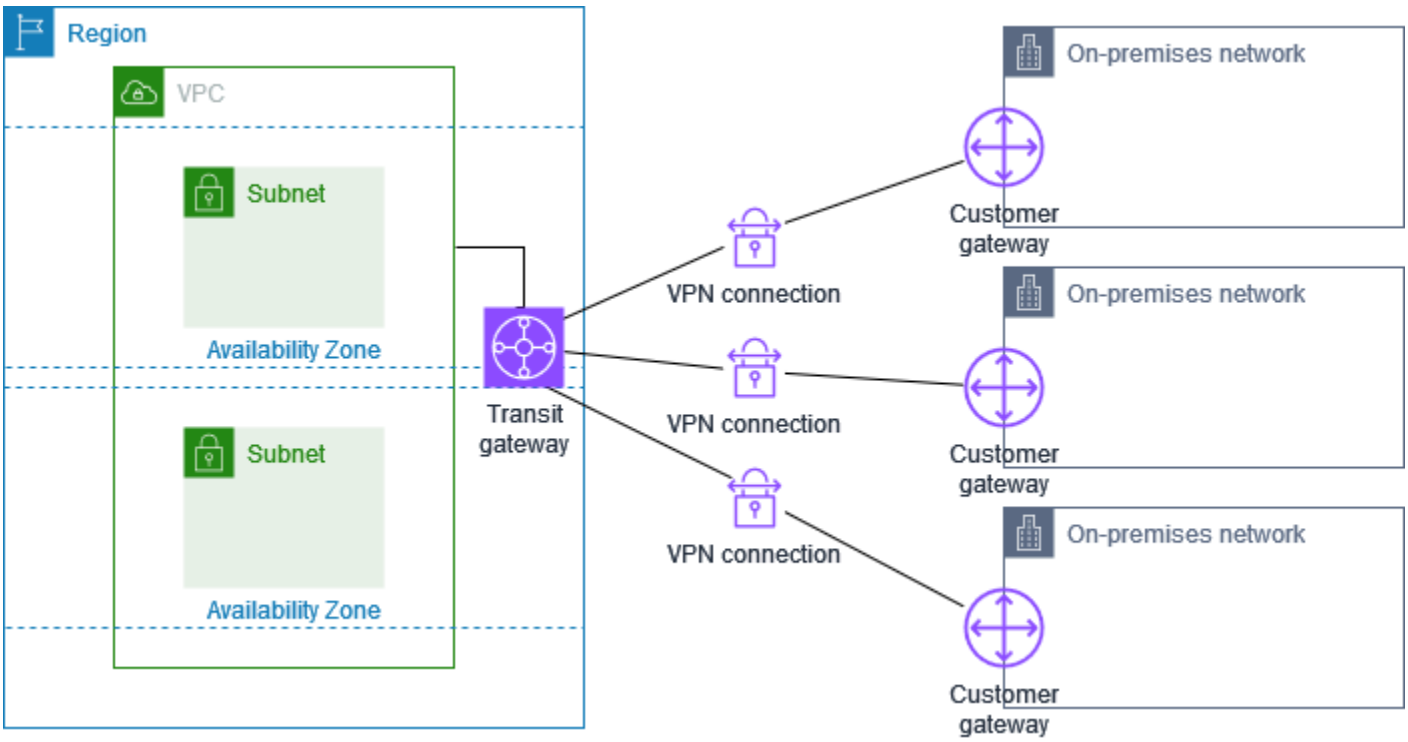


Lorsque vous créez plusieurs connexions Site-to-Site VPN vers un seul VPC, vous pouvez configurer une seconde passerelle client pour créer une connexion redondante vers le même emplacement externe. Pour de plus amples informations, veuillez consulter Utilisation de connexions Site-to-Site VPN redondantes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

Vous pouvez également utiliser ce scénario pour créer des connexions Site-to-Site VPN vers plusieurs emplacements géographiques et fournir une communication sécurisée entre les sites. Pour de plus amples informations, veuillez consulter Fourniture d'une communication sécurisée entre les sites à l'aide du VPN CloudHub.

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

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

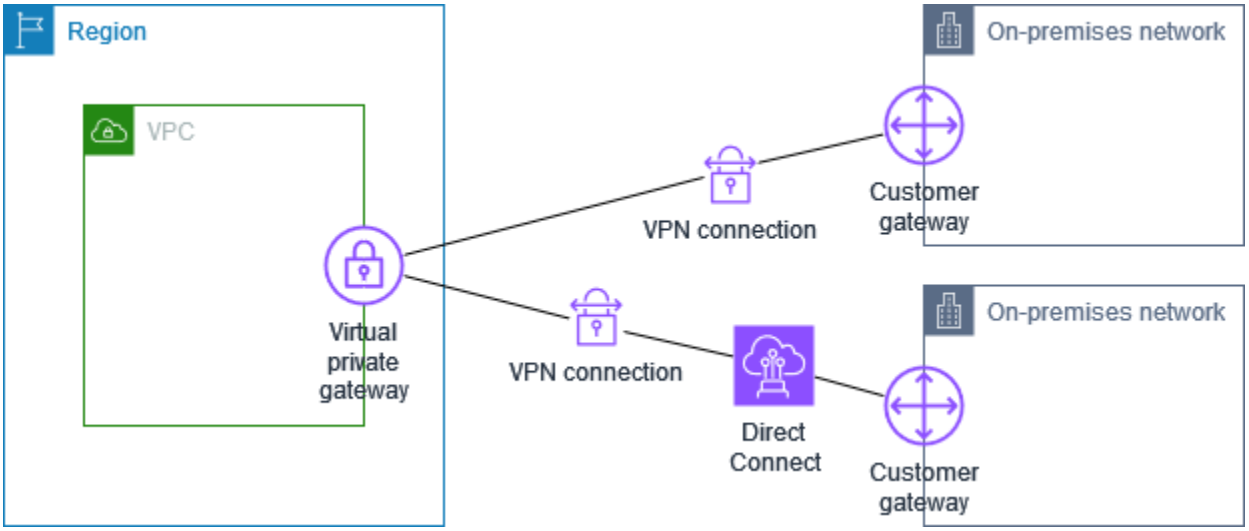


Lorsque vous créez plusieurs connexions Site-to-Site VPN vers une seule passerelle de transit, vous pouvez configurer une seconde passerelle client pour créer une connexion redondante vers le même emplacement externe.

Vous pouvez également utiliser ce scénario pour créer des connexions Site-to-Site VPN vers plusieurs emplacements géographiques et fournir une communication sécurisée entre les sites.

Connexion de site à site VPN avec AWS Direct Connect.

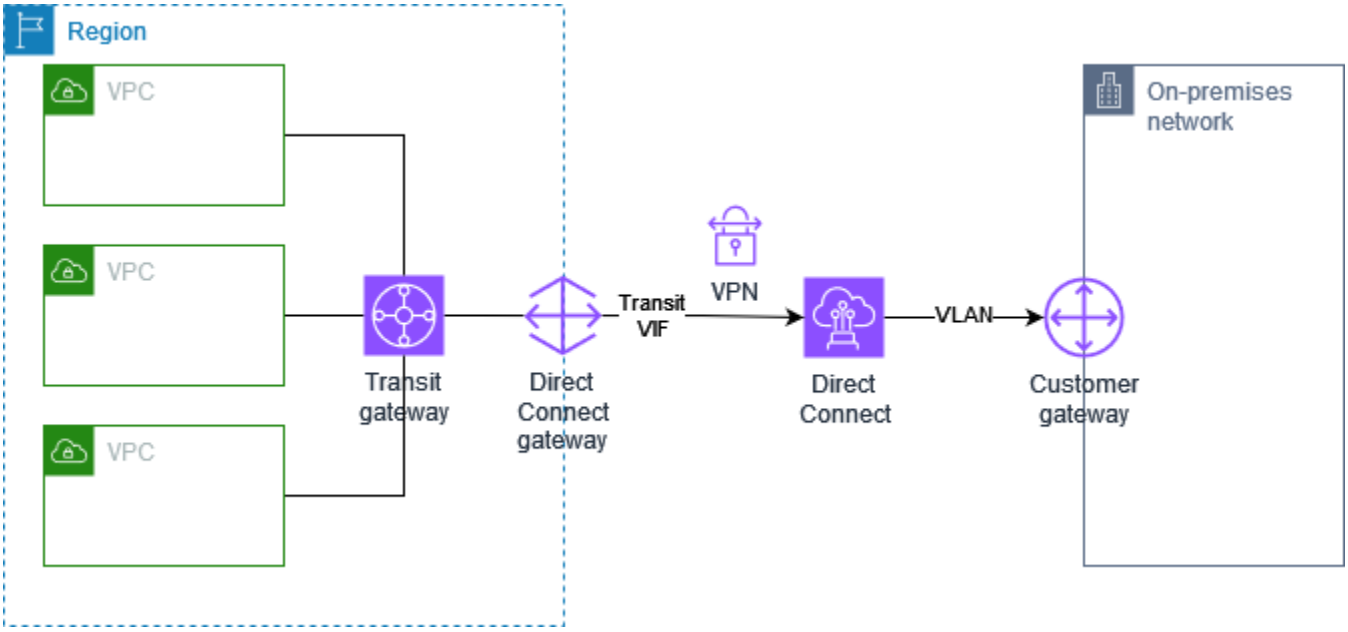
Le VPC dispose d'une passerelle réseau privé virtuel attachée et se connecte à votre réseau sur site (distant) via AWS Direct Connect. Vous pouvez configurer une interface virtuelle publique AWS Direct Connect pour établir une connexion réseau dédiée entre votre réseau et les ressources AWS publiques via une passerelle réseau privé virtuel. Vous configurez le routage afin que le trafic de votre VPC lié à votre réseau soit acheminé vers la passerelle réseau privé virtuel et la connexion AWS Direct Connect.



Quand AWS Direct Connect et la connexion VPN sont configurés sur la même passerelle réseau privé virtuel, l'ajout ou la suppression d'objets peut amener la passerelle réseau privé virtuel à passer à l'état « attachement ». Cela indique qu'une modification est apportée au routage interne qui basculera entre AWS 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 de site à site VPN d'IP privée avec AWS Direct Connect.

Avec un VPN de siste à site d'IP privée, vous pouvez chiffrer le trafic AWS Direct Connect entre votre réseau sur site et AWS sans utiliser d'adresses IP publiques. Le VPN d'IP privée via AWS Direct Connect garantit que le trafic entre AWS et les réseaux locaux sont à la fois sécurisés et privés, ce qui permet aux clients de se conformer aux mandats réglementaires et de sécurité.



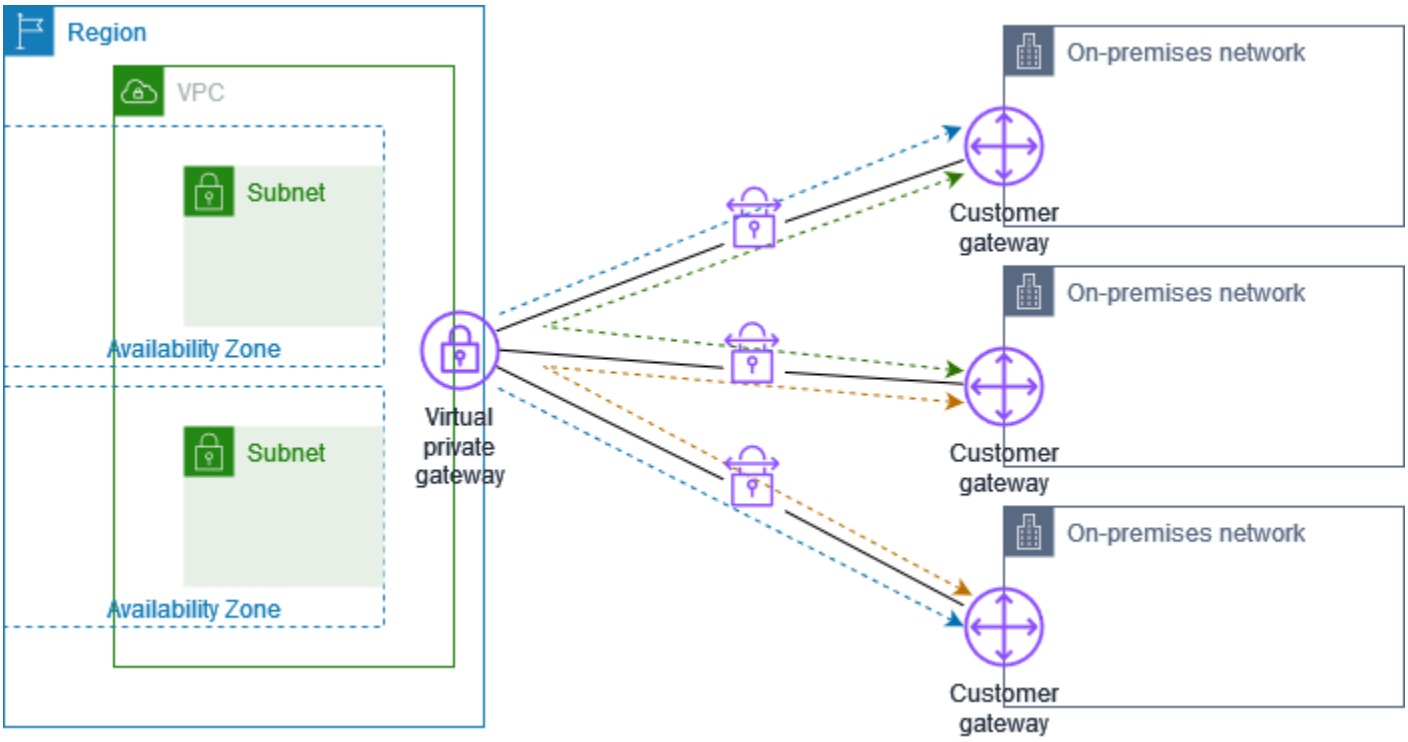
Pour plus d'informations, consultez le billet de blog suivant : Présentation des VPN d'IP privées AWS Site-to-Site VPN.

Fourniture d'une communication sécurisée entre les sites à l'aide du VPN CloudHub

Si vous avez plusieurs connexions AWS Site-to-Site VPN, vous pouvez assurer une communication sécurisée entre les sites à l'aide d'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 sur un simple modèle en étoile (hub and spoke) que vous pouvez utiliser avec ou sans VPC. Ce modèle convient aux clients ayant plusieurs succursales et des connexions Internet existantes qui aimeraient implémenter un modèle en étoile (hub-and-spoke) pratique et potentiellement à bas coût pour une connexion primaire ou de sauvegarde entre ces sites.

Présentation

Le schéma suivant illustre l'architecture VPN CloudHub. 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. Ensuite, créez une connexion Site-to-Site VPN acheminée de manière dynamique pour chaque passerelle client vers une passerelle réseau privé virtuel 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. Ce point est réalisable en utilisant les relevés du réseau 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 des connexions AWS Direct Connect vers la passerelle réseau privé virtuel peuvent également faire partie de AWS VPN CloudHub. Par exemple, votre siège social à New York peut avoir une connexion AWS Direct Connect vers le VPC et vos succursales peuvent utiliser des connexions Site-to-Site VPN vers le VPC. Les succursales de Los Angeles et Miami peuvent envoyer et recevoir des données entre elles et avec votre siège social, tout cela grâce à AWS VPN CloudHub.

Tarification

Pour utiliser AWS VPN CloudHub, vous payez les tarifs de connexion Amazon VPC Site-to-Site VPN standard. Le tarif de la connexion vous est facturé pour chaque heure de connexion de chaque VPN à la passerelle réseau privé virtuel. Quand vous envoyez des données depuis un site vers un autre à l'aide de AWS VPN CloudHub, l'envoi de données depuis votre site vers la passerelle réseau privé virtuel 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 ont une connexion Site-to-Site VPN à la passerelle réseau privé virtuel, vous payez le tarif

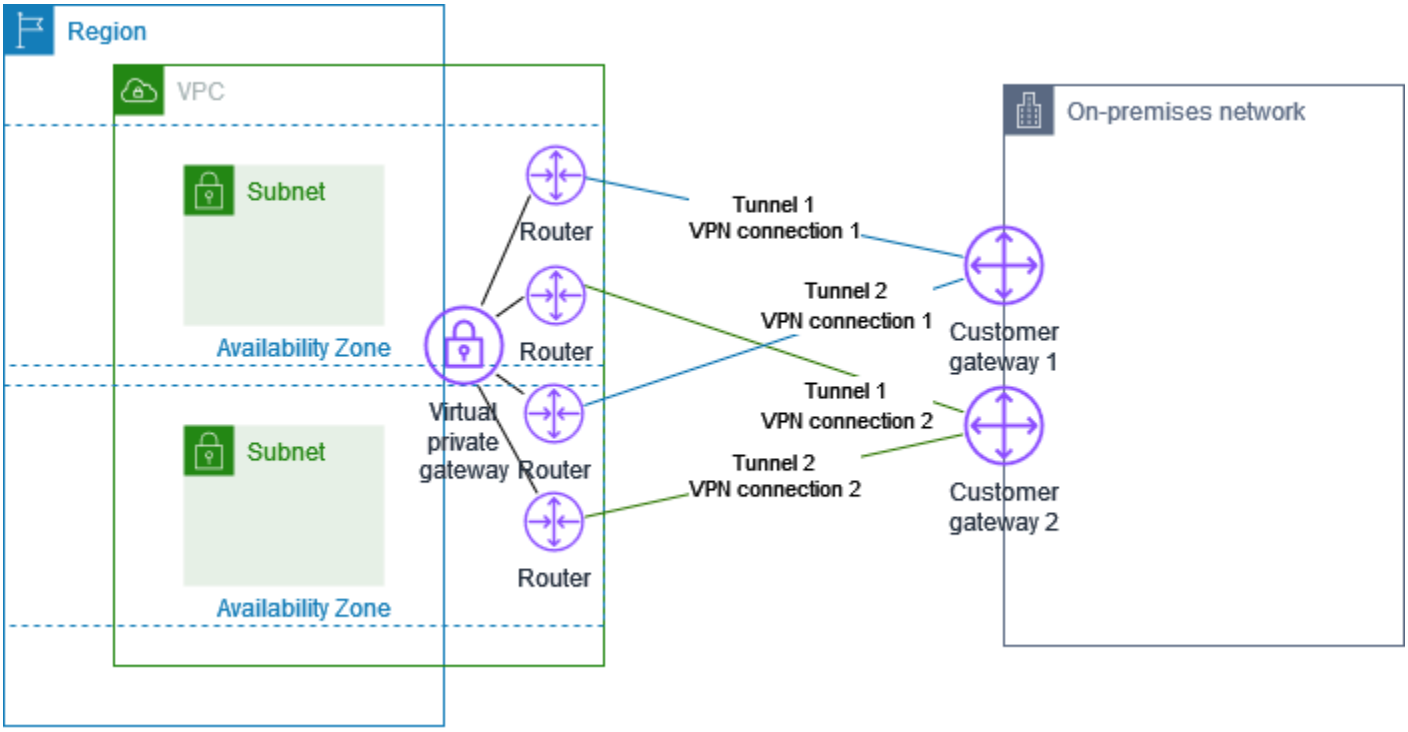
horaire pour chaque connexion Site-to-Site VPN (donc si le tarif est de 0,05 USD l'heure, le total sera de 0,10 USD l'heure). Vous payez également les taux de transfert de données AWS standard pour toutes les données que vous envoyez de Los Angeles à New York (et vice versa) qui traversent chaque connexion Site-to-Site VPN. Le trafic réseau envoyé via la connexion Site-to-Site VPN à la passerelle réseau privé virtuel est gratuit, mais le trafic réseau envoyé via la connexion Site-to-Site VPN depuis la passerelle réseau privé virtuel vers le point de terminaison est facturé au taux de transfert de données AWS standard.

Pour plus d'informations, consultez Tarification des connexions Site-to-Site VPN.

Utilisation de connexions Site-to-Site VPN redondantes pour fournir un basculement

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 Site-to-Site VPN vers votre VPC et votre passerelle réseau privé virtuel en ajoutant un second périphérique 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 seconde connexion Site-to-Site VPN en utilisant la même passerelle réseau privé virtuel et en créant une nouvelle passerelle client. L'adresse IP de la passerelle client pour la seconde connexion Site-to-Site VPN doit être publiquement accessible.
- 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.

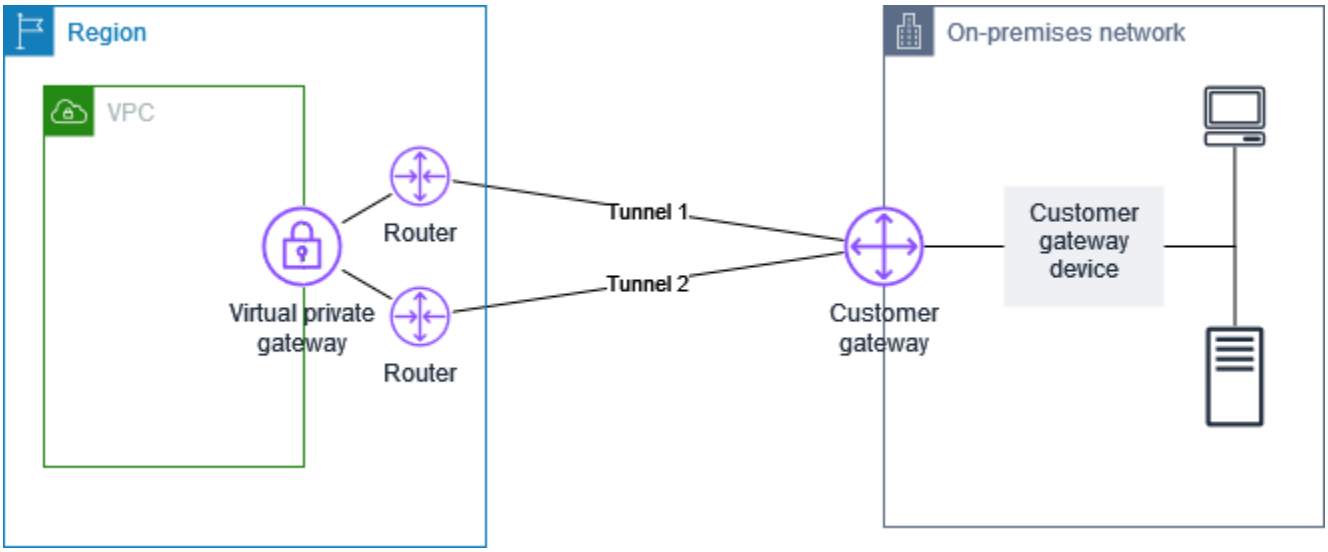
Les connexions Site-to-Site VPN à routage dynamique utilisent le Border Gateway Protocol (BGP) pour échanger des informations de routage entre vos passerelles client et les passerelles réseau privé virtuel. Les connexions Site-to-Site VPN à routage statique nécessitent une saisie des routes statiques pour le réseau distant de votre côté de la passerelle client. Les informations de route saisies statiquement et publiées par BGP permettent aux passerelles de chaque côté 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, consultez Commencer avec AWS Site-to-Site VPN.

Votre périphérique de passerelle client

Un périphérique de passerelle client est une appliance physique ou logicielle que vous possédez ou gérez dans votre réseau sur site (de votre côté d'une connexion Site-to-Site VPN). Vous ou votre administrateur réseau devez configurer le périphérique 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 plus d'informations, consultez Remplacements de points de terminaison de tunnel Site-to-Site VPN. 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 Commencer 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 plus d'informations, consultez Options de passerelle client pour votre connexion Site-to-Site VPN. 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.

Rubriques

Exemples de fichiers de configuration

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 d'exemples de configuration spécifiques pour un routage statique ou dynamique :

Téléchargement des fichiers .zip

- Configuration statique : the section called "Exemples de fichiers de configuration"
- Configuration dynamique : the section called "Exemples de fichiers de configuration"

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 présenté est un simple exemple et peut ne pas correspondre entièrement aux paramètres de connexion Site-to-Site VPN souhaités. Il spécifie les

exigences minimales pour une connexion VPN de site à site de type AES128, SHA1 et Diffie-Hellman groupe 2 dans la plupart des régions, et AES128, SHA2 et Diffie-Hellman groupe 14 dans AWS les régions. AWS GovCloud II 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.

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
Checkpoint	Gaia	R80.10+
Cisco Meraki	MX Series	15.12+ (WebUI)
Cisco Systems, Inc.	ASA 5500 Series	ASA 9.7+ VTI
Cisco Systems, Inc.	CSRv AMI	IOS 12.4+
Fortinet	Fortigate 40+ Series	FortiOS 6.4.4+ (GUI)
Juniper Networks, Inc.	Routeurs J-Series	JunOS 9.5+
Juniper Networks, Inc.	Routeurs SRX	JunOS 11.0+

Vendor	Plateforme	Logiciels
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+

Conditions obligatoires pour votre périphérique de passerelle client

Si votre périphérique ne figure pas dans la liste d'exemples précédente, cette section décrit les conditions requises qu'il doit respecter pour que vous puissiez l'utiliser 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 plus d'informations, consultez Options d'initiation du tunnel Site-to-Site VPN.

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 AWS Private Certificate Authority 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 AWS Private Certificate Authority à utiliser pour votre dispositif de passerelle client. Pour plus d'informations sur la configuration des tunnels VPN, consultez Options de tunnel pour votre connexion Site-to-Site VPN.

Exigence	RFC	Commentaires
		Les versions suivantes sont prises en charge : IKEv1 et IKEv2. Nous prenons en charge le mode Principal uniquement avec la version IKEv1. Le service Site-to-Site VPN est une solution basée sur des routages. Si vous utilisez une configuration basée sur des stratégies, vous devez limiter votre configuration 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 périphérique 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 ou SHA-2 (256)	RFC 2404	Cette fonction de hachage est utilisée pour authentifier les associations de sécurité IKE et IPsec.

Exigence	RFC	Commentaires
Utiliser le protocole de Diffie-Hellman pour une confidentialité persistante parfaite.	RFC 2409	IKE utilise la méthode Diffie-Hellman pour établir des clés éphémères afin de sécuriser toutes les communications entre les passerelles client et les passerelles réseau privé virtuel. Les groupes suivants sont pris en charge : • Phase 1 : groupes 2, 14-24 • Phase 2 : groupes 2, 5, 14-24
(Connexions VPN routées dynamiquement) Utiliser IPsec Dead Peer Detection	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 VPN routées dynamiquement) Relier le tunnel à l'interface logique (VPN basé sur une route) Tunnel	Aucun	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'appaira ge BGP avec la passerelle réseau privé virtuel. Cette interface logique ne doit exécuter aucune encapsula tion supplémentaire (par exemple, GRE ou IP dans IP). Votre interface doit être définie sur une unité de transmission maximale (MTU) de 1 399 octets.

Exigence	RFC	Commentaires
(Connexions VPN routées dynamiquement) Établir des appairages 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'utilise nt. 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 Configuration d'un pare-feu entre Internet et votre périphérique de passerelle client.

Bonnes pratiques pour votre périphérique de passerelle client

Utiliser IKEv2

Nous vous recommandons vivement d'utiliser IKEv2 pour votre connexion VPN Site-to-Site. 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 VPN Site-to-Site 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. Le VPN de site à site réassemble ensuite tous les paquets fragmentés avant de les transférer vers la destination suivante, afin d'augmenter les flux sur le réseau. packet-per-second 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 VPN Site-to-site réassemble tous les paquets fragmentés reçus de votre passerelle client avant de les transférer vers la destination suivante, n'oubliez pas que la taille des paquets et le MTU peuvent être pris en compte pour les réseaux de destination sur lesquels ces paquets seront ensuite transférés, par exemple. AWS Direct Connect

Ajustement des tailles MTU et MSS en fonction des algorithmes utilisés

Les paquets TCP sont souvent le type de paquets le plus répandu dans les tunnels IPsec. Le Site-to-Site 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 définir votre MTU/MSS afin d'éviter la fragmentation et d'obtenir des performances optimales :

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

Algorithme de chiffrement	Algorithme de hachage	NAT-Traversal	MTU	MSS (IPv4)	MSS (IPv6-in-IPv4)
AES-CBC	SHA2-384	activé	1422	1382	1362
AES-CBC	SHA2-512	disabled	1422	1382	1362
AES-CBC	SHA2-512	activé	1406	1366	1346

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

Configuration d'un pare-feu entre Internet et votre périphérique 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 points de terminaison. AWS Site-to-Site VPN Vérifiez si votre périphérique annonce la NAT-T.

Plusieurs scénarios de connexion VPN

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 à partir de votre emplacement sur site vers d'autres VPC à l'aide du même périphérique de passerelle client. De plus, vous pouvez réutiliser la même adresse IP de passerelle client pour chacune de ces connexions VPN.

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 plus d'informations, consultez Utilisation de connexions Site-to-Site VPN redondantes pour fournir un basculement. Lorsque vous établissez des passerelles client redondantes dans un même emplacement, ces dernières doivent publier les mêmes plages d'adresses IP.

Plusieurs dispositifs de passerelle client vers une seule passerelle privée virtuelle (AWS 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 plus d'informations, consultez Fourniture d'une communication sécurisée entre les sites à l'aide du 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.

Routage pour votre périphérique de passerelle client

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 de route VPN.

Exemples de configurations de périphérique de passerelle client pour le routage statique

Rubriques

- Exemples de fichiers de configuration
- Procédures d'interface utilisateur pour le routage statique
- Informations supplémentaires pour les périphériques Cisco
- Test

Exemples de fichiers de configuration

Pour télécharger un exemple de fichier de configuration contenant des valeurs spécifiques à la configuration de votre connexion VPN de site à site, utilisez la console Amazon VPC, la ligne de commande AWS ou l'API Amazon EC2. Pour plus d'informations, consultez 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

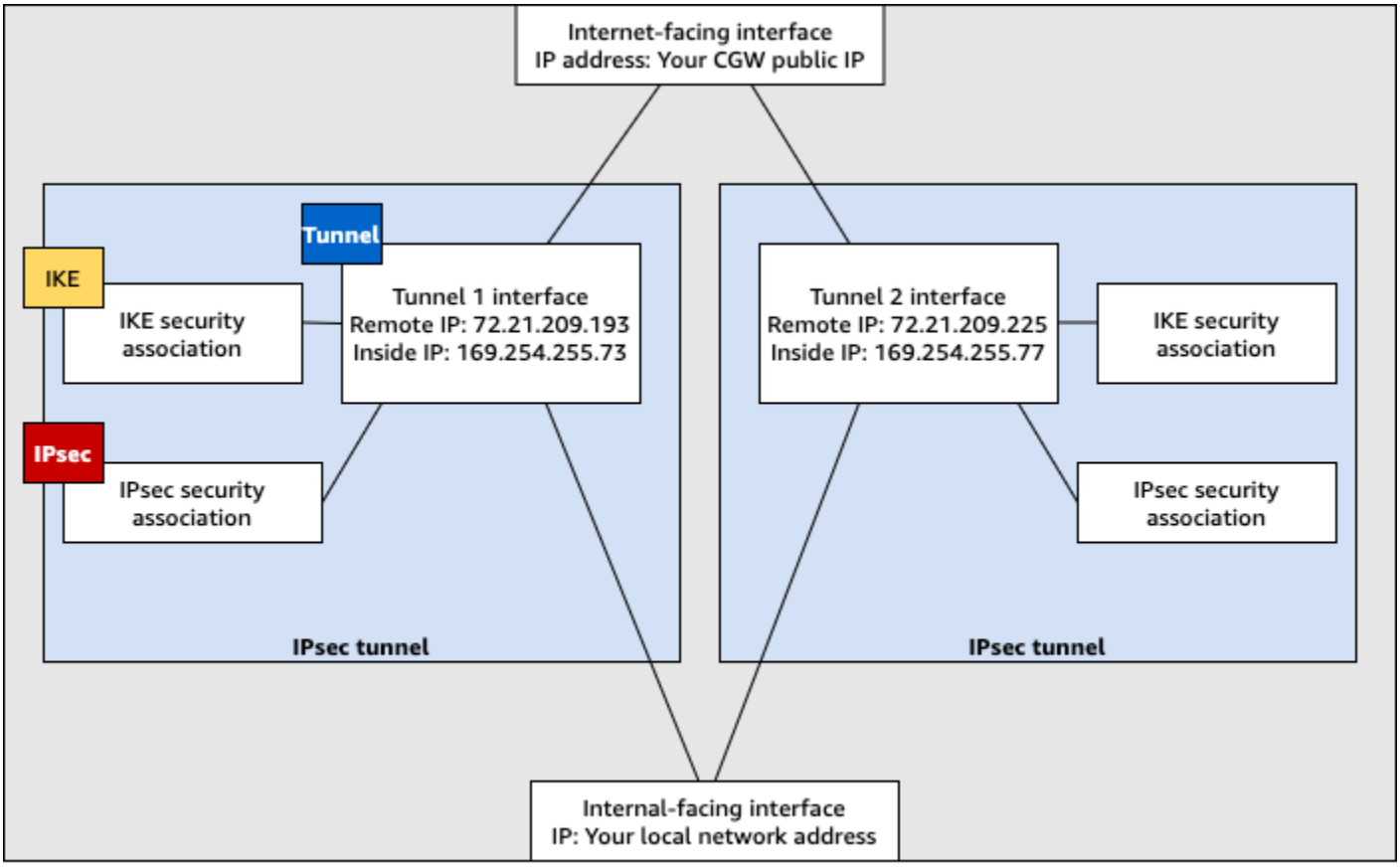
Les fichiers utilisent des valeurs d'espace réservé pour certains composants. Par exemple, ils utilisent :

- 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 (extérieurs) (AWS_ENDPOINT_1 et AWS_ENDPOINT_2)*
- Un espace réservé pour l'adresse IP de l'interface externe routable via Internet sur le périphérique de passerelle client (*votre-adresse-ip-cgw*)
- Un espace réservé pour la valeur de clé prépartagée (clé prépartagée)
- 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 Bonnes pratiques pour votre périphérique 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 VPN de site à site de type AES128, SHA1 et Diffie-Hellman groupe 2 dans la AWS plupart des régions, et AES128, SHA2 et Diffie-Hellman groupe 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

Procédures d'interface utilisateur pour le routage statique

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 Check Point Security Gateway IPsec VPN to Amazon Web Services VPC sur le Centre de support Check Point.

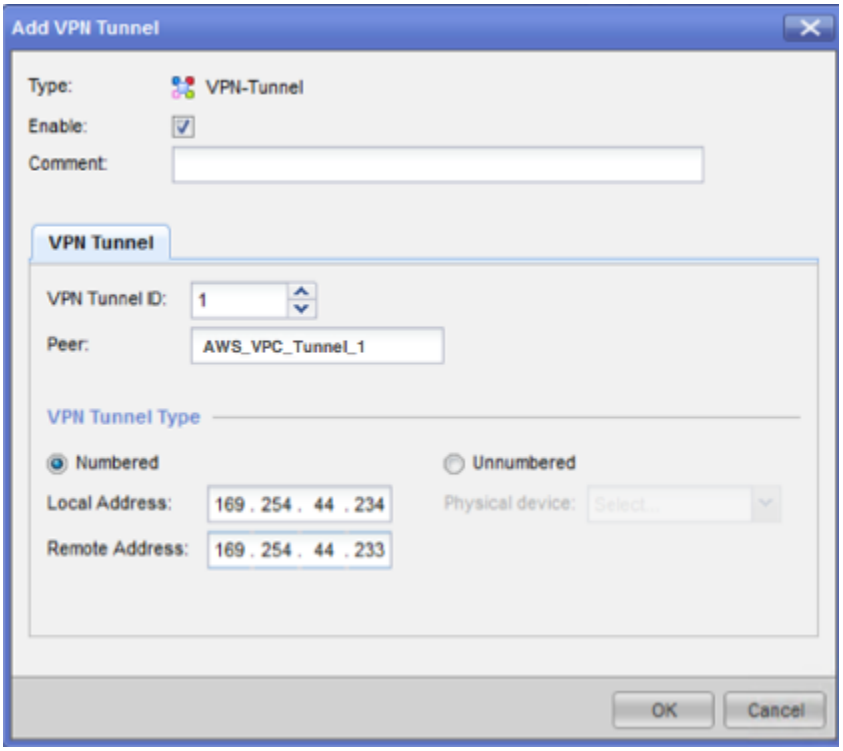
Pour configurer l'interface du tunnel

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. 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 :

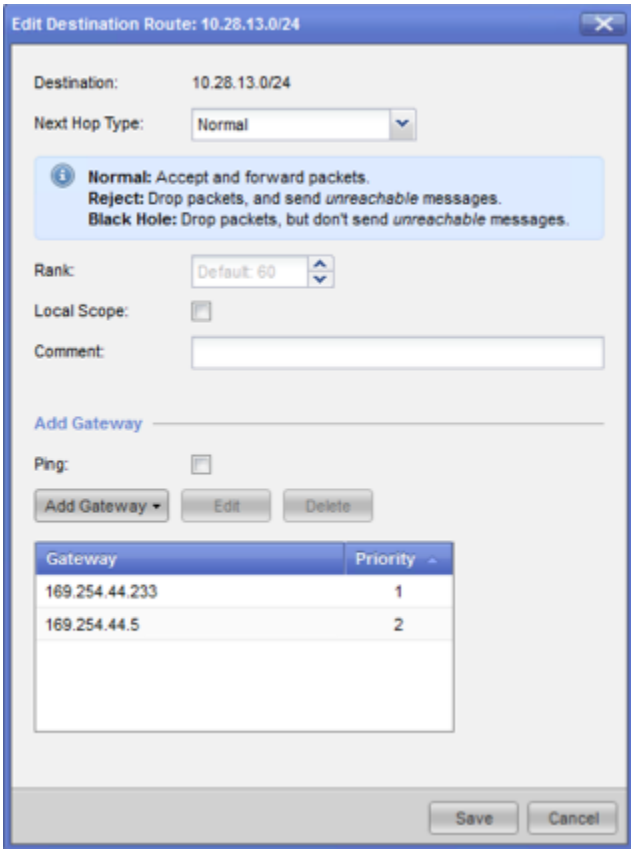
```
set interface vpnt2 mtu 1436
```

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, sélectionnez IPv4 Static Routes, Add.
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.

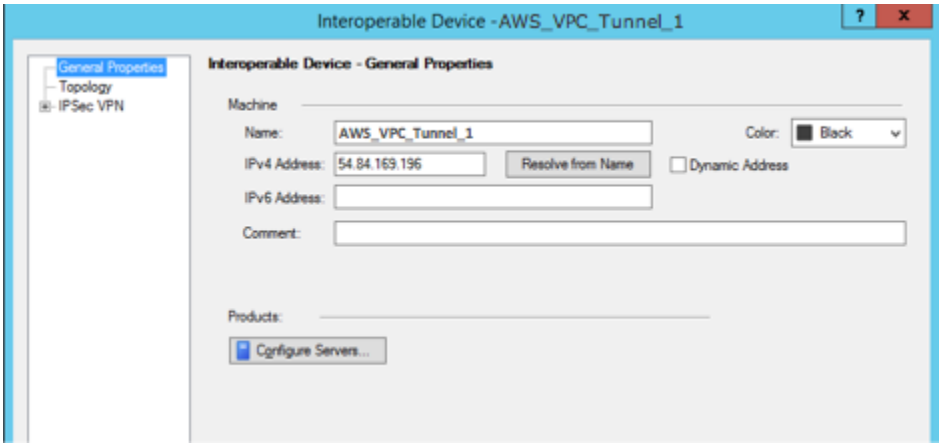
Si vous utilisez un cluster, répétez les étapes précédentes pour les autres membres du cluster.

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 Address, entrez l'adresse IP externe de la passerelle réseau privé virtuel fournie dans le fichier de configuration (`54.84.169.196`, par exemple). 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.

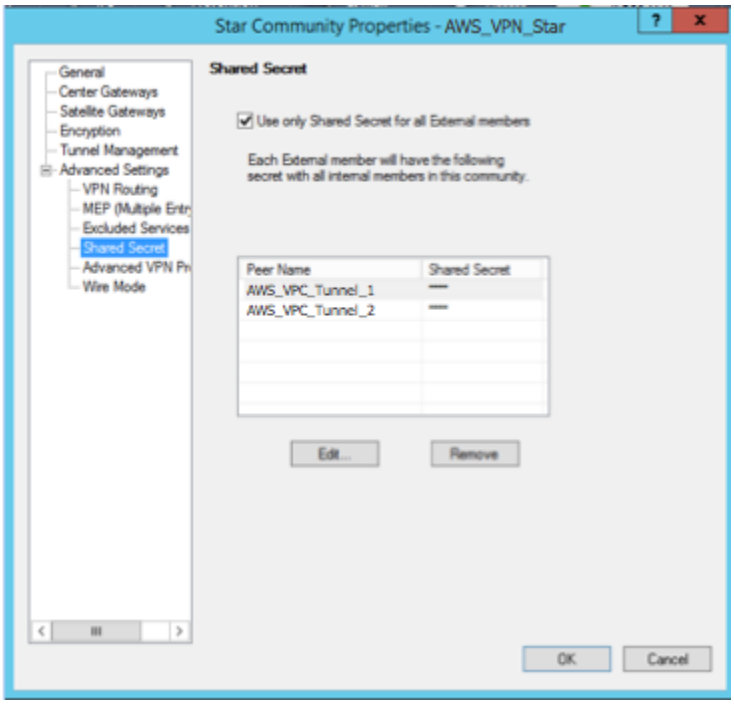
> **Note**
>
> Si vous utilisez des clusters, modifiez la topologie et définissez les interfaces comme interfaces de cluster. Utilisez les adresses IP spécifiées dans le fichier de configuration.

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

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 les paramètres IKE (Internet Key Exchange) et IPsec.

1. A partir des propriétés de votre passerelle, choisissez IPSec VPN 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 Encryption Method, choisissez IKEv1 only. 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
   - Propriétés IPsec Security Association (Phase 2) :
     - Perform IPsec data encryption with : 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`
        - Renegotiate IPsec security associations every `3600` seconds

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 et 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 propriété `tunnel_keepalive_method` en utilisant l'outil GuiDBedit.

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'outil GuiBDedit. 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'outil GuiDBedit.
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.

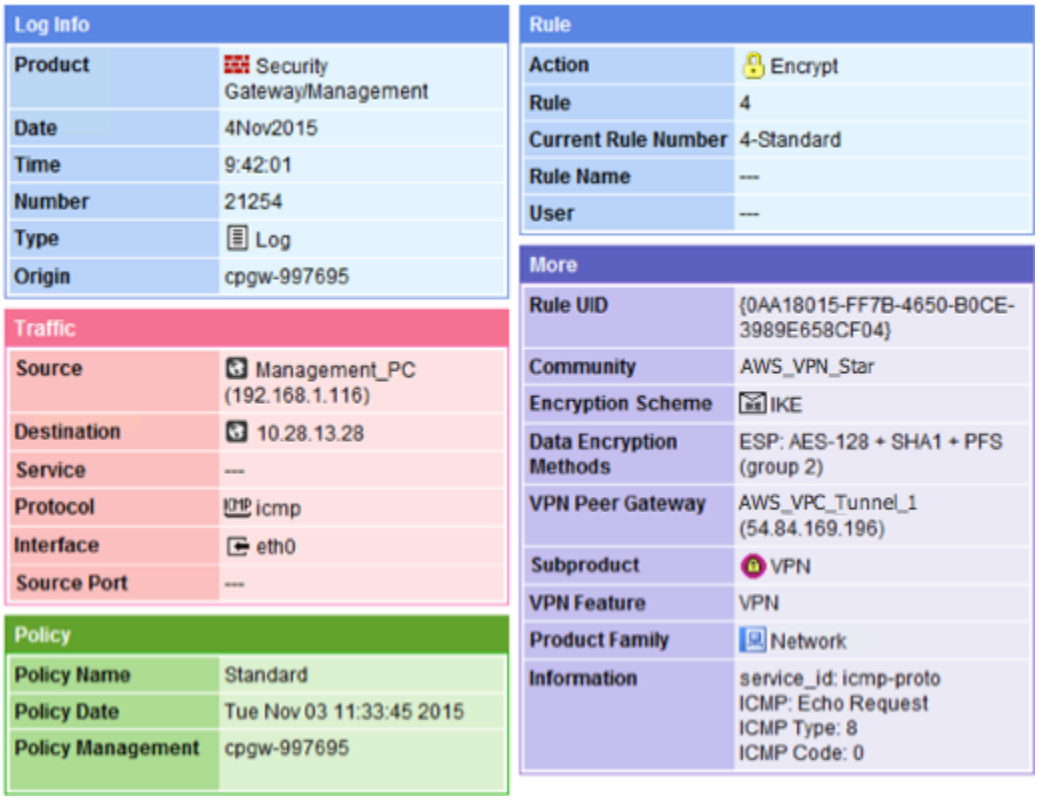
Pour vérifier l'état du tunnel

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, sélectionnez 1 pour vérifier les associations IKE et 2 pour vérifier les associations IPsec.

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 Primary Gateway Name or Address (Nom ou adresse de la passerelle principale IPsec) : saisissez l'adresse IP de la passerelle réseau privé virtuel telle que fournie dans le fichier de configuration (par exemple, `72.21.209.193`).
   - IPsec Secondary Gateway Name or Address : laissez 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.
   - Local IKE ID : entrez l'adresse IPv4 de la passerelle client (l'appareil SonicWALL).
   - Peer IKE ID : saisissez l'adresse IPv4 de la passerelle réseau privé virtuel.
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.

- Authentication : choisissez SHA1 ou SHA256.
- Life Time : entrez `28800`.

- Sous IKE (Phase 2) Proposal, procédez comme suit :
  - Protocol : choisissez ESP.
  - Encryption : choisissez AES-128 ou AES-256.
  - Authentication : choisissez SHA1 ou 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 réseau privé virtuel avant octobre 2015, vous devez spécifier Diffie-Hellman group 2, AES-128 et SHA1 pour les deux phases.

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.

Informations supplémentaires pour les périphériques Cisco

Certains systèmes Cisco ASA ne prennent en charge que le mode actif/en veille. 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 si le premier tunnel devient inaccessible. Avec cette redondance, l'un des tunnels devrait toujours assurer la connexion à votre VPC.

Les systèmes Cisco ASA version 9.7.1 ou ultérieure prennent en charge le mode actif/actif. Lorsque vous utilisez ces systèmes Cisco ASA, vous pouvez avoir les deux tunnels actifs à la fois. 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.
- Vous assurer que le jeu de transformations Crypto IPsec et la séquence de la stratégie Crypto ISAKMP sont en accord avec tous les autres tunnels IPsec configurés sur le périphérique.
- 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.

Test

Pour plus d'informations sur le test de votre connexion Site-to-Site VPN, consultez Test d'une connexion VPN site à site.

Exemples de configurations de périphérique de passerelle client pour le routage dynamique (BGP)

Rubriques

Exemples de fichiers de configuration

Pour télécharger un exemple de fichier de configuration contenant des valeurs spécifiques à la configuration de votre connexion VPN de site à site, utilisez la console Amazon VPC, la

ligne de commande AWS ou l'API Amazon EC2. Pour plus d'informations, consultez 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

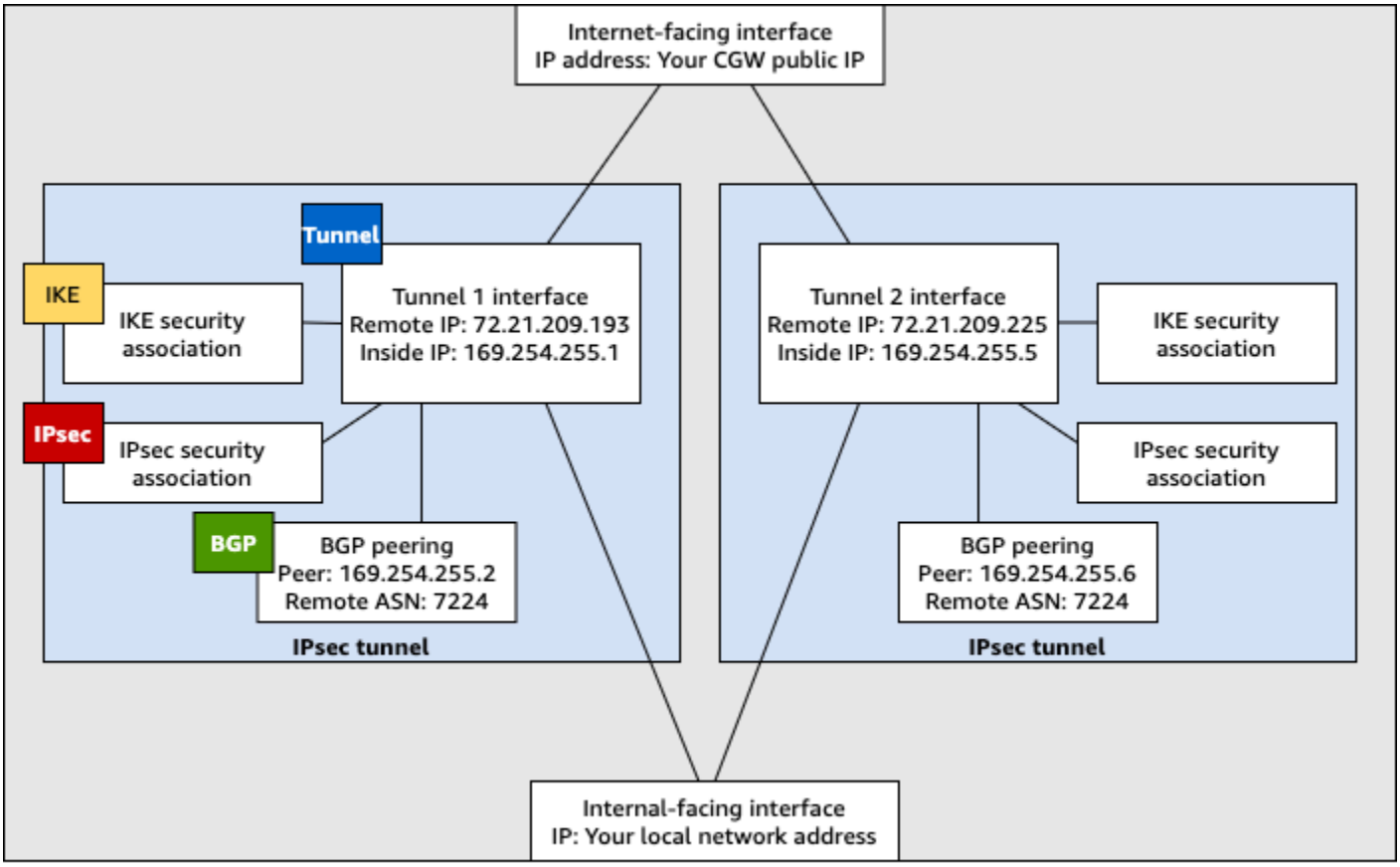
Les fichiers utilisent des valeurs d'espace réservé pour certains composants. Par exemple, ils utilisent :

- 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 (extérieurs) (AWS_ENDPOINT_1 et AWS_ENDPOINT_2)*
- Un espace réservé pour l'adresse IP de l'interface externe routable via Internet sur le périphérique de passerelle client (*votre-adresse-ip-cgw*)
- Un espace réservé pour la valeur de clé prépartagée (clé prépartagée)
- 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 Bonnes pratiques pour votre périphérique 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 VPN de site à site de type AES128, SHA1 et Diffie-Hellman groupe 2 dans la AWS plupart des régions, et AES128, SHA2 et Diffie-Hellman groupe 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

Procédures d'interface utilisateur pour le routage dynamique

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.

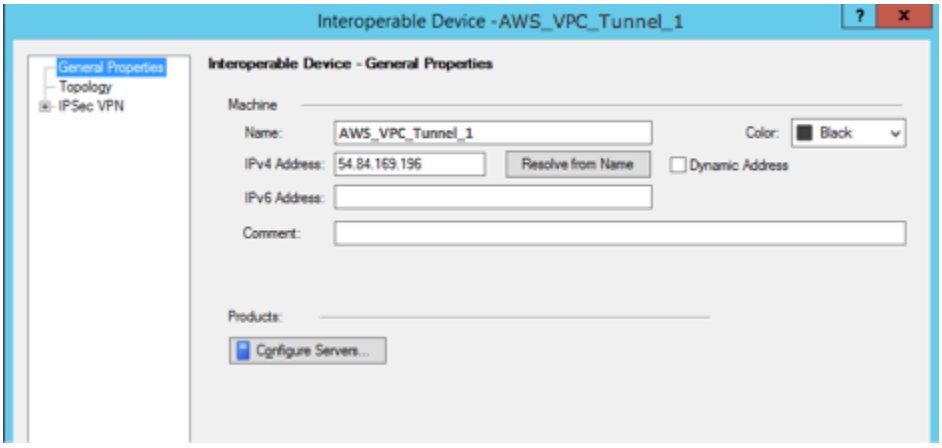
1. Dans l'interface utilisateur Web de Gaia, sélectionnez Advanced Routing, Routing Redistribution. Choisissez Add Redistribution From (Ajouter une redistribution à partir de) et sélectionnez Interface.

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 Address, entrez l'adresse IP externe de la passerelle réseau privé virtuel fournie dans le fichier de configuration (54.84.169.196, par exemple). 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, et les paramètres IKE et IPsec

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

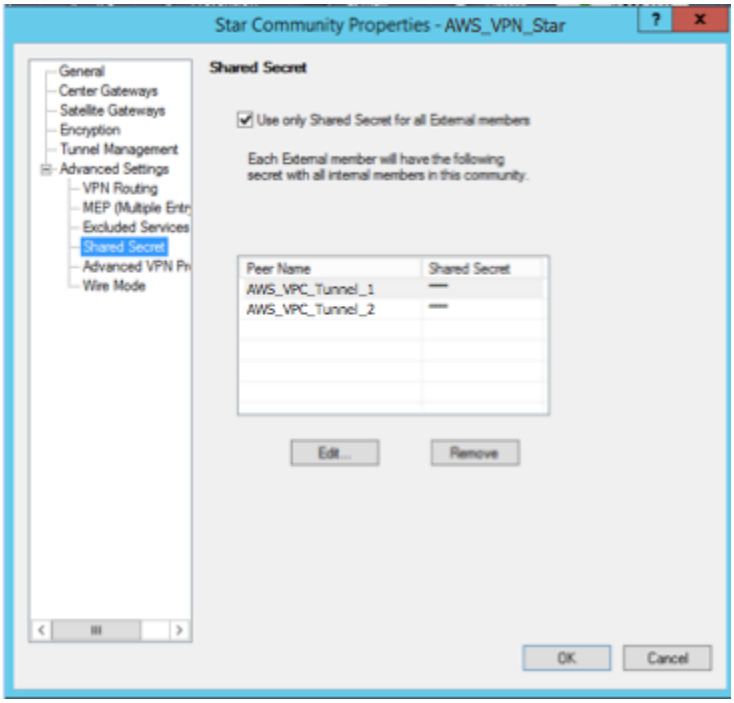
1. A partir des propriétés de votre passerelle, choisissez IPSec VPN dans le volet des catégories.
2. Choisissez Communities, New, Star Community.
3. Entrez un nom pour votre communauté (par exemple, `AWS_VPN_Star`), puis choisissez Center Gateways dans le volet des catégories.
4. Choisissez Add, puis 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 Encryption Method, choisissez IKEv1 for IPv4 and IKEv2 for IPv6. Dans la section Encryption Suite, choisissez Custom, Custom Encryption.

   > **Note**
   >
   > Vous devez sélectionner l'option IKEv1 for IPv4 and IKEv2 for IPv6 (IKEv1 pour IPv4 et IKEv2 pour IPv6) pour la fonctionnalité iKEv1.

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
   - Propriétés IPsec Security Association (Phase 2) :
     - Perform IPsec data encryption with : 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)`
        - Renegotiate IPsec security associations every `3600` seconds

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 et 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 propriété `tunnel_keepalive_method` en utilisant l'outil GuiDBedit.

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'outil GuiBDedit. 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'outil GuiDBedit.
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.

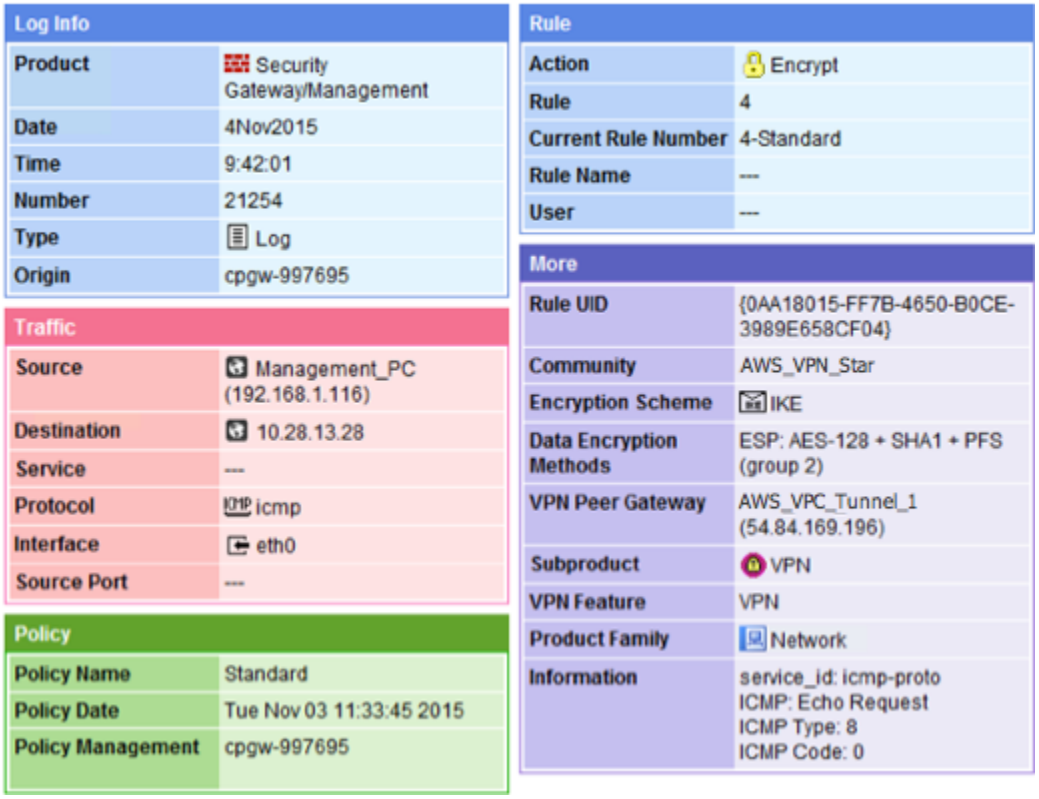
Pour vérifier l'état du tunnel

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, sélectionnez 1 pour vérifier les associations IKE et 2 pour vérifier les associations IPsec.

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 Procédures d'interface utilisateur pour le routage statique.

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.

Informations supplémentaires pour les périphériques Cisco

Certains systèmes Cisco ASA ne prennent en charge que le mode actif/en veille. 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 si le premier tunnel devient inaccessible. Avec cette redondance, l'un des tunnels devrait toujours assurer la connexion à votre VPC.

Les systèmes Cisco ASA version 9.7.1 ou ultérieure prennent en charge le mode actif/actif. Lorsque vous utilisez ces systèmes Cisco ASA, vous pouvez avoir les deux tunnels actifs à la fois. 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.
- Vous assurer que le jeu de transformations Crypto IPsec et la séquence de la stratégie Crypto ISAKMP sont en accord avec tous les autres tunnels IPsec configurés sur le périphérique.
- 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.

Informations supplémentaires pour les périphériques Juniper

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

- L'interface externe est désignée sous le nom *ge-0/0/0.0*.
- Les ID d'interface de tunnel sont désignés sous les noms *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).

Test

Pour plus d'informations sur le test de votre connexion Site-to-Site VPN, consultez Test d'une connexion VPN site à site.

Configuration de Windows Server en tant que périphérique de passerelle 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 checking 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 IPv4 Checksum 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 Utilisation d'adresses IP Elastic. Notez cette adresse, vous en aurez besoin lors de la création de la passerelle client dans votre VPC.
- Assurez-vous que les règles du groupe de sécurité de l'instance autorisent le trafic IPsec 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 sortantes personnalisées suivantes pour le trafic IPsec : 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 plus d'informations, consultez 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 plus d'informations, consultez 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 plus d'informations, consultez (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 (Connexions Site-to-Site VPN).
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`

Clé pré partagée qui permet d'établir la connexion VPN IPsec 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 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.

Le fichier de configuration téléchargé contient des informations supplémentaires sur les associations de sécurité (SA) IKE (Internet Key Exchange) et IPsec.

```
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 recommandés pour la connexion VPN et des paramètres par défaut pour les connexions VPN IPsec de Windows Server.

`MainModeKeyLifetime`

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

`QuickModeSecMethods`

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

`QuickModePFS`

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

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 PFS (Perfect Forward Secrecy) pour vos sessions IPSec. 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.

LocalTunnelPoint de terminaison : 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.

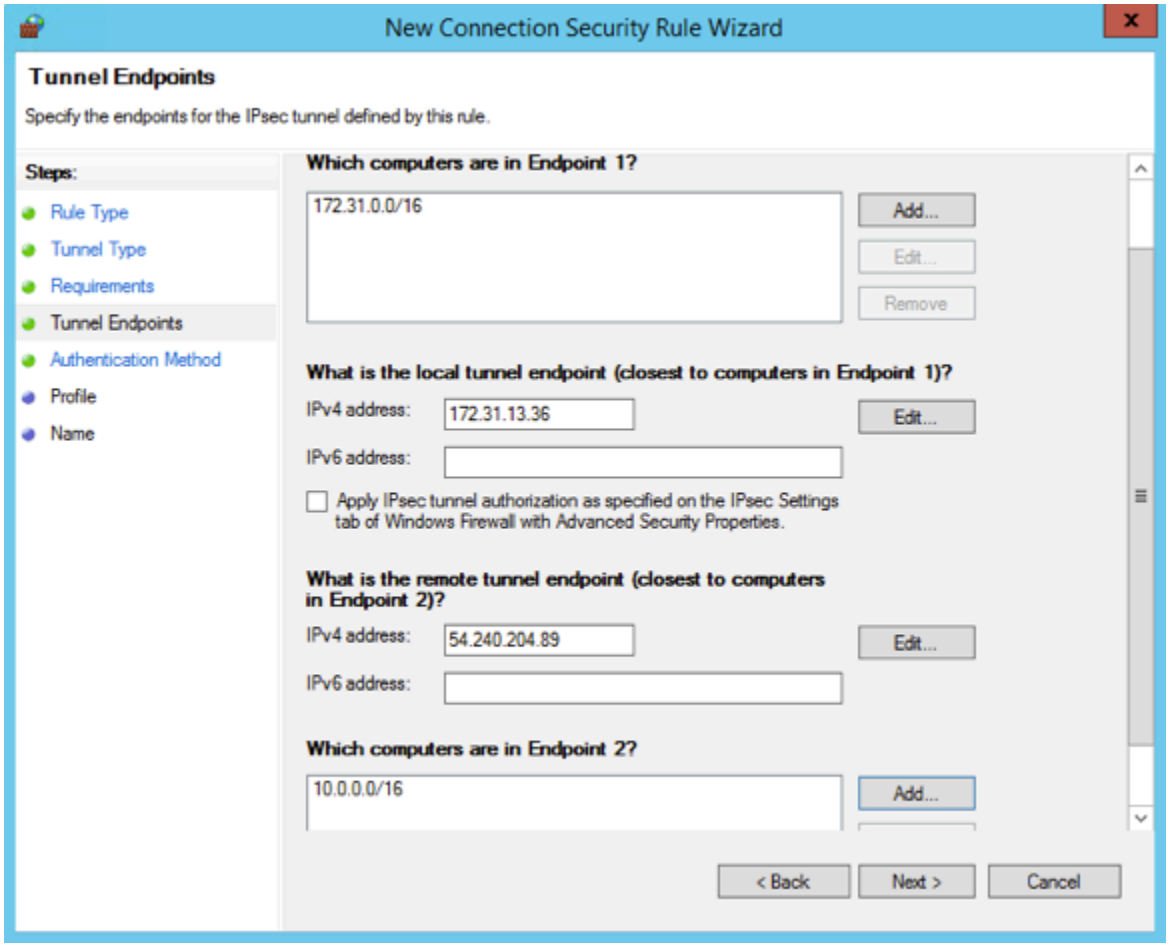
Pour configurer une règle de sécurité pour un tunnel VPN :

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 Voulez-vous exempter les connexions protégées par IPsec de ce tunnel ?, conservez la valeur par défaut (Non. Envoyer tout le trafic réseau qui satisfait à cette règle de sécurité de connexion à travers le tunnel). Sélectionnez ensuite Suivant.
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 IPv4 address (Adresse IPv4), saisissez l'adresse IP privée de votre Windows Server, puis sélectionnez 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 Adresse IPv4, entrez l'adresse IP de la passerelle réseau privé virtuel pour le Tunnel 1 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 Tunneling IPsec, choisissez Personnaliser. Vérifiez les paramètres de tunneling IPsec ci-après, puis choisissez OK et de nouveau OK pour fermer la boîte de dialogue.

   - L'option Utiliser le tunneling IPSec 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 configuré vos règles de sécurité sur votre serveur, configurez les paramètres IPsec de base pour qu'ils fonctionnent avec la passerelle réseau privé virtuel.

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. Sous l'onglet Paramètres IPSec, sous Exemptions IPsec, vérifiez que Exempter ICMP d'IPsec est défini sur Non (par défaut). Assurez-vous que l'option Autorisation de tunnel IPsec est définie sur Aucune.
3. Sous Valeurs par défaut IPsec, 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. Choisissez OK pour revenir dans la boîte de dialogue Customize IPsec Settings (Personnaliser les paramètres IPsec) et choisissez de nouveau 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 SYSTEM, développez CurrentControlSet, développez les services, développez Tcpip, puis développez les paramètres.
3. Dans le menu Editer, sélectionnez Nouveau et sélectionnez Valeur DWORD 32 bits.
4. Entrez le nom EnableDeadGWDetect.
5. Sélectionnez EnableDeadGWDetect, puis choisissez Edition, 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 EnableDeadGWDetect dans la 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 Test d'une connexion VPN site à site.

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 Windows Server est une instance EC2, assurez-vous que les règles sortantes de son groupe de sécurité autorisent le trafic IPsec. Pour plus d'informations, consultez 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 une des AMI Amazon Linux.
- Si l'instance sur laquelle vous effectuez un test ping est une instance Windows, connectez-vous à l'instance et autorisez l'accès ICMPv4 entrant sur le pare-feu Windows.
- Assurez-vous d'avoir correctement configuré les tables de routage pour votre VPC ou votre sous-réseau. Pour plus d'informations, consultez Étape 1: Créer une connexion VPN et configurer votre VPC.
- Si votre périphérique de passerelle client est une instance EC2, assurez-vous d'avoir désactivé la vérification origine/destination pour celle-ci. Pour plus d'informations, consultez 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.

Dépannage de votre périphérique de passerelle client

Les rubriques suivantes peuvent vous aider à résoudre les problèmes de connexion sur les périphériques de passerelle client.

Pour obtenir les instructions générales relatives aux tests, consultez Test d'une connexion VPN site à site.

Outre les rubriques de cette section, vous pouvez également utiliser AWS Site-to-Site VPN journaux pour résoudre les problèmes de connectivité VPN.

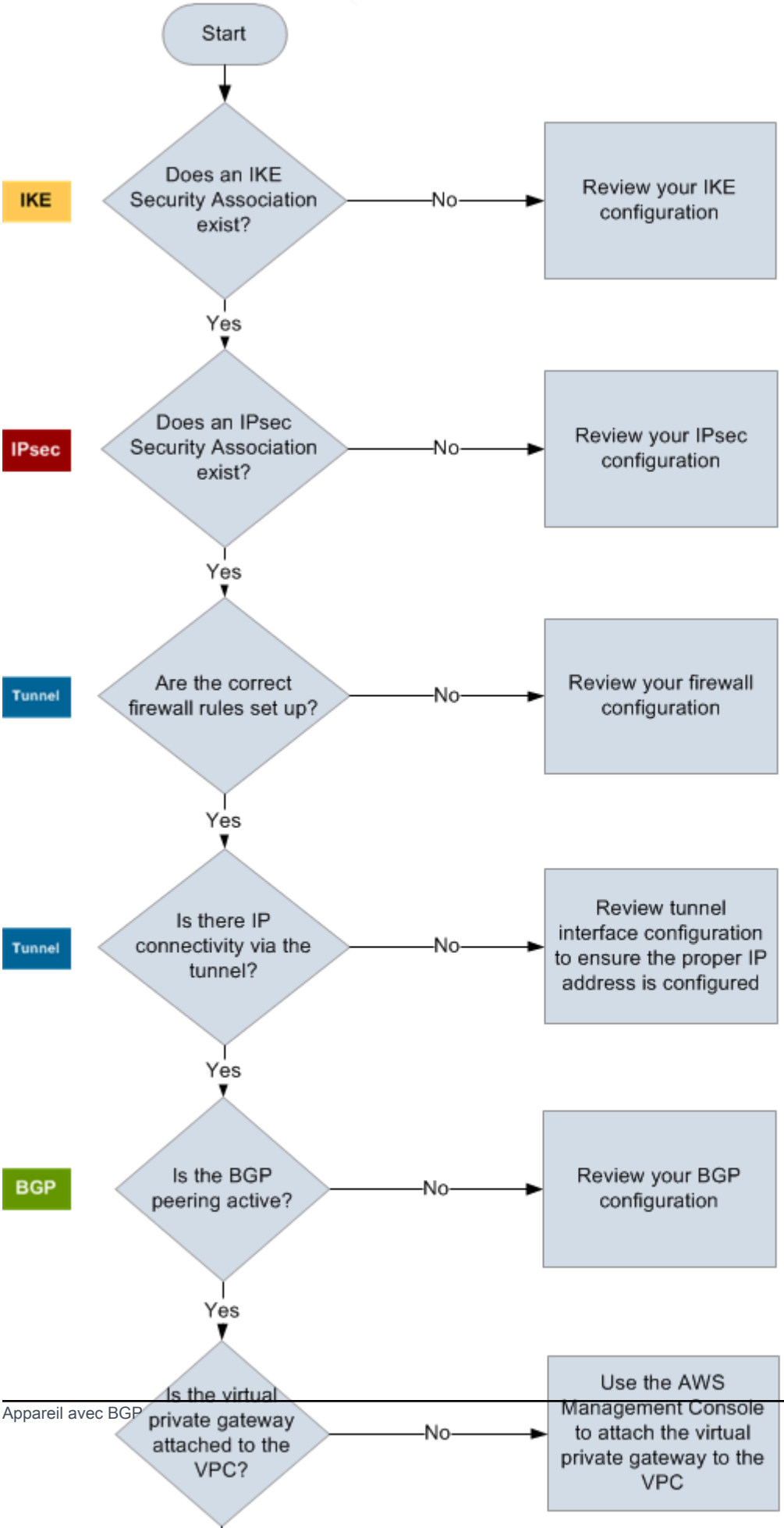
Rubriques

Ressources supplémentaires

- Forum Amazon VPC
- Comment résoudre les problèmes de connexion des tunnels VPN à mon VPC Amazon ?

Résolution des problèmes de connectivité lors de l'utilisation du protocole BGP (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 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.

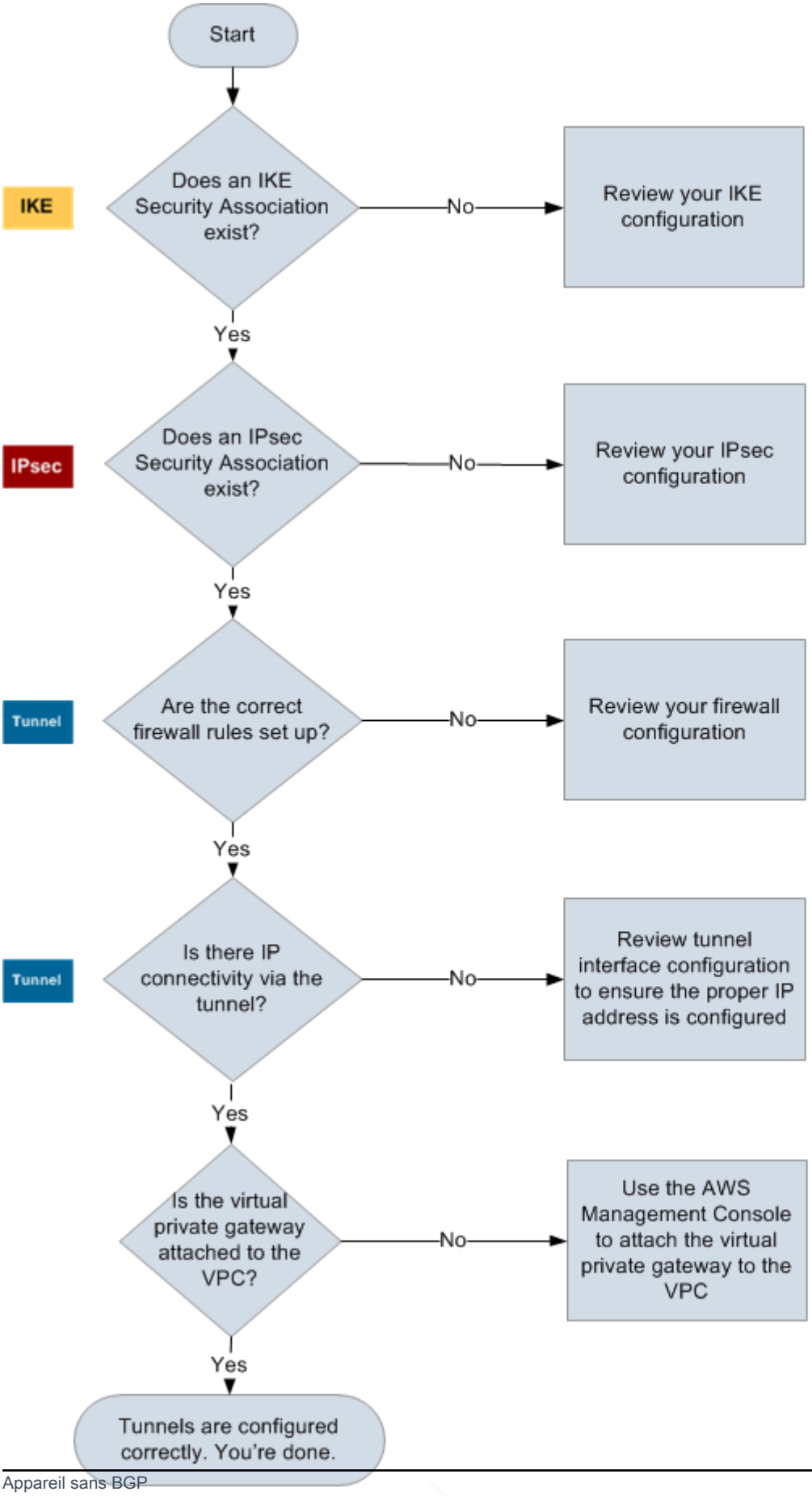

Start
IKE
Does an IKE Security Association exist?
No
Review your IKE configuration
Yes
IPsec
Does an IPsec Security Association exist?
No
Review your IPsec configuration
Yes
Tunnel
Are the correct firewall rules set up?
No
Review your firewall configuration
Yes
Tunnel
Is there IP connectivity via the 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 Configuration d'un pare-feu entre Internet et votre périphérique 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. • Vérifiez que la passerelle client publie la route par défaut (0.0.0.0/0) vers la passerelle réseau privé virtuel. 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 de la connexion sans protocole Border Gateway Protocol (BGP)

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 Configuration d'un pare-feu entre Internet et votre périphérique 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.

Résolution des problèmes de connexion de la 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 systèmes Cisco ASA ne prennent en charge que le mode actif/en veille. 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.

Résolution des problèmes de connexion de la passerelle client Cisco IOS (Internetwork Operating System, système d'exploitation pour la connexion des réseaux)

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 plus d'informations, consultez Configuration d'un pare-feu entre Internet et votre périphérique 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 l'appairage BGP est opérationnel, vérifiez que votre routeur de passerelle client publie la route 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.

Résolution des problèmes de connexion de la passerelle client Cisco IOS sans connexion BGP (Border Gateway Protocol)

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 plus d'informations, consultez Configuration d'un pare-feu entre Internet et votre périphérique 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.

Résolution des problèmes de connexion de la 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 Configuration d'un pare-feu entre Internet et votre périphérique 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 l'appairage BGP est opérationnel, vérifiez que votre routeur de passerelle client publie la route 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
```

Résolution des problèmes de connectivité de la passerelle client Juniper ScreenOS

Quand vous résolvez les problèmes de connexion d'une passerelle client basée sur Juniper ScreenOS, 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 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 Configuration d'un pare-feu entre Internet et votre périphérique 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 l'appairage BGP est opérationnel, vérifiez que votre routeur de passerelle client publie la route 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
```

Résolution des problèmes de connexion de la 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 Configuration d'un pare-feu entre Internet et votre périphérique 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 l'appairage BGP est opérationnel, vérifiez que votre routeur de passerelle client publie la route 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
```

Utilisation d'un VPN site à site

Vous pouvez utiliser des ressources Site-to-Site VPN à l'aide de la console Amazon VPC ou de AWS CLI.

Table des matières

Création d'une pièce jointe VPN de site à site pour Cloud WAN AWS

Suivez la procédure ci-dessous pour créer une connexion VPN Site-to-Site pour Cloud WAN. AWS

Pour créer une pièce jointe VPN pour AWS Cloud WAN 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 Connexions VPN site à site.
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 Target gateway type (Type de passerelle cible), choisissez Not associated (Non associé).
6. Pour Passerelle client, effectuez l'une des actions suivantes :

- Pour utiliser une passerelle client existante, choisissez Existante, puis sélectionnez la passerelle client.
- Pour créer une passerelle client, choisissez New (Nouveau). Dans IP Address (Adresse IP), entrez une adresse IP publique statique. Dans Certificate ARN (ARN du certificat), choisissez l'ARN de votre certificat privé (si vous utilisez l'authentification basée sur certificat). Dans Version du moteur de cache, saisissez le numéro d'ASN (Autonomous System Number) BGP (Border Gateway Protocol) de votre passerelle client. Pour plus d'informations, consultez Options de passerelle client.

7. Pour Options de routage, choisissez Dynamique ou Statique.
8. Pour Version des adresses IP internes du tunnel, choisissez IPv4 ou IPv6.
9. (Facultatif) Dans Enable Acceleration (Activer l'accélération), activez la case à cocher pour activer l'accélération. Pour plus d'informations, consultez Connexions VPN accélérées.

   Si vous activez l'accélération, nous créons deux accélérateurs qui sont utilisés par votre connexion VPN. Des frais supplémentaires seront facturés.
10. (Facultatif) Pour Local IPv4 Network CIDR (CIDR réseau IPv4 local), spécifiez la plage CIDR IPv4 côté passerelle client (sur site) autorisée à communiquer via les tunnels VPN. La valeur par défaut est `0.0.0.0/0`.

    Pour le CIDR du réseau IPv4 distant, spécifiez la plage d'adresses CIDR IPv4 du AWS côté autorisé à communiquer via les tunnels VPN. L'argument par défaut est `0.0.0.0/0`.

    Si vous avez spécifié IPv6 pour la version Tunnel inside IP, spécifiez les plages d'adresses CIDR IPv6 du côté de la passerelle client et du AWS côté de la passerelle client autorisées à communiquer via les tunnels VPN. La valeur par défaut pour les deux plages est `::/0`.
11. (Facultatif) Pour Options de tunnel, vous pouvez spécifier les informations suivantes pour chaque tunnel :

    - Bloc d'adresses CIDR de taille /30 IPv4 de la plage `169.254.0.0/16` pour les adresses IPv4 internes du tunnel.
    - Si vous avez spécifié IPv6 pour Version des adresses IP internes du tunnel, un bloc d'adresses CIDR /126 IPv6 de la plage `fd00::/8` pour les adresses IPv6 internes du tunnel.
    - La clé pré-partagée (PSK) IKE. Les versions suivantes sont prises en charge : IKEv1 et IKEv2.
    - Pour modifier les options avancées de votre tunnel, choisissez Modifier les options du tunnel. Pour plus d'informations, consultez Options de tunnel VPN.
12. Choisissez Créer une connexion VPN.

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

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

Création d'un attachement de VPN de passerelle de transit

Pour créer un attachement VPN sur une passerelle de transit, vous devez spécifier la passerelle de transit et la passerelle client. La passerelle de transit devra être créée avant de suivre cette procédure. Pour plus d'informations sur la création d'une passerelle de transit, consultez Passerelles de transit dans Passerelles de transit Amazon VPC.

Pour créer un attachement de passerelle de transit 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 Connexions VPN site à site.
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 Type de passerelle cible, choisissez Passerelle de transit, puis sélectionnez la passerelle de transit.
6. Pour Passerelle client, effectuez l'une des actions suivantes :
   - Pour utiliser une passerelle client existante, choisissez Existante, puis sélectionnez la passerelle client.

     Si votre passerelle client est située derrière un périphérique de traduction d'adresses réseau (NAT) qui est activé pour NAT Traversal (NAT-T), utilisez l'adresse IP publique de votre périphérique NAT et ajustez vos règles de pare-feu pour débloquer le port UDP 4500.
   - Pour créer une passerelle client, choisissez New (Nouveau). Dans IP Address (Adresse IP), entrez une adresse IP publique statique. Dans Certificate ARN (ARN du certificat), choisissez l'ARN de votre certificat privé (si vous utilisez l'authentification basée sur certificat). 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 Options de routage, choisissez Dynamique ou Statique.

8. Pour Version des adresses IP internes du tunnel, indiquez si les tunnels VPN prennent en charge le trafic IPv4 ou IPv6. Le trafic IPv6 n'est pris en charge que pour les connexions VPN sur une passerelle de transit.
9. (Facultatif) Dans Enable Acceleration (Activer l'accélération), activez la case à cocher 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 seront facturés.
10. (Facultatif) Pour Local IPv4 Network CIDR (CIDR réseau IPv4 local), spécifiez la plage CIDR IPv4 côté passerelle client (sur site) autorisée à communiquer via les tunnels VPN. La valeur par défaut est `0.0.0.0/0`.

    Pour For Remote IPv4 Network CIDR (CIDR réseau IPv4 distant), spécifiez la plage CIDR IPv4 côté AWS autorisée à communiquer via les tunnels VPN. La valeur par défaut est `0.0.0.0/0`.

    Si vous avez spécifié IPv6 pour Tunnel Inside IP Version (Version IP dans tunnel), spécifiez les plages CIDR IPv6 côté passerelle client et côté AWS autorisées à communiquer via les tunnels VPN. La valeur par défaut pour les deux plages est `::/0`.
11. (Facultatif) Pour Options de tunnel, vous pouvez spécifier les informations suivantes pour chaque tunnel :

    - Bloc d'adresses CIDR de taille /30 IPv4 de la plage `169.254.0.0/16` pour les adresses IPv4 internes du tunnel.
    - Si vous avez spécifié IPv6 pour Version des adresses IP internes du tunnel, un bloc d'adresses CIDR /126 IPv6 de la plage `fd00::/8` pour les adresses IPv6 internes du tunnel.
    - La clé pré-partagée (PSK) IKE. Les versions suivantes sont prises en charge : IKEv1 et 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).

Pour créer un attachement VPN à l'aide de AWS CLI

Utilisez la commande create-vpn-connection et spécifiez l'ID de passerelle de transit pour l'option `--transit-gateway-id`.

Test d'une connexion VPN site à site

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 une des AMI Amazon Linux.
- 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 autorisez l'accès ICMPv4 entrant sur le pare-feu Windows afin d'effectuer un test ping de 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 console Amazon EC2 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 console Amazon EC2 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 l'utilisateur Amazon EC2. Pour plus d'informations sur la façon de se connecter à une instance Windows, consultez la section Connect to your Windows User Guide du guide de l'utilisateur Amazon EC2.

Suppression d'une connexion VPN site à site

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 réseau privé virtuel qui était 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 VPN site à site et que vous en créez une nouvelle, vous devez télécharger un nouveau fichier de configuration et reconfigurer l'appareil de passerelle client.

Tâches

- Suppression d'une connexion VPN
- Suppression d'une passerelle client
- Détachement et suppression d'une passerelle réseau privé virtuel

Suppression d'une connexion VPN

Après avoir supprimé votre connexion Site-to-Site VPN, celle-ci reste visible pendant un court moment avec un 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, choisissez Connexions VPN site à site.
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

- DeleteVpnConnexion (API de requête Amazon EC2)

- delete-vpn-connection (AWS CLI)
- Remove-EC2VpnConnection (AWS Tools for Windows PowerShell)

Suppression d'une passerelle client

Si vous n'avez plus besoin d'une passerelle client, vous pouvez la supprimer. Vous ne pouvez supprimer une passerelle client qui est utilisée par 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

- DeleteCustomerPasserelle (API de requête Amazon EC2)
- delete-customer-gateway (AWS CLI)
- Remove-EC2CustomerGateway (AWS Tools for Windows PowerShell)

Détachement et suppression d'une passerelle réseau privé virtuel

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

- DetachVpnPasserelle (API de requête Amazon EC2)
- 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

- DeleteVpnPasserelle (API de requête Amazon EC2)
- delete-vpn-gateway (AWS CLI)
- Remove-EC2VpnGateway (AWS Tools for Windows PowerShell)

Modification de la passerelle cible d'une connexion VPN site à site.

Vous pouvez modifier la passerelle cible d'une connexion AWS Site-to-Site VPN. 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 indisponible pendant une courte période tandis que nous allouons 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

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 les VPC 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. Choisissez 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, choisissez Connexions VPN site à site.
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. Choisissez 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 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

Passerelle existante	Nouvelle passerelle	Modification de table de routage de VPC
		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 la connexion 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 de route VPN.

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 connexion Site-to-Site VPN.

Modification des options de connexion VPN site à site

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.

Lorsque vous modifiez les options de connexion VPN, les adresses IP du point de terminaison VPN côté AWS 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, choisissez Connexions VPN site à site.
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. Choisissez 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)

Modification des options de tunnel Site-to-Site VPN

Vous pouvez modifier les options de tunnel pour les tunnels VPN dans 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, choisissez Connexions VPN site à site.
3. Sélectionnez la connexion VPN site à site, puis choisissez Actions, Modifier les options de 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 de plus amples informations, veuillez consulter Options de tunnel VPN.
6. Choisissez Enregistrer les modifications.

Pour modifier les options du tunnel VPN à l'aide de la ligne de commande ou de l'API

- (AWS CLI) Utilisez describe-vpn-connections pour afficher les options de tunnel actuelles et modify-vpn-tunnel-options pour modifier les options de tunnel.
- (API de requête Amazon EC2) Utilisez DescribeVpnConnections pour afficher les options de tunnel actuelles et ModifyVpnTunnelOptions pour modifier les options de tunnel.

Modification de routes statiques pour une connexion VPN site à site

Pour une connexion Site-to-Site VPN sur une passerelle réseau privé virtuel 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, choisissez Connexions VPN site à site.
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 plus d'informations, consultez (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 de requête Amazon EC2)
- 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 de requête Amazon EC2)
- delete-vpn-connection-route (AWS CLI)
- Remove-EC2VpnConnectionRoute (AWS Tools for Windows PowerShell)

Modification de la passerelle client pour une connexion VPN site à site

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, choisissez Connexions VPN site à site.
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. Choisissez Enregistrer les modifications.

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

- ModifyVpnConnection (API de requête Amazon EC2)
- modify-vpn-connection (AWS CLI)

Remplacement d'informations d'identification compromises pour votre connexion VPN site à site

Si vous pensez que les informations d'identification du tunnel de votre connexion Site-to-Site VPN ont été divulguées, vous pouvez changer 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 Options d'authentification du tunnel Site-to-Site VPN.

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 Modification des options de tunnel Site-to-Site VPN.

Vous pouvez également supprimer la connexion VPN. Pour de plus amples informations, veuillez consulter Suppression d'une connexion VPN. 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 prépartagées pour les tunnels ou laisser AWS générer de nouvelles clés prépartagées 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 côté AWS 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 des points de terminaison du tunnel VPN site à site

Vous pouvez soumettre les certificats à une rotation sur les points de terminaison du tunnel côté AWS à l'aide de la console Amazon VPC. Lorsque le certificat d'un point de terminaison de tunnel est proche de l'expiration, AWS soumet automatiquement le certificat à une rotation à l'aide du rôle lié au service. Pour de plus amples informations, veuillez consulter the section called “Rôles liés à un service”.

Pour soumettre le certificat de point de terminaison de tunnel Site-to-Site VPN à une rotation 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 Connexions VPN site à site.
3. Sélectionnez la connexion VPN site à site, puis choisissez Actions, Modifier le certificat du tunnel VPN.
4. Sélectionnez le point de terminaison du tunnel.
5. Choisissez Save (Enregistrer).

Pour soumettre le certificat de point de terminaison de tunnel Site-to-Site VPN à une rotation à l'aide de la AWS CLI

Utilisez la commande modify-vpn-tunnel-certificate.

VPN IP privé avec AWS Direct Connect

Avec un VPN IP privé, vous pouvez déployer un VPN IPsec par-dessus AWS 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 privé AWS Direct 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 privé AWS 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 à leurs obligations réglementaires et de sécurité.

Table des matières

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 des VPN privés sur AWS 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 AWS Direct Connect virtuelle publique (VIF) pour chiffrer le trafic AWS Direct Connect, ce qui nécessitait des adresses IP publiques pour les points de terminaison VPN. L'utilisation d'adresses IP publiques augmente la probabilité d'attaques externes (DOS), ce qui oblige les clients à déployer des équipements de sécurité supplémentaires pour la protection du 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 des VIF de AWS

Direct Connect transit (au lieu des VIF publics), associée à la possibilité de configurer des adresses IP privées. 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 AWS Direct Connect seules, qui sont actuellement limitées à 200 routes sortantes et 100 routes entrantes.

Comment fonctionne le VPN d'IP privée

Le VPN Site-to-site IP privé fonctionne via une interface virtuelle de AWS Direct Connect transit (VIF). Il utilise une passerelle AWS Direct Connect et une passerelle de transit pour relier vos réseaux sur site avec les VPC AWS . 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 aux extrémités de la passerelle de transit et du dispositif de passerelle client des tunnels IPSec. Vous pouvez utiliser des adresses IP privées issues des plages d'adresses IPv4 privées RFC1918 ou RFC6598.

Vous attachez une connexion VPN d'IP privée à une passerelle de transit. Vous acheminez ensuite le trafic entre la pièce jointe VPN et tous les VPC (ou autres réseaux) également connectés 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 de vos VPC vers l'attachement VPN d'IP privée à l'aide de tables de routage associées aux VPC.

La table de routage associée à la pièce jointe VPN peut être identique ou différente de celle associée à la AWS Direct Connect pièce jointe sous-jacente. Cela vous permet d'acheminer simultanément le trafic chiffré et non chiffré entre vos VPC et vos réseaux sur site.

Pour plus de détails sur le chemin de trafic quittant le VPN, consultez les politiques de routage de l'interface virtuelle privée et de l'interface virtuelle de transit dans le guide de AWS Direct Connect l'utilisateur.

Prérequis

Les ressources suivantes sont nécessaires pour terminer la configuration d'un VPN d'IP privée sur AWS Direct Connect :

- Une AWS Direct Connect connexion entre votre réseau local et AWS
- Une AWS Direct Connect passerelle associée à la passerelle de transit appropriée

- Une passerelle de transit avec un bloc CIDR d'IP privée disponible
- Un appareil de passerelle client sur votre réseau sur site et une passerelle client AWS correspondante

Créer la passerelle client

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.
7. (Facultatif) PourDevice (Appareil) Entrez un nom pour l'appareil qui héberge cette passerelle client.
8. Choisissez Créer la passerelle client.

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

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

Préparer la passerelle de transit

Une passerelle de transit est un hub de transit de réseau que vous pouvez utiliser pour relier votre VPC et vos réseaux 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.

Pour connaître les étapes de AWS console spécifiques à la création ou à la modification d'une passerelle de transit à utiliser pour le VPN IP privé, consultez la section Passerelles de transit dans le guide des passerelles de transit Amazon VPC.

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

- CreateTransitPasserelle (API de requête Amazon EC2)
- create-transit-gateway (AWS CLI)

Création de la AWS Direct Connect passerelle

Créez une AWS Direct Connect passerelle en suivant la procédure de création d'une passerelle Direct Connect dans le guide de AWS Direct Connect l'utilisateur.

Pour créer une AWS Direct Connect passerelle à l'aide de la ligne de commande ou de l'API

- CreateDirectConnectGateway(API AWS Direct Connect de requête)
- create-direct-connect-gateway (AWS CLI)

Créer l'association de passerelle de transit

Après avoir créé la AWS Direct Connect passerelle, créez une association de passerelle de transit pour la AWS Direct Connect passerelle. Spécifiez le CIDR d'IP privée pour la passerelle de transit identifiée précédemment dans la liste des préfixes autorisés.

Pour de plus amples informations, veuillez consulter Associations de passerelle de transit dans le Guide de l'utilisateur AWS Direct Connect .

Pour créer une association de AWS Direct Connect passerelle à l'aide de la ligne de commande ou de l'API

- CreateDirectConnectGatewayAssociation (API de AWS Direct Connect requête)
- create-direct-connect-gateway-association (AWS CLI)

Créer la connexion VPN

Pour créer une connexion VPN en utilisant des adresses IP privées

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Connexions VPN site à site.
3. Choisissez Create VPN connection (Créer une connexion VPN).
4. (Facultatif) Pour la Name tag (Balise de nom), entrez un nom pour votre connexion Site-to-Site VPN. Cette étape crée une balise avec une clé de `Name` et la valeur que vous spécifiez.
5. 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.
6. Pour Customer gateway (Passerelle client), sélectionnez Existing (Existante). Sélectionnez ensuite la passerelle client que vous avez créée précédemment.
7. 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.
8. Pour Version des adresses IP internes du tunnel, indiquez si les tunnels VPN prennent en charge le trafic IPv4 ou IPv6.
9. (Facultatif) Si vous avez spécifié IPv4 pour la version Tunnel inside IP, vous pouvez éventuellement spécifier les plages d'adresses CIDR IPv4 pour la passerelle client et AWS les côtés autorisés à communiquer via les tunnels VPN. L'argument par défaut est `0.0.0.0/0`.

   Si vous avez spécifié IPv6 pour la version Tunnel inside IP, vous pouvez éventuellement spécifier les plages d'adresses CIDR IPv6 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, choisissez PrivateIpv4.

11. Pour l'ID de pièce jointe de transport, choisissez la pièce jointe de passerelle de transit pour la AWS Direct Connect passerelle appropriée.
12. Choisissez Create VPN connection (Créer une connexion VPN).

> **Note**
>
> L'option Enable acceleration (Activer l'accélération) n'est pas applicable aux connexions VPN sur AWS Direct Connect.

Sécurité dans le VPN de AWS site à site

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 entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit cela comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS Cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de AWS conformité Programmes de de conformité. Pour en savoir plus sur les programmes de conformité qui s'appliquent au VPN de AWS site à site, voir AWS Services concernés par programme de conformitéAWS Services couverts par programme 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 de Site-to-Site VPN. Les rubriques suivantes expliquent comment configurer Site-to-Site VPN pour répondre à 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 VPN de site à site.

Table des matières

Protection des données dans le AWS VPN Site-to-Site

Le modèle de responsabilité AWS partagée Le modèle s'applique à la protection des données dans le VPN de AWS site à site. Comme décrit dans ce modèle, AWS est chargé de protéger

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 Questions fréquentes (FAQ) sur la confidentialité des données. Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog Modèle de responsabilité partagée AWS et RGPD (Règlement général sur la protection des données) sur le Blog de sécuritéAWS .

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 AWS Identity and Access Management (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.
- Utilisez le protocole SSL/TLS pour communiquer avec les ressources. AWS Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent 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 140-2 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 (Federal Information Processing Standard) disponibles, consultez Federal Information Processing Standard (FIPS) 140-2 (Normes de traitement de l'information fédérale).

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 Name (Nom). Cela inclut lorsque vous travaillez avec un VPN Site-to-Site ou un autre VPN à Services AWS l'aide de la console, de l'API ou des SDK. AWS CLI AWS 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 sur site. 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 VPN Site-to-site consiste en deux tunnels VPN IPSec cryptés qui relient votre réseau. AWS Le trafic de chaque tunnel peut être chiffré avec AES128 ou AES256 et utiliser des groupes Diffie-Hellman pour l'échange de clés, en fournissant la fonctionnalité PFS (Perfect Forward Secrecy). AWS 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 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 à votre réseau sur site. 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 connexion Site-to-Site VPN : fournit des informations sur les options IPSec et IKE (Internet Key Exchange) disponibles pour chaque tunnel.
- Options d'authentification du tunnel Site-to-Site VPN : fournit des informations sur les options d'authentification pour vos points de terminaison de tunnel VPN.
- Conditions obligatoires pour votre périphérique de passerelle client : fournit des informations sur la configuration requise pour le périphérique de passerelle client de votre côté de la connexion VPN.
- Fourniture d'une communication sécurisée entre les sites à l'aide du VPN CloudHub: Si vous disposez de plusieurs connexions VPN de site à site, vous pouvez sécuriser les communications entre vos sites locaux à l'aide du VPN. AWS CloudHub

Gestion des identités et des accès pour le AWS VPN Site-to-Site

AWS Identity and Access Management (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Des administrateurs IAM contrôlent les personnes qui s'authentifient (sont connectées) et sont autorisées (disposent d'autorisations) à utiliser des ressources Site-to-Site VPN. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez dans le VPN Site-to-Site.

Utilisateur du service – Si vous utilisez le service Site-to-Site VPN pour accomplir votre tâche, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Plus vous utiliserez de fonctions Site-to-Site VPN pour effectuer votre travail, plus vous pourriez avoir besoin d'autorisations supplémentaires. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne pouvez pas accéder à une fonctionnalité dans Site-to-Site VPN, consultez Résolution des problèmes AWS d'identité et d'accès au VPN de site à site.

Administrateur du service – Si vous êtes le responsable des ressources Site-to-Site VPN de votre entreprise, vous bénéficiez probablement d'un accès total à Site-to-Site VPN. Votre responsabilité est de déterminer les fonctionnalités et les ressources Site-to-Site VPN auxquelles les utilisateurs de votre service doivent accéder. Vous devez ensuite soumettre les demandes à votre administrateur IAM pour modifier les autorisations des utilisateurs de votre service. Consultez les informations sur cette page pour comprendre les concepts de base d'IAM. Pour en savoir plus sur la façon dont votre entreprise peut utiliser IAM avec Site-to-Site VPN, veuillez consulter Comment fonctionne le AWS Site-to-site VPN avec IAM.

Administrateur IAM – Si vous êtes un administrateur IAM, vous souhaitez probablement en savoir plus sur la façon d'écrire des politiques pour gérer l'accès à Site-to-Site VPN. Pour voir des exemples de politiques Site-to-Site VPN basées sur l'identité que vous pouvez utiliser dans IAM, veuillez consulter Exemples de politiques basées sur l'identité pour un VPN de site à site AWS.

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identification. Vous devez être authentifié (connecté à AWS) en tant qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

Vous pouvez vous connecter en AWS tant qu'identité fédérée en utilisant les informations d'identification fournies par le biais d'une source d'identité. AWS IAM Identity Center Les utilisateurs (IAM Identity Center), l'authentification unique de votre entreprise et vos informations d'identification Google ou Facebook sont des exemples d'identités fédérées. Lorsque vous vous connectez avec une identité fédérée, votre administrateur aura précédemment configuré une fédération d'identités avec des rôles IAM. Lorsque vous accédez à AWS l'aide de la fédération, vous assumez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter au portail AWS Management Console ou au portail AWS d'accès. Pour plus d'informations sur la connexion à AWS, consultez la section Comment vous connecter à votre compte Compte AWS dans le guide de Connexion à AWS l'utilisateur.

Si vous y accédez AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes à l'aide de vos informations d'identification. Si vous n'utilisez pas d' AWS outils, vous devez signer vous-même les demandes. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer vous-même les demandes, consultez la section Signature des demandes AWS d'API dans le guide de l'utilisateur IAM.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être fournir des informations de sécurité supplémentaires. Par exemple, il vous AWS recommande d'utiliser l'authentification multifactorielle (MFA) pour renforcer la sécurité de votre compte. Pour en savoir plus, consultez Authentification multifactorielle dans le Guide de l'utilisateur AWS IAM Identity Center et Utilisation de l'authentification multifactorielle (MFA) dans l'interface AWS dans le Guide de l'utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à toutes Services AWS les ressources du compte. Cette identité est appelée utilisateur Compte AWS root et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine peut effectuer. Pour obtenir la liste complète des tâches qui vous imposent de vous connecter en tant qu'utilisateur root, consultez Tâches nécessitant des informations d'identification d'utilisateur root dans le Guide de l'utilisateur IAM.

Identité fédérée

La meilleure pratique consiste à obliger les utilisateurs humains, y compris ceux qui ont besoin d'un accès administrateur, à utiliser la fédération avec un fournisseur d'identité pour accéder à l'aide Services AWS d'informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, d'un fournisseur d'identité Web AWS Directory Service, du répertoire Identity Center ou de tout utilisateur qui y accède à l'aide des informations d'identification fournies Services AWS par le biais d'une source d'identité. Lorsque des identités fédérées y accèdent Comptes AWS, elles 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. Vous pouvez créer des utilisateurs et des groupes dans IAM Identity Center, ou vous pouvez vous connecter et synchroniser avec un ensemble d'utilisateurs et de groupes dans votre propre source d'identité afin de les utiliser dans toutes vos applications Comptes AWS et applications. Pour obtenir des informations sur IAM Identity Center, 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 au sein de vous Compte AWS qui possède des autorisations spécifiques pour une seule personne ou application. Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer des utilisateurs IAM ayant des informations d'identification à long terme tels que les clés d'accès. Toutefois, si certains cas d'utilisation spécifiques nécessitent des informations d'identification à long terme avec les utilisateurs IAM, nous vous recommandons de faire pivoter les clés d'accès. Pour plus

d'informations, consultez Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification dans le Guide de l'utilisateur IAM.

Un groupe IAM est une identité qui concerne un ensemble d'utilisateurs IAM. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez avoir un groupe nommé IAMAdmins et accorder à ce groupe les autorisations d'administrer des ressources IAM.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent des informations d'identification temporaires. Pour en savoir plus, consultez Quand créer un utilisateur IAM (au lieu d'un rôle) dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une identité au sein de vous Compte AWS dotée d'autorisations spécifiques. Le concept ressemble à celui d'utilisateur IAM, mais le rôle IAM n'est pas associé à une personne en particulier. Vous pouvez assumer temporairement un rôle IAM dans le en AWS Management Console changeant de rôle. Vous pouvez assumer un rôle en appelant une opération d' AWS API AWS CLI ou en utilisant une URL personnalisée. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez Utilisation de rôles IAM dans le Guide de l'utilisateur IAM.

Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :

- Accès utilisateur fédéré – Pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour obtenir des informations sur les rôles pour la fédération, consultez Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM. Si vous utilisez IAM Identity Center, vous configurez un jeu d'autorisations. IAM Identity Center met en corrélation le jeu d'autorisations avec un rôle dans IAM afin de contrôler à quoi vos identités peuvent accéder après leur authentification. Pour plus d'informations sur les jeux d'autorisations, consultez la rubrique Jeux d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .
- Autorisations d'utilisateur IAM temporaires : un rôle ou un utilisateur IAM peut endosser un rôle IAM pour profiter temporairement d'autorisations différentes pour une tâche spécifique.
- Accès intercompte : vous pouvez utiliser un rôle IAM pour permettre à un utilisateur (principal de confiance) d'un compte différent d'accéder aux ressources de votre compte. Les rôles constituent

le principal moyen d'accorder l'accès intercompte. Toutefois, dans certains Services AWS cas, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme proxy). Pour connaître la différence entre les rôles et les politiques basées sur les ressources pour l'accès entre comptes, consultez la section Accès aux ressources entre comptes dans IAM dans le guide de l'utilisateur IAM.

- Accès multiservices — Certains Services AWS utilisent des fonctionnalités dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, un rôle de service ou un rôle lié au service.
  - Sessions d'accès direct (FAS) : lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez Sessions de transmission d'accès.
  - Rôle de service : il s'agit d'un rôle IAM attribué à un service afin de réaliser des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du 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.
  - Rôle lié à un service — Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.
- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un rôle IAM pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une instance EC2 et qui envoient des demandes d'API. AWS CLI AWS Cette solution est préférable au stockage des clés d'accès au sein de l'instance EC2. Pour attribuer un AWS rôle à une instance EC2 et le mettre à la disposition de toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes qui s'exécutent sur l'instance EC2 d'obtenir des informations d'identification temporaires. Pour plus d'informations,

consultez Utilisation d'un rôle IAM pour accorder des autorisations à des applications s'exécutant sur des instances Amazon EC2 dans le Guide de l'utilisateur IAM.

Pour savoir dans quel cas utiliser des rôles ou des utilisateurs IAM, consultez Quand créer un rôle IAM (au lieu d'un utilisateur) dans le Guide de l'utilisateur IAM.

Gestion des 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 est un objet AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit leurs autorisations. AWS évalue ces politiques lorsqu'un principal (utilisateur, utilisateur root ou session de rôle) fait une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations sur la structure et le contenu des documents de politique JSON, consultez Vue d'ensemble des politiques JSON dans le Guide de l'utilisateur IAM.

Les administrateurs peuvent utiliser les 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.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. 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. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Les politiques IAM définissent les autorisations d'une action, quelle que soit la méthode que vous utilisez pour exécuter l'opération. Par exemple, supposons que vous disposiez d'une politique qui autorise l'action `iam:GetRole`. Un utilisateur appliquant cette politique peut obtenir des informations sur le rôle à partir de AWS Management Console AWS CLI, de ou de l' AWS API.

Politiques basées sur l'identité

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher 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 Création de politiques IAM dans le Guide de l'utilisateur IAM.

Les politiques basées sur l'identité peuvent être classées comme des politiques en ligne ou des politiques gérées. Les politiques en ligne sont intégrées directement à un utilisateur, groupe ou rôle. Les politiques gérées sont des politiques autonomes que vous pouvez associer à plusieurs utilisateurs, groupes et rôles au sein de votre Compte AWS. Les politiques gérées incluent les politiques AWS gérées et les politiques gérées par le client. Pour découvrir comment choisir entre une politique gérée et une politique en ligne, consultez Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment. 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

Les politiques basées sur les ressources 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.

Listes de contrôle d'accès (ACL)

Les listes de contrôle d'accès (ACL) vérifie quels principals (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.

Amazon S3 et Amazon VPC sont des exemples de services qui prennent en charge les ACL. AWS WAF Pour en savoir plus sur les listes de contrôle d'accès, consultez Vue d'ensemble des listes de contrôle d'accès (ACL) dans le Guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge d'autres types de politiques moins courants. Ces types de politiques peuvent définir le nombre maximum d'autorisations qui vous sont accordées par des types de politiques plus courants.

- Limite d'autorisations : une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le nombre maximal d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM (utilisateur ou rôle IAM). Vous pouvez définir une limite d'autorisations pour une entité. Les autorisations en résultant représentent la combinaison des politiques basées sur l'identité d'une entité et de ses limites d'autorisation. Les politiques basées sur les ressources qui spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d'autorisations. Un refus explicite dans l'une de ces politiques remplace l'autorisation. Pour plus d'informations sur les limites d'autorisations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.
- Politiques de contrôle des services (SCP) — Les SCP sont des politiques JSON qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans. AWS Organizations AWS Organizations est un service permettant de regrouper et de gérer de manière centralisée Comptes AWS les multiples propriétés de votre entreprise. Si vous activez toutes les fonctionnalités d'une organisation, vous pouvez appliquer les politiques de contrôle des services (SCP) à l'un ou à l'ensemble de vos comptes. Le SCP limite les autorisations pour les entités figurant dans les comptes des membres, y compris chacune Utilisateur racine d'un compte AWS d'entre elles. Pour plus d'informations sur les organisations et les SCP, consultez Fonctionnement des SCP dans le Guide de l'utilisateur AWS Organizations .
- Politiques de séance : les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de séance en résultant sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de séance. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations, consultez politiques de séance 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 fonctionne le AWS Site-to-site VPN avec IAM

Avant d'utiliser IAM pour gérer l'accès à Site-to-Site VPN, découvrez les fonctions IAM que vous pouvez utiliser avec Site-to-Site VPN.

Fonctionnalités IAM que vous pouvez utiliser avec le VPN AWS Site-to-Site

Fonction IAM	Prise en charge de Site-to-Site VPN
Politiques basées sur l'identité	Oui
Politiques basées sur les ressources	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
Fonctions de service	Oui
Rôles liés à un service	Oui

Pour obtenir une vue d'ensemble de la façon dont le VPN Site-to-site et les autres AWS services fonctionnent avec la plupart des fonctionnalités IAM, consultez la section AWS Services compatibles avec IAM dans le Guide de l'utilisateur IAM.

Politiques basées sur l'identité pour Site-to-Site VPN

Prend en charge les politiques basées sur l'identité	Oui

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher 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 Création de politiques IAM 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. Vous ne pouvez pas spécifier le principal dans une politique basée sur une identité car celle-ci s'applique à l'utilisateur ou au rôle auquel elle est attachée. 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.

Exemples de politiques basées sur l'identité pour Site-to-Site VPN

Pour voir des exemples de politiques Site-to-Site VPN basées sur l'identité, veuillez consulter Exemples de politiques basées sur l'identité pour un VPN de site à site AWS.

Politiques basées sur les ressources dans Site-to-Site VPN

Prend en charge les politiques basées sur les ressources	Non

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment. 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. L'ajout d'un principal entre comptes à une politique basée sur les ressources ne représente qu'une partie de l'instauration de la relation d'approbation. Lorsque le principal et la ressource sont différents Comptes AWS, un administrateur IAM du compte sécurisé doit également accorder à l'entité principale (utilisateur ou rôle) l'autorisation d'accéder à la ressource. Pour ce faire, il attache une

politique basée sur une identité à l'entité. Toutefois, si une politique basée sur des ressources accorde l'accès à un principal dans le même compte, aucune autre politique basée sur l'identité n'est requise. Pour plus d'informations, consultez la section Accès aux ressources entre comptes dans IAM dans le guide de l'utilisateur d'IAM.

Actions de politique pour Site-to-Site VPN

Prend en charge les actions de politique	Oui

Les administrateurs peuvent utiliser les 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. Les actions de stratégie portent généralement le même nom que l'opération AWS d'API associée. Il existe quelques exceptions, telles que les actions avec autorisations uniquement qui n'ont pas d'opération API correspondante. Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d'actions dans une stratégie afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour consulter la liste des actions VPN de site à site, consultez la section Actions définies par le VPN de site à site dans la référence d'autorisation AWS de service.

Les actions de politique dans 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 voir des exemples de politiques Site-to-Site VPN basées sur l'identité, veuillez consulter Exemples de politiques basées sur l'identité pour un VPN de site à site AWS.

Ressources de politique pour Site-to-Site VPN

Prend en charge les ressources de politique	Oui

Les administrateurs peuvent utiliser les 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. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, telles que les opérations de liste, 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 VPN de site à site et de leurs ARN, consultez la section Ressources définies par le VPN de site à site dans le Service Authorization AWS Reference. Pour savoir avec quelles actions vous pouvez spécifier l'ARN de chaque ressource, consultez la section Actions définies par le AWS VPN Site-to-Site.

Pour voir des exemples de politiques Site-to-Site VPN basées sur l'identité, veuillez consulter Exemples de politiques basées sur l'identité pour un VPN de site à site AWS.

Clés de condition de politique pour Site-to-Site VPN

Prend en charge les clés de condition de politique spécifiques au service	Oui

Les administrateurs peuvent utiliser les 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` (ou le bloc `Condition`) vous permet de spécifier des conditions lorsqu'une instruction est appliquée. L'élément `Condition` est facultatif. 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.

Si vous spécifiez plusieurs éléments `Condition` dans une instruction, ou plusieurs clés dans un seul élément `Condition`, AWS les évalue à l'aide d'une opération `AND` logique. Si vous spécifiez plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une `OR` opération logique. Toutes les conditions doivent être remplies avant que les autorisations associées à l'instruction ne soient accordées.

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez accorder à un utilisateur IAM l'autorisation d'accéder à une ressource uniquement si elle est balisée avec son nom d'utilisateur IAM. Pour plus d'informations, consultez Éléments d'une politique IAM : variables et identifications dans le Guide de l'utilisateur IAM.

AWS prend en charge les clés de condition globales et les clés de condition spécifiques au service. Pour voir toutes les clés de condition AWS globales, voir les clés de contexte de condition AWS globales dans le guide de l'utilisateur IAM.

Pour consulter la liste des clés de condition d'un VPN de site à site, consultez la section Clés de condition d'un VPN de site à site dans la référence d'autorisation AWS de service. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, consultez Actions définies par le AWS VPN Site-to-Site.

Pour voir des exemples de politiques Site-to-Site VPN basées sur l'identité, veuillez consulter Exemples de politiques basées sur l'identité pour un VPN de site à site AWS.

ACL dans Site-to-Site VPN

Prend en charge les listes ACL	Non

Les listes de contrôle d'accès (ACL) vérifient 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 Site-to-Site VPN

Prise en charge d'ABAC (identifications dans les politiques)	Non

Le contrôle d'accès par attributs (ABAC) est une stratégie d'autorisation qui définit des autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et à de nombreuses AWS ressources. L'étiquetage des entités et des ressources est la première étape d'ABAC. Vous concevez ensuite des politiques ABAC pour autoriser des opérations quand l'identification du principal correspond à celle de la ressource à laquelle il tente d'accéder.

L'ABAC est utile dans les environnements qui connaissent une croissance rapide et pour les cas où la gestion des politiques devient fastidieuse.

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 l'ABAC, consultez Qu'est-ce que le contrôle d'accès basé sur les attributs (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.

Utilisation des informations d'identification temporaires avec Site-to-Site VPN

Prend en charge les informations d'identification temporaires	Oui

Certains Services AWS ne fonctionnent pas lorsque vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, y compris celles qui Services AWS fonctionnent avec des informations d'identification temporaires, consultez Services AWS la section relative à l'utilisation d'IAM dans le guide de l'utilisateur d'IAM.

Vous utilisez des informations d'identification temporaires si vous vous connectez à l' AWS Management Console aide d'une méthode autre qu'un nom d'utilisateur et un mot de passe. Par exemple, lorsque vous accédez à AWS l'aide du lien d'authentification unique (SSO) de votre entreprise, ce processus crée automatiquement des informations d'identification temporaires. Vous créez également automatiquement des informations d'identification temporaires lorsque vous vous connectez à la console en tant qu'utilisateur, puis changez de rôle. Pour plus d'informations sur le changement de rôle, consultez Changement de rôle (console) dans le Guide de l'utilisateur IAM.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide de l' AWS API AWS CLI or. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour y accéder AWS. 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.

Autorisations de principal entre services pour Site-to-Site VPN

Prend en charge les sessions d'accès direct (FAS)	Oui

Lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur une politique lors de la formulation de demandes FAS, consultez Transmission des sessions d'accès.

Rôles de service pour Site-to-Site VPN

Prend en charge les fonctions du service	Oui

Une fonction 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 une fonction du 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 d'un rôle du service peut altérer la fonctionnalité de Site-to-Site VPN. Ne modifiez des fonctions du service que quand Site-to-Site VPN vous le conseille.

Rôles liés à un service pour 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 endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire 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 Rôle lié à un service. Choisissez le lien Oui pour consulter la documentation du rôle lié à ce service.

Exemples de politiques basées sur l'identité pour un VPN de site à site AWS

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou modifier les ressources Site-to-Site VPN. Ils ne peuvent pas non plus effectuer de tâches à l'aide de l'API AWS Management Console, AWS Command Line Interface (AWS CLI) ou de AWS l'API. 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. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

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 dans l'onglet JSON dans le Guide de l'utilisateur IAM.

Pour plus de détails sur les actions et les types de ressources définis par le VPN de site à site, y compris le format des ARN pour chacun des types de ressources, consultez la section Actions, ressources et clés de condition pour le VPN AWS de site à site dans la référence d'autorisation de service.

Rubriques

- Bonnes pratiques en matière de politiques
- Utilisation de la console Site-to-Site VPN
- Décrire les connexions VPN spécifiques de site à site
- Création et description des ressources nécessaires à une AWS Site-to-Site VPN connexion

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si une personne peut créer, consulter ou supprimer des ressources Site-to-Site VPN dans votre compte. 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 du 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 les AWS clients 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.
- Accorder 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 de IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.

- Utiliser 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 service spécifique Service AWS, tel que AWS CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez IAM Access Analyzer pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : IAM Access Analyzer 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 politique IAM Access Analyzer dans le Guide de l'utilisateur IAM.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root, activez l'authentification MFA pour une sécurité accrue. Compte AWS Pour exiger le MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Configuration de l'accès aux API protégé par 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 VPN Site-to-Site, vous devez disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent vous permettre de répertorier et de consulter les détails des ressources VPN de site à site de votre. Compte AWS Si vous créez une stratégie 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 stratégie.

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 garantir que les utilisateurs et les rôles peuvent toujours utiliser la console VPN de site à site, associez également le VPN de site à site ou la politique gérée aux entités. `AmazonVPCFullAccess`

`AmazonVPCReadOnlyAccess` AWS Pour plus d'informations, consultez Ajout d'autorisations à un utilisateur dans le Guide de l'utilisateur IAM.

Décrire les connexions VPN spécifiques de site à site

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "ec2:DescribeVpnConnections"
         ],
         "Resource": [
         "arn:aws:ec2:us-west-2:123456789012:vpn-connection/vpn-04d5cc9b88example",
         "arn:aws:ec2:us-west-2:123456789012:vpn-connection/vpn-903004f88example"
         ]
      }
   ]
}
```

Création et description des ressources nécessaires à une AWS Site-to-Site VPN connexion

```
{
   "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 d'identité et d'accès au VPN de site à site

Utilisez les informations suivantes pour identifier et résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec Site-to-Site VPN et IAM.

Rubriques

- Je ne suis pas autorisé à effectuer une action dans Site-to-Site VPN
- Je ne suis pas autorisé à effectuer iam : PassRole
- Je souhaite autoriser des personnes extérieures à moi Compte AWS à accéder à mes ressources VPN Site-to-Site

Je ne suis pas autorisé à effectuer une action dans 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 une erreur selon laquelle vous n'êtes pas autorisé à exécuter l'action `iam:PassRole`, vos politiques doivent être mises à jour afin de vous permettre de transmettre un rôle à 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, un utilisateur doit disposer des autorisations nécessaires pour transmettre le rôle au service.

L'erreur suivante se produit quand un utilisateur IAM nommé `marymajor` tente d'utiliser la console pour exécuter une action dans Site-to-Site VPN. Toutefois, l'action nécessite que le service ait des autorisations accordées par un rôle de service. Mary ne dispose pas des autorisations nécessaires pour transférer 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 moi Compte AWS à accéder à mes ressources VPN Site-to-Site

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 en savoir plus, consultez les éléments suivants :

- Pour savoir si Site-to-Site VPN prend en charge ces fonctionnalités, consultez Comment fonctionne le AWS Site-to-site VPN avec IAM.

- Pour savoir comment fournir l'accès à vos ressources sur celles Comptes AWS que vous possédez, consultez la section Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS que vous possédez dans le Guide de l'utilisateur IAM.
- Pour savoir comment fournir l'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 connaître la différence entre l'utilisation de rôles et de politiques basées sur les ressources pour l'accès entre comptes, consultez la section Accès aux ressources entre comptes dans IAM dans le guide de l'utilisateur d'IAM.

Utilisation des rôles liés à un service pour Site-to-Site VPN

AWS Le VPN de site à site utilise des rôles liés à un service AWS Identity and Access Management (IAM). Un rôle lié à un service est un type unique de rôle IAM lié directement à Site-to-Site VPN. Les rôles liés aux services sont prédéfinis par le VPN Site-to-Site et incluent toutes les autorisations dont le service a besoin pour AWS appeler d'autres services en votre nom.

Un rôle lié à un service simplifie la configuration de Site-to-Site VPN, car vous n'avez pas besoin d'ajouter manuellement les autorisations requises. Site-to-Site VPN définit les autorisations de ses rôles liés à un service ; sauf définition contraire, seul Site-to-Site VPN peut endosser ses rôles. Les autorisations définies comprennent la politique d'approbation 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. Vos ressources Site-to-Site VPN sont ainsi protégées, car vous ne pouvez pas involontairement supprimer l'autorisation d'accéder aux ressources.

Pour plus d'informations sur les autres services prenant en charge les rôles liés à un service, consultez Services AWS qui fonctionnent avec IAM et recherchez les services présentant la mention Yes (Oui) dans la colonne Service-linked roles (Rôles liés à un service). Sélectionnez un Oui ayant un lien pour consulter la documentation du rôle lié à un service, pour ce service.

Autorisations de rôle lié à un service pour Site-to-Site VPN

Le VPN de site à site utilise le rôle lié à un service nommé — Autoriser le VPN de site à AWSServiceRoleForVPCS2SVPNsite à créer et à gérer des ressources liées à vos connexions VPN.

Le rôle AWSServiceRoleForVPCS2SVPN lié à un service fait confiance aux services suivants pour assumer le rôle :

- `AWS Certificate Manager`
- `AWS Private Certificate Authority`

La politique d'autorisation de rôle nommée AWSVPCS2SVpnServiceRolePolicy permet au Site-to-Site VPN d'effectuer les actions suivantes sur les ressources spécifiées :

- Action : `acm:ExportCertificate` sur `Resource: "*"`
- Action : `acm:DescribeCertificate` sur `Resource: "*"`
- Action : `acm:ListCertificates` sur `Resource: "*"`
- Action : `acm-pca:DescribeCertificateAuthority` sur `Resource: "*"`

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, un groupe ou un rôle) de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez Autorisations de rôles liés à un service dans le Guide de l'utilisateur IAM.

Création d'un rôle lié à un service pour Site-to-Site VPN

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 AWS Management Console, le ou l' AWS API AWS CLI, le VPN Site-to-Site 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, Site-to-Site VPN crée à nouveau le rôle lié à un service pour vous.

Modification d'un rôle lié à un service pour Site-to-Site VPN

Le VPN de site à site ne vous permet pas de modifier le rôle lié au service. AWSServiceRoleForVPCS2SVPN Une fois que vous avez 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 Modification d'un rôle lié à un service dans le guide de l'utilisateur IAM.

Suppression d'un rôle lié à un service pour Site-to-Site VPN

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 peut échouer. Si cela se produit, patientez quelques minutes et réessayez.

Pour supprimer les ressources VPN de site à site 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. Ceci vous évite de supprimer par inadvertance l'autorisation d'accéder à vos certificats ACM utilisés par les connexions Site-to-Site VPN.

Pour supprimer manuellement le rôle lié à un service à l'aide d'IAM

Utilisez la console IAM, le AWS CLI, ou l' AWS API pour supprimer le rôle lié au AWSServiceRoleForVPCS2SVPN service. Pour plus d'informations, consultez 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, connectées par un réseau à faible latence, à 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 mondiale.

Outre l'infrastructure AWS mondiale, le VPN Site-to-Site 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, pour augmenter la disponibilité de votre VPC. 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 votre connexion VPN, ce qui peut désactiver brièvement l'un des deux tunnels de votre connexion VPN. Pour plus d'informations, consultez Remplacements de points de terminaison de tunnel Site-to-Site VPN. Lorsque vous configurez votre passerelle client, il est donc important de configurer les deux tunnels.

Redondance

Pour vous protéger contre une perte de connectivité si votre passerelle client devient indisponible, vous pouvez configurer une deuxième connexion Site-to-Site VPN. Pour plus d'informations, consultez la documentation de suivante :

- Utilisation de connexions Site-to-Site VPN redondantes pour fournir un basculement
- Amazon Virtual Private Cloud Connectivity Options
- Création d'une infrastructure réseau multi-VPC AWS évolutive et sécurisée

Sécurité de l'infrastructure dans le VPN de AWS site à site

En tant que service géré, le AWS Site-to-Site VPN est protégé par AWS la sécurité du réseau mondial. Pour plus d'informations sur les services AWS de sécurité et sur la manière dont AWS l'infrastructure est protégée, consultez la section Sécurité du AWS cloud. 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 le cadre AWS bien architecturé du pilier de sécurité.

Vous utilisez des appels d'API AWS publiés pour accéder au VPN Site-to-Site 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.
- Ses suites de chiffrement PFS (Perfect Forward Secrecy) comme DHE (Ephemeral Diffie-Hellman) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

En outre, les demandes doivent être signées à l'aide d'un ID de clé d'accès et d'une clé d'accès secrète associée à un principal IAM. Vous pouvez également utiliser AWS Security Token Service (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

Surveillance de votre connexion Site-to-Site VPN

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 afin de pouvoir déboguer plus facilement une éventuelle défaillance à plusieurs points. Avant de commencer la supervision de votre connexion Site-to-Site VPN, toutefois, vous devez créer un plan de surveillance qui contient 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

Table des matières

Outils de surveillance

AWS fournit différents outils que vous pouvez utiliser pour surveiller une connexion VPN de site à site. 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 sont dans un état particulier ; l'état doit avoir changé et être maintenu pendant un certain nombre de périodes. Pour plus d'informations, consultez Surveillance des tunnels VPN 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 Journalisation des appels d'API AWS CloudTrailà l'aide du 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 VPN de site à site, 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 Surveillance des connexions VPN à l'aide d' AWS Health événements.

Outils de surveillance manuelle

Un autre élément important de la surveillance d'une connexion VPN de site à site 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 VPN Site-to-site, tels que « Status » et « Last status change », 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
  - Connexions Site-to-Site VPN
  - Statut du tunnel VPN (Dans le volet de navigation, sélectionnez Site-to-Site VPN Connections (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 utiliser CloudWatch pour 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 de VPN de site à site. Cette fonctionnalité vous permet d'accéder aux journaux de connexion Site-to-Site VPN

qui fournissent des détails sur l'établissement d'un tunnel IP Security (IPsec), les négociations IKE (Internet Key Exchange) et les messages de protocole DPD (Dead Peer Detection).

Les journaux VPN de site à site peuvent être publiés sur Amazon Logs. CloudWatch Cette fonctionnalité permet aux clients d'accéder et d'analyser de manière cohérente les journaux détaillés de toutes leurs connexions Site-to-Site VPN.

Table des matières

Avantages des journaux Site-to-Site VPN

- Résolution des problèmes VPN simplifiés : les journaux VPN de site à site vous aident à identifier les incohérences de configuration entre le dispositif de passerelle de votre client AWS 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 VPN de site à site peuvent fournir des journaux d'activité des tunnels pour les différentes manières dont le VPN de site à site est connecté : passerelle virtuelle, passerelle de transit et utilisation à la fois d'Internet et CloudHub comme moyen de transport. AWS Direct Connect Cette fonctionnalité permet aux clients d'accéder et d'analyser de manière cohérente les journaux détaillés de toutes leurs connexions Site-to-Site VPN.

- Sécurité et conformité : les journaux VPN de site à site 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 VPN Site-to-Site 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/`.

Contenu des journaux Site-to-Site VPN

Les informations suivantes sont incluses dans le journal d'activité de tunnel Site-to-Site VPN.

Champ	Description
VpnLogCreationTimestamp	Horodatage de création du journal au format lisible par l'utilisateur.
VpnConnectionId	Identifiant de connexion au VPN.
TunnelOutsideAdresse IP	Adresse IP externe du tunnel VPN qui a généré l'entrée de journal.
TunnelDPDEnabled	Statut d'activation du protocole Dead Peer Detection (True/False).
Tunnel CGWnatt DetectionStatus	Détection de NAT-T sur l'appareil de passerelle client (True/False).
TunnelIKEPhase1State	État du protocole IKE en phase 1 (Established | Rekeying | Negotiating | Down).

Champ	Description
TunnelIKEPhase2State	État du protocole IKE en phase 2 (Established | Rekeying | Negotiating | Down).
VpnLogDétail	Messages détaillés pour les protocoles IPsec, IKE et DPD.

Table des matières

Messages d'erreur IKEv1

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, par exemple 3DES
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/politiques correctes doivent être configurées pour la phase 2 sur les pairs IKE.

Message	Explication
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

Messages d'erreur IKEv2

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	Le pair a envoyé le message Delete_SA pour Parent/IKE_SA
AWS tunnel a reçu DELETE pour la phase 2 SA avec SPI : xxxx	Le pair 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	À cause de la collision, si des SA redondant es sont générées, les pairs fermeront les SA redondantes après avoir fait correspondre les valeurs nonce conformément à la norme 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, p. ex. une propositi on incorrecte.
AWS : sélecteur de trafic : TS_UNACCE PTABLE : reçu du répondeur	Le pair a proposé des sélecteurs de trafic/ un domaine de chiffrement incorrect(s). Les

Message	Explication
	pairs doivent être configurés avec des CIDR identiques et corrects.
AWS le tunnel envoie AUTHENTICATION_FAILED 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.
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 (chiffrement, hachage et groupe DH) ne sont pas pris en charge par le point de terminaison AWS VPN. Par exemple 3DES

Messages de négociation IKEv2

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

Message	Explication
AWS réponse traitée par tunnel (id=xxx) pour CREATE_CHILD_SA	AWS a reçu la réponse CREATE_CHILD_SA de CGW

Exigences relatives à l'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.

```
{
  "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"
```

```
    }
  ]
}
```

Affichage de la configuration des journaux Site-to-Site 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, choisissez Site-to-Site VPN Connections (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 journalisation dans le journal Tunnel VPN et le groupe de CloudWatch journaux actuellement configuré (le cas échéant) sous groupe de CloudWatch journaux.

Pour consulter les paramètres actuels de journalisation du tunnel sur une connexion VPN Site-to-Site à l'aide de la AWS ligne de commande ou de l'API

- DescribeVpnConnexions (API de requête Amazon EC2)
- describe-vpn-connections (AWS CLI)

Activation des journaux Site-to-Site VPN

> **Note**
>
> Lorsque vous activez les journaux Site-to-Site VPN pour un tunnel de connexion VPN existant, votre connectivité à 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 plus d'informations, consultez Remplacements de points de terminaison de tunnel Site-to-Site VPN.

Pour activer la journalisation du VPN lors de la création d'une 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 connexion Site-to-Site VPN.

Pour activer la journalisation par tunnel sur une nouvelle connexion VPN Site-to-Site à l'aide de la AWS ligne de commande ou de l'API

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

Pour activer la journalisation 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, choisissez Site-to-Site VPN Connections (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 par tunnel sur une connexion VPN Site-to-Site existante à l'aide de la AWS ligne de commande ou de l'API

- ModifyVpnTunnelOptions(API de requête Amazon EC2)
- modify-vpn-tunnel-options (AWS CLI)

Désactivation des journaux Site-to-Site VPN

Pour désactiver la journalisation 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 (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), 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 par tunnel sur une connexion VPN Site-to-Site à l'aide de la AWS ligne de commande ou de l'API

- ModifyVpnTunnelOptions(API de requête Amazon EC2)
- modify-vpn-tunnel-options (AWS CLI)

Surveillance des tunnels VPN 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

- Création d' CloudWatch alarmes pour surveiller les tunnels VPN

Métriques et dimensions VPN

Les CloudWatch statistiques suivantes sont disponibles pour vos connexions VPN de site à site.

Métrique	Description
`TunnelState`	État des tunnels. Pour les VPN statiques, 0 indique DOWN et 1 indique UP. Pour les VPN BGP, 1 indique ESTABLISHED et 0 est utilisé pour tous les autres états. Pour les deux types de VPN, des valeurs comprises entre 0 et 1 indiquent qu'au moins un tunnel n'est pas à l'état « UP ». 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

Métrique	Description
	statistique Somme pour afficher le nombre total d'octets envoyés pendant la période. Cette métrique comptabilise les données avant chiffrement. Unités : octets

† 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 des métriques en fonction de l'ID de la 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 CloudWatch métriques du VPN

Lorsque vous créez une connexion VPN Site-to-Site, le service VPN envoie des statistiques concernant votre connexion VPN dès qu'elles sont CloudWatch 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 de métrique pour afficher les métriques (par exemple, Métriques de tunnel VPN).

> **Note**
>
> L'espace de noms VPN n'apparaîtra pas dans la CloudWatch console tant qu'une connexion VPN Site-to-Site n'aura pas été créée dans AWS la 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"
```

Création d' CloudWatch alarmes pour surveiller les tunnels VPN

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 pour l'état de 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 VPN de site à site et la métrique. TunnelState Choisissez Sélectionner une métrique.
6. Pour Statistic (Statistiques), spécifiez Maximum.

   Si vous avez configuré votre connexion Site-to-Site VPN de manière à ce que les deux tunnels soient actifs, vous pouvez aussi spécifier une statistique Minimum pour envoyer une notification lorsqu'au moins un tunnel ne fonctionne plus.
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 métrique TunnelDataIn. 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 métrique TunnelDatade sortie. 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.

Surveillance des connexions VPN à l'aide d' AWS Health événements

AWS Site-to-Site VPN envoie automatiquement des notifications au AWS AWS Health Dashboard(PHD), qui est alimenté par l' AWS Health API. 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 AWS Health Dashboard.

AWS Health Dashboard 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 AWS Health Dashboard 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 plus d'informations, consultez Remplacements de points de terminaison de tunnel Site-to-Site VPN.

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 AWS Health Dashboard événement.

Notifications de VPN à tunnel unique

Une connexion Site-to-Site VPN se compose de deux tunnels pour la 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 AWS Health Dashboard . 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.

Quotas de Site-to-Site VPN

Votre AWS compte possède les quotas suivants, anciennement appelés limites, liés au VPN Site-to-Site. Sauf indication contraire, chaque quota est spécifique à la 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.

Ressources Site-to-Site VPN

Nom	Par défaut	Ajustable
Passerelles client par région	50	Oui
Passerelles réseau privé virtuel par région	5	Oui
Connexions Site-to-Site VPN par région	50	Oui
Connexions Site-to-Site VPN par passerelle réseau privé virtuel	10	Oui
Connexions Site-to-Site VPN accélérées par région	10	Oui
Connexions Site-to-Site VPN non associées par région	10	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 VPC, nous vous recommandons d'explorer plutôt au

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

Les connexions Site-to-Site VPN sur une passerelle de transit sont soumises à la limite totale des attachements de passerelle de transit. Pour plus d'informations, consultez Quotas de passerelle Transit Gateway.

Acheminements

Les sources d'acheminement annoncées incluent les acheminements VPC, les autres acheminements VPN et les acheminements provenant d'interfaces virtuelles AWS 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.

Nom	Par défaut	Ajustable
Acheminements dynamiques annoncés à partir d'une passerelle client sur une passerelle réseau privé virtuel vers une connexion Site-to-Site VPN	100	Non
Acheminements annoncés à partir d'une connexion Site-to-Site VPN sur une passerell e réseau privé virtuel vers un périphérique de passerelle client	1 000	Non
Acheminements dynamiques annoncés à partir d'une passerelle client sur une passerelle Transit Gateway vers une connexion Site-to-S ite VPN	1 000	Non

Nom	Par défaut	Ajustable
Acheminements annoncés à partir d'une connexion Site-to-Site VPN sur une passerelle Transit Gateway vers un périphérique de passerelle client	5 000	Non
Acheminement statique d'un périphérique de passerelle client vers une connexion Site-to-Site VPN sur une passerelle réseau privé virtuel	100	Non

Bande passante et débit

De nombreux facteurs peuvent affecter la bande passante réalisée via une connexion Site-to-Site VPN, y compris, sans s'y limiter, la taille des paquets, le mélange de 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.

Nom	Par défaut	Ajustable
Bande passante maximale par tunnel VPN	Jusqu'à 1,25 Gbit/s	Non
Nombre maximal de paquets par seconde (PPS) par tunnel VPN	Jusqu'à 140 000	Non

Pour les connexions Site-to-Site VPN sur une passerelle de transit, vous pouvez utiliser ECMP pour obtenir une bande passante VPN supérieure en regroupant 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.

Unité de transmission maximale (MTU)

Le Site-to-Site 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 Bonnes pratiques pour votre périphérique 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 l'utilisateur Amazon EC2.

Une connexion Site-to-Site VPN ne prend pas en charge la détection de la MTU du chemin.

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 du document Guide de l'utilisateur Site-to-Site VPN

Le tableau suivant décrit les mises à jour du Guide de l’utilisateur AWS Site-to-Site VPN.

Modification	Description	Date
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	Les clients Site-to-Site VPN peuvent générer des modèles de configuration pour les périphériques de passerelle client (CGW) compatibles, ce qui facilite la création de connexions VPN à AWS. Cette mise à jour ajoute une prise en charge des paramètres d'IKEv2 (Internet Key Exchange version 2) pour de nombreux périphériques CGW très répandus et comprend deux nouvelles API : GetVPNConnectionDeviceTypes et GetVPNConnectionDeviceSampleConfiguration.	21 septembre 2021
Notifications de connexion VPN	Site-to-Site VPN envoie automatiquement des	29 octobre 2020

	notifications concernant votre connexion VPN au AWS Health Dashboard.	
Lancement du tunnel VPN	Vous pouvez configurer vos tunnels VPN de sorte que AWS les active.	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
Prise en charge d'IPv6	Vos tunnels VPN peuvent prendre en charge le trafic IPv6 à l'intérieur des tunnels.	12 août 2020
Fusionner les guides AWS Site-to-Site VPN	Cette version fusionne le contenu de « AWS Site-to-Site VPN Network Administrator Guide » avec ce guide.	31 mars 2020
Connexions AWS Site-to-Site VPN accélérées	Vous pouvez activer l'accélération de votre connexion AWS Site-to-Site VPN.	3 décembre 2019
Modifier les options de tunnel AWS Site-to-Site VPN	Vous pouvez modifier les options d'un tunnel VPN d'une connexion AWS Site-to-Site VPN. Vous pouvez également configurer d'autres options de tunnel.	29 août 2019

Support des certificats privés AWS Private Certificate Authority	Vous pouvez utiliser un certificat privé de AWS Private Certificate Authority pour authentifier votre VPN.	15 août 2019
Nouveau guide de l'utilisateur Site-to-Site VPN	Cette version sépare le contenu AWS Site-to-Site VPN (anciennement connu sous le nom AWS Managed VPN) du Guide de l'utilisateur Amazon VPC.	18 décembre 2018
Modification de la passerelle cible	Vous pouvez modifier la passerelle cible d'une connexion AWS Site-to-Site VPN.	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 afficher les métriques CloudWatch pour 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 VPN IPsec à Amazon VPC à l'aide de configurations de routage statique. 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 maintenant configurer la propagation automatique d'acheminements depuis vos liens VPN et AWS Direct Connect vers vos tables de routage VPC.	13 septembre 2012
AWS VPN CloudHub et connexions VPN redondantes	Vous pouvez communiquer en toute sécurité entre deux sites avec ou sans un VPC. Vous pouvez utiliser des connexion s 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.