Guía del usuario

AWS Site-to-Site VPN

AWS Site-to-Site VPN: Guía del usuario

Table of Contents

¿Qué es AWS Site-to-Site VPN?

De forma predeterminada, una instancia que lances dentro de una Amazon VPC no se puede comunicar con una red local (Nube de AWS) y un dispositivo remoto; por ejemplo, puede ser un sitio o un dispositivo local. Puede habilitar el acceso a sus dispositivos remotos desde su VPC creando una conexión AWS Site-to-Site VPN (Site-to-Site VPN) y configurando el enrutamiento para que pase el tráfico a través de la conexión.

Aunque el término conexión VPN es un término general, en esta documentación, una conexión VPN hace referencia a la conexión entre tu VPC y tu propia red local. Site-to-Site La VPN admite conexiones VPN de seguridad mediante el Protocolo de Internet (IPsec).

Contenido

Conceptos

Los conceptos clave de la Site-to-Site VPN son los siguientes:

- Conexión VPN: una conexión segura entre su equipo local y su VPCs.
- Túnel de VPN: enlace cifrado donde los datos pueden pasar desde la red del cliente hasta AWS o salir de allí.

  Cada conexión de VPN incluye dos túneles de VPN que puede utilizar simultáneamente para conseguir alta disponibilidad.
- Pasarela de cliente: un AWS recurso que proporciona información AWS sobre su dispositivo de pasarela de cliente.
- Dispositivo de puerta de enlace para el cliente: un dispositivo físico o una aplicación de software en su lado de la conexión Site-to-Site VPN.
- Puerta de enlace de destino: término genérico para el punto final de la VPN en el lado Amazon de la conexión Site-to-Site VPN.

- Puerta de enlace privada virtual: una puerta de enlace privada virtual es el punto final de la conexión VPN en el lado Amazon de la conexión Site-to-Site VPN que se puede conectar a una sola VPC.
- Puerta de enlace de tránsito: un centro de tránsito que se puede usar para interconectar redes múltiples VPCs y locales, y como punto final de VPN para el lado Amazon de la conexión Site-to-Site VPN.

Site-to-Site Características de la VPN

Las AWS Site-to-Site VPN conexiones admiten las siguientes funciones:

- Internet Key Exchange versión 2 (IKEv2)
- Recorrido de NAT
- ASN de 4 bytes comprendidos entre 1 y 2147483647 para la configuración de puerta de enlace privada virtual (VGW). Para obtener más información, consulte Opciones de pasarela de clientes para su AWS Site-to-Site VPN conexión.
- ASN de 2 bytes para puerta de enlace de cliente (CGW) comprendidos entre 1 y 65535. Para obtener más información, consulte Opciones de pasarela de clientes para su AWS Site-to-Site VPN conexión.
- CloudWatch métricas
- Direcciones IP reutilizables para sus gateways de cliente
- Opciones de cifrado adicionales; incluido el cifrado AES de 256 bits, hash SHA-2 y grupos adicionales Diffie-Hellman
- Opciones de túnel configurables
- ASN privado personalizado para el lado de Amazon de una sesión BGP
- Certificado privado de una CA subordinada de AWS Private Certificate Authority
- Soporte para IPv6 soporte para AWS Site-to-Site VPN
  - IPv6 para direcciones IP de túnel interno (IP de paquete)
  - IPv6 para direcciones IP de túnel exterior (IP de túnel) en Transit Gateway y Cloud WAN
- Soporte de IPv6 migración completo con las siguientes combinaciones:
  - IPv6 IP de túnel exterior con IP de paquete IPv6 interior (IPv6-in-IPv6)
  - IPv6 IP de túnel exterior con IP de paquete IPv4 interior (IPv4-in-IPv6)

Site-to-Site Limitaciones de la VPN

Una conexión Site-to-Site VPN tiene las siguientes limitaciones.

- IPv6 el tráfico no es compatible con las conexiones VPN en una puerta de enlace privada virtual. IPv6 para túnel exterior solo IPs es compatible con Transit Gateway y Cloud WAN.
- Una AWS VPN conexión no admite Path MTU Discovery.
- Una sola conexión Site-to-Site VPN no puede admitir ambos tipos IPv4 de IPv6 tráfico simultáneamente. Necesita conexiones VPN independientes para el transporte IPv4 y IPv6 los paquetes.
- Las conexiones VPN con IP privadas no admiten IPv6 direcciones para el túnel exterior IPs.
- No puede modificar una conexión IPv4 VPN existente para utilizarla IPv6. Debe eliminar la conexión existente y crear una nueva.

Además, tenga en cuenta lo siguiente cuando utilice Site-to-Site una VPN.

- Al conectarse VPCs a una red local común, le recomendamos que utilice bloques CIDR que no se superpongan en sus redes.

Site-to-Site Recursos de VPN

Puede crear, acceder y administrar sus recursos de Site-to-Site VPN mediante cualquiera de las siguientes interfaces:

- AWS Management Console— Proporciona una interfaz web que puede utilizar para acceder a sus recursos de Site-to-Site VPN.
- AWS Command Line Interface (AWS CLI) — Proporciona comandos para un amplio conjunto de AWS servicios, incluido Amazon VPC, y es compatible con Windows, macOS y Linux. Las líneas de comandos se incluyen en la AWS Site-to-Site VPN referencia de línea de comandos más amplia EC2
  - Para obtener información general sobre la interfaz de línea de comandos, consulte. AWS Command Line Interface
  - Para ver la lista de EC2 comandos disponibles, incluidos los comandos de la Site-to-Site VPN, consulte EC2 la Referencia de la línea de comandos.

> **Note**
>
> La referencia de la línea de comandos no diferencia entre los comandos de la Site-to-Site VPN y el conjunto más amplio de EC2 comandos

- AWS SDKs— Especifica un idioma específico APIs y se ocupa de muchos de los detalles de la conexión, como el cálculo de las firmas, la gestión de los reintentos de las solicitudes y la gestión de los errores. Para obtener más información, consulte AWS SDKs.
- Query API (API de consulta): proporciona acciones de la API de nivel bajo a las que se llama mediante solicitudes HTTPS. La API de consulta es la forma más directa de acceder a Amazon VPC, pero requiere que la aplicación controle niveles de detalle de bajo nivel, como la generación de hash para firmar la solicitud y el control de errores. Para obtener más información, consulta la referencia de la EC2 API de Amazon.

Precios

Se le cobra por cada hora de conexión VPN que aprovisione su conexión VPN y esté disponible. Para obtener más información, consulte los precios AWS Site-to-Site VPN de Accelerated Site-to-Site VPN Connection.

Se te cobrará por la transferencia de datos de Amazon EC2 a Internet. Para obtener más información, consulta Data Transfer en la página de precios de Amazon EC2 On-Demand.

Cuando usted crea una conexión de VPN acelerada, nosotros creamos y administramos dos aceleradores en su nombre. Se le cobrará una tarifa por hora y los costos de transferencia de datos para cada acelerador. Para obtener más información, consulte Precios de AWS Global Accelerator.

El uso de IPv6 direcciones con sus conexiones Site-to-Site VPN no conlleva cargos adicionales.

Cómo AWS Site-to-Site VPN funciona

Una conexión Site-to-Site VPN consta de los siguientes componentes:

- Una puerta de enlace privada virtual o una puerta de enlace de tránsito
- Un dispositivo de puerta de enlace de cliente
- Una puerta de enlace de cliente

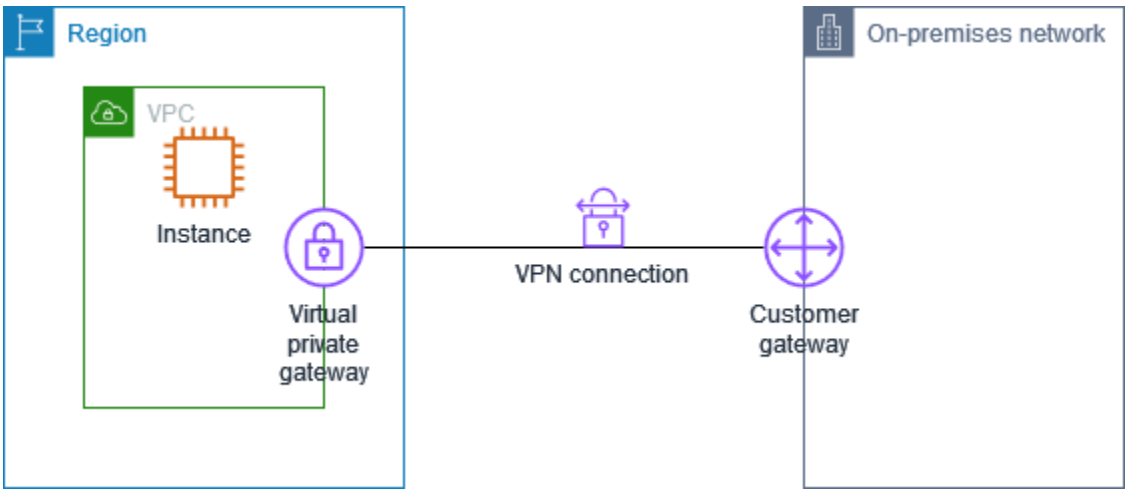
La conexión VPN ofrece dos túneles VPN entre una puerta de enlace privada virtual o una puerta de enlace de tránsito, por un AWS lado, y una puerta de enlace de cliente, por el lado local.

Para obtener más información sobre las cuotas de Site-to-Site VPN, consulteAWS Site-to-Site VPN cuotas.

Gateway privada virtual

Una puerta de enlace privada virtual es el concentrador de VPN en el lado Amazon de la conexión Site-to-Site VPN. Cree una puerta de enlace privada virtual y la conecte a una nube privada virtual (VPC) con recursos que deben acceder a la Site-to-Site conexión VPN.

El siguiente diagrama muestra una conexión de VPN entre una VPC y la red en las instalaciones mediante una puerta de enlace privada virtual.



Al crear una gateway privada virtual, puede especificar el número de sistema autónomo (ASN) privado en el lado de Amazon de la gateway. Si no especifica un ASN, la gateway privada virtual se crea con el ASN predeterminado (64 512). No se puede cambiar el ASN una vez que ha creado

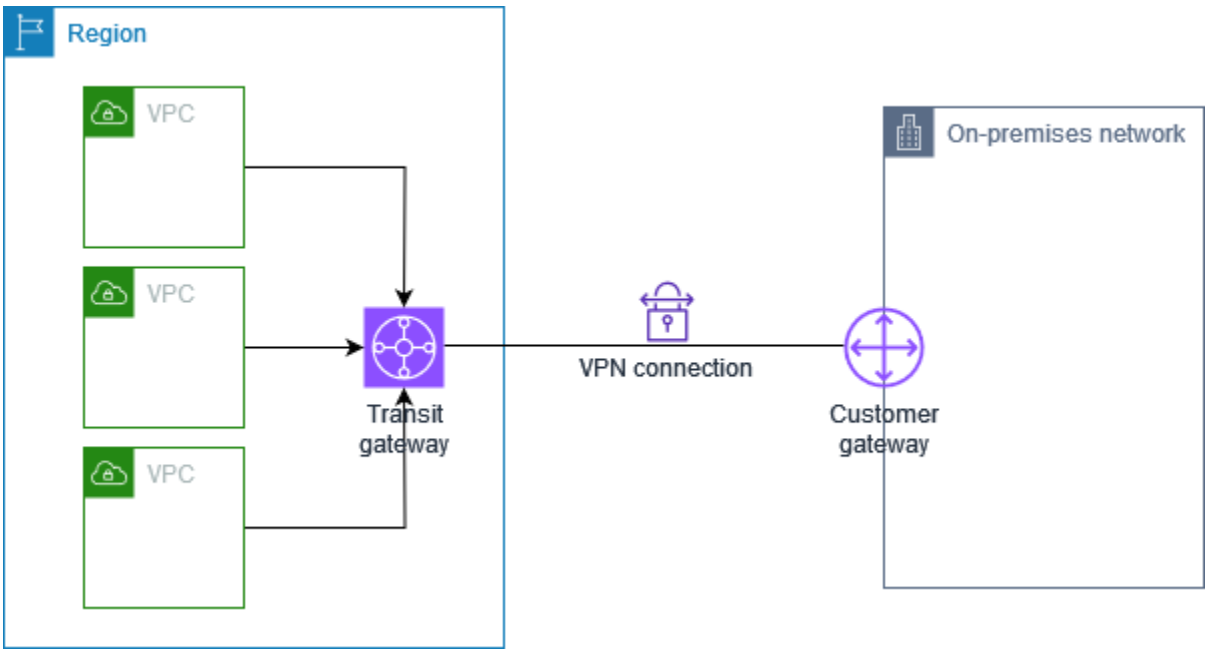
la gateway privada virtual. Para comprobar el ASN de su puerta de enlace privada virtual, consulte sus detalles en la página de pasarelas privadas virtuales de la consola de Amazon VPC o utilice el comando. describe-vpn-gateways AWS CLI

> **Note**
>
> Las pasarelas privadas virtuales no admiten IPv6 conexiones VPN. Site-to-Site Si necesitas IPv6 asistencia, usa una pasarela de tránsito o una WAN en la nube para tu conexión VPN.

Puerta de enlace de tránsito

Una pasarela de tránsito es un centro de tránsito que puedes usar para interconectar tus redes VPCs con las locales. Para obtener más información, consulte Gateways de tránsito de Amazon VPC. Puedes crear una conexión Site-to-Site VPN como un archivo adjunto en una pasarela de tránsito.

El siguiente diagrama muestra una conexión VPN entre varias redes VPCs y la local mediante una puerta de enlace de tránsito. La puerta de enlace de tránsito tiene tres conexiones de VPC y una conexión de VPN.



La conexión Site-to-Site VPN en una puerta de enlace de tránsito puede soportar IPv4 el IPv6 tráfico dentro de los túneles VPN (direcciones IP internas). Además, las pasarelas de tránsito admiten IPv6 direcciones para las direcciones IP del túnel exterior. Para obtener más información, consulte IPv4 y IPv6 tráfico en AWS Site-to-Site VPN.

Puede modificar la puerta de enlace de destino de una conexión Site-to-Site VPN de una puerta de enlace privada virtual a una puerta de enlace de tránsito. Para obtener más información, consulte the section called “Modificación de la puerta de enlace de destino de una conexión de VPN”.

Dispositivo de gateway de cliente

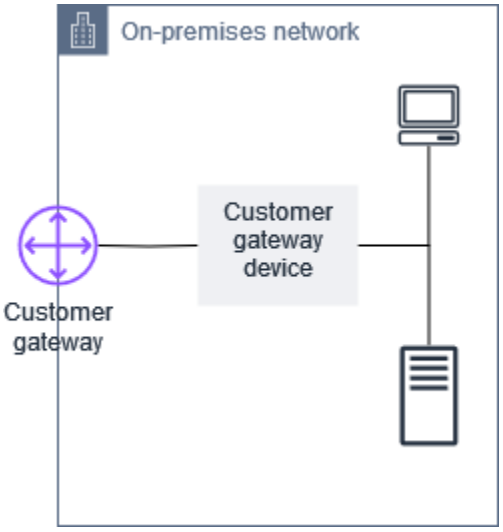
Un dispositivo de puerta de enlace para clientes es un dispositivo físico o una aplicación de software que se encuentra en su lado de la conexión Site-to-Site VPN. Usted configura el dispositivo para que funcione con la conexión Site-to-Site VPN. Para obtener más información, consulte AWS Site-to-Site VPN dispositivos de puerta de enlace para clientes.

De forma predeterminada, el dispositivo de puerta de enlace del cliente debe abrir los túneles de su conexión Site-to-Site VPN generando tráfico e iniciando el proceso de negociación del intercambio de claves de Internet (IKE). Puede configurar su conexión Site-to-Site VPN para especificar que, en su lugar, AWS debe iniciar el proceso de negociación del IKE. Para obtener más información, consulte AWS Site-to-Site VPN opciones de inicio de túnel.

Si utiliza direcciones IP IPv6 para el túnel exterior, el dispositivo de puerta de enlace del cliente debe admitir el IPv6 direccionamiento y poder establecer IPsec túneles con IPv6 puntos finales.

Puerta de enlace de cliente

Una gateway del cliente es un recurso que se crea en AWS y que representa el dispositivo de la gateway del cliente en la red local. Cuando crea una pasarela para clientes, proporciona información sobre su dispositivo a AWS. Para obtener más información, consulte the section called “Opciones de gateway de cliente”.



Para usar Amazon VPC con una conexión Site-to-Site VPN, usted o su administrador de red también deben configurar el dispositivo o la aplicación de puerta de enlace del cliente en su red remota. Cuando crea la conexión Site-to-Site VPN, le proporcionamos la información de configuración necesaria y, por lo general, el administrador de red realiza esta configuración. Para obtener información sobre los requisitos y la configuración de la gateway de cliente, consulte AWS Site-to-Site VPN dispositivos de puerta de enlace para clientes.

IPv6 pasarela de clientes

Al crear una pasarela de clientes para usarla con el túnel IPv6 exterior IPs, debe especificar una IPv6 dirección en lugar de una IPv4 dirección. Puede crear una pasarela de IPv6 cliente mediante la consola AWS de administración o la AWS CLI.

Para crear una pasarela de IPv6 clientes mediante la AWS CLI, utilice el siguiente comando:

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

La IPv6 dirección debe ser una IPv6 dirección válida y enrutable por Internet para su dispositivo de pasarela de clientes.

IPv6 Conexiones VPN

Site-to-Site Las conexiones VPN VPN admiten las siguientes IPv6 configuraciones:

- IPv4 túnel exterior con paquetes IPv4 internos: la capacidad IPv4 VPN básica compatible con Virtual Private Gateway (VGW), Transit Gateway (TGW) y Cloud WAN.
- IPv4 túnel exterior con paquetes IPv6 internos: permite el IPv6 transporte y las aplicaciones dentro del túnel VPN. Compatible con TGW y Cloud WAN (no compatible con VGW).
- IPv6 túnel exterior con paquetes IPv6 internos: permite la IPv6 migración completa con IPv6 direcciones tanto para el túnel IPs exterior como para el paquete interno. IPs Compatible con TGW y Cloud WAN.
- IPv6 túnel exterior con paquetes IPv4 internos: permite el direccionamiento del túnel IPv6 exterior y, al mismo tiempo, admite IPv4 aplicaciones antiguas dentro del túnel. Compatible con TGW y Cloud WAN.

Para crear una conexión VPN con un túnel IPv6 exterior IPs, debe especificarlo `0utsideIPAddressType=Ipv6` al crear la conexión VPN. AWS configura automáticamente las IPv6 direcciones de los túneles exteriores para el lado de AWS de los túneles de la VPN.

Ejemplo de comando CLI para crear una conexión VPN con un túnel IPv6 exterior IPs y un túnel IPv6 interior IPs:

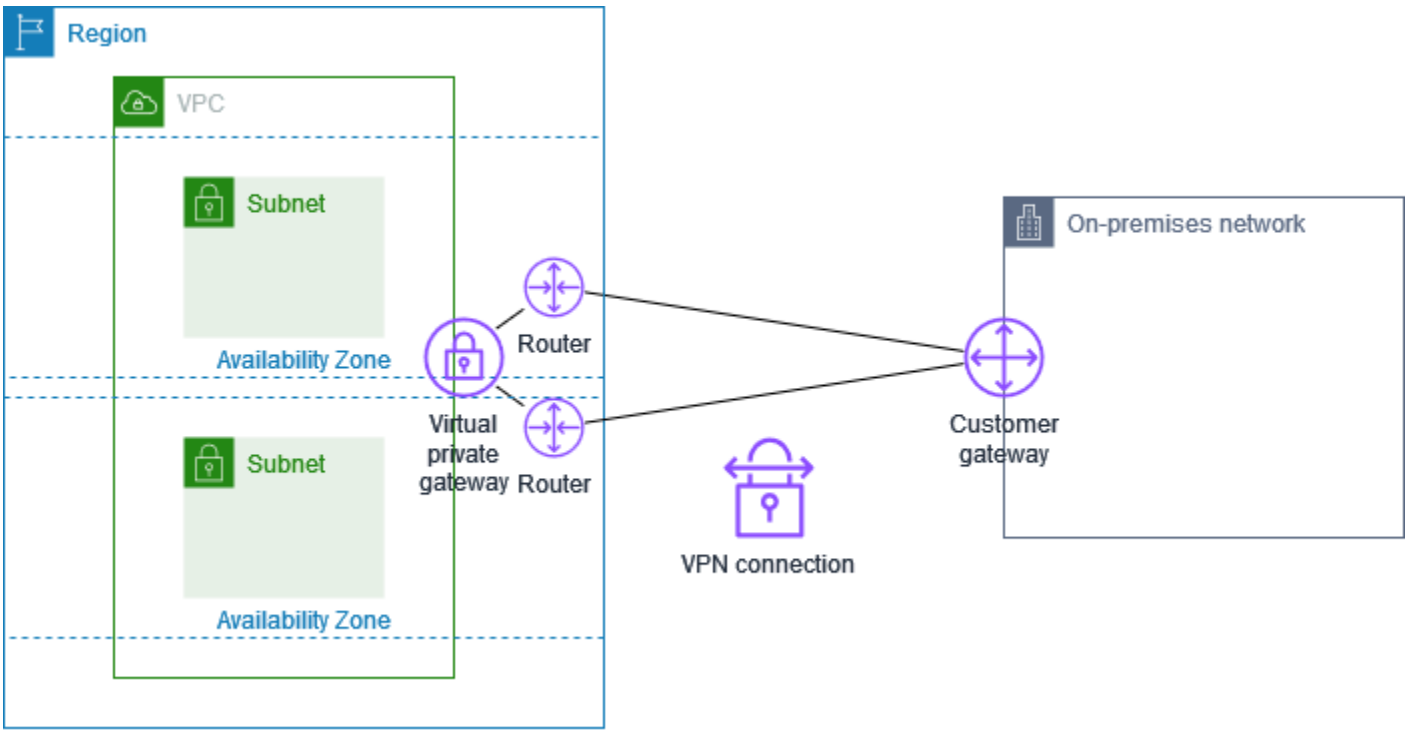
```
aws ec2 create-vpn-connection --type ipsec.1 --transit-gateway-id
 tgw-12312312312312312 --customer-gateway-id cgw-001122334455aabbc --options
 OutsideIPAddressType=Ipv6,TunnelInsideIpVersion=ipv6,TunnelOptions=[{StartupAction=start},
{StartupAction=start}]
```

Puede ver las IPv6 direcciones asignadas a su conexión VPN mediante el comando `describe-vpn-connection` CLI.

Opciones de túnel para su AWS Site-to-Site VPN conexión

Utiliza una conexión Site-to-Site VPN para conectar la red remota a una VPC. Cada conexión Site-to-Site VPN tiene dos túneles, cada uno de los cuales utiliza una dirección IP pública única. Es importante configurar ambos túneles para la redundancia. Cuando un túnel deja de estar disponible (por ejemplo, está inactivo por mantenimiento), el tráfico de la red se enruta automáticamente al túnel disponible para esa conexión Site-to-Site VPN específica.

El siguiente diagrama muestra los dos túneles de la conexión de VPN. Cada túnel termina en una zona de disponibilidad diferente para aumentar la disponibilidad. El tráfico desde la red local AWS utiliza ambos túneles. El tráfico que se dirige AWS a la red local prefiere uno de los túneles, pero puede conmutar automáticamente por error al otro túnel si se produce un fallo lateral. AWS



Al crear una conexión Site-to-Site VPN, se descarga un archivo de configuración específico para el dispositivo de pasarela del cliente que contiene información para configurar el dispositivo, incluida la información para configurar cada túnel. Si lo desea, puede especificar algunas de las opciones del túnel usted mismo al crear la conexión Site-to-Site VPN. De lo contrario, AWS proporciona los valores predeterminados.

> **Note**
>
> Site-to-Site Los puntos finales del túnel VPN evalúan las propuestas de su pasarela de clientes empezando por el valor configurado más bajo de la lista siguiente, independientemente del pedido de propuestas de la pasarela de clientes. Puede usar el `modify-vpn-connection-options` comando para restringir la lista de opciones que aceptarán AWS los puntos finales. Para obtener más información, consulte modify-vpn-connection-optionsAmazon EC2 Command Line Reference.

A continuación, se muestran las opciones de túnel que puede configurar.

> **Note**
>
> Algunas opciones de túnel tienen varios valores predeterminados. Por ejemplo, las versiones de IKE tienen dos valores de opciones de túnel predeterminados: `ikev1` y `ikev2`. Todos los valores predeterminados se asociarán a esa opción de túnel si no elige valores específicos. Haga clic para eliminar cualquier valor predeterminado que no desee asociar a la opción de túnel. Por ejemplo, si solo desea utilizar `ikev1` para la versión de IKE, haga clic en `ikev2` para eliminarla.

Tiempo de espera de detección de pares muertos (DPD)

El número de segundos después del cual se produce un tiempo de espera de DPD. Un tiempo de espera de DPD de 30 segundos significa que el punto final de la VPN considerará que el par está inactivo 30 segundos después del primer intento fallido de mantenimiento con vida. Puede especificar 30 o un valor superior.

Predeterminado: 40

Acción de tiempo de espera de DPD

La acción que se debe realizar después de que se agote el tiempo de espera de detección de pares muertos (DPD). Puede especificar lo siguiente:

- `Clear`: finalice la sesión de IKE cuando se cumpla el tiempo de espera de DPD (detenga el túnel y borre las rutas)
- `None`: no realice ninguna acción cuando se cumpla el tiempo de espera de DPD
- `Restart`: reinicie la sesión de IKE cuando se cumpla el tiempo de espera de DPD

Para obtener más información, consulte AWS Site-to-Site VPN opciones de inicio de túnel.

Valor predeterminado: `Clear`

Opciones de registro de VPN

Con los registros de la Site-to-Site VPN, puede acceder a los detalles sobre el establecimiento del túnel de seguridad IP (IPsec), las negociaciones sobre el intercambio de claves de Internet (IKE) y los mensajes del protocolo de detección de pares muertos (DPD).

Para obtener más información, consulte AWS Site-to-Site VPN registros.

Formatos de registro disponibles: `json`, `text`

Versiones de IKE

Las versiones de IKE permitidas para el túnel de VPN. Puede especificar uno o varios valores predeterminados.

Valores predeterminados: `ikev1`, `ikev2`

Túnel IPv4 interior: CIDR

El rango de IPv4 direcciones internas (internas) del túnel VPN. Pude especificar un bloque de CIDR de tamaño /30 desde el rango `169.254.0.0/16`. El bloque CIDR debe ser único en todas las conexiones Site-to-Site VPN que utilizan la misma puerta de enlace privada virtual.

> **Note**
>
> El bloque de CIDR no tiene por qué ser único en todas las conexiones de una puerta de enlace de tránsito. En caso de no ser único, puede crear un conflicto en la puerta de enlace de cliente. Proceda con cuidado al reutilizar el mismo bloque CIDR en varias conexiones Site-to-Site VPN en una puerta de enlace de tránsito.

Los siguientes bloques de CIDR están reservados y no se pueden utilizar:

- `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`

Predeterminado: un bloque IPv4 CIDR de tamaño /30 del rango. `169.254.0.0/16`

Almacenamiento de claves previamente compartidas

El tipo de almacenamiento de la clave previamente compartida:

- Estándar: la clave previamente compartida se almacena directamente en el Site-to-Site servicio de VPN.

- Secrets Manager: la clave previamente compartida se almacena mediante AWS Secrets Manager. Para obtener más información sobre Secrets Manager, consulteFunciones de seguridad mejoradas con Secrets Manager.

Túnel interior (IPv6 CIDR)

(Solo conexiones IPv6 VPN) El rango de IPv6 direcciones internas (internas) del túnel VPN. Puede especificar un bloque CIDR de tamaño /126 desde el rango local `fd00::/8`. El bloque CIDR debe ser único en todas las conexiones Site-to-Site VPN que utilizan la misma puerta de enlace de tránsito. Si no especificas una IPv6 subred, Amazon selecciona automáticamente una subred /128 de este rango. Independientemente de si especificas la subred o si Amazon la selecciona, Amazon usa la primera IPv6 dirección utilizable de la subred para su lado de la conexión y tu lado usa la segunda dirección utilizable IPv6 .

Predeterminado: un bloque IPv6 CIDR de tamaño /126 del rango local. `fd00::/8`

Tipo de dirección IP de túnel exterior

El tipo de dirección IP de las direcciones IP del túnel exterior (externo). Puede especificar uno de los siguientes valores:

- `PrivateIpv4`: Use una IPv4 dirección privada para implementar conexiones Site-to-Site VPN a través de Direct Connect.
- `PublicIpv4`: (Predeterminado) Usa IPv4 direcciones para el túnel exterior IPs.
- `Ipv6`: Utilice IPv6 direcciones para el túnel exterior IPs. Esta opción solo está disponible para las conexiones VPN en una pasarela de tránsito o en una WAN en la nube.

Si lo seleccionaIpv6, AWS configura automáticamente las IPv6 direcciones de los túneles exteriores para el lado de AWS de los túneles de la VPN. El dispositivo de puerta de enlace del cliente debe admitir el IPv6 direccionamiento y poder establecer IPsec túneles con puntos de IPv6 enlace.

Valor predeterminado: `PublicIpv4`

IPv4 Red local (CIDR)

(Solo para conexión IPv4 VPN) El rango CIDR utilizado durante la negociación de la fase 2 de IKE para el lado del cliente (local) del túnel VPN. Este rango se usa para proponer rutas, pero no impone restricciones de tráfico, ya que AWS se basa exclusivamente en rutas VPNs . No VPNs se admiten los sistemas basados en políticas, ya que limitarían la capacidad de admitir protocolos AWS de enrutamiento dinámico y arquitecturas multirregionales. Esto debería incluir los rangos

de IP de su red local que necesitan comunicarse a través del túnel VPN. Se deben utilizar las configuraciones de la tabla de enrutamiento y los grupos de seguridad adecuados para controlar el flujo de tráfico real. NACLs

Valor predeterminado: 0.0.0.0/0

IPv4 Red remota (CIDR)

(Solo para conexión IPv4 VPN) El rango CIDR utilizado durante la negociación de la fase 2 del IKE para el AWS lado del túnel VPN. Este rango se utiliza para proponer rutas, pero no impone restricciones de tráfico, ya que AWS utiliza exclusivamente las rutas basadas en rutas VPNs. AWS no admite los sistemas basados en políticas VPNs porque carecen de la flexibilidad necesaria para escenarios de enrutamiento complejos y son incompatibles con funciones como las pasarelas de tránsito y las VPN Equal Cost Multi-Path (ECMP). Para VPCs, este suele ser el rango CIDR de su VPC. En el caso de las puertas de enlace de tránsito, esto podría incluir varios rangos de CIDR procedentes de una red conectada VPCs o de otro tipo.

Valor predeterminado: 0.0.0.0/0

Red local IPv6 (CIDR)

(Solo para conexión IPv6 VPN) El rango IPv6 CIDR del lado de la puerta de enlace del cliente (local) que puede comunicarse a través de los túneles de la VPN.

Predeterminado:: :/0

Red remota IPv6 (CIDR)

(Solo para conexión IPv6 VPN) El rango IPv6 CIDR del AWS lado que puede comunicarse a través de los túneles VPN.

Predeterminado:: :/0

Números de grupo Diffie-Hellman (DH) de fase 1

Los números del grupo DH permitidos para el túnel de VPN para las negociaciones IKE de la fase 1. Puede especificar uno o varios valores predeterminados.

Valores predeterminados: 2, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24

Números de grupo Diffie-Hellman (DH) de fase 2

Los números del grupo DH permitidos para el túnel de VPN para las negociaciones IKE de la fase 2. Puede especificar uno o varios valores predeterminados.

Valores predeterminados: 2, 5, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24

Algoritmos de cifrado de la fase 1

Los algoritmos de cifrado permitidos para el túnel VPN para las negociaciones IKE de fase 1. Puede especificar uno o varios valores predeterminados.

Valores predeterminados: AES128,, -GCM-16 AES256, AES128 -GCM-16 AES256

Algoritmos de cifrado de la fase 2

Los algoritmos de cifrado permitidos para el túnel VPN para las negociaciones IKE de fase 2. Puede especificar uno o varios valores predeterminados.

Predeterminados:, -GCM-16, -GCM-16 AES128 AES256 AES128 AES256

Algoritmos de integridad de la fase 1

Los algoritmos de integridad permitidos para el túnel VPN para las negociaciones IKE de fase 1. Puede especificar uno o varios valores predeterminados.

Predeterminados:, -256, -384, -512 SHA1 SHA2 SHA2 SHA2

Algoritmos de integridad de la fase 2

Los algoritmos de integridad permitidos para el túnel VPN para las negociaciones IKE de fase 2. Puede especificar uno o varios valores predeterminados.

Predeterminados:, -256 SHA1, -384, -512 SHA2 SHA2 SHA2

Vida útil de la fase 1

> **Note**
>
> AWS inicie el cambio de claves con los valores de temporización establecidos en los campos Duración de la fase 1 y Duración de la fase 2. Si tales campos de vida útil son diferentes a los valores de protocolo de enlace negociados, esto puede interrumpir la conectividad del túnel.

La duración en segundos de la fase 1 de las negociaciones IKE. Puede especificar un número comprendido entre 900 y 28 800.

Predeterminado: 28 800 (8 horas)

Vida útil de la fase 2

> **Note**
>
> AWS inicie los cambios de clave con los valores de temporización establecidos en los campos Duración de la fase 1 y Duración de la fase 2. Si tales campos de vida útil son diferentes a los valores de protocolo de enlace negociados, esto puede interrumpir la conectividad del túnel.

La duración en segundos de la fase 2 de las negociaciones IKE. Puede especificar un número comprendido entre 900 y 3600. El número que especifique debe ser inferior al número de segundos para la duración de la fase 1.

Predeterminado: 3600 (1 hora)

Clave previamente compartida (PSK)

La clave previamente compartida (PSK) para establecer la asociación de seguridad de intercambio de claves de Internet (IKE) inicial entre la puerta de enlace de destino y la puerta de enlace de cliente.

La PSK debe tener un mínimo de 8 caracteres y un máximo de 64 y no puede comenzar por cero (0). Se permiten caracteres alfanuméricos, puntos (.) y guiones bajos (_).

Predeterminado: una cadena alfanumérica de 32 caracteres.

Difusión de cambio de clave

El porcentaje de la ventana de cambio de clave (determinado por el tiempo del margen de cambio de clave) dentro del cual se selecciona aleatoriamente el tiempo de cambio de clave.

Puede especificar un valor porcentual entre 0 y 100.

Predeterminado: 100

Tiempo de margen de cambio de clave

El margen de tiempo, expresado en segundos, antes de que venza la vida útil de las fases 1 y 2, durante el cual el AWS lado de la conexión VPN realiza un cambio de clave de IKE.

Puede especificar un número comprendido entre 60 y la mitad del valor de la duración de la fase 2.

El tiempo exacto de cambio de clave se selecciona aleatoriamente en función del valor de la difusión del cambio de clave.

Predeterminado: 270 (4,5 minutos)

Tamaño de paquetes del período de reproducción

El número de paquetes de un período de reproducción de IKE.

Puede especificar un valor comprendido entre 64 y 2048.

Predeterminado: 1024

Acción de inicio

La acción que se debe realizar al establecer el túnel para una conexión de VPN. Puede especificar lo siguiente:

- `Start`: AWS inicia la negociación del IKE para abrir el túnel. Solo se admite si la gateway del cliente está configurada con una dirección IP.
- `Add`: su dispositivo de gateway de cliente debe iniciar la negociación de IKE para mostrar el túnel.

Para obtener más información, consulte AWS Site-to-Site VPN opciones de inicio de túnel.

Valor predeterminado: `Add`

Control del ciclo de vida del punto de conexión del túnel

El control del ciclo de vida del punto de conexión del túnel permite controlar el programa de sustituciones de los puntos de conexión.

Para obtener más información, consulte AWS Site-to-Site VPN control del ciclo de vida de los puntos finales.

Valor predeterminado: `Off`

Puede especificar las opciones de túnel al crear una conexión Site-to-Site VPN o puede modificar las opciones de túnel para una conexión VPN existente. Para obtener más información, consulte los temas siguientes:

- Paso 5: Crear una conexión de VPN
- Modificar las opciones AWS Site-to-Site VPN del túnel

AWS Site-to-Site VPN opciones de autenticación de túnel

Puede utilizar claves o certificados previamente compartidos para autenticar los puntos finales de su túnel Site-to-Site VPN.

Claves previamente compartidas

La opción de autenticación predeterminada para los túneles VPN es una clave previamente compartida (PSK). Site-to-Site Al crear un túnel, puede especificar su propio PSK o AWS permitir que se genere uno automáticamente. El PSK se almacena mediante uno de los siguientes métodos:

- Directamente en el servicio Site-to-Site VPN. Para obtener más información, consulte Site-to-Site dispositivos VPN de puerta de enlace para clientes.
- AWS Secrets Manager Para mejorar la seguridad. Para obtener más información sobre el uso de Secrets Manager para almacenar una PSK, consulteFunciones de seguridad mejoradas con Secrets Manager.

A continuación, la cadena PSK se utiliza al configurar el dispositivo de pasarela de clientes.

Certificado privado de AWS Private Certificate Authority

Si no quiere utilizar claves previamente compartidas, puede utilizar un certificado privado de AWS Private Certificate Authority para autenticar la VPN.

Tiene que crear un certificado privado de una entidad emisora de certificados subordinada que use AWS Private Certificate Authority (Autoridad de certificación privada de AWS). Para firmar la CA subordinada de ACM, puede utilizar una CA raíz de ACM o una CA externa. Para obtener información sobre cómo crear un certificado privado, consulte la sección sobre Creación y administración de una CA privada en la Guía del usuario de AWS Private Certificate Authority .

Debe crear un rol vinculado al servicio para generar y usar el certificado para el AWS extremo del túnel Site-to-Site VPN. Para obtener más información, consulte the section called “Roles vinculados a servicios”.

> **Note**
>
> Para facilitar la rotación de certificaciones sin problemas, basta con cualquier certificado que tenga la misma cadena de entidades de certificación que la especificada originalmente en la llamada a la `CreateCustomerGateway` API para establecer una conexión VPN.

Si no especifica la dirección IP de su dispositivo de gateway de cliente, no verificaremos la dirección IP. Esta operación le permite trasladar el dispositivo de gateway de cliente a otra dirección IP sin tener que volver a configurar la conexión de VPN.

Site-to-Site Al crear un certificado de VPN, la VPN verifica la cadena de certificados en el certificado de la pasarela del cliente. Además de las comprobaciones básicas de autenticidad y validez, la Site-to-Site VPN comprueba si las extensiones X.509 están presentes, incluidos el identificador de clave de autoridad, el identificador de clave de asunto y las restricciones básicas.

AWS Site-to-Site VPN opciones de inicio de túnel

De forma predeterminada, el dispositivo de puerta de enlace del cliente debe abrir los túneles de su conexión Site-to-Site VPN generando tráfico e iniciando el proceso de negociación del intercambio de claves de Internet (IKE). Puede configurar sus túneles VPN para especificar si, en su lugar, AWS deben iniciar o reiniciar el proceso de negociación del IKE.

Opciones de iniciación de IKE de túnel de VPN

Las siguientes opciones de iniciación de IKE están disponibles. Puede implementar una o ambas opciones para uno o ambos túneles de su conexión Site-to-Site VPN. Consulte Opciones de túnel de VPN para obtener más información sobre estas y otras opciones de configuración del túnel.

- Acción de inicio: acción que se debe realizar al establecer el túnel de VPN para una conexión de VPN nueva o modificada. De forma predeterminada, el dispositivo de gateway de cliente inicia el proceso de negociación de IKE para mostrar el túnel. Puede AWS especificar que, en su lugar, se inicie el proceso de negociación de IKE.
- Acción de tiempo de espera de DPD: la acción que se debe realizar después de que se cumpla el tiempo de espera de detección de pares muertos (DPD). De forma predeterminada, la sesión de IKE se detiene, el túnel se desactiva y se eliminan las rutas. Puede especificar que AWS debe reiniciarse la sesión de IKE cuando se agote el tiempo de espera de DPD, o puede especificar que no se AWS debe realizar ninguna acción cuando se agote el tiempo de espera de DPD.

Reglas y limitaciones

Se aplican las siguientes reglas y limitaciones:

- Para iniciar la negociación del IKE, AWS necesita la dirección IP pública del dispositivo de puerta de enlace del cliente. Si configuró la autenticación basada en certificados para su conexión VPN y no especificó una dirección IP al crear el recurso de puerta de enlace de cliente AWS, debe crear una nueva puerta de enlace de cliente y especificar la dirección IP. A continuación, modifique la conexión de VPN y especifique la nueva gateway de cliente. Para obtener más información, consulte Cambiar la pasarela del cliente por una AWS Site-to-Site VPN conexión.
- Solo se admite la iniciación mediante IKE (acción de inicio) desde el AWS lado de la conexión VPN. IKEv2
- Si se utiliza la iniciación IKE desde el AWS lado de la conexión VPN, no se incluye una configuración de tiempo de espera. Intentará establecer una conexión continuamente hasta que se establezca una. Además, el AWS lado de la conexión VPN reiniciará la negociación de IKE cuando reciba un mensaje de eliminación de SA desde la pasarela del cliente.
- Si su dispositivo de pasarela de clientes está protegido por un firewall u otro dispositivo que utilice la traducción de direcciones de red (NAT), debe tener una identidad (IDr) configurada. Para obtener más información al respecto IDr, consulte el RFC 7296.

Si no configura la iniciación de IKE desde un AWS lado para su túnel VPN y la conexión VPN pasa por un período de inactividad (normalmente 10 segundos, según la configuración), es posible que el túnel deje de funcionar. Para evitar este problema, utilice una herramienta de monitoreo de red para generar pings keepalive.

Uso de opciones de iniciación de túnel de VPN

Para obtener más información sobre cómo trabajar con las opciones de iniciación de túnel de VPN, consulte los temas siguientes:

- Para crear una nueva conexión de VPN y especificar las opciones de iniciación del túnel de VPN: Paso 5: Crear una conexión de VPN
- Para modificar las opciones de iniciación del túnel de VPN en una conexión de VPN existente: Modificar las opciones AWS Site-to-Site VPN del túnel

AWS Site-to-Site VPN reemplazos de puntos finales de túneles

Su conexión Site-to-Site VPN consta de dos túneles VPN para garantizar la redundancia. A veces, uno o ambos puntos finales del túnel VPN se sustituyen al AWS realizar actualizaciones del túnel o al modificar la conexión VPN. Durante la sustitución de un punto de enlace del túnel, la conectividad a través del túnel podría verse interrumpida mientras se aprovisiona el nuevo punto de enlace.

Temas

Sustituciones de puntos de conexión iniciadas por el cliente

Cuando se modifican los siguientes componentes de una conexión de VPN, se reemplazan uno o ambos puntos de enlace del túnel.

Modificación	Acción de la API	Impacto en el túnel
Modificación de la gateway de destino de la conexión de VPN	ModifyVpnConnection	Los dos túneles dejan de estar disponibles mientras se aprovisionan los nuevos puntos de enlace del túnel.
Cambio de la gateway de cliente de la conexión de VPN	ModifyVpnConnection	Los dos túneles dejan de estar disponibles mientras se aprovisionan los nuevos puntos de enlace del túnel.
Modificación de las opciones de la conexión de VPN	ModifyVpnConnectionOptions	Los dos túneles dejan de estar disponibles mientras se aprovisionan los nuevos puntos de enlace del túnel.
Modificación de las opciones del túnel de VPN	ModifyVpnTunnelOptions	El túnel modificado no está disponible durante la actualiza ción.

Sustituciones de puntos de conexión administrados por AWS

AWS Site-to-Site VPN es un servicio gestionado y actualiza periódicamente los puntos finales de los túneles de la VPN. Estas actualizaciones se producen por una variedad de razones, entre las que se incluyen las siguientes:

- Al aplicar actualizaciones generales, como parches, mejoras de resiliencia y otras mejoras
- Al retirar el hardware subyacente
- Cuando las tareas de monitoreo automatizadas determinan que un punto de enlace del túnel de VPN no está en buen estado

AWS aplica las actualizaciones de los puntos finales del túnel a un túnel de su conexión VPN a la vez. Durante una actualización del punto de conexión del túnel, es posible que la conexión de VPN experimente una breve pérdida de redundancia. Por tanto, es importante configurar los dos túneles de la conexión de VPN para que ofrezcan una alta disponibilidad.

AWS Site-to-Site VPN control del ciclo de vida de los puntos finales

El control del ciclo de vida de los puntos finales del túnel permite controlar el calendario de sustituciones de los puntos finales y puede ayudar a minimizar las interrupciones de conectividad durante las sustituciones AWS gestionadas de los puntos finales del túnel. Con esta función, puede optar por aceptar las actualizaciones AWS gestionadas de los puntos finales del túnel en el momento que mejor se adapte a su empresa. Utilice esta característica si tiene necesidades empresariales a corto plazo o si solo puede admitir un único túnel por conexión VPN.

> **Note**
>
> En raras ocasiones, AWS puede aplicar las actualizaciones críticas a los puntos finales del túnel de forma inmediata, incluso si la función de control del ciclo de vida de los puntos finales del túnel está habilitada.

Temas

- Compruebe si hay actualizaciones de AWS Site-to-Site VPN túnel disponibles
- Acepte una actualización de mantenimiento AWS Site-to-Site VPN del túnel
- Desactive el control del ciclo de vida de los terminales del AWS Site-to-Site VPN túnel

Cómo funciona el control del ciclo de vida del punto de conexión del túnel

Active la característica de control del ciclo de vida del punto de conexión del túnel para túneles individuales dentro de una conexión VPN. Se puede habilitar en el momento de la creación de la VPN o modificando las opciones de túnel para una conexión VPN existente.

Una vez activado el control del ciclo de vida del punto de conexión del túnel, obtendrá una visibilidad adicional de los próximos eventos de mantenimiento del túnel de dos maneras:

- Recibirá AWS Health notificaciones sobre las próximas sustituciones de los puntos finales del túnel.
- El estado del mantenimiento pendiente, junto con las marcas de tiempo del mantenimiento aplicado automáticamente después y el último mantenimiento aplicado, se pueden ver en el comando -status AWS Management Console o mediante el comando get-vpn-tunnel-replacement AWS CLI -status.

Cuando esté disponible el mantenimiento de un punto de conexión de túnel, tendrá la oportunidad de aceptar la actualización en el momento que más le convenga, antes de la marca temporal Mantenimiento automático aplicado después proporcionada.

Si no aplica las actualizaciones antes de la fecha de mantenimiento aplicada automáticamente después, se AWS realizará automáticamente la sustitución del punto final del túnel poco después, como parte del ciclo de actualizaciones de mantenimiento regular.

Active el control AWS Site-to-Site VPN del ciclo de vida de los puntos finales

El control del ciclo de vida del punto de conexión se puede habilitar en una conexión de VPN nueva o existente. Esto se puede hacer usando las teclas AWS Management Console o AWS CLI.

> **Note**
>
> De forma predeterminada, al activar la característica para una conexión VPN existente, se iniciará la sustitución del punto de conexión del túnel al mismo tiempo. Si desea activar la

característica, pero no iniciar inmediatamente la sustitución del punto de conexión del túnel, puede utilizar la opción omitir la sustitución del túnel.

Existing VPN connection

Los siguientes pasos demuestran cómo habilitar el control del ciclo de vida del punto de conexión del túnel en una conexión VPN existente.

Para habilitar el control del ciclo de vida del punto de conexión del túnel con la AWS Management Console

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación de la izquierda, selecciona Conexiones Site-to-Site VPN.
3. Seleccione la conexión adecuada en Conexiones de VPN.
4. Elija Acciones y, a continuación, Modificar opciones de túnel de VPN.
5. Seleccione el túnel específico que desea modificar; para ello, elija la dirección IP fuera del túnel de VPN adecuada.
6. En Control del ciclo de vida del punto de conexión del túnel, seleccione la casilla Habilitar.
7. (Opcional) Seleccione Omitir la sustitución del túnel.
8. Elija Guardar cambios.

Para habilitar el control del ciclo de vida del punto de conexión del túnel con la AWS CLI

Usa el modify-vpn-tunnel-optionscomando para activar el control del ciclo de vida de los puntos finales del túnel.

New VPN connection

Los siguientes pasos demuestran cómo habilitar el control del ciclo de vida del punto de conexión del túnel durante la creación de una nueva conexión de VPN.

Para habilitar el control del ciclo de vida de los puntos finales del túnel durante la creación de una nueva conexión VPN mediante AWS Management Console

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Site-to-Site VPN Connections.

3. Elija Create VPN Connection (Crear conexión VPN).
4. En las secciones de opciones del Túnel 1 y opciones del Túnel 2, en Control del ciclo de vida del punto de conexión del túnel, seleccione Habilitar.
5. Elija Create VPN Connection (Crear conexión de VPN).

Para habilitar el control del ciclo de vida de los puntos finales del túnel durante la creación de una nueva conexión VPN mediante AWS CLI

Usa el create-vpn-connectioncomando para activar el control del ciclo de vida de los puntos finales del túnel.

Compruebe si el control del ciclo de vida de los puntos finales del AWS Site-to-Site VPN túnel está activado

Puede comprobar si el control del ciclo de vida de los puntos finales del túnel está habilitado en un túnel VPN existente mediante la CLI AWS Management Console o la CLI.

- Si el control del ciclo de vida de los puntos de conexión del túnel está desactivado y desea habilitarlo, consulte Habilitación del control del ciclo de vida del punto de conexión del túnel de .
- Si el control del ciclo de vida de los puntos de conexión del túnel está habilitado y desea desactivarlo, consulte Desactivación del control del ciclo de vida del punto de conexión del túnel de .

Para comprobar si el control del ciclo de vida del punto de conexión del túnel está habilitado con la AWS Management Console

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación de la izquierda, selecciona Conexiones Site-to-Site VPN.
3. Seleccione la conexión adecuada en Conexiones de VPN.
4. Seleccione la pestaña Detalles del túnel.
5. En los detalles del túnel, busque Control del ciclo de vida del punto de conexión del túnel, que indicará si la característica está Habilitada o Desactivada.

Para comprobar si el control del ciclo de vida del punto de conexión del túnel está habilitado con la AWS CLI

Utilice el describe-vpn-connectionscomando para verificar si el control del ciclo de vida de los puntos finales del túnel está habilitado.

Compruebe si hay actualizaciones de AWS Site-to-Site VPN túnel disponibles

Tras habilitar la característica de control del ciclo de vida del punto de conexión del túnel, puede consultar si una actualización de mantenimiento está disponible para la conexión de VPN con la AWS Management Console o la CLI. Al comprobar si hay una actualización de túnel Site-to-Site VPN disponible, no se descarga ni despliega automáticamente la actualización. Puede elegir cuándo quiere implementarla. Para conocer los pasos para descargar e implementar una actualización, consulte Aceptar una actualización de mantenimiento.

Para comprobar si hay actualizaciones disponibles, utilice la AWS Management Console

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación de la izquierda, selecciona Conexiones Site-to-Site VPN.
3. Seleccione la conexión adecuada en Conexiones de VPN.
4. Seleccione la pestaña Detalles del túnel.
5. Compruebe la columna Mantenimiento pendiente. El estado será Disponible o Ninguno.

Para comprobar si hay actualizaciones disponibles, utilice el AWS CLI

Utilice el comando get-vpn-tunnel-replacement-status para comprobar si hay actualizaciones disponibles.

Acepte una actualización de mantenimiento AWS Site-to-Site VPN del túnel

Cuando haya una actualización de mantenimiento disponible, puede aceptarla mediante la AWS Management Console o CLI. Puede optar por aceptar la actualización de mantenimiento del túnel Site-to-Site VPN en el momento que más le convenga. Una vez que acepte la actualización de mantenimiento, se implementará.

> **Note**
>
> Si no aceptas la actualización de mantenimiento, la AWS implementará automáticamente durante un ciclo de actualización de mantenimiento normal.

Para aceptar una actualización de mantenimiento disponible mediante el AWS Management Console

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación de la izquierda, selecciona Conexiones Site-to-Site VPN.
3. Seleccione la conexión adecuada en Conexiones de VPN.
4. Elija Acciones y, a continuación, Sustituir túnel de VPN.
5. Seleccione el túnel específico que desea sustituir; para ello, elija la dirección IP fuera del túnel de VPN adecuada.
6. Elija Reemplazar.

Para aceptar una actualización de mantenimiento disponible mediante el AWS CLI

Utilice el replace-vpn-tunnelcomando para aceptar una actualización de mantenimiento disponible.

Desactive el control del ciclo de vida de los terminales del AWS Site-to-Site VPN túnel

Si ya no desea utilizar la función de control del ciclo de vida de los puntos finales del túnel, puede desactivarla con AWS Management Console o con AWS CLI. Cuando desactive esta característica, AWS implementará automáticamente actualizaciones de mantenimiento de forma periódica y es posible que estas actualizaciones se realicen durante el horario laboral. Para evitar el impacto empresarial, le recomendamos encarecidamente que configure los túneles de la conexión de VPN para una disponibilidad alta.

> **Note**
>
> Mientras haya un mantenimiento pendiente disponible, no puede especificar la opción Omitir la sustitución del túnel mientras se desactiva la característica. Siempre puede desactivar la función sin utilizar la opción de sustitución del punto final del túnel, pero AWS implementará automáticamente las actualizaciones de mantenimiento pendientes disponibles al iniciar la sustitución inmediata del punto final del túnel.

Para desactivar el control del ciclo de vida de los puntos finales del túnel mediante el AWS Management Console

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación de la izquierda, selecciona Conexiones Site-to-Site VPN.

3. Seleccione la conexión adecuada en Conexiones de VPN.
4. Elija Acciones y, a continuación, Modificar opciones de túnel de VPN.
5. Seleccione el túnel específico que desea modificar; para ello, elija la dirección IP fuera del túnel de VPN adecuada.
6. Para desactivar el control del ciclo de vida del punto de conexión del túnel, en Control del ciclo de vida del punto de conexión del túnel, desactive la casilla Habilitar.
7. (Opcional) Seleccione Omitir la sustitución del túnel.
8. Elija Guardar cambios.

Para desactivar el control del ciclo de vida de los puntos finales del túnel mediante AWS CLI

Utilice el modify-vpn-tunnel-optionscomando para desactivar el control del ciclo de vida de los puntos finales del túnel.

Opciones de pasarela de clientes para su AWS Site-to-Site VPN conexión

La siguiente tabla describe la información que necesitará para crear un recurso de gateway de cliente en AWS.

Elemento	Descripción
(Opcional) Etiqueta de nombre.	Crea una etiqueta con una clave de "Nombre" y un valor que especifique.
(Solo direccionamiento dinámico) Número de sistema autónomo (ASN) para protocolo de gateway fronteriza (BGP) de la gateway de cliente.	El ASN en el rango comprendido entre 1 y 4 294 967 295 es compatible. Puede utilizar un ASN público existente asignado a su red, con excepción de lo siguiente: • 7224: reservado en todas las regiones • 9059: reservado en la región `eu-west-1` • 10 124: reservado en la región `ap-northeast-1`

Elemento	Descripción
	• 17 943: reservado en la región `ap-southeast-1` Si no tiene ningún ASN público, puede utilizar un ASN privado en el rango comprendido entre 64 512 y 65 534 o 4 200 000 000 y 4 294 967 294. El ASN predeterminado es 64512. Para obtener más información sobre el enrutamiento, consulte AWS Site-to-Site VPN opciones de enrutamiento.
La dirección IP de la interfaz externa del dispositivo de puerta de enlace del cliente.	La dirección IP debe ser estática y puede ser una IPv4 u otra IPv6. Para IPv4 las direcciones: si el dispositivo de puerta de enlace del cliente está detrás de un dispositivo de traducción de direcciones de red (NAT), utilice la dirección IP de su dispositivo NAT. Además, asegúrese de que los paquetes UDP del puerto 500 (y del puerto 4500, si se utiliza el cruce de NAT) puedan pasar entre la red y los puntos AWS Site-to-Site VPN finales. Consulte Reglas de firewall para obtener más información. Para IPv6 las direcciones: la dirección debe ser una dirección válida que se pueda enrutar por Internet IPv6 . IPv6 las direcciones solo se admiten para las conexiones VPN en una puerta de enlace de tránsito o en una WAN en la nube. No se requiere una dirección IP cuando se utiliza un certificado privado de AWS Private Certificate Authority y una VPN pública.

Elemento	Descripción
(Opcional) Certificado privado de una CA subordinada que utiliza AWS Certificate Manager (ACM).	Si quiere utilizar la autenticación basada en certificados, proporcione el ARN de un certifica do privado ACM para usarlo en el dispositivo de gateway de cliente. Al crear una pasarela de cliente, puede configurarla para que utilice certificados AWS Private Certificate Authority privados a fin de autenticar la VPN. Site-to-Site Si elige usar esta opción, crea una autoridad de certificación (CA) privada totalmente AWS alojada para uso interno de su organizac ión. Tanto el certificado de CA raíz como los certificados de CA subordinados los almacena y administra. Autoridad de certificación privada de AWS Antes de crear la pasarela de cliente, debe crear un certificado privado de una CA subordinada utilizando y AWS Private Certifica te Authority, a continuación, especificar el certificado al configurar la pasarela de cliente. Para obtener información sobre la creación de un certificado privado, consulte la sección de creación y administración de una CA privada en la Guía del usuario de AWS Private Certifica te Authority .
(Opcional) Dispositivo.	Un nombre para el dispositivo de puerta de enlace de cliente asociado con esta puerta de enlace de cliente.

IPv6 opciones de puerta de enlace para clientes

Al crear una pasarela de clientes con una IPv6 dirección, tenga en cuenta lo siguiente:

- IPv6 Las pasarelas de cliente solo son compatibles con las conexiones VPN en una pasarela de tránsito o en una WAN en la nube.
- La IPv6 dirección debe ser una dirección válida y enrutable por Internet IPv6 .
- El dispositivo de puerta de enlace para clientes debe admitir el IPv6 direccionamiento y poder establecer IPsec túneles con los puntos finales. IPv6
- Para crear una pasarela de IPv6 clientes mediante la AWS CLI, utilice una IPv6 dirección para el `--ip-address` parámetro:

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

AWS Site-to-Site VPN Conexiones aceleradas

Si lo desea, puede activar la aceleración de su conexión Site-to-Site VPN. Una conexión Site-to-Site VPN acelerada (conexión VPN acelerada) se utiliza AWS Global Accelerator para enrutar el tráfico desde la red local a la ubicación AWS perimetral más cercana al dispositivo de puerta de enlace del cliente. AWS Global Accelerator optimiza la ruta de la red y utiliza la red AWS global libre de congestión para dirigir el tráfico al punto final que proporciona el mejor rendimiento de las aplicaciones (para obtener más información, consulte). AWS Global Accelerator Puede utilizar una conexión de VPN acelerada para evitar las interrupciones en la red que podrían producirse cuando el tráfico se direcciona a través del Internet público.

Cuando usted crea una conexión de VPN acelerada, nosotros creamos y administramos dos aceleradores en su nombre, uno para cada túnel de VPN. No puede ver ni administrar estos aceleradores usted mismo mediante la consola o. AWS Global Accelerator APIs

Para obtener información sobre las AWS regiones que admiten conexiones VPN aceleradas, consulte la Site-to-SiteVPN AWS FAQs acelerada.

Habilitación de la aceleración

De forma predeterminada, al crear una conexión Site-to-Site VPN, la aceleración está deshabilitada. Si lo desea, puede activar la aceleración al crear un nuevo adjunto de Site-to-Site VPN en una

pasarela de tránsito. Para obtener más información y ver los pasos, consulte Crear un AWS Site-to-Site VPN adjunto a una pasarela de transporte.

Las conexiones de VPN aceleradas utilizan un grupo independiente de direcciones IP para las direcciones IP del punto de enlace del túnel. Las direcciones IP de los dos túneles de VPN se seleccionan en dos zonas de red distintas.

Reglas y restricciones

Para utilizar una conexión de VPN acelerada, se aplican las siguientes reglas:

- La aceleración solo se admite para las conexiones Site-to-Site VPN que están conectadas a una pasarela de tránsito. Las gateway privadas virtuales no admiten conexiones de VPN aceleradas.
- No se puede usar una conexión Site-to-Site VPN acelerada con una interfaz virtual AWS Direct Connect pública.
- No puede activar ni desactivar la aceleración de una conexión Site-to-Site VPN existente. En su lugar, puedes crear una nueva conexión Site-to-Site VPN con la aceleración activada o desactivada según sea necesario. A continuación, configure el dispositivo de puerta de enlace del cliente para que utilice la nueva conexión Site-to-Site Site-to-Site VPN y elimine la antigua.
- Se requiere NAT-Traversal (NAT-T) para una conexión de VPN acelerada y está habilitado de forma predeterminada. Si ha descargado un archivo de configuración de la consola de Amazon VPC, compruebe la configuración de NAT-T y ajústela si es necesario.
- La negociación de IKE para los túneles de VPN acelerados se debe iniciar desde el dispositivo de puerta de enlace de cliente. Las dos opciones de túnel que afectan a este comportamiento son `Startup Action` y `DPD Timeout Action`. Para obtener más información, consulte Opciones de túnel de VPN y Opciones de iniciación de túnel de VPN.
- Site-to-Site Es posible que las conexiones VPN que utilizan la autenticación basada en certificados no sean compatibles AWS Global Accelerator, debido a la limitada compatibilidad con la fragmentación de paquetes en Global Accelerator. Para obtener más información, consulte Cómo funciona AWS Global Accelerator. Si necesita una conexión de VPN acelerada que utilice autenticación basada en certificados, el dispositivo de la gateway del cliente debe admitir la fragmentación de IKE. De lo contrario, no habilite su VPN para la aceleración.

AWS Site-to-Site VPN opciones de enrutamiento

AWS recomienda anunciar rutas BGP específicas para influir en las decisiones de enrutamiento en la pasarela privada virtual. Compruebe la documentación de su proveedor acerca de los comandos específicos de su dispositivo.

Al crear varias conexiones de VPN, la gateway privada virtual envía el tráfico de red a la conexión de VPN apropiada utilizando las rutas asignadas estáticamente o anuncios de ruta de BGP, La ruta depende de cómo se haya configurado la conexión de VPN. Las rutas asignadas estáticamente son preferibles frente a las rutas anunciadas de BGP en los casos en los que existen rutas idénticas en la gateway privada virtual. Si selecciona la opción de utilizar el anuncio de BGP, no podrá especificar rutas estáticas.

Para obtener más información sobre la prioridad de una ruta, consulte Tablas de enrutamiento y prioridad de rutas.

Al crear una conexión Site-to-Site VPN, debe hacer lo siguiente:

- Especifique el tipo de direccionamiento que va a usar (estático o dinámico)
- Actualice la tabla de enrutamiento de la subred

No hay ninguna cuota en el número de rutas que puede agregar a una tabla de enrutamiento. Para obtener más información, consulte la sección Tablas de ruteo del artículo Cuotas de Amazon VPC en la Guía del usuario de Amazon VPC.

Temas

Enrutamiento estático y dinámico en AWS Site-to-Site VPN

El tipo de enrutamiento seleccionado puede depender del fabricante y el modelo de su dispositivo de gateway de cliente. Si el dispositivo de puerta de enlace de su cliente es compatible con el protocolo Border Gateway (BGP), especifique el enrutamiento dinámico al configurar la conexión Site-to-Site VPN. Si el dispositivo de gateway de cliente no admite BGP, especifique un enrutamiento estático.

Si utilizas un dispositivo que admite publicidad BGP, no especificas rutas estáticas a la conexión Site-to-Site VPN porque el dispositivo usa BGP para anunciar sus rutas a la puerta de enlace privada virtual. Si utiliza un dispositivo que no admite publicidad BGP, debe seleccionar el enrutamiento estático y escribir las rutas (prefijos IP) de su red que deben comunicarse a la gateway privada virtual.

Se recomienda utilizar dispositivos que admitan BGP, siempre que estén disponibles, ya que el protocolo BGP ofrece comprobaciones de detección de conexión que pueden ayudar en la conmutación por error al segundo túnel de VPN en caso de error en el primero. Los dispositivos que no admiten BGP también pueden realizar comprobaciones de estado para ayudar en la conmutación por error al segundo túnel siempre que sea necesario.

Debe configurar el dispositivo de puerta de enlace del cliente para que dirija el tráfico de su red local a la Site-to-Site conexión VPN. La configuración depende del fabricante y el modelo del dispositivo. Para obtener más información, consulte AWS Site-to-Site VPN dispositivos de puerta de enlace para clientes.

Tablas de enrutamiento y prioridad de rutas de AWS Site-to-Site VPN

Las tablas de enrutamiento determinan dónde se dirige el tráfico de red de la VPC. En la tabla de enrutamiento de la VPC, tiene que agregar una ruta para su red remota y especificar la gateway privada virtual como destino. Esto permite que el tráfico desde su VPC que está dirigido a su red remota se enrute a través de la gateway privada virtual y a través de uno de los túneles de VPN. Puede habilitar la propagación de rutas para que su tabla de ruteo propague automáticamente las rutas de red a la tabla.

Para determinar cómo dirigir tráfico, se utiliza la ruta más específica de su tabla de ruteo que coincida con el tráfico en cuestión (coincidencia del prefijo más largo). Si la tabla de enrutamiento tiene rutas superpuestas o coincidentes, se aplican las siguientes reglas:

- Si las rutas propagadas desde una conexión Site-to-Site VPN o una AWS Direct Connect conexión se superponen con la ruta local de su VPC, la ruta local es la más preferida, incluso si las rutas propagadas son más específicas.
- Si las rutas propagadas desde una conexión Site-to-Site VPN o una AWS Direct Connect conexión tienen el mismo bloque CIDR de destino que otras rutas estáticas existentes (no se puede aplicar la coincidencia de prefijo más larga), priorizamos las rutas estáticas cuyos destinos son una puerta de enlace de Internet, una puerta de enlace privada virtual, una interfaz de red, un ID de instancia, una conexión de emparejamiento de VPC, una puerta de enlace de NAT, una puerta de enlace de tránsito o un punto final de VPC de puerta de enlace.

Por ejemplo, la siguiente tabla de enrutamiento tiene una ruta estática a una gateway de Internet y una ruta propagada a una gateway privada virtual. Ambas rutas tienen el destino `172.31.0.0/24`. En este caso, todo el tráfico con destino `172.31.0.0/24` se dirige a la gateway de Internet, ya que se trata de una ruta estática con prioridad sobre la ruta propagada.

Destino	Objetivo
10.0.0.0/16	Local
172.31.0.0/24	vgw-11223344556677889 (propagada)
172.31.0.0/24	igw-12345678901234567 (estática)

Solo los prefijos IP que la gateway privada virtual conozca, ya sea mediante anuncios de BGP o por introducción de una ruta estática, podrán recibir tráfico de su VPC. La gateway privada virtual no direcciona el tráfico cuyo destino no sea el mencionado en los anuncios de BGP recibidos, las entradas de ruta estática o los CIDR de VPC asociados. Las puertas de enlace privadas virtuales no admiten tráfico. IPv6

Cuando una gateway privada virtual recibe información de direccionamiento, usa la selección de rutas para determinar cómo debe dirigir el tráfico de las rutas. Se aplica la coincidencia de prefijos más larga si todos los puntos de conexión están en buen estado. El estado de un punto de conexión de túnel tiene prioridad sobre otros atributos de enrutamiento. Esta prioridad se aplica a las pasarelas privadas virtuales y a VPNs las pasarelas de tránsito. Si los prefijos son los mismos, la gateway privada virtual da prioridad a las rutas de la siguiente manera, desde la más preferida a la menos preferida:

- Rutas propagadas por BGP desde una conexión AWS Direct Connect

  Las rutas de Blackhole no se propagan a la pasarela de un cliente de Site-to-Site VPN a través de BGP.
- Rutas estáticas añadidas manualmente para una conexión VPN Site-to-Site
- Rutas propagadas por BGP desde una conexión VPN Site-to-Site
- Para los prefijos coincidentes en los que cada conexión Site-to-Site VPN usa BGP, se compara la RUTA AS y se prefiere el prefijo con la RUTA AS más corta.

> **Note**
>
> AWS recomienda encarecidamente utilizar dispositivos de puerta de enlace para clientes que admitan el enrutamiento asimétrico.
> Para los dispositivos de puerta de enlace de clientes que admiten enrutamiento asimétrico, no recomiendamos usar la ruta AS PATH prepending para asegurar que ambos túneles tengan la misma ruta AS PATH. Esto ayuda a garantizar que el multi-exit discriminator valor (MED) que establecemos en un túnel durante las actualizaciones de puntos de enlace del túnel VPN se utilice para determinar la prioridad del túnel.
> En el caso de los dispositivos de puerta de enlace de cliente que no admiten enrutamiento asimétrico, puede utilizar AS PATH antepuesto y la preferencia local para dar prioridad a un túnel sobre el otro. Sin embargo, cuando la ruta de salida cambia, esto puede provocar una caída del tráfico.

- Cuando los AS PATHs tienen la misma longitud y si el primer AS del AS_SEQUENCE es el mismo en varias rutas, multi-exit discriminators (MEDs) se comparan. Se prefiere la ruta con el valor de MED más bajo.

La prioridad de ruta se ve afectada durante las actualizaciones del punto de enlace del túnel de la VPN.

En una conexión Site-to-Site VPN, AWS selecciona uno de los dos túneles redundantes como ruta de salida principal. Esta selección puede cambiar en algún momento, por lo que le recomendamos que configure ambos túneles para una alta disponibilidad y que permita el enrutamiento asimétrico. El estado de un punto de conexión de túnel tiene prioridad sobre otros atributos de enrutamiento. Esta prioridad se aplica a las pasarelas privadas virtuales y a VPNs las pasarelas de tránsito.

En el caso de una puerta de enlace privada virtual, se seleccionará un túnel que atraviese todas las conexiones Site-to-Site VPN de la puerta de enlace. Para usar más de un túnel, le recomendamos que explore la opción de rutas múltiples de igual costo (ECMP), que es compatible con las conexiones Site-to-Site VPN en una puerta de enlace de tránsito. Para obtener más información, consulte Gateways de tránsito en Gateways de tránsito de Amazon VPC. El ECMP no es compatible con las conexiones Site-to-Site VPN en una puerta de enlace privada virtual.

En el Site-to-Site caso de las conexiones VPN que utilizan BGP, el túnel principal se puede identificar mediante el multi-exit discriminator el valor (MED). Recomendamos anunciar rutas ASN más específicas para influir en las decisiones de enrutamiento.

En el Site-to-Site caso de las conexiones VPN que utilizan enrutamiento estático, el túnel principal se puede identificar mediante estadísticas o métricas de tráfico.

Enrutamiento durante las actualizaciones de punto de enlace del túnel de VPN

Una conexión Site-to-Site VPN consta de dos túneles VPN entre un dispositivo de puerta de enlace del cliente y una puerta de enlace privada virtual o una puerta de enlace de tránsito. Recomendamos configurar ambos túneles para la redundancia. De vez en cuando, AWS también realiza un mantenimiento rutinario de la conexión VPN, lo que podría deshabilitar brevemente uno de los dos túneles de la conexión VPN. Para obtener más información, consulte Notificaciones de sustitución de puntos de enlace de un túnel.

Cuando realizamos actualizaciones en un túnel de VPN, establecemos un valor más bajo de multi-exit discriminator (MED) saliente en el otro túnel. Si ha configurado su dispositivo de gateway de cliente para que utilice ambos túneles, la conexión de VPN utilizará el otro túnel (activo) durante el proceso de actualización del punto de enlace del túnel.

> **Note**
>
> - Para asegurarse de que se prefiere el túnel activo con el MED inferior, asegúrese de que su dispositivo de gateway de cliente utilice los mismos valores de peso y preferencia local para ambos túneles (el peso y la preferencia local tienen mayor prioridad que el MED).

IPv4 y IPv6 tráfico en AWS Site-to-Site VPN

Su conexión Site-to-Site VPN en una puerta de enlace de tránsito puede admitir IPv4 tráfico o IPv6 tráfico dentro de los túneles VPN. De forma predeterminada, una conexión Site-to-Site VPN admite el IPv4 tráfico dentro de los túneles VPN. Puede configurar una nueva conexión Site-to-Site VPN para admitir el IPv6 tráfico dentro de los túneles VPN. A continuación, si la VPC y la red local están configuradas para el IPv6 direccionamiento, puede enviar IPv6 tráfico a través de la conexión VPN.

Si habilitas IPv6 los túneles VPN para tu conexión Site-to-Site VPN, cada túnel tiene dos bloques CIDR. Uno es un bloque IPv4 CIDR de tamaño /30 y el otro es un bloque CIDR de tamaño IPv6 /126.

IPv4 y soporte IPv6

Site-to-Site Las conexiones VPN VPN admiten las siguientes configuraciones de IP:

- IPv4 túnel exterior con paquetes IPv4 internos: la capacidad IPv4 VPN básica compatible con las puertas de enlace privadas virtuales, las puertas de enlace de tránsito y la WAN en la nube.
- IPv4 túnel exterior con paquetes IPv6 internos: permite el IPv6 transporte y las aplicaciones dentro del túnel VPN. Compatible con pasarelas de tránsito y WAN en la nube. Esto no es compatible con las puertas de enlace privadas virtuales.
- IPv6 túnel exterior con paquetes IPv6 internos: permite la IPv6 migración completa con IPv6 direcciones tanto para el túnel IPs exterior como para el paquete IPs interno. Compatible tanto con las pasarelas de tránsito como con la WAN en la nube.
- IPv6 túnel exterior con paquetes IPv4 internos: permite el direccionamiento del túnel IPv6 exterior y, al mismo tiempo, admite IPv4 aplicaciones antiguas dentro del túnel. Compatible tanto con las pasarelas de tránsito como con la WAN en la nube.

Se aplican las siguientes reglas:

- IPv6 las direcciones del túnel exterior solo IPs se admiten en las conexiones Site-to-Site VPN que terminan en una puerta de enlace de tránsito o en una WAN de nube. Site-to-Site Las conexiones VPN en una puerta de enlace privada virtual no admiten IPv6 el túnel IPs exterior.
- Si se utiliza IPv6 como túnel exterior IPs, debe asignar IPv6 direcciones tanto en el AWS lado de la conexión VPN como en la puerta de enlace del cliente para ambos túneles VPN.
- No puedes habilitar la IPv6 compatibilidad con una conexión Site-to-Site VPN existente. Debe eliminar la conexión existente y crear una nueva.
- Una conexión Site-to-Site VPN no puede admitir ambos IPv4 tipos de IPv6 tráfico simultáneamente. Los paquetes encapsulados internos pueden ser uno IPv6 o ambos IPv4, pero no ambos. Necesita conexiones Site-to-Site VPN independientes para el transporte IPv4 y IPv6 los paquetes.
- Las direcciones IP privadas VPNs no admiten IPv6 direcciones para el túnel exterior IPs. Utilizan direcciones RFC 1918 o CGNAT. Para obtener más información acerca de la RFC 1918, consulte la RFC 1918: Asignación de direcciones para Internet privadas.
- IPv6 VPNs admiten los mismos límites de rendimiento (Gbps y PPS), MTU y ruta que. IPv4 VPNs
- El IPSec cifrado y el intercambio de claves funcionan de la misma manera para ambos. IPv4 IPv6 VPNs

Para obtener más información sobre cómo crear una conexión VPN IPv6 compatible, consulte Crear una conexión VPN en Comenzar con Site-to-Site VPN.

Comience con AWS Site-to-Site VPN

Utilice el siguiente procedimiento para configurar una AWS Site-to-Site VPN conexión. Durante la creación, especificará una puerta de enlace privada virtual, una puerta de enlace de tránsito o “No asociada” como tipo de puerta de enlace de destino. Si especificas «No asociada», puedes elegir el tipo de puerta de enlace de destino más adelante o puedes usarla como un adjunto de VPN para AWS Cloud WAN. Este tutorial le ayuda a crear una conexión de VPN mediante una puerta de enlace privada virtual. Supone que dispone de una VPC existente con una o varias subredes.

Para establecer una conexión de VPN mediante una puerta de enlace privada virtual, siga estos pasos:

Tareas

- Requisitos previos
- Paso 1: Crear una puerta de enlace de cliente
- Paso 2: Crear una puerta de enlace de destino
- Paso 3: Configuración del enrutamiento
- Paso 4: Actualizar el grupo de seguridad
- Paso 5: Crear una conexión de VPN
- Paso 6: Descargar el archivo de configuración
- Paso 7: Configurar el dispositivo de puerta de enlace de cliente

Tareas relacionadas

- Para crear una conexión VPN para AWS Cloud WAN, consultaCreación de un archivo adjunto de VPN de WAN en la nube.
- Para crear una conexión de VPN en una puerta de enlace de tránsito, consulte Creación de una asociación de VPN de puerta de enlace de tránsito.

Requisitos previos

Necesita la siguiente información para establecer y configurar los componentes de una conexión de VPN.

Elemento	Información
Dispositivo de gateway de cliente	El dispositivo físico o de software del lado de la conexión de VPN. Necesita el proveedor (por ejemplo, Cisco Systems), la plataforma (por ejemplo, ISR Series Routers) y la versión de software (por ejemplo, IOS 12.4).
Puerta de enlace de cliente	Para crear el recurso de pasarela de clientes en AWS, necesita la siguiente información: • La dirección IP direccionable de Internet para la interfaz externa del dispositivo • El tipo de direccionamiento: estático o dinámico • Para el direccionamiento dinámico: el número de sistema autónomo (ASN) para protocolo de gateway fronteriza (BGP) • (Opcional) Certificado privado de AWS Private Certificate Authority para autenticar su VPN Para obtener más información, consulte Opciones de gateway de cliente.
(Opcional) El ASN del AWS lado de la sesión de BGP	Debe especificarse al crear una gateway privada virtual o una gateway de tránsito. Si no especifica un valor, se aplica el ASN predeterminado. Para obtener más información, consulte Gateway privada virtual.
conexión de VPN	Para crear una conexión de VPN, necesita la siguiente información: • Para el enrutamiento estático, los prefijos IP para la red privada.

Elemento	Información
	• (Opcional) Opciones de túnel para cada túnel VPN. Para obtener más información, consulte Opciones de túnel para su AWS Site-to-Site VPN conexión.

Paso 1: Crear una puerta de enlace de cliente

Una pasarela de cliente proporciona información AWS sobre su dispositivo o aplicación de software de pasarela de cliente. Para obtener más información, consulte Puerta de enlace de cliente.

Si planea usar un certificado privado para autenticar su VPN, cree un certificado privado de una CA subordinada utilizando. AWS Private Certificate Authority Para obtener información sobre la creación de un certificado privado, consulte la sección de creación y administración de una CA privada en la Guía del usuario de AWS Private Certificate Authority .

> **Note**
>
> Tiene que especificar una dirección IP o el nombre de recurso de Amazon del certificado privado.

Para crear una gateway de cliente con la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Puertas de enlace de cliente.
3. Elija Crear puerta de enlace de cliente.
4. (Opcional) En Name tag (Etiqueta de nombre), ingrese un nombre para la puerta de enlace de cliente. Esta acción creará una etiqueta con una clave de `Name` y el valor que especifique.
5. En BGP ASN, ingrese un número de sistema autónomo (ASN) para protocolo de puerta de enlace fronteriza (BGP) de la puerta de enlace de cliente.
6. Para el tipo de dirección IP, seleccione una de las siguientes opciones:
   - IPv4- (Predeterminado) Especifique una IPv4 dirección para su dispositivo de pasarela de clientes.

- IPv6- Especifique una IPv6 dirección para su dispositivo de pasarela de clientes. Esta opción es necesaria al crear una conexión VPN con el túnel IPv6 exterior IPs.

7. En el caso de la dirección IP, introduzca la dirección IP estática y enrutable por Internet de su dispositivo de pasarela de cliente. Si el dispositivo de la puerta de enlace de cliente se encuentra detrás de un dispositivo NAT habilitado para NAT-T, utilice la dirección IP pública del dispositivo NAT.
8. (Opcional) Si desea utilizar un certificado privado, para Certificate ARN (ARN de certificado), elija el nombre de recurso de Amazon del certificado privado.
9. (Opcional) En Dispositivo, introduzca un nombre para el dispositivo de puerta de enlace de cliente asociado a esta puerta de enlace de cliente.
10. Elija Crear puerta de enlace de cliente.

Para crear una gateway de cliente mediante la línea de comando o API

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

  Ejemplo de creación de una pasarela de IPv6 clientes:

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

- New-EC2CustomerGateway (AWS Tools for Windows PowerShell)

Paso 2: Crear una puerta de enlace de destino

Para establecer una conexión VPN entre la VPC y la red local, debe crear una puerta de enlace de destino en el AWS lateral de la conexión. La gateway de destino puede ser una gateway privada virtual o una gateway de tránsito.

Creación de una gateway privada virtual

Al crear una puerta de enlace privada virtual, puede especificar un número de sistema autónomo (ASN) privado personalizado en el lado de Amazon de la puerta de enlace o usar el ASN predeterminado de Amazon. Este ASN tiene que ser distinto del ASN especificado para la puerta de enlace de cliente.

Después de crear una puerta de enlace privada virtual, debe asociarla a la VPC.

Para crear una puerta de enlace privada virtual y adjuntarla a la VPC.

1. En el panel de navegación, elija Puertas de enlace privadas virtuales.
2. Elija Create virtual private gateway (Crear puerta de enlace privada virtual).
3. (Opcional) En Etiqueta de nombre, introduzca un nombre para su puerta de enlace privada virtual. Esta acción creará una etiqueta con una clave de `Name` y el valor que especifique.
4. En Número de Sistema Autónomo (ASN), mantenga la selección predeterminada, ASN predeterminado de Amazon, para utilizar el ASN predeterminado de Amazon. De lo contrario, elija Custom ASN (ASN personalizado) y escriba un valor. Para un ASN de 16 bits ASN, el valor debe estar dentro del rango de 64 512 a 65 534. Para un ASN de 32 bits ASN, el valor debe estar dentro del rango de 4 200 000 000 a 4 294 967 294.
5. Elija Create virtual private gateway (Crear puerta de enlace privada virtual).
6. Seleccione la puerta de enlace privada virtual que ha creado y, a continuación, elija Actions (Acciones), Attach to VPC (Adjuntar a VPC).
7. VPCsEn Disponible, elija su VPC y, a continuación, elija Adjuntar a la VPC.

Para crear una puerta de enlace privada virtual mediante la línea de comando o API

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

Para asociar una puerta de enlace privada virtual a una VPC mediante la línea de comando o API

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

Crear una puerta de enlace de tránsito

Para obtener más información acerca de cómo crear una gateway de tránsito, consulte Gateways de tránsito en Gateways de tránsito de Amazon VPC.

Paso 3: Configuración del enrutamiento

Para permitir que las instancias de su VPC lleguen a la puerta de enlace de cliente, debe configurar la tabla de enrutamiento para incluir las rutas que utiliza la conexión de VPN y dirigirlas a la puerta de enlace privada virtual o a la puerta de enlace de tránsito.

(Gateway privada virtual) Habilitar la propagación de rutas en la tabla de enrutamiento

Puede activar la propagación de rutas en su tabla de rutas para propagar automáticamente las rutas Site-to-Site VPN.

Para el direccionamiento estático, los prefijos de IP estática que especifique en la configuración de su VPN se propagarán a la tabla de ruteo cuando el estado de la conexión de VPN sea UP. Del mismo modo, para el direccionamiento dinámico, las rutas anunciadas mediante GBP de su gateway de cliente se propagarán a la tabla de ruteo cuando el estado de la conexión de VPN sea UP.

> **Note**
>
> Si la conexión se interrumpe pero la conexión de VPN permanece ACTIVA, las rutas propagadas que se encuentren en la tabla de enrutamiento no se eliminarán automáticamente. Téngalo en cuenta si, por ejemplo, desea que el tráfico se conmute por error a una ruta estática. En dicho caso, es posible que tenga que deshabilitar la propagación de rutas para eliminar las rutas propagadas.

Para habilitar la propagación de rutas utilizando la consola

1. En el panel de navegación, elija Tablas de enrutamiento.
2. Seleccione la tabla de enrutamiento asociada a la subred.
3. En la pestaña Propagación de rutas, elija Editar propagación de rutas. Seleccione la puerta de enlace privada virtual que creó en el procedimiento anterior y, a continuación, elija Guardar.

> **Note**
>
> Si no activa la propagación de rutas, deberá introducir manualmente las rutas estáticas que utiliza su conexión de VPN. Para ello, seleccione su tabla de ruteo, elija Routes, Edit.

En Destino, agrega la ruta estática que usa tu conexión Site-to-Site VPN. Para Target, seleccione el ID de gateway privada virtual y elija Save.

Para deshabilitar la propagación de rutas utilizando la consola

1. En el panel de navegación, elija Tablas de enrutamiento.
2. Seleccione la tabla de enrutamiento asociada a la subred.
3. En la pestaña Propagación de rutas, elija Editar propagación de rutas. Desactive la casilla Propagar correspondiente a la puerta de enlace privada virtual.
4. Seleccione Save.

Para habilitar la propagación de rutas mediante la línea de comando o un API

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

Para deshabilitar la propagación de rutas mediante la línea de comando o un API

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

(Gateway de tránsito) Agregar una ruta a la tabla de enrutamiento

Si ha habilitado la propagación de la tabla de enrutamiento para la gateway de tránsito, las rutas de los datos adjuntos de VPN se propagarán a la tabla de rutas de la gateway de tránsito. Para obtener más información, consulte Direccionamiento en Gateways de tránsito de Amazon VPC.

Si asocia una VPC a la gateway de tránsito y desea habilitar recursos de la VPC para llegar a la gateway de cliente, tiene que agregar una ruta a la tabla de enrutamiento de subred para apuntar a la gateway de tránsito.

Para añadir una ruta a una tabla de ruteo de VPC

1. En el panel de navegación, elija Tablas de enrutamiento.
2. Elija la tabla de enrutamiento asociada a su VPC.
3. En la pestaña Rutas, elija Editar rutas.
4. Seleccione Añadir ruta.
5. En Destino, introduzca el intervalo de direcciones IP de destino. En Target (Destino), elija la gateway de tránsito.
6. Seleccione Save changes (Guardar cambios).

Paso 4: Actualizar el grupo de seguridad

Para permitir el acceso a instancias en su VPC desde su red, debe actualizar las reglas del grupo de seguridad para habilitar acceso SSH, RDP e ICMP entrante.

Para agregar reglas a su grupo de seguridad con el fin de permitir el acceso

1. En el panel de navegación, selecciona Grupos de seguridad.
2. Seleccione el grupo de seguridad de las instancias de la VPC al que desea permitir el acceso.
3. En la pestaña Reglas de entrada, seleccione Editar reglas de entrada.
4. Agregue reglas que permitan el acceso SSH, RDP e ICMP entrante desde su red y, a continuación, elija Guardar reglas. Para obtener más información, consulte Trabajar con reglas de grupos de seguridad en la Guía del usuario de Amazon VPC.

Paso 5: Crear una conexión de VPN

Cree la conexión de VPN mediante la puerta de enlace de cliente en combinación con la puerta de enlace privada virtual o la puerta de enlace de tránsito que creó anteriormente.

Para crear una conexión de VPN

1. En el panel de navegación, selecciona Conexiones Site-to-Site VPN.
2. Elija Create VPN Connection (Crear conexión VPN).
3. (Opcional) En Etiqueta de nombre, escriba el nombre de la conexión de VPN. Esta acción creará una etiqueta con una clave de `Name` y el valor que especifique.

4. En Target gateway type (Tipo de puerta de enlace de destino), elija Virtual private gateway (Puerta de enlace privada virtual) o Transit Gateway (Puerta de enlace de tránsito). A continuación, elija la gateway privada virtual o la gateway de tránsito que ha creado anteriormente.
5. En Puerta de enlace de cliente, seleccione Existente y, a continuación, elija la puerta de enlace de cliente que creó anteriormente en ID de puerta de enlace de cliente.
6. Seleccione una de las opciones de enrutamiento en función de si el dispositivo de puerta de enlace de su cliente es compatible con el protocolo Border Gateway (BGP):

   - Si el dispositivo de gateway de cliente da soporte a BGP, elija Dynamic (requires BGP) (Dinámico [requiere BGP]).
   - Si el dispositivo de gateway de cliente no da soporte a BGP, elija Static (Estático). En Static IP Prefixes (Prefijos de IP estática), especifique cada prefijo de IP para la red privada de su conexión de VPN.
7. Elija el tipo de almacenamiento de claves previamente compartidas:

   - Estándar: la clave previamente compartida se almacena directamente en el Site-to-Site servicio de VPN.
   - Secrets Manager: la clave previamente compartida se almacena mediante AWS Secrets Manager. Para obtener más información sobre Secrets Manager, consulteFunciones de seguridad mejoradas con Secrets Manager.
8. Si el tipo de puerta de enlace de destino es una puerta de enlace de tránsito, en la versión Tunnel inside IP, especifique si los túneles VPN admiten IPv4 o no el IPv6 tráfico. IPv6 el tráfico solo es compatible con las conexiones VPN en una puerta de enlace de tránsito.
9. Si especificó IPv4la versión Túnel dentro de IP, si lo desea, puede especificar los rangos de IPv4 CIDR para la puerta de enlace del cliente y AWS los lados que pueden comunicarse a través de los túneles VPN. El valor predeterminado es `0.0.0.0/0`.

   Si especificó IPv6la versión Túnel dentro de IP, puede especificar opcionalmente los rangos de IPv6 CIDR para la puerta de enlace del cliente y AWS los lados que pueden comunicarse a través de los túneles VPN. El valor predeterminado para ambos rangos es `::/0`.
10. Para el tipo de dirección IP externa, seleccione una de las siguientes opciones:

    - PublicIpv4: (predeterminado) Usa IPv4 direcciones para el túnel exterior IPs.
    - IPv6- Usa IPv6 direcciones para el túnel exterior IPs. Esta opción solo está disponible para las conexiones VPN en una pasarela de tránsito o en una WAN en la nube.

11. (Opcional) En Opciones de túnel, puede especificar la siguiente información para cada túnel:
    - Un bloque IPv4 CIDR de tamaño /30 del `169.254.0.0/16` rango de las direcciones del túnel IPv4 interior.
    - Si especificó IPv6para la versión Tunnel inside IP, un bloque IPv6 CIDR /126 del `fd00::/8` rango para las direcciones del túnel interno. IPv6
    - La clave previamente compartida de IKE (PSK). Se admiten las siguientes versiones: IKEv1 o. IKEv2
    - Para editar las opciones avanzadas del túnel, seleccione Editar opciones de túnel. Para obtener más información, consulte Opciones de túnel de VPN.
12. Elija Create VPN Connection (Crear conexión VPN). Es posible que la conexión de VPN tarde unos minutos en crearse.

Para crear una conexión de VPN mediante la línea de comandos o la API

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

  Ejemplo de creación de una conexión VPN con un túnel IPv6 exterior IPs y un túnel IPv6 interior IPs:

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

  Ejemplo de creación de una conexión VPN con un túnel IPv6 exterior IPs y un túnel IPv4 interior IPs:

```
aws ec2 create-vpn-connection --type ipsec.1 --transit-gateway-id
 tgw-12312312312312312 --customer-gateway-id cgw-001122334455aabbc --options
 OutsideIPAddressType=IPv6,TunnelInsideIpVersion=ipv4,TunnelOptions=[{StartupAction=start},
{StartupAction=start}]
```

- New-EC2VpnConnection (AWS Tools for Windows PowerShell)

Paso 6: Descargar el archivo de configuración

Después de crear la conexión de VPN, podrá descargar un archivo de configuración de muestra que podrá utilizar para configurar el dispositivo de puerta de enlace de cliente.

> **Important**
>
> El archivo de configuración es solo un ejemplo y es posible que no coincida con la configuración de conexión de VPN prevista en su totalidad. Especifica los requisitos mínimos para una conexión VPN de AES128 SHA1, y Diffie-Hellman del grupo 2 en la mayoría de AWS las regiones, y de AES128 SHA2, y Diffie-Hellman del grupo 14 en las regiones. AWS GovCloud También especifica claves previamente compartidas para la autenticación. Debe modificar el archivo de configuración de ejemplo para aprovechar los algoritmos de seguridad, los grupos de Diffie-Hellman, los certificados privados y el tráfico adicionales. IPv6 Hemos introducido la IKEv2 compatibilidad en los archivos de configuración para muchos de los dispositivos de pasarela de clientes más populares y seguiremos añadiendo archivos adicionales con el tiempo. Para obtener una lista de los archivos de configuración IKEv2 compatibles, consulteAWS Site-to-Site VPN dispositivos de puerta de enlace para clientes.

Permisos

Para cargar correctamente la pantalla de configuración de descargas desde AWS Management Console, debe asegurarse de que su rol o usuario de IAM tenga permiso para los siguientes Amazon EC2 APIs: `GetVpnConnectionDeviceTypes` y`GetVpnConnectionDeviceSampleConfiguration`.

Para descargar el archivo de configuración mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, selecciona conexiones Site-to-Site VPN.
3. Seleccione su conexión de VPN y elija Descargar configuración.
4. Seleccione el Proveedor, la Plataforma , el Software y la Versión de IKE que corresponda al dispositivo de puerta de enlace de cliente. Si su dispositivo no aparece en la lista, seleccione Generic (Genérico).
5. Elija Download (Descargar).

Para descargar un archivo de configuración de ejemplo mediante la línea de comandos o API

- GetVpnConnectionDeviceTypes(EC2 API de Amazon)
- GetVpnConnectionDeviceSampleConfiguration(API de Amazon EC2 Query)
- get-vpn-connection-device-tipos ()AWS CLI
- get-vpn-connection-device-configuración de muestra ()AWS CLI

Paso 7: Configurar el dispositivo de puerta de enlace de cliente

Utilice el archivo de configuración de ejemplo para configurar su dispositivo de gateway de cliente. El dispositivo de puerta de enlace de cliente es un dispositivo físico o de software en su lado de la conexión de VPN. Para obtener más información, consulte AWS Site-to-Site VPN dispositivos de puerta de enlace para clientes.

AWS Site-to-Site VPN escenarios arquitectónicos

A continuación, presentamos varios escenarios en los que puede crear varias conexiones de VPN con uno o varios dispositivos de gateway de cliente.

Varias conexiones de VPN que utilizan el mismo dispositivo de gateway de cliente

Puede crear conexiones VPN adicionales desde su ubicación local a otra VPCs mediante el mismo dispositivo de puerta de enlace del cliente. Puede reutilizar la misma dirección IP de gateway de cliente para cada una de estas conexiones de VPN.

Varios dispositivos de puerta de enlace del cliente a una única puerta de enlace privada virtual ()AWS VPN CloudHub

Puede establecer varias conexiones de VPN a una única gateway privada virtual desde varios dispositivos de gateway de cliente. Esto le permite tener varias ubicaciones conectadas a la AWS VPN CloudHub. Para obtener más información, consulte Comunicación segura entre AWS Site-to-Site VPN conexiones mediante VPN CloudHub. Si tiene dispositivos de gateway de cliente en distintas ubicaciones geográficas, cada dispositivo debería anunciar un único conjunto de rangos IP específicos de la ubicación.

Conexión de VPN redundante que usa otro dispositivo de gateway de cliente

Para protegerse contra la pérdida de conectividad en caso de que el dispositivo de gateway de cliente deje de estar disponible, puede configurar otra conexión de VPN que use otro dispositivo de gateway de cliente. Para obtener más información, consulte AWS Site-to-Site VPN Conexiones redundantes para conmutación por error. Al establecer dispositivos de gateway de cliente redundantes en una única ubicación, ambos dispositivos deberían anunciar los mismos rangos IP.

Las siguientes son arquitecturas de Site-to-Site VPN comunes:

- Conexiones de VPN únicas y múltiples
- the section called “Conexiones de VPN redundantes”
- Comunicaciones seguras entre conexiones VPN mediante VPN CloudHub

AWS Site-to-Site VPN ejemplos de conexiones VPN únicas y múltiples

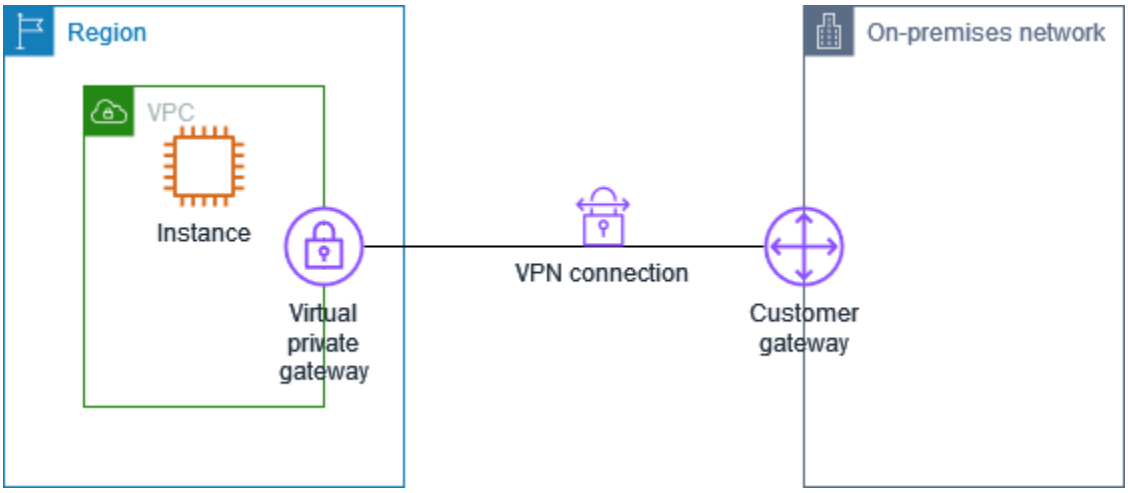
Los siguientes diagramas ilustran las conexiones Site-to-Site VPN únicas y múltiples.

Ejemplos

- Conexión Site-to-Site VPN única
- Conexión Site-to-Site VPN única con una pasarela de tránsito
- Múltiples conexiones Site-to-Site VPN
- Varias conexiones Site-to-Site VPN con una puerta de enlace de tránsito
- Site-to-Site Conexión VPN con AWS Direct Connect
- Conexión Site-to-Site VPN IP privada con AWS Direct Connect

Conexión Site-to-Site VPN única

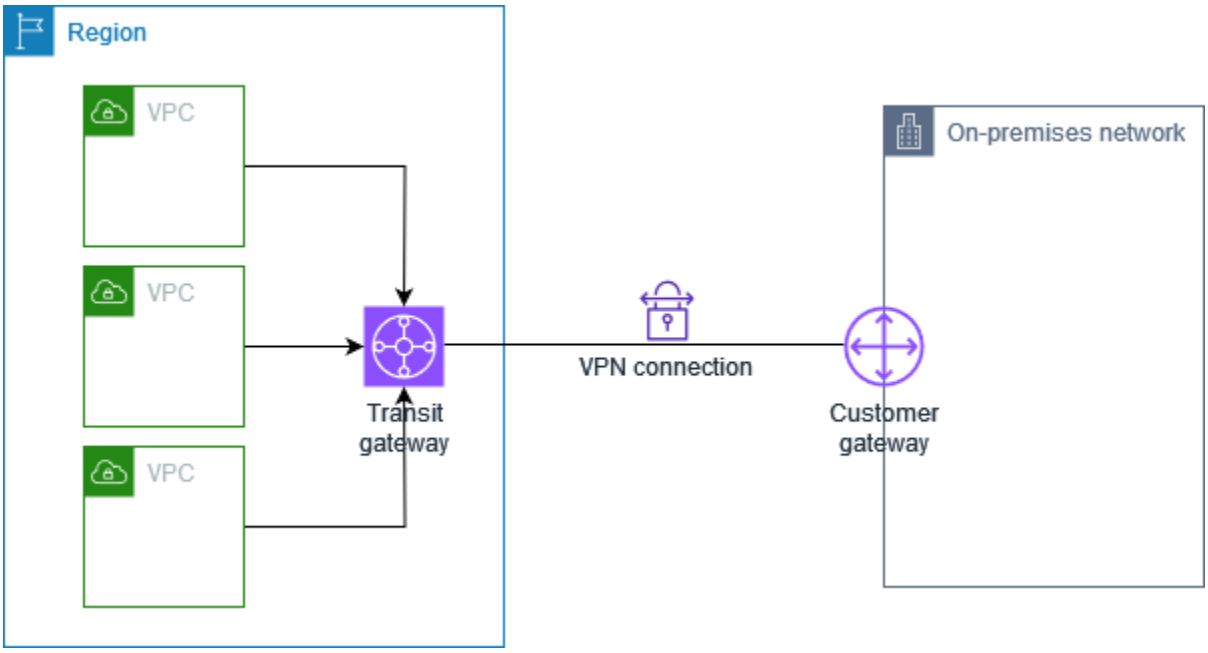
La VPC dispone de una puerta de enlace privada virtual asociada y su red en las instalaciones (remota) incluye un dispositivo de puerta de enlace de cliente que deberá configurar para habilitar la conexión VPN. Debe configurar tablas de enrutamiento de VPC para que el tráfico procedente de la VPC vinculada a su red vaya a la puerta de enlace privada virtual.



Si desea ver los pasos necesarios para configurar este escenario, consulte Comience con AWS Site-to-Site VPN.

Conexión Site-to-Site VPN única con una pasarela de tránsito

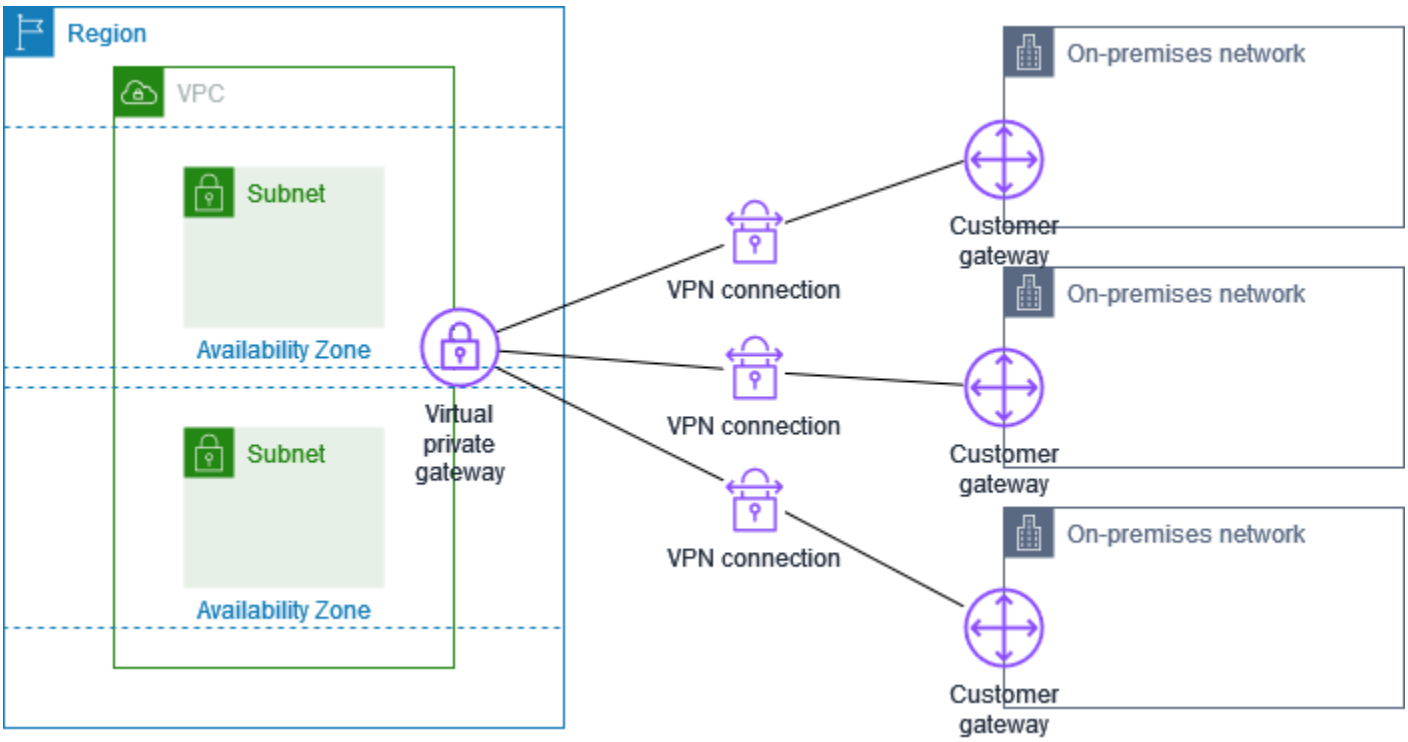
La VPC dispone de una puerta de enlace de tránsito asociada y la red en las instalaciones (remota) contiene un dispositivo de puerta de enlace de cliente que deberá configurar para habilitar la conexión de VPN. Debe configurar tablas de enrutamiento de VPC para que el tráfico procedente de la VPC vinculada a su red vaya a la puerta de enlace de tránsito.



Si desea ver los pasos necesarios para configurar este escenario, consulte Comience con AWS Site-to-Site VPN.

Múltiples conexiones Site-to-Site VPN

La VPC tiene una puerta de enlace privada virtual adjunta y usted tiene varias conexiones de Site-to-Site VPN a varias ubicaciones locales. Configure el direccionamiento para que el tráfico procedente de la VPC vinculada a su red se dirija a la gateway privada virtual.

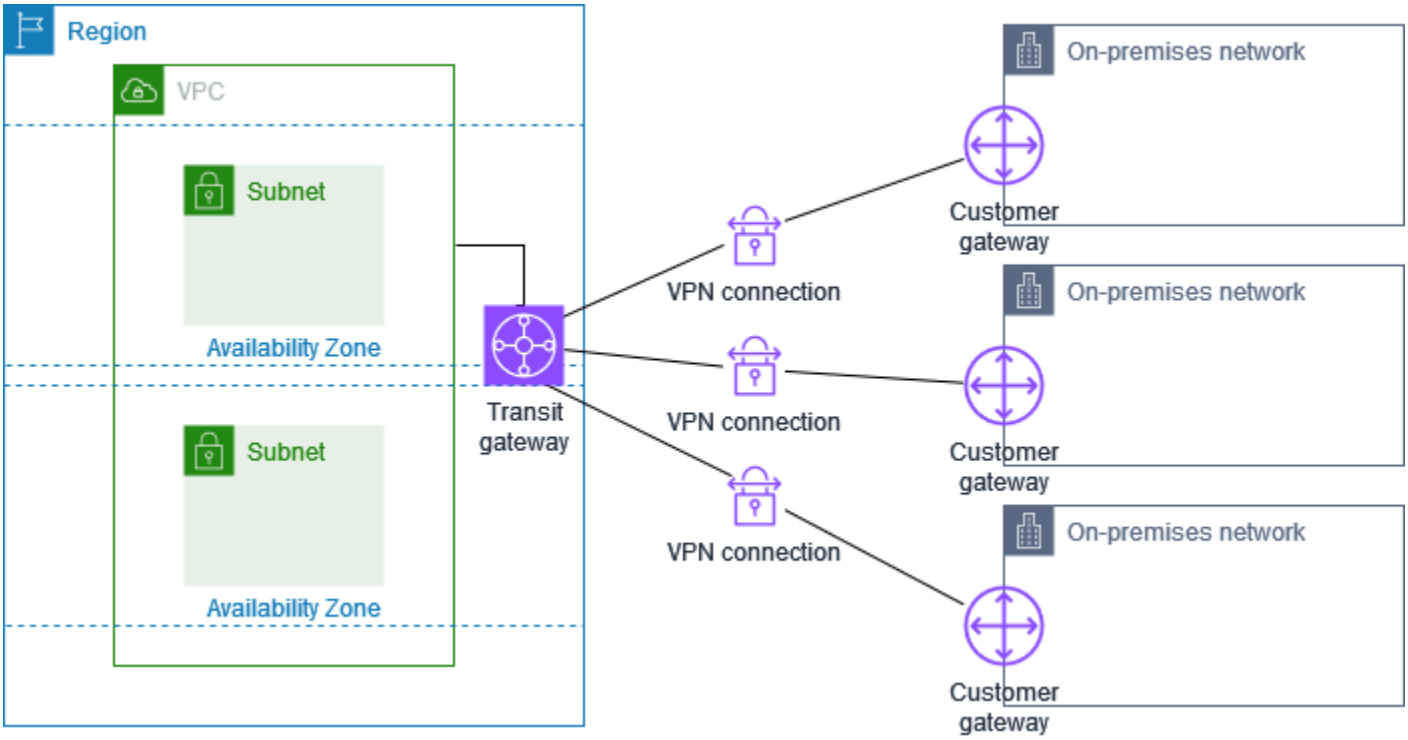


Al crear varias conexiones Site-to-Site VPN a una sola VPC, puede configurar una segunda puerta de enlace de cliente para crear una conexión redundante a la misma ubicación externa. Para obtener más información, consulte AWS Site-to-Site VPN Conexiones redundantes para conmutación por error.

También puede utilizar este escenario para crear conexiones Site-to-Site VPN a varias ubicaciones geográficas y proporcionar una comunicación segura entre sitios. Para obtener más información, consulte Comunicación segura entre AWS Site-to-Site VPN conexiones mediante VPN CloudHub.

Varias conexiones Site-to-Site VPN con una puerta de enlace de tránsito

La VPC tiene una puerta de enlace de tránsito adjunta y usted tiene varias conexiones de Site-to-Site VPN a varias ubicaciones locales. Tiene que configurar el direccionamiento para que el tráfico procedente de la VPC vinculada a la red se direccione a la gateway de tránsito.

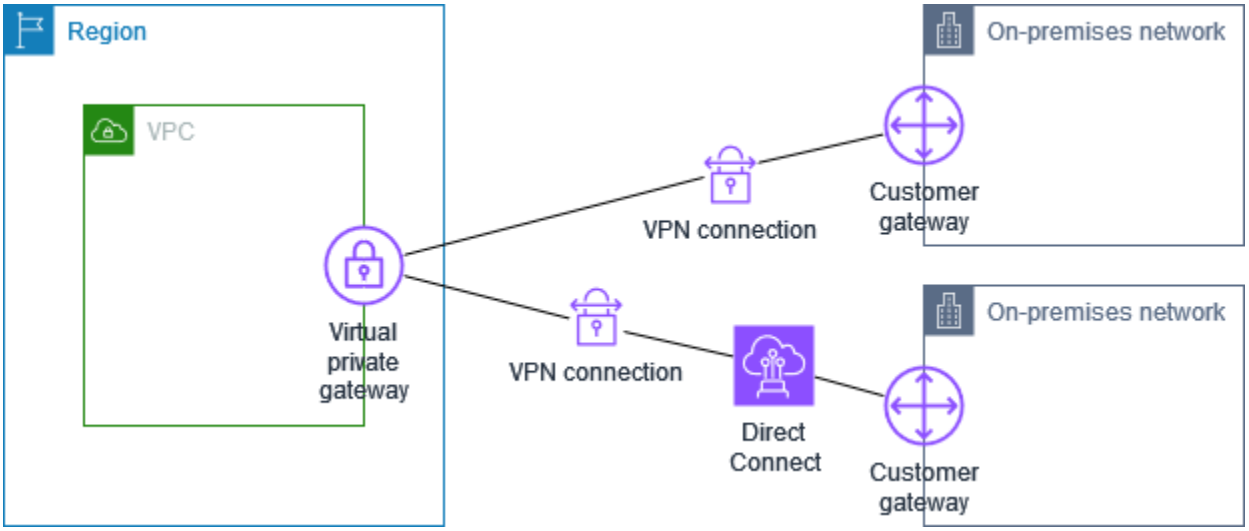


Al crear varias conexiones Site-to-Site VPN a una única puerta de enlace de tránsito, puede configurar una segunda puerta de enlace de cliente para crear una conexión redundante a la misma ubicación externa.

También puede utilizar este escenario para crear conexiones Site-to-Site VPN a varias ubicaciones geográficas y proporcionar una comunicación segura entre sitios.

Site-to-Site Conexión VPN con AWS Direct Connect

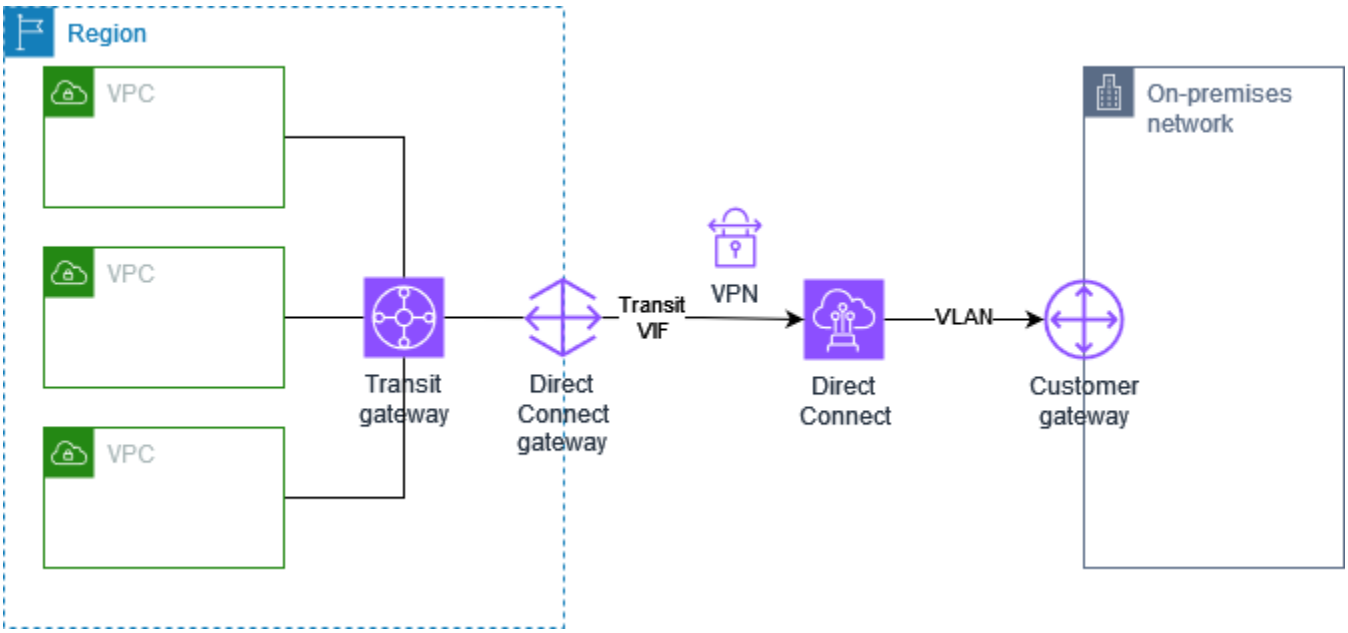
La VPC tiene una puerta de enlace privada virtual adjunta y se conecta a la red local (remota) a través de ella. AWS Direct Connect Puede configurar una interfaz virtual AWS Direct Connect pública para establecer una conexión de red dedicada entre su red y los AWS recursos públicos a través de una puerta de enlace privada virtual. Configura el enrutamiento de manera que cualquier tráfico de la VPC con destino a su red se dirija a la puerta de enlace privada virtual y a la AWS Direct Connect conexión.



Cuando ambas AWS Direct Connect y la conexión VPN están configuradas en la misma puerta de enlace privada virtual, añadir o quitar objetos puede provocar que la puerta de enlace privada virtual pase al estado de «conexión». Esto indica que se está realizando un cambio en el enrutamiento interno que cambiará entre AWS Direct Connect y la conexión de VPN para minimizar las interrupciones y la pérdida de paquetes. Cuando esto se completa, la gateway privada virtual vuelve al estado “adjunto”.

Conexión Site-to-Site VPN IP privada con AWS Direct Connect

Con una Site-to-Site VPN IP privada, puede cifrar el AWS Direct Connect tráfico entre su red local y AWS sin el uso de direcciones IP públicas. La conexión VPN con IP privada AWS Direct Connect garantiza que el tráfico entre las redes locales AWS y las redes locales sea seguro y privado, lo que permite a los clientes cumplir con los requisitos normativos y de seguridad.



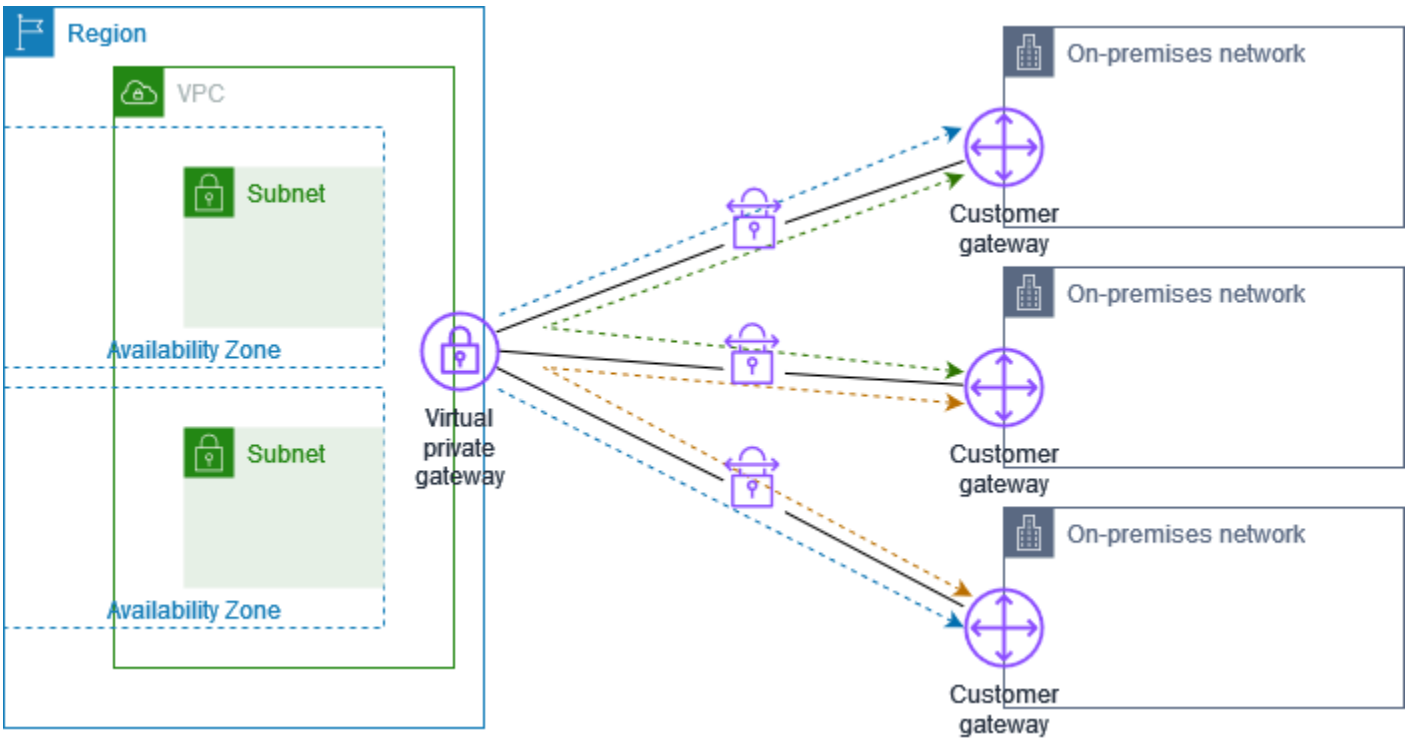
Para obtener más información, consulte la siguiente entrada del blog: Introducción a la IP AWS Site-to-Site VPN privada VPNs.

Comunicación segura entre AWS Site-to-Site VPN conexiones mediante VPN CloudHub

Si tiene varias AWS Site-to-Site VPN conexiones, puede proporcionar una comunicación segura entre sitios mediante la AWS VPN CloudHub. Esto permite que los sitios puedan comunicarse entre sí y no solo con los recursos de la VPC. La VPN CloudHub funciona con un hub-and-spoke modelo simple que puede usar con o sin una VPC. Este diseño es adecuado si tiene varias sucursales y conexiones a Internet existentes y desea implementar un hub-and-spoke modelo práctico y potencialmente económico para la conectividad principal o de respaldo entre estos sitios.

Descripción general

El siguiente diagrama muestra la CloudHub arquitectura de la VPN. Las líneas discontinuas muestran el tráfico de red entre sitios remotos que se enruta a través de las conexiones VPN. Los sitios no pueden tener rangos de IP solapados.



En esta situación, haga lo siguiente:

1. Cree una única gateway privada virtual.
2. Cree varias gateway de cliente, cada una con la dirección IP pública de la gateway. Debe utilizar un Número de sistema autónomo (ASN) para protocolo de gateway fronteriza (BGP) único para cada gateway de cliente.
3. Cree una conexión Site-to-Site VPN enrutada dinámicamente desde la puerta de enlace de cada cliente a la puerta de enlace privada virtual común.
4. Configure los dispositivos de gateway de cliente para que indiquen un prefijo específico del sitio (como 10.0.0.0/24, 10.0.1.0/24) a la gateway privada virtual. Estos anuncios de direccionamiento se reciben y se vuelven a anunciar a cada parte de BGP, lo que permite que cada sitio pueda enviar y recibir datos de otros sitios. Esto se hace mediante las instrucciones de red de los archivos de configuración de la VPN para la conexión Site-to-Site VPN. Las instrucciones de red varían en función del tipo de router que utilice.
5. Configure las rutas en las tablas de enrutamiento de subred para permitir que las instancias de la VPC se comuniquen con los sitios. Para obtener más información, consulte (Gateway privada virtual) Habilitar la propagación de rutas en la tabla de enrutamiento. Puede configurar una ruta agregada en la tabla de enrutamiento (por ejemplo, 10.0.0.0/16). Utilice prefijos más específicos entre los dispositivos de gateway de cliente y la gateway privada virtual.

Los sitios que utilizan AWS Direct Connect conexiones a la puerta de enlace privada virtual también pueden formar parte de la AWS VPN CloudHub. Por ejemplo, su sede corporativa en Nueva York puede tener una AWS Direct Connect conexión a la VPC y sus sucursales pueden usar conexiones Site-to-Site VPN a la VPC. Las sucursales de Los Ángeles y Miami pueden enviar y recibir datos entre sí y con su sede corporativa, todo ello mediante la AWS VPN. CloudHub

Precios

Para usar AWS una VPN CloudHub, paga las tarifas de conexión típicas de Amazon VPC Site-to-Site VPN. De este modo, se le facturará las tasas de conexión por cada hora que cada VPN permanezca conectada a la gateway privada virtual. Cuando envía datos de un sitio a otro mediante la AWS VPN CloudHub, el envío de datos desde su sitio a la puerta de enlace privada virtual no conlleva ningún coste. Solo pagará tasas de transferencia de datos de AWS estándar de los datos que se reenvíen desde la gateway privada virtual al punto de enlace.

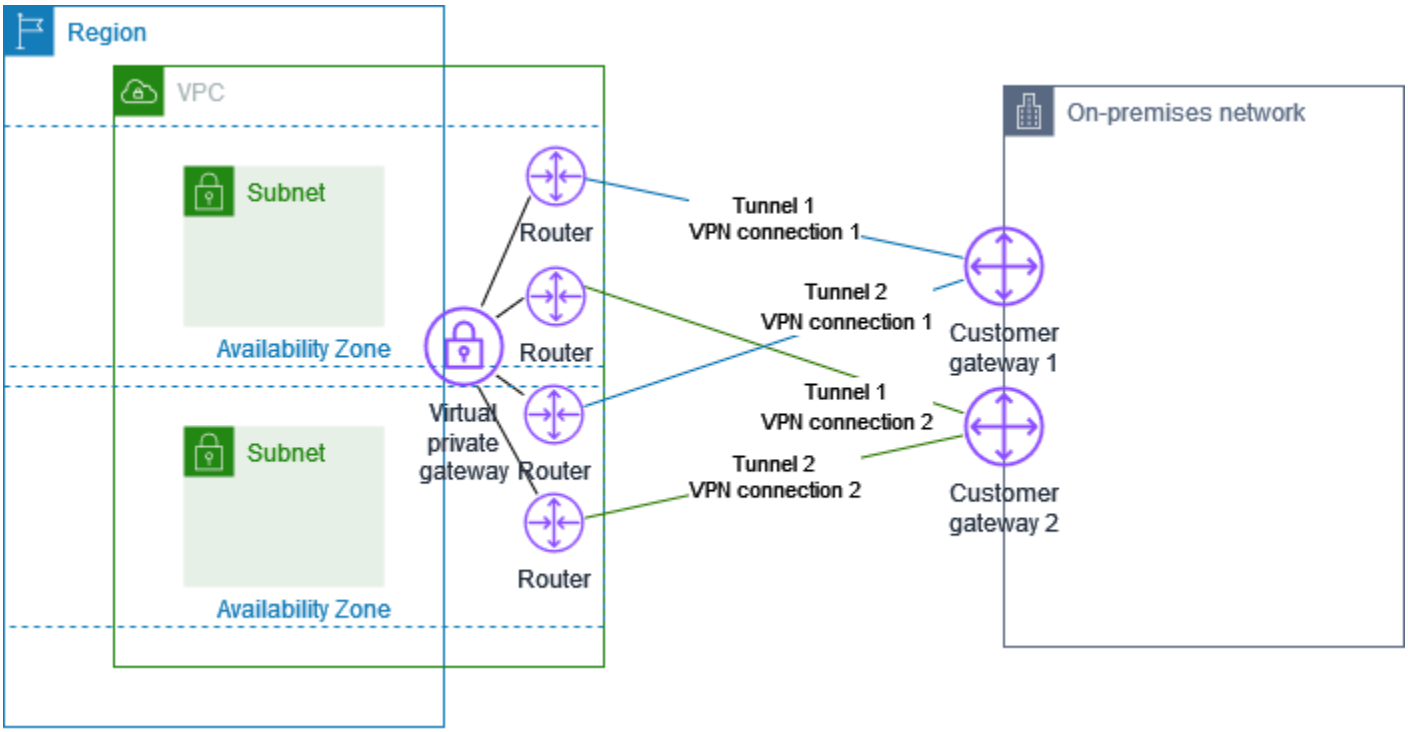
Por ejemplo, si tiene un sitio en Los Ángeles y un segundo sitio en Nueva York y ambos sitios tienen una conexión Site-to-Site VPN a la puerta de enlace privada virtual, paga la tarifa por hora por cada conexión Site-to-Site VPN (por lo que si la tarifa fuera de 0,05$ por hora, sería un total de 0,10$ por hora). También pagas las tarifas de transferencia de AWS datos estándar por todos los datos que envíes de Los Ángeles a Nueva York (y viceversa) que atraviesen cada conexión Site-to-Site VPN. El tráfico de red enviado a través de la conexión Site-to-Site VPN a la puerta de enlace privada virtual es gratuito, pero el tráfico de red enviado a través de la conexión Site-to-Site VPN desde la puerta de enlace privada virtual al punto final se factura según la tarifa de transferencia de AWS datos estándar.

Para obtener más información, consulte Site-to-Site Precios de las conexiones de VPN.

AWS Site-to-Site VPN Conexiones redundantes para conmutación por error

Para protegerse contra la pérdida de conectividad en caso de que su dispositivo de puerta de enlace de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su VPC y a su puerta de enlace privada virtual añadiendo un segundo dispositivo de puerta de enlace de cliente. El uso de dispositivos de puerta de enlace de cliente y conexiones de VPN redundantes permite realizar tareas de mantenimiento en uno de los dispositivos y, a la vez, mantener el flujo de tráfico a través de la segunda conexión de VPN.

En el siguiente diagrama se muestran dos conexiones de VPN. Cada conexión de VPN tiene sus propios túneles y su propia puerta de enlace de cliente.



En esta situación, haga lo siguiente:

- Configure una segunda conexión Site-to-Site VPN mediante la misma puerta de enlace privada virtual y cree una nueva puerta de enlace para el cliente. La dirección IP de la pasarela del cliente para la segunda conexión Site-to-Site VPN debe ser de acceso público.
- Configure el otro dispositivo de gateway de cliente. Ambos dispositivos deben anunciar los mismos rangos de IP a la gateway privada virtual. Utilizamos el direccionamiento de BGP para determinar la ruta del tráfico. Si se produce un error en un dispositivo de gateway de cliente, la gateway privada virtual dirigirá todo el tráfico al dispositivo de gateway de cliente que sí funciona.

Las conexiones Site-to-Site VPN enrutadas dinámicamente utilizan el protocolo Border Gateway (BGP) para intercambiar información de enrutamiento entre las puertas de enlace de sus clientes y las puertas de enlace privadas virtuales. Las conexiones Site-to-Site VPN con enrutamiento estático requieren que introduzca rutas estáticas para la red remota de su lado de la pasarela del cliente. La información acerca de las rutas que se especifica manualmente y que anuncia mediante BGP permite a las gateways de ambos extremos determinar qué túneles están disponibles para, de este modo, redireccionar el tráfico en caso de error. Por lo tanto, se recomienda configurar su red para

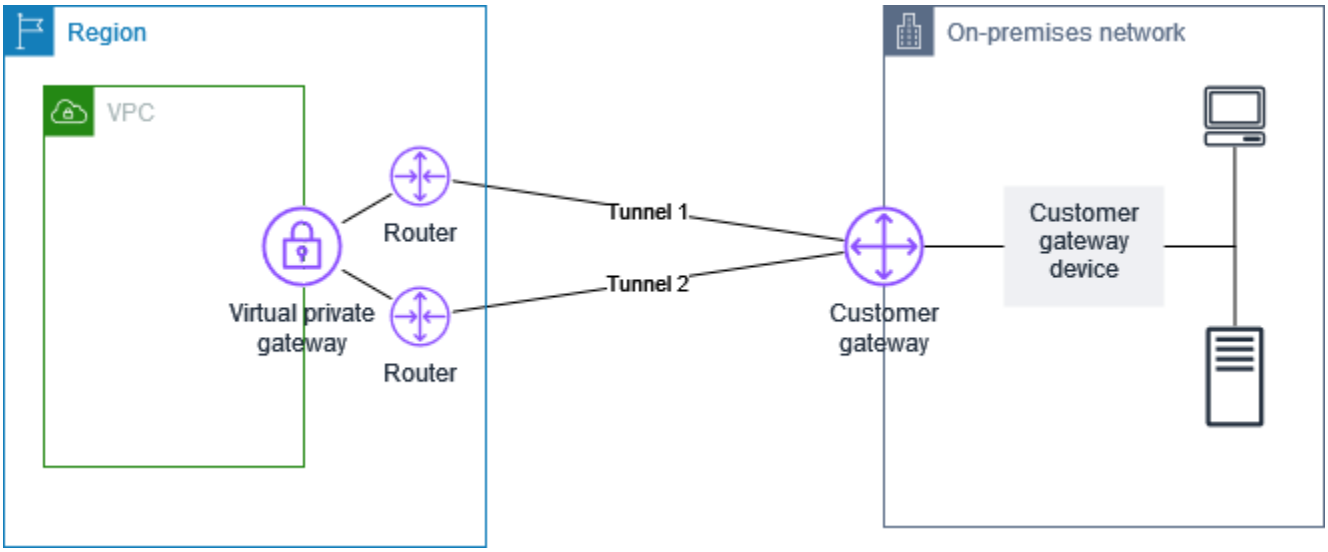
que utilice la información de direccionamiento que proporciona BGP (si está disponible) y seleccionar una ruta alternativa. La configuración exacta dependerá de la arquitectura de su red.

Para obtener más información sobre la creación y configuración de una pasarela de cliente y una conexión Site-to-Site VPN, consulte. Comience con AWS Site-to-Site VPN

AWS Site-to-Site VPN dispositivos de puerta de enlace para clientes

Un dispositivo de puerta de enlace para clientes es un dispositivo físico o de software que usted posee o administra en su red local (en su lado de una conexión Site-to-Site VPN). Usted o el administrador de la red deben configurar el dispositivo para que funcione con la conexión Site-to-Site VPN.

En el siguiente diagrama se muestra su red, el dispositivo de puerta de enlace de cliente y la conexión de VPN que va a una puerta de enlace privada virtual que está asociada a su VPC. Las dos líneas entre la puerta de enlace de cliente y la puerta de enlace privada virtual representan los túneles para la conexión de VPN. Si se produce un fallo en el dispositivo AWS, la conexión VPN pasa automáticamente al segundo túnel para que el acceso no se interrumpa. De vez en cuando, AWS también realiza un mantenimiento rutinario de la conexión VPN, lo que podría deshabilitar brevemente uno de los dos túneles de la conexión VPN. Para obtener más información, consulte AWS Site-to-Site VPN reemplazos de puntos finales de túneles. Por lo tanto, es importante que configure el dispositivo de puerta de enlace de cliente para utilizar ambos túneles.



Si desea ver los pasos necesarios para configurar una conexión de VPN, consulte Comience con AWS Site-to-Site VPN. Durante este proceso, se crea un recurso de pasarela de clientes en AWS el que se proporciona información AWS sobre el dispositivo, por ejemplo, su dirección IP pública. Para obtener más información, consulte Opciones de pasarela de clientes para su AWS Site-to-Site VPN conexión. El recurso de puerta de enlace de cliente AWS no configura ni crea el dispositivo de puerta de enlace de cliente. Debe configurar el dispositivo usted mismo.

También puede encontrar dispositivos de VPN por software en AWS Marketplace.

Requisitos para un dispositivo de pasarela de AWS Site-to-Site VPN clientes

AWS es compatible con varios dispositivos Site-to-Site VPN de puerta de enlace para clientes, para los que proporcionamos archivos de configuración descargables. Para obtener una lista de los dispositivos compatibles y los pasos para descargar los archivos de configuración, consulteArchivos de configuración de enrutamiento estático y dinámico.

Si tiene un dispositivo que no figura en la lista de dispositivos compatibles, en la siguiente sección se describen los requisitos que debe cumplir el dispositivo para establecer una conexión Site-to-Site VPN.

Hay cuatro puntos principales para la configuración del dispositivo de gateway de cliente. Los siguientes símbolos representan cada parte de la configuración.

IKE	Asociación de seguridad de intercambio de claves de Internet (IKE). Esto es necesario para intercambiar las claves utilizadas para establecer la asociación IPsec de seguridad.
IPsec	IPsec asociación de seguridad. Gestiona el cifrado del túnel, la autenticación, etc.
Tunnel	Interfaz de túnel. Recibe el tráfico entrante y saliente del túnel.
BGP	(Opcional) Asociación entre pares con protocolo de gateway fronterizo (BGP) Para dispositivos que usan BGP, intercambia rutas entre el dispositivo de gateway de cliente y la gateway privada virtual.

En la siguiente tabla se indican los requisitos que debe cumplir el dispositivo de gateway de cliente, el RFC relacionado (a modo de referencia) y comentarios acerca de los requisitos.

Cada conexión de VPN consta de dos túneles independientes. Cada túnel contiene una asociación de seguridad IKE, una asociación de IPsec seguridad y un emparejamiento BGP. Está limitado a un par de asociaciones de seguridad (SA) único por túnel (uno de entrada y otro de salida) y, por lo tanto, a dos pares de SA únicos en total para dos túneles (cuatro). SAs Algunos dispositivos utilizan

una VPN basada en políticas y crean tantas SAs entradas de ACL como sea posible. Por lo tanto, es posible que necesite consolidar sus reglas y luego filtrar para no permitir el tráfico no deseado.

De forma predeterminada, el túnel de VPN aparece cuando se genera tráfico y se inicia la negociación de IKE desde el lado de la conexión de VPN. En su lugar, puede configurar la conexión VPN para iniciar la negociación del IKE desde el AWS lado de la conexión. Para obtener más información, consulte AWS Site-to-Site VPN opciones de inicio de túnel.

Los puntos de enlace de VPN dan soporte al cambio de clave y comienzan las nuevas negociaciones cuando la primera fase está a punto de caducar si el dispositivo de gateway de cliente no ha enviado tráfico de renegociación.

Requisito	RFC	Comentarios
Establecimiento de una asociación de seguridad de IKE IKE	RFC 2409 RFC 7296	La asociación de seguridad IKE se establece primero entre la puerta de enlace privada virtual y el dispositivo de puerta de enlace del cliente mediante una clave previamente compartida o un certificado privado que se utiliza AWS Private Certificate Authority como autenticador. Cuando se establece, IKE negocia una clave efímera para proteger los mensajes futuros de IKE. Tiene que haber un acuerdo completo entre los parámetros, incluidos los parámetros de cifrado y autenticación. Al crear una conexión VPN en AWS, puede especificar su propia clave previamente compartida para cada túnel o puede dejar que AWS genere una por usted. Como alternativa, puede especificar el certificado privado que se utilizará AWS Private Certificate Authority para el dispositivo de pasarela de su cliente. Para obtener más información sobre la configuración de túneles de VPN, consulte Opciones de túnel para su AWS Site-to-Site VPN conexión. Se admiten las siguientes versiones: IKEv1 y IKEv2. Solo admitimos el modo principal con IKEv1.

Requisito	RFC	Comentarios
		El servicio Site-to-Site VPN es una solución basada en rutas. Si utiliza una configuración basada en políticas , debe limitar su configuración a una asociación de seguridad (SA) única.
Establezca asociaciones IPsec de seguridad en modo túnel IPsec	RFC 4301	Mediante la clave efímera IKE, las claves se establecen entre la puerta de enlace privada virtual y el dispositivo de puerta de enlace del cliente para formar una asociación de IPsec seguridad (SA). El tráfico entre las gateways se cifra y se descifra mediante esta SA. IKE rota automáticamente y de forma regular las claves efímeras que se utilizan para cifrar el tráfico dentro de la IPsec SA para garantizar la confidencialidad de las comunicaciones.
Uso del cifrado AES de 128 bits o la función de cifrado AES de 256 bits	RFC 3602	La función de cifrado se utiliza para garantizar la privacidad tanto de IKE como de las asociaciones de seguridad. IPsec
Uso de la función de hash SHA-1 o SHA-2 (256)	RFC 2404	Esta función de hash se utiliza para autenticar tanto las asociaciones IKE como las de IPsec seguridad.
Uso de la confidencialidad directa total Diffie-Hellman	RFC 2409	IKE utiliza Diffie-Hellman para establecer claves efímeras para proteger todas las comunicaciones entre los dispositivos de gateway de cliente y las gateways privadas virtuales. Se admiten los siguientes grupos: • Grupos de fase 1: 2, 14-24 • Grupos de fase 2: 2, 5, 14-24

Requisito	RFC	Comentarios
(Conexiones VPN enrutadas dinámicamente) Utilice la detección de pares muertos IPsec	RFC 3706	La detección de pares muertos permite a los dispositivos de VPN identificar rápidamente cuándo una condición de red impide la entrega de paquetes a través de Internet. Cuando esto sucede, las gateways eliminan las asociaciones de seguridad e intentan crear nuevas asociaciones. Durante este proceso, si es posible, se utiliza el IPsec túnel alternativo.
(Conexiones de VPN enrutadas dinámicamente) Vincular el túnel a la interfaz lógica (VPN basada en rutas) Tunnel	Ninguno	El dispositivo debe poder vincular el IPsec túnel a una interfaz lógica. La interfaz lógica contiene una dirección IP utilizada para establecer el intercambio de tráfico BGP con la gateway privada virtual. Esta interfaz lógica no debería realizar ninguna encapsulación adicional (por ejemplo, GRE o IP en IP). Su interfaz debería configurarse en una unidad de transmisión máxima (MTU) de 1399 bytes.
(Conexiones de VPN enrutadas dinámicamente) Establecimiento de intercambio de tráfico BGP BGP	RFC 4271	BGP se utiliza para intercambiar rutas entre el dispositivo de gateway de cliente y la gateway privada virtual para dispositivos que utilizan BGP. Todo el tráfico BGP se cifra y se transmite a través de la Asociación IPsec de Seguridad. Se requiere el BGP para que ambas puertas de enlace intercambien los prefijos IP a los que se puede acceder a través de la SA. IPsec

Una conexión AWS VPN no admite Path MTU Discovery (RFC 1191).

Si tiene un firewall entre el dispositivo de gateway de cliente e Internet, consulte Reglas de firewall para un dispositivo de puerta de enlace del AWS Site-to-Site VPN cliente.

Prácticas recomendadas para un dispositivo de puerta de enlace para clientes AWS Site-to-Site VPN

Utilice IKEv2

Le recomendamos encarecidamente que lo utilice IKEv2 para su conexión Site-to-Site VPN. IKEv2 es un protocolo más simple, robusto y seguro que IKEv1. Solo debe usarlo IKEv1 si su dispositivo de pasarela de clientes no es compatible IKEv2. Para obtener más información sobre las diferencias entre IKEv1 y IKEv2, consulte el apéndice A de RFC7296.

Restablecimiento de la marca “Don't Fragment (DF)” en los paquetes

Algunos paquetes llevan una marca, conocida como la marca "Don't Fragment" (DF), que indica que el paquete no debe fragmentarse. Si los paquetes llevan la marca, las gateways generan un mensaje "ICMP Path MTU Exceeded". En algunos casos, las aplicaciones no contienen los mecanismos suficientes para procesar estos mensajes ICMP y reducir la cantidad de datos transmitidos en cada paquete. Algunos dispositivos VPN pueden anular la marca DF y fragmentar los paquetes de forma incondicional según sea necesario. Si el dispositivo de gateway de cliente tiene esta capacidad, recomendamos que la utilice según corresponda. Consulte RFC 791 para obtener más información.

Fragmentación de paquetes IP antes del cifrado

Si los paquetes que se envían a través de su conexión Site-to-Site VPN superan el tamaño de la MTU, deben estar fragmentados. Para evitar una disminución del rendimiento, le recomendamos que configure el dispositivo de puerta de enlace del cliente para fragmentar los paquetes antes de cifrarlos. Site-to-Site Luego, la VPN volverá a ensamblar los paquetes fragmentados antes de reenviarlos al siguiente destino, a fin de lograr mayores packet-per-second flujos a través de la red. AWS Consulte RFC 4459 para obtener más información.

Asegurarse de que el tamaño del paquete no supere la MTU para las redes de destino

Como la Site-to-Site VPN reagrupará todos los paquetes fragmentados que reciba desde el dispositivo de pasarela del cliente antes de reenviarlos al siguiente destino, tenga en cuenta que las redes de destino a las que se reenvíen después estos paquetes pueden tener en cuenta el tamaño del paquete o la MTU, por ejemplo, a través de determinados protocolos, como Radius AWS Direct Connect.

Ajuste los tamaños de MTU y MSS de acuerdo con los algoritmos en uso

Los paquetes TCP suelen ser el tipo de paquete más común en los túneles. IPsec Site-to-Site La VPN admite una unidad de transmisión máxima (MTU) de 1446 bytes y un tamaño de segmento máximo (MSS) correspondiente de 1406 bytes. Sin embargo, los algoritmos de cifrado tienen distintos tamaños de encabezado y pueden impedir la capacidad de alcanzar estos valores máximos. Para obtener un rendimiento óptimo evitando la fragmentación, le recomendamos que configure la MTU y el MSS basándose específicamente en los algoritmos que se utilizan.

Utilice la siguiente tabla para configurar su MTU o MSS a fin de evitar la fragmentación y lograr un rendimiento óptimo:

Algoritmo de cifrado	Algoritmo hash	NAT transversal	MTU	MSS () IPv4	MSS (IPv6-in-) IPv4
AES-GCM-16	N/A	disabled	1446	1406	1386
AES-GCM-16	N/A	enabled	1438	1398	1378
AES-CBC	SHA1/-256 SHA2	disabled	1438	1398	1378
AES-CBC	SHA1/-256 SHA2	enabled	1422	1382	1362
AES-CBC	SHA2-384	disabled	1422	1382	1362
AES-CBC	SHA2-384	enabled	1422	1382	1362
AES-CBC	SHA2-512	disabled	1422	1382	1362
AES-CBC	SHA2-512	enabled	1406	1366	1346

> **Note**
>
> Los algoritmos AES-GCM cubren tanto el cifrado como la autenticación, por lo que no existe una opción distinta de algoritmo de autenticación que afecte a la MTU.

Desactivar el IKE único IDs

Algunos dispositivos de puerta de enlace de cliente admiten una configuración que garantiza que, como máximo, exista una asociación de seguridad de fase 1 por configuración de túnel. Esta configuración puede provocar estados de fase 2 incoherentes entre los pares de VPN. Si el dispositivo de la puerta de enlace de cliente admite esta configuración, le recomendamos desactivarla.

Reglas de firewall para un dispositivo de puerta de enlace del AWS Site-to-Site VPN cliente

Debe tener una dirección IP estática para utilizarla como punto final para los IPsec túneles que conectan el dispositivo de puerta de enlace del cliente con los AWS Site-to-Site VPN puntos finales. Si hay un firewall entre AWS y el dispositivo de pasarela del cliente, deben existir las reglas de las siguientes tablas para establecer los IPsec túneles. Las direcciones IP del AWS lado -estarán en el archivo de configuración.

Entrante (de Internet)

Regla de entrada I1	
IP de origen	IP externa de Tunnel1
IP destino	Gateway de cliente
Protocolo	UDP
Puerto de origen	500
Destino	500
Regla de entrada I2	
IP de origen	IP externa de Tunnel2
IP destino	Gateway de cliente
Protocolo	UDP
Puerto de origen	500
Puerto de destino	500
Regla de entrada I3	
IP de origen	IP externa de Tunnel1
IP destino	Gateway de cliente

Protocolo	IP 50 (ESP)
Regla de entrada I4	
IP de origen	IP externa de Tunnel2
IP destino	Gateway de cliente
Protocolo	IP 50 (ESP)

Saliente (a Internet)

Regla de salida O1	
IP de origen	Gateway de cliente
IP destino	IP externa de Tunnel1
Protocolo	UDP
Puerto de origen	500
Puerto de destino	500
Regla de salida O2	
IP de origen	Gateway de cliente
IP destino	IP externa de Tunnel2
Protocolo	UDP
Puerto de origen	500
Puerto de destino	500
Regla de salida O3	
IP de origen	Gateway de cliente
IP destino	IP externa de Tunnel1

Protocolo	IP 50 (ESP)
Regla de salida O4	
IP de origen	Gateway de cliente
IP destino	IP externa de Tunnel2
Protocolo	IP 50 (ESP)

Las reglas I1, I2, O1 y O2 permiten la transmisión de paquetes IKE. Las reglas I3, I4, O3 y O4 permiten la transmisión de IPsec paquetes que contienen el tráfico de red cifrado.

> **Note**
>
> Si utiliza el cruce de NAT (NAT-T) en su dispositivo, asegúrese de que el tráfico UDP del puerto 4500 también pueda pasar entre la red y los puntos finales. AWS Site-to-Site VPN Compruebe si su dispositivo anuncia NAT-T.

Archivos de configuración estáticos y dinámicos para un dispositivo de puerta de enlace del cliente AWS Site-to-Site VPN

Después de crear la conexión VPN, también tiene la opción de descargar un archivo AWS de configuración de muestra proporcionado desde la consola de Amazon VPC o mediante EC2 la API. Para obtener más información, consulte Paso 6: Descargar el archivo de configuración. También puede descargar archivos .zip de configuraciones de ejemplo específicamente para enrutamiento estático frente a dinámico de estas páginas respectivas.

El archivo AWS de configuración de muestra proporcionado contiene información específica sobre su conexión VPN que puede utilizar para configurar su dispositivo de pasarela de clientes. Estos archivos de configuración específicos del dispositivo sólo están disponibles para los dispositivos que han sido probados por AWS. Si su dispositivo específico gateway de cliente no aparece en la lista, puede descargar un archivo de configuración genérico para empezar.

Important

El archivo de configuración es solo un ejemplo y es posible que no coincida por completo con la configuración de conexión Site-to-Site VPN prevista. Especifica los requisitos mínimos para una conexión Site-to-Site VPN de AES128 SHA1, y Diffie-Hellman del grupo 2 en la mayoría de AWS las regiones, y de AES128 SHA2, y Diffie-Hellman del grupo 14 en las regiones. AWS GovCloud También especifica claves previamente compartidas para la autenticación. Debe modificar el archivo de configuración de ejemplo para aprovechar los algoritmos de seguridad adicionales, los grupos de Diffie-Hellman, los certificados privados y el tráfico. IPv6

Note

Estos archivos de configuración específicos del dispositivo se proporcionan con el máximo esfuerzo. AWS Si bien han sido probados por AWS, estas pruebas son limitadas. Si experimenta un problema con los archivos de configuración, es posible que deba contactar al proveedor específico para obtener asistencia adicional.

La siguiente tabla contiene una lista de dispositivos que tienen un archivo de configuración de ejemplo disponible para descargar que se ha actualizado para que sea compatible IKEv2. Hemos introducido la IKEv2 compatibilidad en los archivos de configuración para muchos dispositivos de pasarela de clientes populares y seguiremos añadiendo archivos adicionales a lo largo del tiempo. Esta lista se actualizará a medida que se agreguen más archivos de configuración de ejemplo.

Proveedor	Plataforma	Software
Punto de comprobación	Gaia	R80.10+
Cisco Meraki	Serie MX	15.12+ (WebUI)
Cisco Systems, Inc.	Serie ASA 5500	ASA 9.7+ VTI
Cisco Systems, Inc.	CSRv AMI	IOS 12.4+
Fortinet	Serie Fortigate 40+	ForTIOS 6.4.4+ (GUI)

Proveedor	Plataforma	Software
Juniper Networks, Inc.	Routers Serie J	JunOS 9.5+
Juniper Networks, Inc.	Routers SRX	JunOS 11.0+
Mikrotik	RouterOS	6.44.3
Palo Alto Networks	Serie PA	PANOS 7.0+
SonicWall	NSA, TZ	OS 6.5
Sophos	Sophos Firewall	v19+
Strongswan	Ubuntu 16.04	Strongswan 5.5.1+
Yamaha	Routers RTX	Rev.10.01.16+

Archivos de configuración de enrutamiento estático descargables para un dispositivo de puerta de enlace del AWS Site-to-Site VPN cliente

Para descargar un archivo de configuración de muestra con valores específicos para la configuración de su conexión de Site-to-Site VPN, utilice la consola de Amazon VPC, la línea de AWS comandos o la API de Amazon EC2 . Para obtener más información, consulte Paso 6: Descargar el archivo de configuración.

También puede descargar archivos de configuración genéricos de ejemplo para el enrutamiento estático que no incluyan valores específicos de la configuración de su conexión Site-to-Site VPN: .zip static-routing-examples

Los archivos utilizan valores de marcadores de posición para algunos componentes. Por ejemplo, usan:

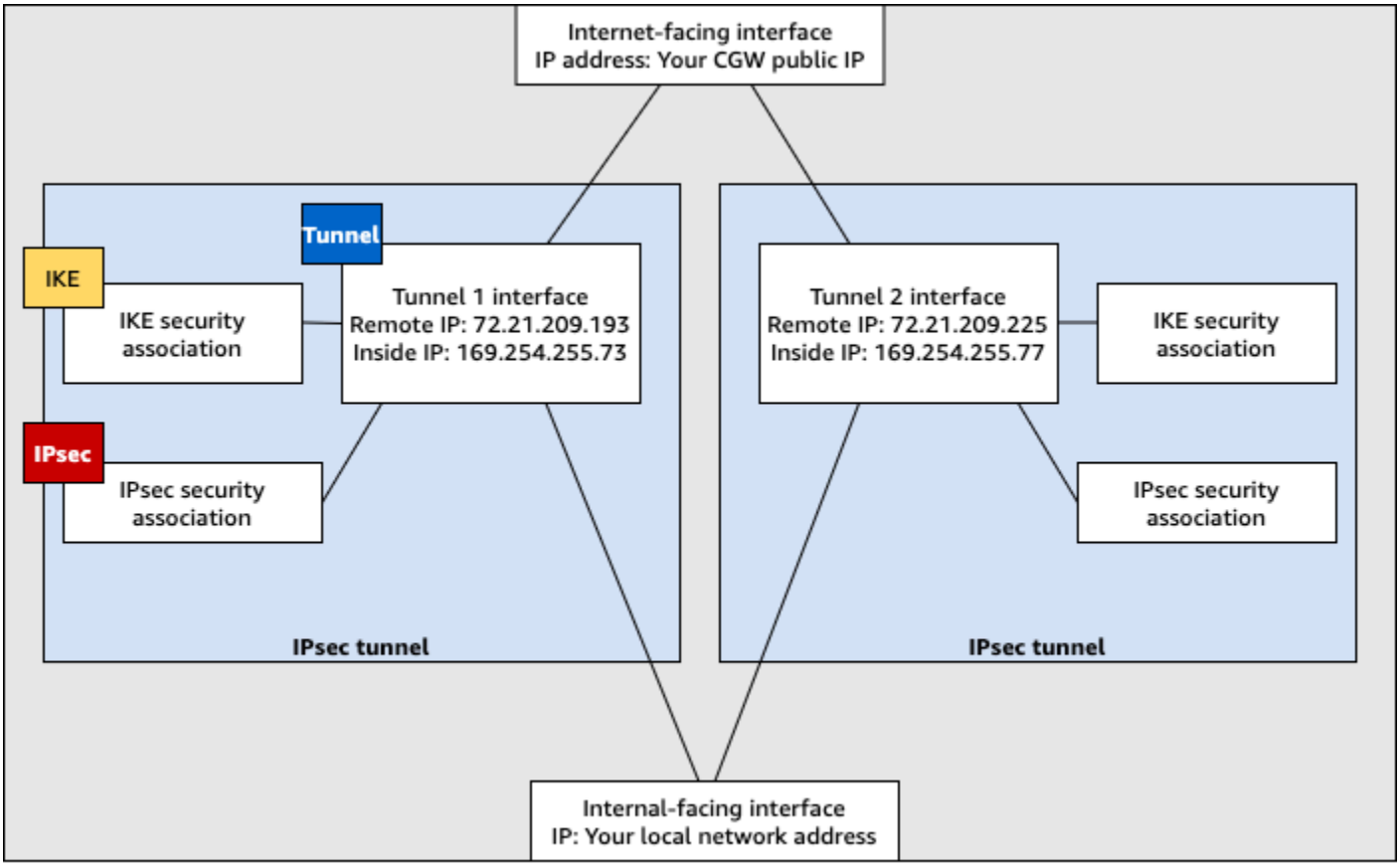
- Valores de ejemplo para el ID de conexión de VPN, el ID de gateway de cliente y el ID de gateway privada virtual
- Marcadores de posición para los AWS puntos finales de la dirección IP remota (externa) (y) *AWS_ENDPOINT_1* *AWS_ENDPOINT_2*
- Un marcador de posición para la dirección IP de la interfaz externa enrutable a Internet del dispositivo de pasarela del cliente () *your-cgw-ip-address*

- Un marcador de posición para el valor clave previamente compartido () pre-shared-key
- Valores de ejemplo de direcciones IP interiores para el túnel.
- Valores de muestra para la configuración de MTU.

> **Note**
>
> La configuración de MTU proporcionada en los archivos de configuración de muestra son solo ejemplos. Consulte Prácticas recomendadas para un dispositivo de puerta de enlace para clientes AWS Site-to-Site VPN para obtener información sobre cómo establecer el valor de MTU óptimo para su situación.

Además de proporcionar valores de marcador de posición, los archivos especifican los requisitos mínimos para una conexión Site-to-Site VPN del grupo 2 de Diffie-Hellman en la mayoría de las regiones y AES128 SHA1, y del grupo 14 de Diffie-Hellman en AWS las regiones. AES128 SHA2 AWS GovCloud También se especifican claves previamente compartidas para la autenticación. Debe modificar el archivo de configuración de ejemplo para aprovechar los algoritmos de seguridad adicionales, los grupos de Diffie-Hellman, los certificados privados y el tráfico. IPv6

En el siguiente diagrama se ofrece una descripción general de los diferentes componentes que se configuran en el dispositivo de gateway de cliente. Incluye valores de ejemplo para las direcciones IP de la interfaz del túnel.



Configuración del enrutamiento estático para un dispositivo de puerta de enlace de cliente de AWS Site-to-Site VPN

A continuación, se presentan algunos procedimientos de ejemplo para configurar un dispositivo de gateway de cliente a través de su interfaz de usuario (si está disponible).

Check Point

Los siguientes son los pasos para configurar su dispositivo de pasarela de cliente si se trata de un dispositivo Check Point Security Gateway que ejecute la versión 77.10 o superior y utilice el sistema operativo Gaia y Check Point. SmartDashboard También puede consultar el artículo de Check Point Security Gateway IPsec VPN to Amazon Web Services VPC en el Check Point Support Center.

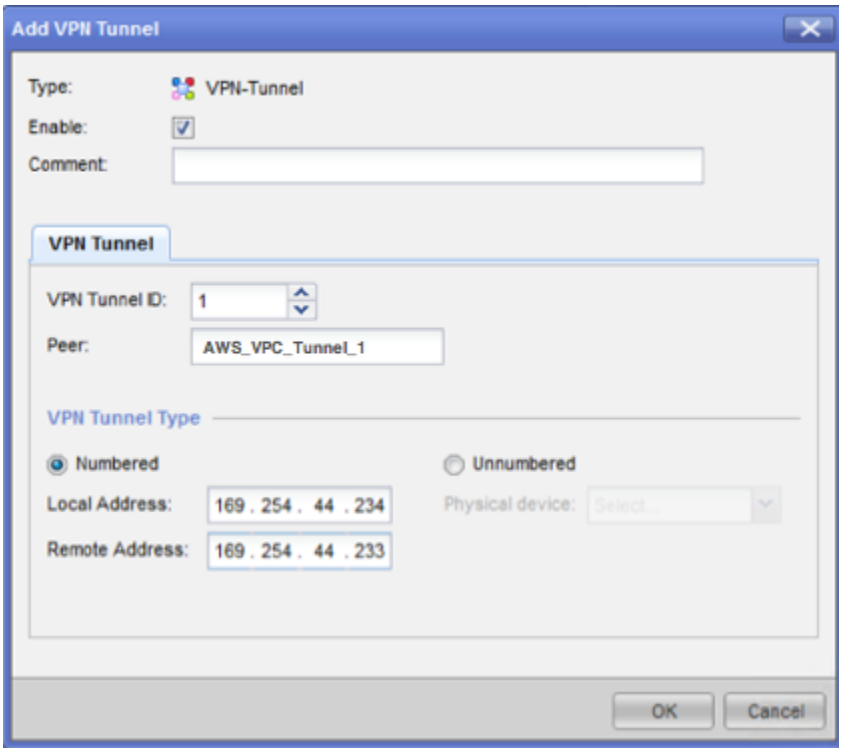
Para configurar la interfaz de túnel

El primer paso es crear los túneles de VPN y proporcionar las direcciones IP privadas (internas) de la gateway de cliente y la gateway privada virtual de cada túnel. Para crear el primer

túnel, utilice la información proporcionada en la sección `IPSec Tunnel #1` del archivo de configuración. Para crear el segundo túnel, utilice los valores proporcionados en la sección `IPSec Tunnel #2` del archivo de configuración.

1. Abra el portal de Gaia de su dispositivo Check Point Security Gateway.
2. Elija Network Interfaces, Add, VPN tunnel.
3. En el cuadro de diálogo, configure los ajustes tal como se muestra y elija OK cuando haya terminado:

   - Para VPN Tunnel ID, escriba cualquier valor único, como 1.
   - Para Peer, escriba un nombre único para cada túnel, como `AWS_VPC_Tunnel_1` o `AWS_VPC_Tunnel_2`.
   - Asegúrese de que la opción Numbered (Numerado) esté seleccionada y, en Local Address (Dirección local), escriba la dirección IP especificada para `CGW Tunnel IP` en el archivo de configuración; por ejemplo: `169.254.44.234`.
   - Para Remote Address, escriba la dirección IP especificada para `VGW Tunnel IP` en el archivo de configuración; por ejemplo: `169.254.44.233`.



4. Conéctese a su gateway de seguridad a través de SSH. Si va a utilizar el shell no predeterminado, cambie a clish ejecutando el siguiente comando: `clish`.

5. Para el túnel 1, ejecute el siguiente comando:

```
set interface vpnt1 mtu 1436
```

   Para el túnel 2, ejecute el siguiente comando:

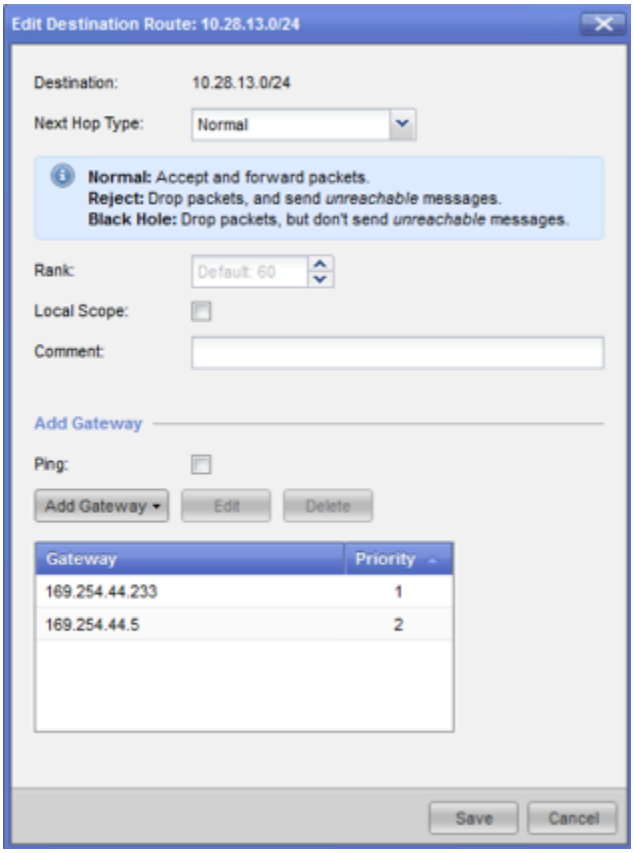
```
set interface vpnt2 mtu 1436
```

6. Repita estos pasos para crear un segundo túnel, utilizando la información de la sección `IPSec Tunnel #2` del archivo de configuración.

Para configurar las rutas estáticas

En este paso, debe especificar la ruta estática de la subred en la VPC para que cada túnel le permita enviar tráfico a través de las interfaces del túnel. El segundo túnel permite la conmutación por error en caso de que haya un problema con el primer túnel. Si se detecta un problema, la ruta estática basada en políticas se quitará de la tabla de ruteo y se activará la segunda ruta. También debe habilitar la gateway de Check Point para hacer ping al otro extremo del túnel y comprobar si el túnel está activo.

1. En el portal de Gaia, elija Rutas IPv4 estáticas y, a continuación, Agregar.
2. Especifique el CIDR de su subred; por ejemplo: `10.28.13.0/24`.
3. Elija Add Gateway, IP Address.
4. Escriba la dirección IP especificada para `VGW Tunnel IP` en el archivo de configuración (por ejemplo: `169.254.44.233`) y especifique una prioridad de 1.
5. Seleccione Ping.
6. Repita los pasos 3 y 4 para el segundo túnel, utilizando el valor `VGW Tunnel IP` de la sección `IPSec Tunnel #2` del archivo de configuración. Especifique una prioridad de 2.



7. Seleccione Guardar.

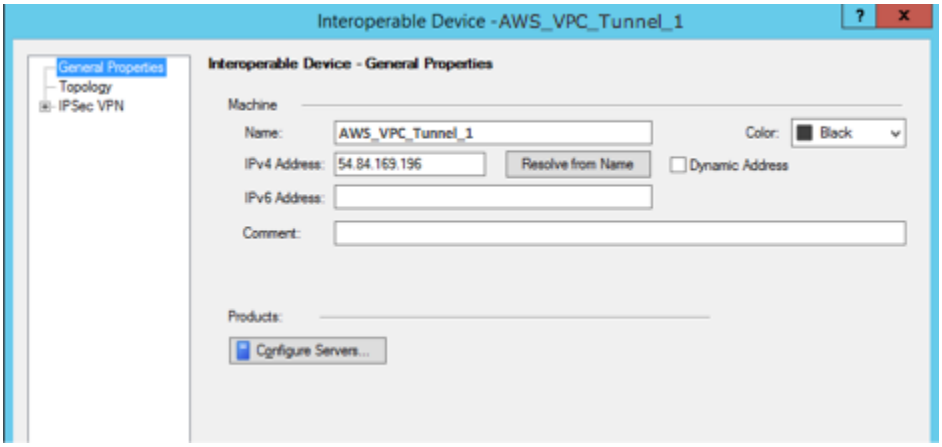
Si va a utilizar un clúster, repita los pasos anteriores para los demás miembros del clúster.

Para definir un nuevo objeto de red

En este paso, creará un objeto de red para cada túnel de VPN, especificando las direcciones IP públicas (externas) de la gateway privada virtual. Más tarde añadirá estos objetos de red como gateways satélite para su comunidad de VPN. También debe crear un grupo vacío para que actúe como marcador de posición para el dominio de VPN.

1. Abre el punto SmartDashboard de control.
2. Para Groups, abra el menú contextual y elija Groups, Simple Group. Puede utilizar el mismo grupo para cada objeto de red.
3. Para Network Objects, abra el menú contextual (clic con el botón derecho) y elija New, Interoperable Device.
4. Para Name (Nombre), escriba el nombre que ha proporcionado para cada túnel, por ejemplo: `AWS_VPC_Tunnel_1` o `AWS_VPC_Tunnel_2`.

5. En IPv4 Dirección, introduzca la dirección IP externa de la puerta de enlace privada virtual proporcionada en el archivo de configuración, por ejemplo,`54.84.169.196`. Guarde la configuración y cierre el cuadro de diálogo.



6. En SmartDashboard, abra las propiedades de la puerta de enlace y, en el panel de categorías, elija Topología.
7. Para recuperar la configuración de la interfaz, elija Get Topology.
8. En la sección VPN Domain (Dominio de VPN), elija Manually defined (Definido manualmente), desplácese hasta el grupo sencillo vacío que creó en el paso 2 y selecciónelo. Seleccione OK.

> **Note**
>
> Puede conservar cualquier dominio de VPN existente que haya configurado. No obstante, asegúrese de que los hosts y las redes utilizados o servidos por la nueva conexión de VPN no estén declarados en ese dominio de VPN, especialmente si el dominio de VPN se obtiene automáticamente.

9. Repita estos pasos para crear un segundo objeto de red, utilizando la información de la sección `IPSec Tunnel #2` del archivo de configuración.

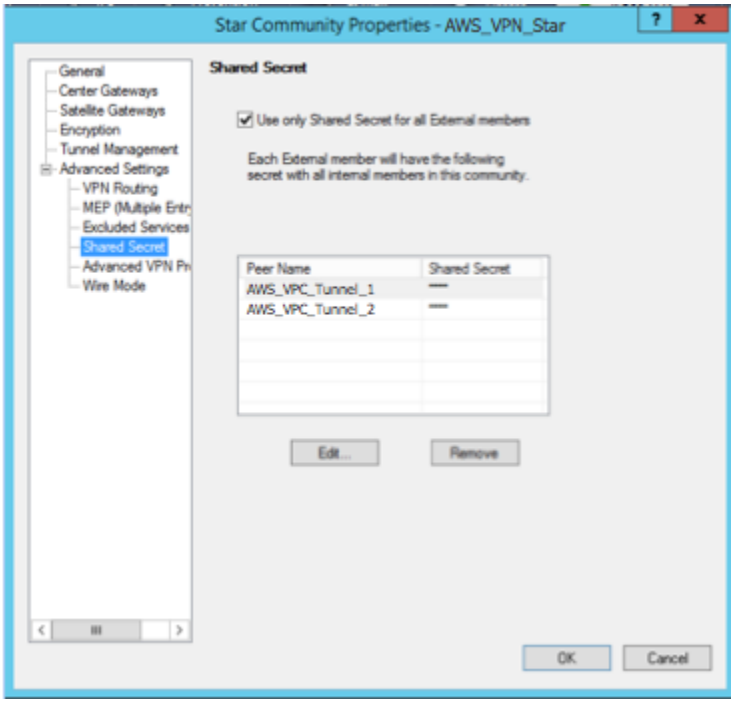
> **Note**
>
> Si va a utilizar clústeres, edite la topología y defina las interfaces como interfaces de clúster. Utilice las direcciones IP especificadas en el archivo de configuración.

Para crear y configurar la comunidad VPN, el IKE y los ajustes IPsec

En este paso, creará una comunidad de VPN en su gateway de Check Point, a la que agregará los objetos de red (dispositivos interoperables) para cada túnel. También puede configurar el intercambio de claves de Internet (IKE) y los IPsec ajustes.

1. En las propiedades de la puerta de enlace, elija IPSecVPN en el panel de categorías.
2. Elija Communities, New, Star Community.
3. Proporcione un nombre para su comunidad (por ejemplo, `AWS_VPN_Star`) y, a continuación, elija Center Gateways en el panel Category.
4. Elija Add y agregue su gateway o clúster a la lista de gateways participantes.
5. En el panel Category (Categoría), elija Satellite Gateways (Gateways satélite), Add (Agregar), y luego agregue los dispositivos interoperables que creó anteriormente (`AWS_VPC_Tunnel_1` y `AWS_VPC_Tunnel_2`) a la lista de gateways participantes.
6. En el panel Category, elija Encryption. En la sección Método de cifrado, elija IKEv1 solo. En la sección Encryption Suite, elija Custom, Custom Encryption.
7. En el cuadro de diálogo, configure las propiedades de cifrado tal como se muestra y elija OK cuando haya terminado:

   - Propiedades de asociación de seguridad de IKE (fase 1):
     - Perform key exchange encryption with: AES-128
     - Perform data integrity with: SHA-1
   - IPsec Propiedades de la asociación de seguridad (fase 2):
     - Realice el cifrado IPsec de datos con: AES-128
     - Perform data integrity with: SHA-1
8. En el panel Category, elija Tunnel Management. Elija Set Permanent Tunnels, On all tunnels in the community. En la sección VPN Tunnel Sharing, elija One VPN tunnel per Gateway pair.
9. En el panel Category, expanda Advanced Settings y elija Shared Secret.
10. Seleccione el nombre homólogo para el primer túnel, elija Edit (Editar) y escriba la clave previamente compartida según lo especificado en la sección `IPSec Tunnel #1` del archivo de configuración.
11. Seleccione el nombre homólogo para el segundo túnel, elija Edit (Editar) y escriba la clave previamente compartida según lo especificado en la sección `IPSec Tunnel #2` del archivo de configuración.



12. Aún en la categoría Advanced Settings (Configuración avanzada), elija Advanced VPN Properties (Propiedades avanzadas de VPN), configure las propiedades según se indica y elija OK (Aceptar) cuando haya terminado:

    - IKE (fase 1):
      - Use Diffie-Hellman group (Usar el grupo Diffie-Hellman): `Group 2`
      - Renegotiate IKE security associations every `480` minutes
    - IPsec (Fase 2):
      - Elija Use Perfect Forward Secrecy
      - Use Diffie-Hellman group (Usar el grupo Diffie-Hellman): `Group 2`
      - Renegocie las asociaciones de IPsec seguridad cada segundo **`3600`**

Para crear reglas de firewall

En este paso, configurará una política con reglas de firewall y reglas de coincidencia direccional que permitan la comunicación entre la VPC y la red local. Luego instalará la política en su gateway.

1. En el SmartDashboard, elija Propiedades globales para su puerta de enlace. En el panel Category, expanda VPN y elija Advanced.
2. Elija Enable VPN Directional Match in VPN Column y guarde los cambios.

3. En el SmartDashboard, elija Firewall y cree una política con las siguientes reglas:
   - Permitir que la subred de VPC se comunique con la red local a través de los protocolos necesarios.
   - Permitir que la red local se comunique con la subred de VPC a través de los protocolos necesarios.
4. Abra el menú contextual para la celda de la columna de VPN, y elija Edit Cell.
5. En el cuadro de diálogo VPN Match Conditions, elija Match traffic in this direction only. Cree las siguientes reglas de coincidencia direccional; para ello, elija Add para cada una, y seleccione OK cuando haya terminado:
   - `internal_clear` > VPN community (Comunidad VPN) (la comunidad Star de VPN que creó antes; por ejemplo: `AWS_VPN_Star`)
   - VPN community > VPN community
   - Comunidad VPN > `internal_clear`
6. En el SmartDashboard, selecciona Política e instala.
7. En el cuadro de diálogo, elija su gateway y seleccione OK para instalar la política.

Para modificar la propiedad tunnel_keepalive_method

Su gateway de Check Point puede utilizar la detección de pares muertos (DPD) para identificar cuándo se desactiva una asociación de IKE. Para configurar DPD para un túnel permanente, el túnel permanente debe configurarse en la comunidad de AWS VPN (consulte el paso 8).

De forma predeterminada, la propiedad `tunnel_keepalive_method` de una gateway de VPN está configurada como `tunnel_test`. Debe cambiar el valor a `dpd`. Cada gateway de VPN de la comunidad de VPN que requiera monitorización de DPD debe configurarse con la propiedad `tunnel_keepalive_method`, incluida cualquier gateway de VPN de terceros. No puede configurar mecanismos de monitorización distintos para la misma gateway.

Puede actualizar la `tunnel_keepalive_method` propiedad mediante la DBedit herramienta GUI.

1. Abra el Check Point SmartDashboard y elija Security Management Server, Domain Management Server.
2. Elija File, Database Revision Control..., y cree una instantánea de revisión.

3. Cierre todas las SmartConsole ventanas, como la del SmartDashboard SmartView Rastreador y la del SmartView Monitor.
4. Inicie la BDedit herramienta GUI. Para obtener más información, consulte el artículo Check Point Database Tool, en el centro de soporte técnico de Check Point.
5. Elija Security Management Server, Domain Management Server.
6. En el panel superior izquierdo, elija Table, Network Objects, network_objects.
7. En el panel superior derecho, seleccione el objeto de Security Gateway, Cluster correspondiente.
8. Presione CTRL+F, o utilice el menú Search para buscar lo siguiente: `tunnel_keepalive_method`.
9. En el panel inferior, abra el menú contextual de `tunnel_keepalive_method` y seleccione Edit... (Editar...). Elija dpd y luego OK (Aceptar).
10. Repita los pasos del 7 al 9 por cada gateway que forme parte de la comunidad de AWS VPN.
11. Elija File, Save All.
12. Cierre la DBedit herramienta Gui.
13. Abra el Check Point SmartDashboard y elija Security Management Server, Domain Management Server.
14. Instale la política en el objeto Security Gateway, Cluster correspondiente.

Para obtener más información, consulte el artículo New VPN features in R77.10, en el centro de soporte técnico de Check Point.

Para habilitar el bloqueo TCP MSS

El bloqueo de TCP MSS reduce el tamaño máximo de segmento de los paquetes TCP para evitar la fragmentación de los paquetes.

1. Vaya al siguiente directorio: `C:\Program Files (x86)\CheckPoint\SmartConsole\R77.10\PROGRAM\`.
2. Abra la herramienta Check Point Database ejecutando el archivo `GuiDBEdit.exe`.
3. Elija Table, Global Properties, properties.
4. Para `fw_clamp_tcp_mss`, elija Edit. Cambie el valor a `true` y elija OK.

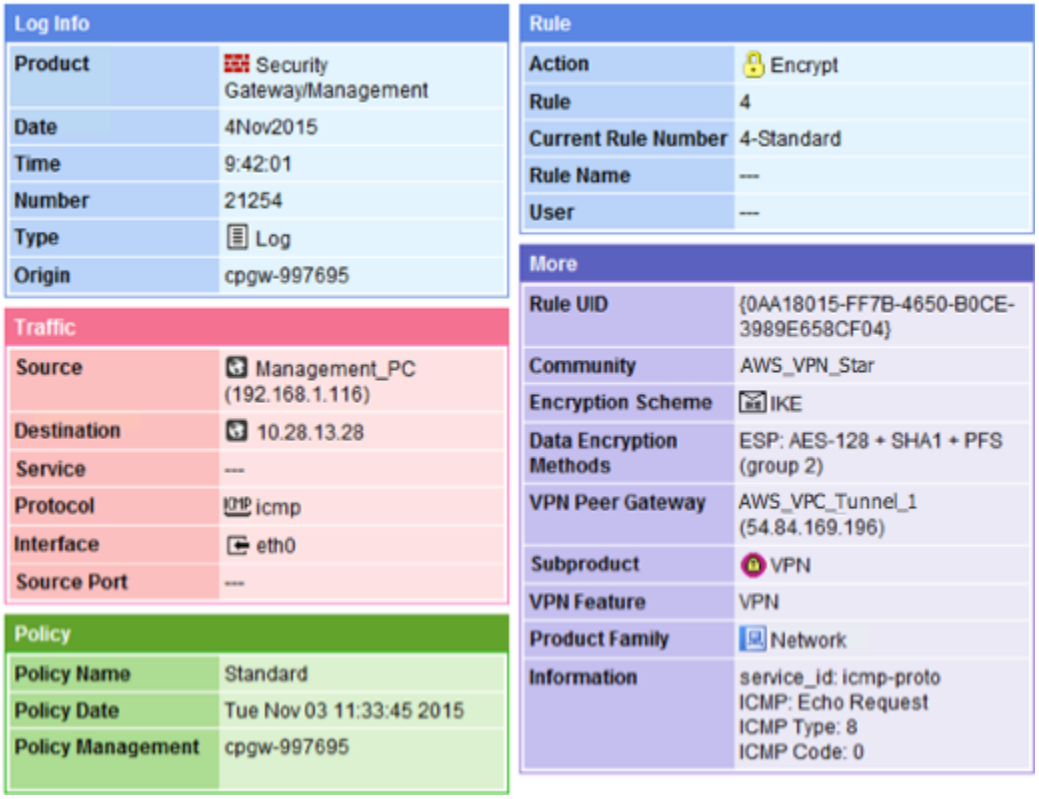
Para verificar el estado del túnel

Puede verificar el estado del túnel ejecutando el siguiente comando desde la herramienta de línea de comandos en el modo experto.

```
vpn tunnelutil
```

En las opciones que aparecen, elija 1 para comprobar las asociaciones IKE y 2 para comprobar las IPsec asociaciones.

También puede utilizar Check Point Smart Tracker Log para verificar que los paquetes de la conexión se están cifrando. Por ejemplo, el siguiente log indica que un paquete para la VPC se ha enviado a través del túnel 1 y se ha cifrado.



SonicWALL

El procedimiento siguiente muestra cómo configurar los túneles de VPN en el dispositivo SonicWALL utilizando la interfaz de gestión SonicOS.

Para configurar los túneles

1. Abra la interfaz de gestión SonicWALL SonicOS.
2. En el panel izquierdo, elija VPN, Settings. En VPN Policies, elija Add....
3. En la ventana de política de VPN de la pestaña General , complete la información siguiente:

- Policy Type (Tipo de política): seleccione Tunnel Interface (Interfaz de túnel).
- Authentication Method: elija IKE using Preshared Secret.
- Name: escriba un nombre para la política de VPN. Le recomendamos utilizar el nombre del ID de VPN tal como se indica en el archivo de configuración.
- IPsec Nombre o dirección de la puerta de enlace principal: introduzca la dirección IP de la puerta de enlace privada virtual tal como se indica en el archivo de configuración (por ejemplo,`72.21.209.193`).
- IPsec Nombre o dirección de la puerta de enlace secundaria: deje el valor predeterminado.
- Shared Secret: escriba la clave previamente compartida tal como se indica en el archivo de configuración y vuelva a escribirla en Confirm Shared Secret.
- ID IKE local: introduzca la IPv4 dirección de la pasarela del cliente (el dispositivo SonicWall).
- ID IKE del mismo nivel: introduzca la IPv4 dirección de la puerta de enlace privada virtual.

4. En la pestaña Network, complete la información siguiente:

   - En Local Networks, elija Any address. Se recomienda utilizar esta opción para evitar problemas de conectividad en su red local.
   - En Remote Networks, elija Choose a destination network from list. Cree un objeto de dirección con el CIDR de su VPC en AWS.

5. En la pestaña Proposals (Propuestas), complete la información siguiente:

   - En IKE (Phase 1) Proposal, haga lo siguiente:
     - Exchange: elija Main Mode.
     - DH Group (Grupo de DH): escriba un valor para el grupo Diffie-Hellman (por ejemplo, 2).
     - Encryption: elija AES-128 o AES-256.
     - Autenticación: elija SHA1o SHA256.
     - Life Time: escriba `28800`.
   - En IKE (Phase 2) Proposal, haga lo siguiente:
     - Protocol: elija ESP.
     - Encryption: elija AES-128 o AES-256.
     - Autenticación: elija SHA1o SHA256.

- Seleccione la casilla de verificación Enable Perfect Forward Secrecy y elija el grupo Diffie-Hellman.
- Life Time: escriba `3600`.

> **Important**
>
> Si creó su puerta de enlace privada virtual antes de octubre de 2015, debe especificar el grupo 2 de Diffie-Hellman, AES-128, y para ambas fases. SHA1

6. En la pestaña Advanced, complete la información siguiente:
   - Seleccione Enable Keep Alive.
   - Seleccione Enable Phase2 Dead Peer Detection y escriba lo siguiente:
     - En Dead Peer Detection Interval, escriba `60` (este es el valor mínimo que puede aceptar el dispositivo SonicWALL).
     - En Failure Trigger Level, escriba `3`.
   - En VPN Policy bound to, seleccione Interface X1. Esta es la interfaz que suele designarse para las direcciones IP públicas.
7. Seleccione OK. En la página Settings, debe seleccionar la casilla de verificación Enable para el túnel de manera predeterminada. El punto verde indica que el túnel está activo.

Dispositivos Cisco: información adicional

Algunos Cisco solo admiten el modo activo/en espera. ASAs Cuando utiliza estos dispositivos Cisco ASAs, solo puede tener un túnel activo a la vez. El otro túnel en espera se activará si el primer túnel se vuelve no disponible. Con esta redundancia, siempre debería tener conectividad a su VPC a través de uno de los túneles.

ASAs A partir de la versión 9.7.1 y posteriores, Cisco admite el modo activo/activo. Al utilizar estos dispositivos Cisco ASAs, puede tener ambos túneles activos al mismo tiempo. Con esta redundancia, siempre debería tener conectividad a su VPC a través de uno de los túneles.

Para los dispositivos Cisco, debe hacer lo siguiente:

- Configurar la interfaz externa.
- Asegurarse de que el número de secuencia de política de Crypto ISAKMP es único.

- Asegurarse de que el número de secuencia de política de Crypto List es único.
- Asegúrese de que el conjunto de IPsec transformación criptográfica y la secuencia de políticas ISAKMP de criptografía estén en armonía con cualquier otro IPsec túnel que esté configurado en el dispositivo.
- Asegurarse de que el número de monitorización de SLA es único.
- Configurar todo el direccionamiento interno que mueve el tráfico entre el dispositivo de gateway de cliente y su red local.

Archivos de configuración de enrutamiento dinámico descargables para el dispositivo de puerta de enlace del AWS Site-to-Site VPN cliente

Para descargar un archivo de configuración de muestra con valores específicos para la configuración de su conexión de Site-to-Site VPN, utilice la consola Amazon VPC, la línea de AWS comandos o la API de Amazon EC2 . Para obtener más información, consulte Paso 6: Descargar el archivo de configuración.

También puede descargar archivos de configuración genéricos de ejemplo para el enrutamiento dinámico que no incluyan valores específicos de la configuración de su conexión Site-to-Site VPN: .zip dynamic-routing-examples

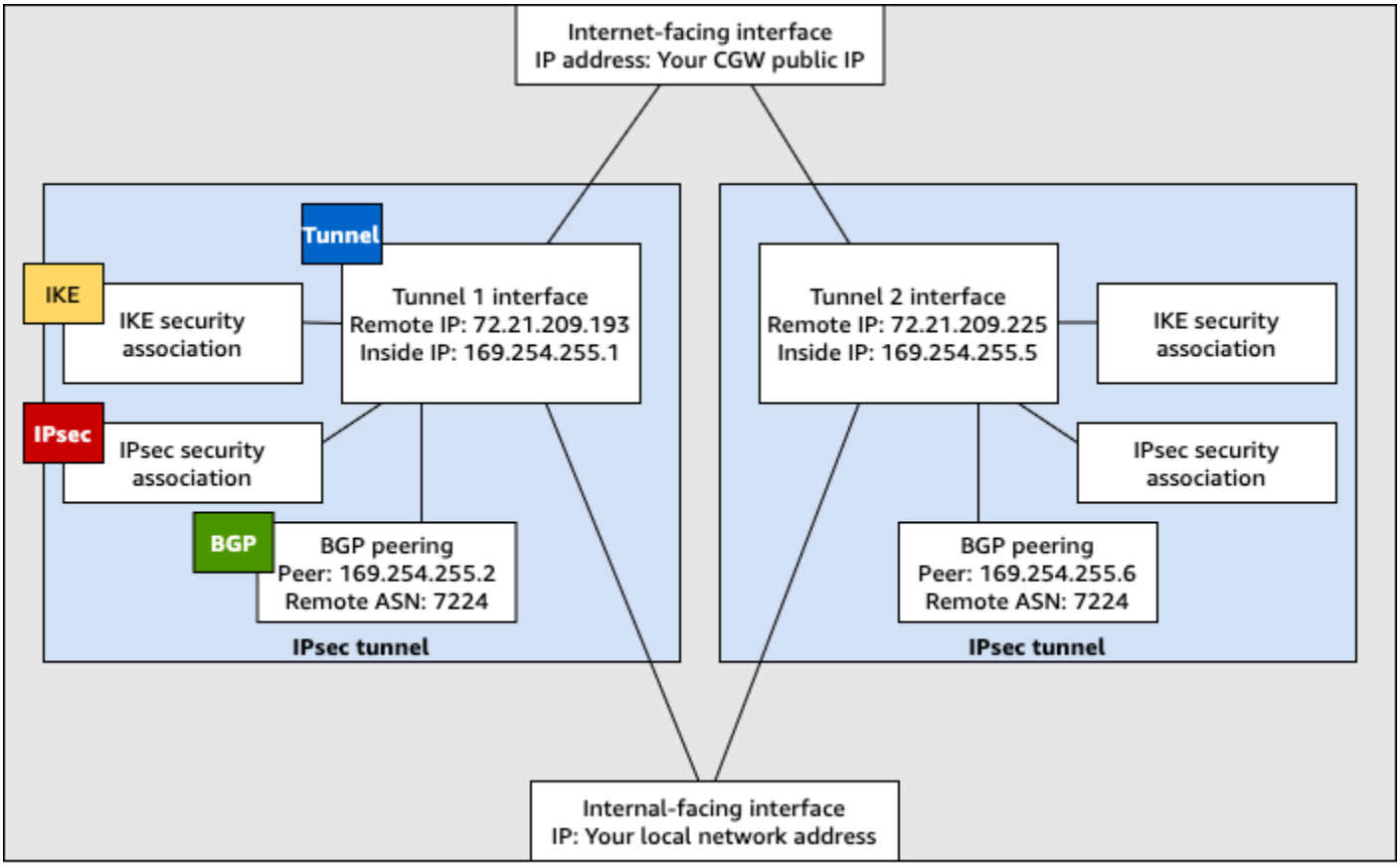
Los archivos utilizan valores de marcadores de posición para algunos componentes. Por ejemplo, usan:

- Valores de ejemplo para el ID de conexión de VPN, el ID de gateway de cliente y el ID de gateway privada virtual
- Marcadores de posición para los AWS puntos finales de la dirección IP remota (externa) (y) *AWS_ENDPOINT_1* *AWS_ENDPOINT_2*
- Un marcador de posición para la dirección IP de la interfaz externa enrutable a Internet del dispositivo de pasarela del cliente () *your-cgw-ip-address*
- Un marcador de posición para el valor clave previamente compartido () pre-shared-key
- Valores de ejemplo de direcciones IP interiores para el túnel.
- Valores de muestra para la configuración de MTU.

> **Note**
>
> La configuración de MTU proporcionada en los archivos de configuración de muestra son solo ejemplos. Consulte Prácticas recomendadas para un dispositivo de puerta de enlace para clientes AWS Site-to-Site VPN para obtener información sobre cómo establecer el valor de MTU óptimo para su situación.

Además de proporcionar valores de marcador de posición, los archivos especifican los requisitos mínimos para una conexión Site-to-Site VPN del grupo 2 de Diffie-Hellman en la mayoría de las regiones y AES128 SHA1, y del grupo 14 de Diffie-Hellman en AWS las regiones. AES128 SHA2 AWS GovCloud También se especifican claves previamente compartidas para la autenticación. Debe modificar el archivo de configuración de ejemplo para aprovechar los algoritmos de seguridad adicionales, los grupos de Diffie-Hellman, los certificados privados y el tráfico. IPv6

En el siguiente diagrama se ofrece una descripción general de los diferentes componentes que se configuran en el dispositivo de gateway de cliente. Incluye valores de ejemplo para las direcciones IP de la interfaz del túnel.



Customer gateway device

Configure el enrutamiento dinámico para un dispositivo de puerta de enlace del cliente AWS Virtual Private Network

A continuación, se presentan algunos procedimientos de ejemplo para configurar un dispositivo de gateway de cliente a través de su interfaz de usuario (si está disponible).

Check Point

Los siguientes son los pasos para configurar un dispositivo Check Point Security Gateway que ejecute la versión R77.10 o superior, mediante el portal web de Gaia y Check Point. SmartDashboard También puede consultar el artículo Amazon Web Services (AWS) VPN BGP en el centro de soporte técnico de Check Point.

Para configurar la interfaz de túnel

El primer paso es crear los túneles de VPN y proporcionar las direcciones IP privadas (internas) de la gateway de cliente y la gateway privada virtual de cada túnel. Para crear el primer túnel, utilice la información proporcionada en la sección `IPSec Tunnel #1` del archivo de

configuración. Para crear el segundo túnel, utilice los valores proporcionados en la sección `IPSec Tunnel #2` del archivo de configuración.

1. Conéctese a su gateway de seguridad a través de SSH. Si va a utilizar el shell no predeterminado, cambie a clish ejecutando el siguiente comando: `clish`.
2. Configure el ASN de la puerta de enlace del cliente (el ASN que se proporcionó cuando se creó la puerta de enlace del cliente en AWS) ejecutando el siguiente comando.

```
set as 65000
```

3. Cree la interfaz del primer túnel utilizando la información que se proporciona en la sección `IPSec Tunnel #1` del archivo de configuración. Especifique un nombre exclusivo para su túnel como, por ejemplo, `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. Repita estos comandos para crear el segundo túnel utilizando la información que se proporciona en la sección `IPSec Tunnel #2` del archivo de configuración. Especifique un nombre exclusivo para su túnel como, por ejemplo, `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. Establezca el ASN de la gateway privada virtual.

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

6. Configure BGP para el primer túnel utilizando la información que se proporciona en la sección `IPSec Tunnel #1` del archivo de configuración.

```
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. Configure BGP para el segundo túnel utilizando la información que se proporciona en la sección `IPSec Tunnel #2` del archivo de configuración.

```
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. Guarde la configuración.

```
save config
```

Para crear una política de BGP

A continuación, cree una política de BGP que permita importar las rutas que anuncia AWS. A continuación, configurará la gateway de cliente para anunciar estas rutas locales a AWS.

1. En Gaia WebUI, elija Advanced Routing, Inbound Route Filters. Elija Add y seleccione Add BGP Policy (Based on AS).
2. En Add BGP Policy (Añadir política de BGP), seleccione un valor entre 512 y 1024 en el primer campo y escriba el ASN de la gateway privada virtual en el segundo campo (por ejemplo, 7224).
3. Seleccione Guardar.

Para anunciar rutas locales

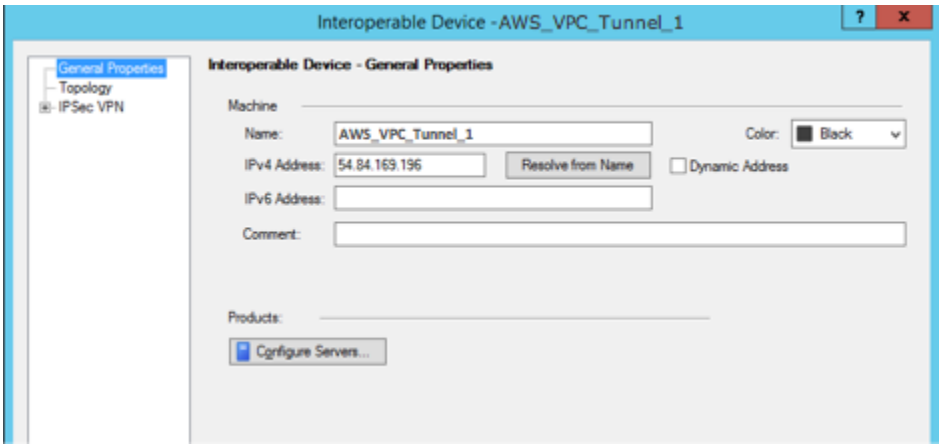
A continuación se presentan los pasos para distribuir rutas de interfaces locales. También puede redistribuir rutas desde distintos orígenes (por ejemplo, rutas estáticas o rutas obtenidas mediante protocolos de direccionamiento dinámico). Para obtener más información, consulte la Gaia Advanced Routing R77 Versions Administration Guide.

1. En Gaia WebUI, elija Advanced Routing, Routing Redistribution. Elija Add Redistribution From (Añadir redistribución desde) y luego seleccione Interface (Interfaz).
2. En To Protocol (A protocolo), seleccione el ASN de la gateway privada virtual (por ejemplo, 7224).
3. En Interface, seleccione una interfaz interna. Seleccione Guardar.

Para definir un nuevo objeto de red

A continuación, cree un objeto de red para cada túnel de VPN, especificando las direcciones IP públicas (externas) de la gateway privada virtual. Más tarde añadirá estos objetos de red como gateways satélite para su comunidad de VPN. También debe crear un grupo vacío para que actúe como marcador de posición para el dominio de VPN.

1. Abra el punto de control. SmartDashboard
2. Para Groups, abra el menú contextual y elija Groups, Simple Group. Puede utilizar el mismo grupo para cada objeto de red.
3. Para Network Objects, abra el menú contextual (clic con el botón derecho) y elija New, Interoperable Device.
4. En Name (Nombre), escriba el nombre que ha proporcionado para el túnel en el paso 1, por ejemplo: `AWS_VPC_Tunnel_1` o `AWS_VPC_Tunnel_2`.
5. En IPv4 Dirección, introduzca la dirección IP externa de la puerta de enlace privada virtual proporcionada en el archivo de configuración, por ejemplo,`54.84.169.196`. Guarde la configuración y cierre el cuadro de diálogo.



6. En el panel de categorías izquierdo, elija Topology.
7. En la sección VPN Domain (Dominio de VPN), elija Manually defined (Definido manualmente), desplácese hasta el grupo sencillo vacío que creó en el paso 2 y selecciónelo. Seleccione OK.
8. Repita estos pasos para crear un segundo objeto de red, utilizando la información de la sección `IPSec Tunnel #2` del archivo de configuración.
9. Vaya a su objeto de red de gateway, abra el objeto de clúster o gateway y elija Topology.

10. En la sección VPN Domain (Dominio de VPN), elija Manually defined (Definido manualmente), desplácese hasta el grupo sencillo vacío que creó en el paso 2 y selecciónelo. Seleccione OK.

> **Note**
>
> Puede conservar cualquier dominio de VPN existente que haya configurado. No obstante, asegúrese de que los hosts y las redes utilizados o servidos por la nueva conexión de VPN no estén declarados en ese dominio de VPN, especialmente si el dominio de VPN se obtiene automáticamente.

> **Note**
>
> Si va a utilizar clústeres, edite la topología y defina las interfaces como interfaces de clúster. Utilice las direcciones IP especificadas en el archivo de configuración.

Para crear y configurar la comunidad VPN, el IKE y los IPsec ajustes

A continuación, cree una comunidad de VPN en su gateway de Check Point, a la que agregará los objetos de red (dispositivos interoperables) para cada túnel. También puede configurar el intercambio de claves de Internet (IKE) y los IPsec ajustes.

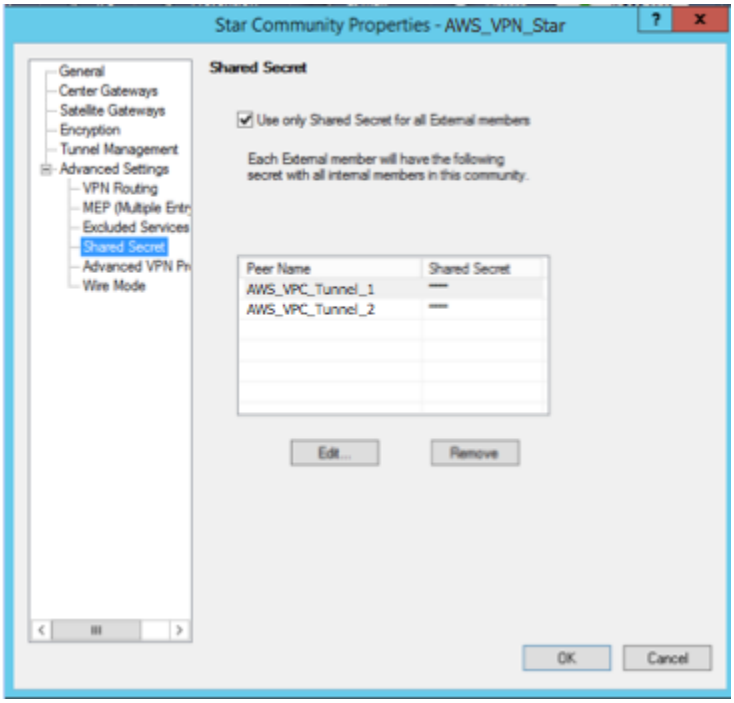
1. En las propiedades de la puerta de enlace, elija IPSecVPN en el panel de categorías.
2. Elija Communities, New, Star Community.
3. Proporcione un nombre para su comunidad (por ejemplo, `AWS_VPN_Star`) y, a continuación, elija Center Gateways en el panel Category.
4. Elija Add y agregue su gateway o clúster a la lista de gateways participantes.
5. En el panel Category (Categoría), elija Satellite Gateways (Gateways satélite), Add (Agregar), y agregue los dispositivos interoperables que creó anteriormente (`AWS_VPC_Tunnel_1` y `AWS_VPC_Tunnel_2`) a la lista de gateways participantes.
6. En el panel Category, elija Encryption. En la sección Método de cifrado, elija IKEv1 para IPv4 y IKEv2 para IPv6. En la sección Encryption Suite, elija Custom, Custom Encryption.

> **Note**
>
> Debe seleccionar la IPv6 opción IKEv1 para IPv4 y IKEv2 para que IKEv1 funcione.

7. En el cuadro de diálogo, configure las propiedades de cifrado tal como se muestra y elija OK (Aceptar) cuando haya terminado:

   - Propiedades de asociación de seguridad de IKE (fase 1):
     - Perform key exchange encryption with: AES-128
     - Perform data integrity with: SHA-1
   - IPsec Propiedades de la asociación de seguridad (fase 2):
     - Realice el cifrado IPsec de datos con: AES-128
     - Perform data integrity with: SHA-1

8. En el panel Category, elija Tunnel Management. Elija Set Permanent Tunnels, On all tunnels in the community. En la sección VPN Tunnel Sharing, elija One VPN tunnel per Gateway pair.
9. En el panel Category, expanda Advanced Settings y elija Shared Secret.
10. Seleccione el nombre homólogo para el primer túnel, elija Edit (Editar) y escriba la clave previamente compartida según lo especificado en la sección `IPSec Tunnel #1` del archivo de configuración.
11. Seleccione el nombre homólogo para el segundo túnel, elija Edit (Editar) y escriba la clave previamente compartida según lo especificado en la sección `IPSec Tunnel #2` del archivo de configuración.



12. Aún en la categoría Advanced Settings (Configuración avanzada), elija Advanced VPN Properties (Propiedades avanzadas de VPN), configure las propiedades según se indica y elija OK (Aceptar) cuando haya terminado:

    - IKE (fase 1):
        - Use Diffie-Hellman group (Usar el grupo Diffie-Hellman): `Group 2 (1024 bit)`
        - Renegotiate IKE security associations every `480` minutes
    - IPsec (Fase 2):
        - Elija Use Perfect Forward Secrecy
        - Use Diffie-Hellman group (Usar el grupo Diffie-Hellman): `Group 2 (1024 bit)`
        - Renegocie las asociaciones de IPsec seguridad cada segundo **`3600`**

Para crear reglas de firewall

A continuación, configurará una política con reglas de firewall y reglas de coincidencia direccional que permitan la comunicación entre la VPC y la red local. Luego instalará la política en su gateway.

1. En el SmartDashboard, elija Propiedades globales para su puerta de enlace. En el panel Category, expanda VPN y elija Advanced.
2. Elija Enable VPN Directional Match in VPN Column y elija OK.

3. En el SmartDashboard, elija Firewall y cree una política con las siguientes reglas:
   - Permitir que la subred de VPC se comunique con la red local a través de los protocolos necesarios.
   - Permitir que la red local se comunique con la subred de VPC a través de los protocolos necesarios.
4. Abra el menú contextual para la celda de la columna de VPN, y elija Edit Cell.
5. En el cuadro de diálogo VPN Match Conditions, elija Match traffic in this direction only. Cree las siguientes reglas de coincidencia direccional; para ello, elija Add (Agregar) para cada una y seleccione OK (Aceptar) cuando haya terminado:
   - `internal_clear` > VPN community (Comunidad VPN) (la comunidad Star de VPN que creó antes; por ejemplo: `AWS_VPN_Star`)
   - VPN community > VPN community
   - Comunidad VPN > `internal_clear`
6. En el SmartDashboard, selecciona Política e instala.
7. En el cuadro de diálogo, elija su gateway y seleccione OK para instalar la política.

Para modificar la propiedad tunnel_keepalive_method

Su gateway de Check Point puede utilizar la detección de pares muertos (DPD) para identificar cuándo se desactiva una asociación de IKE. Para configurar DPD para un túnel permanente, el túnel permanente debe configurarse en la comunidad de AWS VPN.

De forma predeterminada, la propiedad `tunnel_keepalive_method` de una gateway de VPN está configurada como `tunnel_test`. Debe cambiar el valor a `dpd`. Cada gateway de VPN de la comunidad de VPN que requiera monitorización de DPD debe configurarse con la propiedad `tunnel_keepalive_method`, incluida cualquier gateway de VPN de terceros. No puede configurar mecanismos de monitorización distintos para la misma gateway.

Puede actualizar la `tunnel_keepalive_method` propiedad mediante la DBedit herramienta GUI.

1. Abra el Check Point SmartDashboard y elija Security Management Server, Domain Management Server.
2. Elija File, Database Revision Control..., y cree una instantánea de revisión.

3. Cierre todas las SmartConsole ventanas, como el SmartDashboard SmartView Rastreador y el SmartView Monitor.
4. Inicie la BDedit herramienta GUI. Para obtener más información, consulte el artículo Check Point Database Tool, en el centro de soporte técnico de Check Point.
5. Elija Security Management Server, Domain Management Server.
6. En el panel superior izquierdo, elija Table, Network Objects, network_objects.
7. En el panel superior derecho, seleccione el objeto de Security Gateway, Cluster correspondiente.
8. Presione CTRL+F, o utilice el menú Search para buscar lo siguiente: `tunnel_keepalive_method`.
9. En el panel inferior, abra el menú contextual de `tunnel_keepalive_method` y seleccione Edit... Elija dpd, OK (Aceptar).
10. Repita los pasos del 7 al 9 por cada gateway que forme parte de la comunidad de AWS VPN.
11. Elija File, Save All.
12. Cierre la DBedit herramienta Gui.
13. Abra el Check Point SmartDashboard y elija Security Management Server, Domain Management Server.
14. Instale la política en el objeto Security Gateway, Cluster correspondiente.

Para obtener más información, consulte el artículo New VPN features in R77.10, en el centro de soporte técnico de Check Point.

Para habilitar el bloqueo TCP MSS

El bloqueo de TCP MSS reduce el tamaño máximo de segmento de los paquetes TCP para evitar la fragmentación de los paquetes.

1. Vaya al siguiente directorio: `C:\Program Files (x86)\CheckPoint\SmartConsole\R77.10\PROGRAM\`.
2. Abra la herramienta Check Point Database ejecutando el archivo `GuiDBEdit.exe`.
3. Elija Table, Global Properties, properties.
4. Para `fw_clamp_tcp_mss`, elija Edit. Cambie el valor a `true` y luego elija OK (Aceptar).

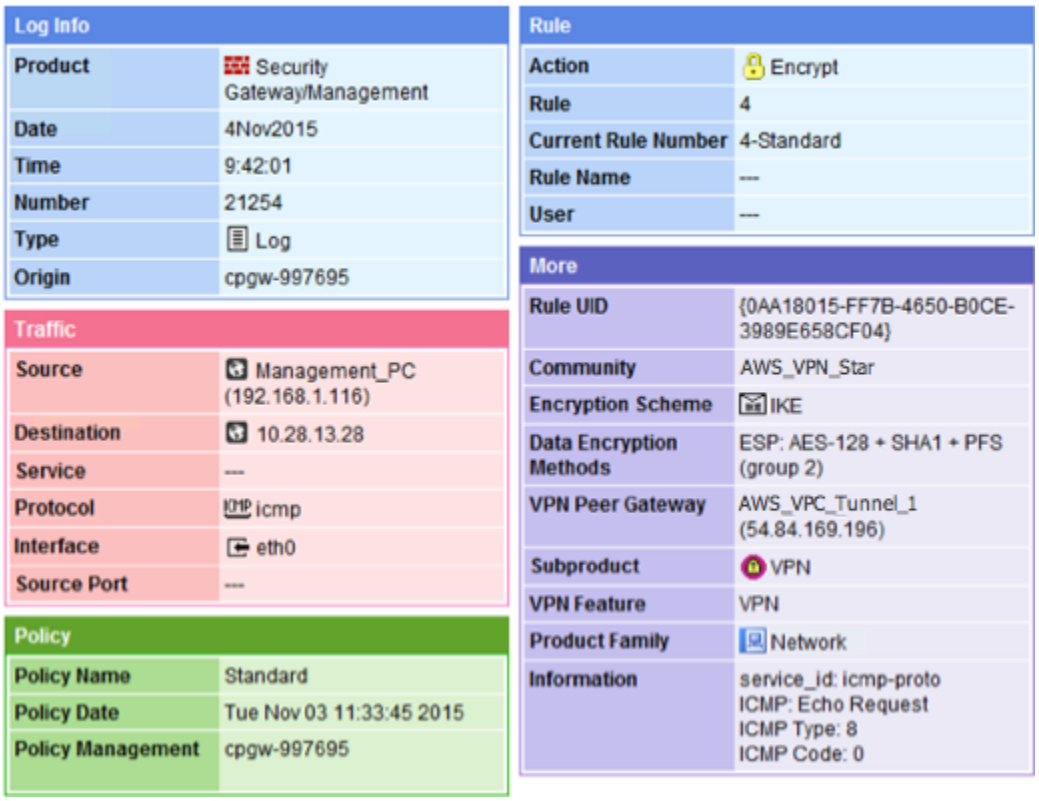
Para verificar el estado del túnel

Puede verificar el estado del túnel ejecutando el siguiente comando desde la herramienta de línea de comandos en el modo experto.

```
vpn tunnelutil
```

En las opciones que aparecen, elija 1 para comprobar las asociaciones IKE y 2 para comprobar las IPsec asociaciones.

También puede utilizar Check Point Smart Tracker Log para verificar que los paquetes de la conexión se están cifrando. Por ejemplo, el siguiente log indica que un paquete para la VPC se ha enviado a través del túnel 1 y se ha cifrado.



SonicWALL

Puede configurar el dispositivo SonicWALL mediante la interfaz de administración de SonicOS. Para obtener más información sobre la configuración de los túneles, consulte Configuración del enrutamiento estático para un dispositivo de puerta de enlace de cliente de AWS Site-to-Site VPN.

Sin embargo, no es posible configurar BGP para el dispositivo utilizando la interfaz de administración. En su lugar, utilice las instrucciones de la línea de comandos que se ofrecen en el archivo de configuración de ejemplo, en la sección BGP.

Dispositivos Cisco: información adicional

Algunos Cisco ASAs solo admiten el modo activo/en espera. Cuando utiliza estos dispositivos Cisco ASAs, solo puede tener un túnel activo a la vez. El otro túnel en espera se activará si el primer túnel se vuelve no disponible. Con esta redundancia, siempre debería tener conectividad a su VPC a través de uno de los túneles.

ASAs A partir de la versión 9.7.1 y posteriores, Cisco admite el modo activo/activo. Al utilizar estos dispositivos Cisco ASAs, puede tener ambos túneles activos al mismo tiempo. Con esta redundancia, siempre debería tener conectividad a su VPC a través de uno de los túneles.

Para los dispositivos Cisco, debe hacer lo siguiente:

- Configurar la interfaz externa.
- Asegurarse de que el número de secuencia de política de Crypto ISAKMP es único.
- Asegurarse de que el número de secuencia de política de Crypto List es único.
- Asegúrese de que el conjunto de IPsec transformación criptográfica y la secuencia de políticas ISAKMP de criptografía estén en armonía con cualquier otro IPsec túnel que esté configurado en el dispositivo.
- Asegurarse de que el número de monitorización de SLA es único.
- Configurar todo el direccionamiento interno que mueve el tráfico entre el dispositivo de gateway de cliente y su red local.

Dispositivos Juniper: información adicional

La siguiente información se aplica a los archivos de configuración de ejemplo para dispositivos de gateway de cliente SRX y Juniper J-Series.

- La interfaz exterior se denomina. *ge-0/0/0.0*
- La interfaz del túnel IDs se denomina *st0.1* y*st0.2*.
- Asegúrese de identificar la zona de seguridad para la interfaz del enlace de subida (la información de configuración utiliza la zona predeterminada "poco fiable").
- Asegúrese de identificar la zona de seguridad para la interfaz interior (la información de configuración utiliza la zona predeterminada "de confianza").

Configurar Windows Server como dispositivo de puerta de enlace para AWS Site-to-Site VPN clientes

Puede configurar el servidor que ejecute Windows Server como dispositivo de gateway de cliente para la VPC. Utilice el siguiente proceso tanto si ejecuta Windows Server en una EC2 instancia de una VPC como en su propio servidor. Los siguientes procedimientos se aplican a Windows Server 2012 R2 y versiones posteriores.

Contenido

Configuración de instancias de Windows

Si está configurando Windows Server en una EC2 instancia que lanzó desde una AMI de Windows, haga lo siguiente:

- Deshabilite la comprobación de origen/destino para la instancia:
  1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
  2. Seleccione la instancia de Windows y elija Actions (Acciones), Networking (Redes), Change source/destination check (Cambiar comprobación de origen o destino). Elija Stop (Detener)y, a continuación, seleccione Save (Guardar).
- Actualice la configuración del adaptador para poder direccionar el tráfico procedente de otras instancias:
  1. Conéctese a la instancia de Windows. Para obtener más información, consulte Conexión con la instancia de Windows.
  2. Abra el Panel de control e inicie el Administrador de dispositivos.
  3. Expanda el nodo Adaptadores de red.

4. Seleccione el adaptador de red (según el tipo de instancia, puede ser Amazon Elastic Network Adapter o Intel 82599 Virtual Function) y elija Action (Acción), Properties (Propiedades).
5. En la pestaña Avanzadas, desactive las propiedades IPv4Checksum Offload, TCP Checksum Offload (IPv4) y UDP Checksum Offload () y, a continuación, pulse Aceptar. IPv4

- Asigne una dirección IP elástica a su cuenta y asóciela a la instancia. Para obtener más información, consulte Direcciones IP elásticas en la Guía del EC2 usuario de Amazon. Tome nota de esta dirección: la necesitará al crear la pasarela de clientes.
- Asegúrese de que las reglas del grupo de seguridad de la instancia permitan el IPsec tráfico saliente. De forma predeterminada, un grupo de seguridad permite todo el tráfico saliente. Sin embargo, si las reglas de salida del grupo de seguridad se han modificado con respecto a su estado original, debe crear las siguientes reglas de protocolo de salida personalizadas para el IPsec tráfico: protocolo IP 50, protocolo IP 51 y UDP 500.

Tome nota del intervalo CIDR de la red en la que se encuentra la instancia de Windows, por ejemplo, `172.31.0.0/16`.

Paso 1: Crear una conexión de VPN y configurar la VPC

Para crear una conexión VPN desde la VPC, haga lo siguiente:

1. Cree una gateway privada virtual y conéctela a su VPC. Para obtener más información, consulte Creación de una gateway privada virtual.
2. A continuación, cree una conexión de VPN y una nueva gateway para cliente. Para la gateway de cliente, especifique la dirección IP pública del servidor de Windows. Para la conexión de VPN, elija el direccionamiento estático y, a continuación, escriba el intervalo de CIDR de la red en la que se encuentra el servidor de Windows, por ejemplo, `172.31.0.0/16`. Para obtener más información, consulte Paso 5: Crear una conexión de VPN.

Después de crear la conexión VPN, configure la VPC para habilitar la comunicación a través de la conexión VPN.

Para configurar la VPC

- Cree una subred privada en la VPC (en caso de que no disponga de ninguna) para lanzar instancias que se comunicarán con el servidor de Windows. Para obtener más información, consulte Creación de una subred en la VPC.

> **Note**
>
> La subred privada es una subred que no dispone de una ruta a ninguna gateway de Internet. El direccionamiento de esta subred se describe en la sección siguiente.

- Actualice las tablas de ruteo de la conexión de VPN:
  - Agregue una ruta a la tabla de rutas de la subred privada con la gateway privada virtual como destino y la red del servidor de Windows (intervalo CIDR) como destino. Para obtener más información, consulte Agregar y eliminar rutas de una tabla de rutas en la Guía del usuario de Amazon VPC.
  - Habilite la propagación de rutas para la gateway privada virtual. Para obtener más información, consulte (Gateway privada virtual) Habilitar la propagación de rutas en la tabla de enrutamiento.
- Cree un grupo de seguridad para las instancias que permita la comunicación entre la VPC y la red:
  - Añada reglas que permitan el acceso a SSH o RDP entrante desde su red. Esto le permitirá conectarse a instancias de su VPC desde la red. Por ejemplo, para permitir a los equipos de la red obtener acceso a instancias de Linux de su VPC, cree una regla entrante del tipo SSH y establezca el origine en el rango de CIDR de su red (por ejemplo, `172.31.0.0/16`). Para obtener más información, consulte Grupos de seguridad de su VPC en la Guía del usuario de Amazon VPC.
  - Añada una regla que permita el acceso a ICMP entrante desde su red. Esto permite probar la conexión VPN al hacer ping a una instancia de la VPC desde el servidor de Windows.

Paso 2: Descargar el archivo de configuración de la conexión de VPN

Puede utilizar la consola de Amazon VPC a fin de descargar un archivo de configuración de servidor de Windows para la conexión de VPN.

Cómo descargar el archivo de configuración

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Site-to-Site VPN Connections.
3. Seleccione su conexión de VPN y elija Download Configuration (Descargar configuración).
4. Seleccione Microsoft como proveedor, Windows Server como plataforma y 2012 R2 como software. Elija Descargar. Puede abrir el archivo o guardarlo.

El archivo de configuración contiene una sección de información similar al siguiente ejemplo. Verá que esta información se muestra dos veces, una para cada túnel.

```
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`

La dirección IP que especificó para la gateway del cliente al crear la conexión de VPN.

`Remote Tunnel Endpoint`

Una de las dos direcciones IP de la puerta de enlace privada virtual que termina la conexión VPN en el AWS lateral de la conexión.

`Endpoint 1`

El prefijo de IP que especificó como ruta estática al crear la conexión de VPN. Estas son las direcciones IP de su red que pueden utilizar la conexión de VPN para obtener acceso a su VPC.

`Endpoint 2`

Rango de direcciones IP (bloque de CIDR) de la VPC asociada a la gateway privada virtual (por ejemplo 10.0.0.0/16).

`Preshared key`

La clave previamente compartida que se utiliza para establecer la conexión IPsec VPN entre y`Local Tunnel Endpoint`. `Remote Tunnel Endpoint`

Se recomienda que configure ambos túneles como parte de la conexión de VPN. Cada túnel se conecta a un concentrador de VPN independiente en Amazon de la conexión de VPN. Aunque solo haya un túnel activo cada vez, el segundo túnel se establece automáticamente si el primero se desactiva. Tener túneles redundantes garantiza disponibilidad continua en caso de un error del dispositivo. Puesto que solo hay disponible un túnel cada vez, la consola de Amazon VPC indica que hay un túnel inactivo. Este es el comportamiento esperado, de modo que no necesita realizar ninguna acción.

Con dos túneles configurados, si se produce un fallo en un dispositivo interno AWS, la conexión VPN pasa automáticamente al segundo túnel de la puerta de enlace privada virtual en cuestión de minutos. Al configurar su dispositivo de gateway de cliente, es importante que configure ambos túneles.

> **Note**
>
> De vez en cuando, AWS realiza tareas de mantenimiento rutinarias en la puerta de enlace privada virtual. Este mantenimiento podría deshabilitar uno de los dos túneles de su conexión de VPN durante un breve periodo. Cuando esto ocurra, su conexión de VPN cambiará automáticamente al segundo túnel mientras duren las tareas de mantenimiento.

En el archivo de configuración descargado se presenta información adicional sobre el intercambio de claves de Internet (IKE) y las asociaciones de IPsec seguridad (SA).

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

`MainModeSecMethods`

Algoritmos de cifrado y autenticación para IKE SA. Estas son las configuraciones sugeridas para la conexión VPN y son las configuraciones predeterminadas para las conexiones IPsec VPN de Windows Server.

`MainModeKeyLifetime`

Vida útil de la clave de IKE SA. Esta es la configuración sugerida para la conexión VPN y es la configuración predeterminada para las conexiones IPsec VPN de Windows Server.

`QuickModeSecMethods`

Los algoritmos de cifrado y autenticación de la IPsec SA. Estas son las configuraciones sugeridas para la conexión VPN y son las configuraciones predeterminadas para las conexiones IPsec VPN de Windows Server.

`QuickModePFS`

Le sugerimos que utilice la clave maestra Perfect Forward Secret (PFS) para sus IPsec sesiones.

Paso 3: Configuración de Windows Server

Antes de configurar el túnel VPN, debe instalar y configurar los servicios de direccionamiento y acceso remoto en el servidor de Windows. De esta forma, los usuarios remotos podrán obtener acceso a los recursos de su red.

Para instalar servicios de direccionamiento y acceso remoto

1. Inicie sesión en su servidor de Windows.
2. Vaya al menú Inicio y elija Administrador del servidor.
3. Instale los servicios de acceso remoto y direccionamiento:
    a. Desde el menú Administrar, elija Agregar roles y características.
    b. En la página Antes de comenzar, asegúrese de que su servidor cumple todos los requisitos previos. A continuación, elija Siguiente.
    c. Elija Instalación basada en características o en roles y, a continuación, elija Siguiente.
    d. Elija Select a server from the server pool (Seleccionar un servidor del grupo de servidores), seleccione el servidor de Windows y, a continuación, elija Next (Siguiente).
    e. Seleccione Servicios de acceso y directivas de redes en la lista. En el cuadro de diálogo que aparecerá, elija Agregar características para confirmar las características necesarias para esta función.
    f. En la misma lista, elija Acceso remoto y elija Siguiente.
    g. En la página Seleccionar características, elija Siguiente.
    h. En la página Servicios de acceso y directivas de redes, elija Siguiente.
    i. En la página Acceso remoto, elija Siguiente. En la página siguiente, selecciona DirectAccess una VPN (RAS). En el cuadro de diálogo que aparecerá, elija Agregar características para confirmar las características necesarias para este servicio de función. En la misma lista, elija Enrutamiento y, a continuación, elija Siguiente.
    j. En la página Rol de servidor web (IIS), elija Siguiente. Deje la selección predeterminada y elija Siguiente.
    k. Elija Instalar. Cuando finalice la instalación, elija Cerrar.

Para configurar y habilitar el servidor de enrutamiento y acceso remoto

1. En el panel, elija Notificaciones (icono con la marca). Debería haber una tarea para completar la configuración posterior a la implementación. Elija el enlace Abrir el Asistente para introducción.
2. Elija Implementar solo VPN.
3. En el cuadro de diálogo Enrutamiento y acceso remoto, elija el nombre del servidor, elija Acción y luego seleccione Configurar y habilitar Enrutamiento y acceso remoto.
4. En el Asistente para instalación del servidor de enrutamiento y acceso remoto, en la primera página, elija Siguiente.
5. En la página Configuración, elija Configuración personalizada y Siguiente.
6. Elija Enrutamiento LAN, Siguiente y Finalizar.
7. Cuando lo solicite el cuadro de diálogo Enrutamiento y acceso remoto, elija Iniciar servicio.

Paso 4: Configurar el túnel de VPN

Puede configurar el túnel VPN al ejecutar los scripts netsh incluidos en el archivo de configuración descargado o mediante la interfaz de usuario del servidor de Windows.

> **Important**
>
> Le sugerimos que utilice la clave maestra Perfect Forward Secret (PFS) para sus IPsec sesiones. Si decide ejecutar el script netsh, incluye un parámetro para habilitar PFS (). `qmpfs=dhgroup2` No puede habilitar PFS mediante la interfaz de usuario de Windows; debe hacerlo mediante la línea de comandos.

Opciones

- Opción 1: ejecutar el script netsh
- Opción 2: utilizar la interfaz de usuario del servidor de Windows

Opción 1: ejecutar el script netsh

Copie el script netsh del archivo de configuración descargado y reemplace las variables. A continuación se muestra un ejemplo 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: puede sustituir el nombre recomendado (`vgw-1a2b3c4d Tunnel 1`) por el nombre que prefiera.

LocalTunnelEndpoint: Introduzca la dirección IP privada del servidor Windows de la red.

Endpoint1: el bloque de CIDR de la red en la que reside el servidor de Windows. Por ejemplo, `172.31.0.0/16`. Rodee este valor con comillas dobles (“).

Endpoint2: bloque de CIDR de su VPC o subred de su VPC. Por ejemplo, `10.0.0.0/16`. Rodee este valor con comillas dobles (“).

Ejecute el script actualizado en una ventana de símbolo del sistema en el servidor de Windows. (El signo ^ le permite cortar y pegar texto incluido en la línea de comandos). Para configurar el segundo túnel de VPN para esta conexión de VPN, repita el proceso utilizando el script netsh en el archivo de configuración.

Cuando haya terminado, vaya a Configurar el firewall de Windows.

Para obtener más información acerca de los parámetros netsh, consulte Comandos Netsh AdvFirewall Consec en la biblioteca de Microsoft. TechNet

Opción 2: utilizar la interfaz de usuario del servidor de Windows

También puede utilizar la interfaz de usuario del servidor de Windows para configurar el túnel de VPN.

> **Important**
>
> No puede habilitar la confidencialidad directa total (PFS) de clave maestra desde la interfaz de usuario del servidor de Windows. PFS debe habilitarse con la línea de comandos, tal como se describe en Habilitación de la confidencialidad directa total (PFS) de clave maestra.

Tareas

- Configurar una regla de seguridad para un túnel VPN
- Confirmar la configuración del túnel
- Habilitación de la confidencialidad directa total (PFS) de clave maestra
- Configurar el firewall de Windows

Configurar una regla de seguridad para un túnel VPN

En esta sección, configure una regla de seguridad en el servidor de Windows para crear un túnel VPN.

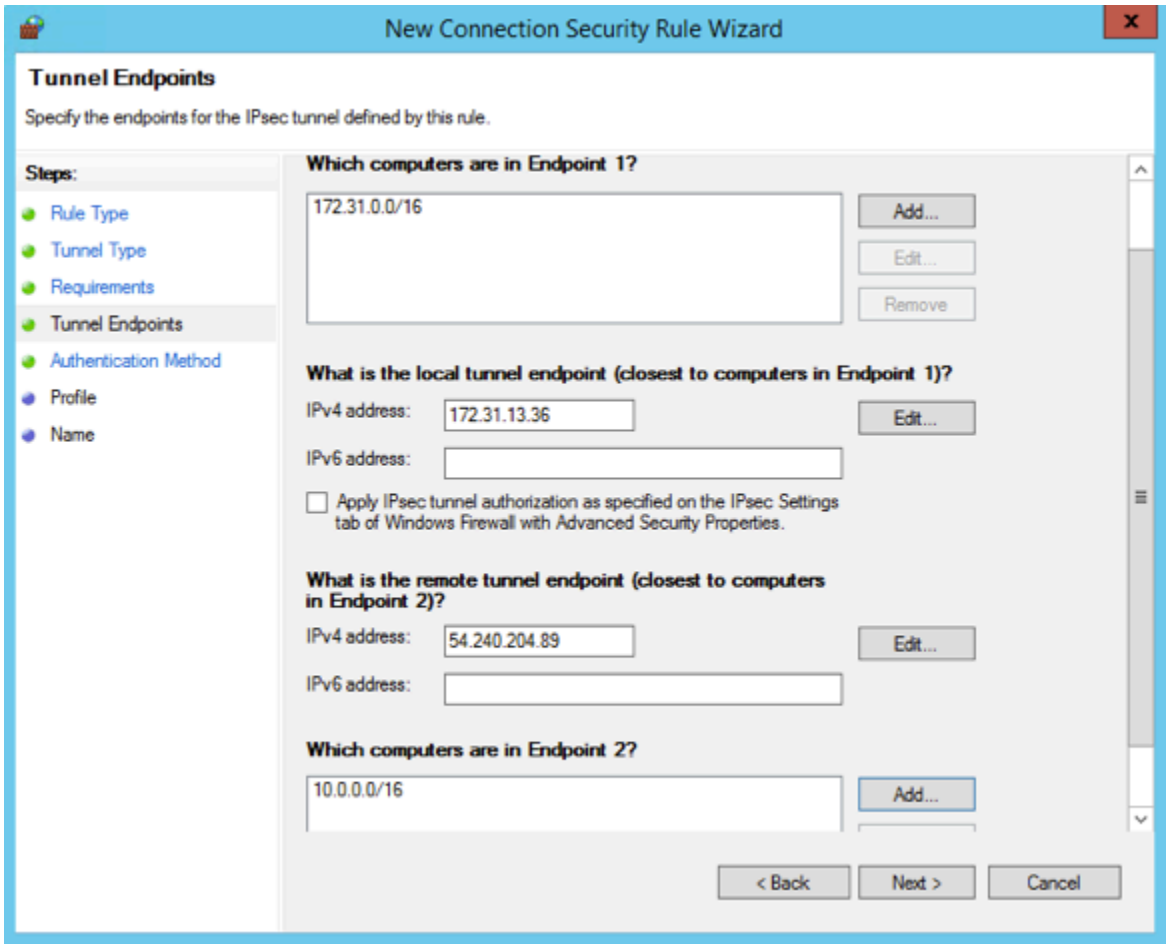
Para configurar una regla de seguridad para un túnel de VPN

1. Abra el administrador del servidor, elija Tools (Herramientas)y, a continuación, seleccione Windows Defender Firewall with Advanced Security (Firewall de Windows Defender con seguridad avanzada).
2. Seleccione Reglas de seguridad de conexión, elija Acción y, a continuación, Nueva regla.
3. En el Asistente para nueva regla de seguridad de conexión, en la página Tipo de regla, elija Túnel y, a continuación, elija Siguiente.
4. En la página Tipo de túnel, en ¿Qué tipo de túnel desea crear?, elija Configuración personalizada. En ¿Desea eximir de este túnel a las conexiones IPsec protegidas?, deje el valor predeterminado marcado (No). Envía todo el tráfico de red que coincida con esta regla de seguridad de conexión (a través del túnel) y, a continuación, selecciona Siguiente.
5. En la página Requisitos, elija Requerir autenticación para las conexiones entrantes. No establezca túneles para las conexiones salientes y, a continuación, elija Siguiente.
6. En la página Extremos de túnel, en ¿Qué equipos están en el Extremo 1?, elija Agregar. Escriba el intervalo de CIDR de la red (detrás del dispositivo de gateway de cliente del servidor de Windows, por ejemplo `172.31.0.0/16`) y, a continuación, seleccione OK (Aceptar). El intervalo puede incluir la dirección IP de su dispositivo de gateway de cliente.
7. En ¿Cuál es el extremo de túnel local (más cercano a los equipos del Extremo 1)?, elija Editar. En el campo de IPv4 dirección, introduce la dirección IP privada de tu servidor Windows y, a continuación, selecciona Aceptar.
8. En ¿Cuál es el extremo de túnel remoto (más cercano a los equipos del Extremo 2)?, elija Editar. En el campo de IPv4 dirección, introduzca la dirección IP de la puerta de enlace privada virtual para el túnel 1 del archivo de configuración (consulte`Remote Tunnel Endpoint`) y, a continuación, pulse Aceptar.

> **Important**
>
> Si va a repetir este procedimiento para el Túnel 2, asegúrese de seleccionar el punto de conexión para el Túnel 2.

9. En ¿Qué equipos están en el Extremo 2?, elija Agregar. En el campo Esta dirección IP o subred:, escriba el bloque de CIDR de su VPC y, a continuación, elija Aceptar.

> **Important**
>
> Debe desplazarse por el cuadro de diálogo hasta encontrar ¿Qué equipos están en el Extremo 2?. No elija Siguiente hasta que no haya completado este paso, ya que, de lo contrario, no podrá conectarse a su servidor.



10. Asegúrese de que todos los parámetros especificados son correctos. A continuación, elija Siguiente.
11. En la página Método de autenticación, seleccione Avanzado y elija Personalizar.
12. En Métodos de primera autenticación, elija Agregar.
13. Seleccione Clave previamente compartida, escriba el valor de la clave previamente compartida del archivo de configuración y luego elija Aceptar.

    > **Important**
    >
    > Si va a repetir este procedimiento para el Túnel 2, asegúrese de seleccionar la clave previamente compartida para el Túnel 2.

14. Asegúrese de que la opción La primera autenticación es opcional no esté seleccionada y, a continuación, elija Aceptar.
15. Elija Next (Siguiente).
16. En la página Perfil, active las tres casillas de verificación: Dominio, Privado y Público. Elija Next (Siguiente).
17. En la página Nombre, escriba un nombre para la regla de conexión, por ejemplo, `VPN to Tunnel 1` y, a continuación, elija Finalizar.

Repita el procedimiento anterior, especificando los datos para el túnel 2 de su archivo de configuración.

Una vez que haya terminado, tendrá dos túneles configurados para su conexión de VPN.

Confirmar la configuración del túnel

Para confirmar la configuración del túnel

1. Abra Administrador del servidor, elija Herramientas, seleccione Firewall de Windows con seguridad avanzada y, a continuación, seleccione Reglas de seguridad de conexión.
2. Realice las comprobaciones siguientes para ambos túneles:

   - Habilitado está configurado con el valor `Yes`.
   - Extremo 1 corresponde con el bloque de CIDR de su red.
   - Extremo 2 corresponde con el bloque de CIDR de su VPC.

- El modo de autenticación está configurado con el valor `Require inbound and clear outbound`.
- Método de autenticación está configurado como `Custom`.
- Puerto de extremo 1 es `Any`.
- Puerto de extremo 2 es `Any`.
- Protocolo es `Any`.

3. Seleccione la primera regla y elija Propiedades.
4. En la pestaña Autenticación, en Método, elija Personalizar. Compruebe que el campo Métodos de primera autenticación contiene la clave previamente compartida correcta del archivo de configuración para el túnel y, a continuación, elija Aceptar.
5. En la pestaña Avanzado, asegúrese de que las opciones Dominio, Privado y Público estén seleccionadas.
6. En la sección de IPsec tunelización, elija Personalizar. Compruebe la siguiente configuración de IPsec tunelización y, a continuación, pulse Aceptar y volver a pulsar Aceptar para cerrar el cuadro de diálogo.

   - Está seleccionada la opción Utilizar IPsec tunelización.
   - El punto de enlace del túnel local (más cercano al punto de enlace 1) contiene la dirección IP del servidor de Windows. Si el dispositivo de puerta de enlace del cliente es una EC2 instancia, esta es la dirección IP privada de la instancia.
   - Extremo de túnel remoto (más cercano al Extremo 2) contiene la dirección IP de la gateway privada virtual de este túnel.

7. Abra las propiedades del segundo túnel. Repita los pasos del 4 al 7 para este túnel.

Habilitación de la confidencialidad directa total (PFS) de clave maestra

La confidencialidad directa total (PFS) de clave maestra se puede habilitar mediante la línea de comandos. Esta característica no puede habilitarse desde la interfaz de usuario.

Para habilitar la confidencialidad directa total de clave maestra

1. En el servidor de Windows, abra una nueva ventana del símbolo del sistema.
2. Introduzca el comando siguiente sustituyendo `rule_name` por el nombre que asignó en la primera regla de conexión.

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

3. Repta el paso 2 para el segundo túnel. Esta vez, sustituya `rule_name` por el nombre que asignó a la segunda regla de conexión.

Configurar el firewall de Windows

Tras configurar las reglas de seguridad en el servidor, configure algunos IPsec ajustes básicos para que funcionen con la puerta de enlace privada virtual.

Para configurar el firewall de Windows

1. Abra el administrador del servidor, elija Tools (Herramientas), seleccione Windows Defender Firewall with Advanced Security (Firewall de Windows Defender con seguridad avanzada)y, a continuación, elija Properties (Propiedades).
2. En la pestaña IPsec Configuración, en la sección de IPsecexenciones, compruebe que Exentar ICMP de IPsec es No (opción predeterminada). Compruebe que la autorización IPsec del túnel sea Ninguna.
3. En IPsec los valores predeterminados, elija Personalizar.
4. En Intercambio de claves (modo principal), seleccione Avanzado y, a continuación, elija Personalizar.
5. En Personalizar configuración avanzada de intercambio de claves, en Métodos de seguridad, asegúrese de que se utilizan los siguientes valores predeterminados para la primera entrada:

   - Integridad: SHA-1
   - Cifrado: AES-CBC 128
   - Algoritmo de intercambio de claves: Grupo Diffie-Hellman 2
   - En Duración de la clave, asegúrese de que Minutos tenga el valor `480` y de que Sesiones tenga el valor `0`.

   Estos valores corresponden a estas entradas en el archivo de configuración.

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

6. En Opciones de intercambio de claves, seleccione Usar Diffie-Hellman para mayor seguridad y, a continuación, elija Aceptar.
7. En Protección de datos (modo rápido), seleccione Avanzado y, a continuación, elija Personalizar.
8. Seleccione Requerir cifrado para todas las reglas de seguridad de conexión que usan esta configuración.
9. En Integridad y cifrado de datos, deje los valores predeterminados:

   - Protocolo: ESP
   - Integridad: SHA-1
   - Cifrado: AES-CBC 128
   - Vigencia: 60 minutos

   Estos valores corresponden a la entrada del archivo de configuración que se muestra a continuación.

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

10. Pulse Aceptar para volver al cuadro de diálogo Personalizar IPsec ajustes y pulse Aceptar de nuevo para guardar la configuración.

Paso 5: Habilitar la detección de gateways inactivas

A continuación, configure TCP para detectar cuándo una gateway deja de estar disponible. Para ello, modifique la siguiente clave de registro: `HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters`. No realice este paso hasta no haber completado las secciones anteriores. Después de cambiar la clave de registro, deberá reiniciar el servidor.

Para habilitar la detección de gateways inactivas

1. Desde su servidor Windows, inicie la línea de comandos o una PowerShell sesión e introduzca regedit para iniciar el Editor del Registro.
2. Expanda HKEY_LOCAL_MACHINE, expanda SYSTEM, expanda, expanda Servicios, expanda CurrentControlSetTcpip y, después, expanda Parámetros.
3. Desde el menú Editar, seleccione Nuevo y seleccione Valor de DWORD (32 bits).

4. Introduzca el nombre EnableDeadGWDetect.
5. Seleccione y elija Editar, Modificar. EnableDeadGWDetect
6. En Información del valor, escriba 1 y, a continuación, elija Aceptar.
7. Cierre el Editor del Registro y reinicie el servidor.

Para obtener más información, consulte EnableDeadGWDetecten la TechNetBiblioteca de Microsoft.

Paso 6: Comprobar la conexión de VPN

Para comprobar que la conexión de VPN está funcionando correctamente, lance una instancia en su VPC y asegúrese de que no tiene conexión a Internet. Después de lanzar la instancia, haga ping a la dirección IP privada desde el servidor de Windows. El túnel VPN aparece cuando se genera tráfico desde el dispositivo de gateway de cliente. Por lo tanto, el comando ping también inicia la conexión de VPN.

Si desea ver los pasos para probar la conexión de VPN, consulte Probar una AWS Site-to-Site VPN conexión.

En caso de error en el comando `ping`, compruebe la información siguiente:

- Asegúrese de haber configurado las reglas de su grupo de seguridad para que permitan ICMP en la instancia de su VPC. Si su Windows Server es una EC2 instancia, asegúrese de que las reglas de salida de su grupo de seguridad permitan IPsec el tráfico. Para obtener más información, consulte Configuración de instancias de Windows.
- Asegúrese de que el sistema operativo de la instancia en la que está haciendo ping esté configurado para responder a ICMP. Le recomendamos que utilice uno de los sistemas Amazon Linux AMIs.
- Si la instancia a la que está haciendo ping es una instancia de Windows, conéctese a la instancia y habilite la entrada ICMPv4 en el firewall de Windows.
- Asegúrese de haber configurado las tablas de ruteo correctamente para su VPC o su subred. Para obtener más información, consulte Paso 1: Crear una conexión de VPN y configurar la VPC.
- Si el dispositivo de pasarela de tu cliente es una EC2 instancia, asegúrate de haber desactivado la comprobación del origen y el destino de la instancia. Para obtener más información, consulte Configuración de instancias de Windows.

En la consola de Amazon VPC, en la página VPN Connections, seleccione su conexión de VPN. El primer túnel está en estado activo. El segundo túnel debería configurarse, pero no se utiliza a menos que se desactive el primer túnel. Puede que los túneles cifrados tarden unos minutos en establecerse.

Solución de problemas AWS Site-to-Site VPN del dispositivo de pasarela de clientes

Al solucionar problemas con el dispositivo de puerta de enlace de cliente, es importante tener un enfoque estructurado. Los dos primeros temas de esta sección proporcionan diagramas de flujo generalizados para solucionar problemas al utilizar un dispositivo configurado para el enrutamiento dinámico (habilitado para BGP) y un dispositivo configurado para el enrutamiento estático (sin BGP habilitado), respectivamente. Los siguientes temas incluyen guías de solución de problemas específicas para los dispositivos de puerta de enlace de cliente de Cisco, Juniper y Yamaha.

Además de los temas de esta sección, la habilitación de AWS Site-to-Site VPN registros puede ser útil para solucionar problemas de conectividad de VPN. Para instrucciones de prueba generales, consulte también Probar una AWS Site-to-Site VPN conexión.

Temas

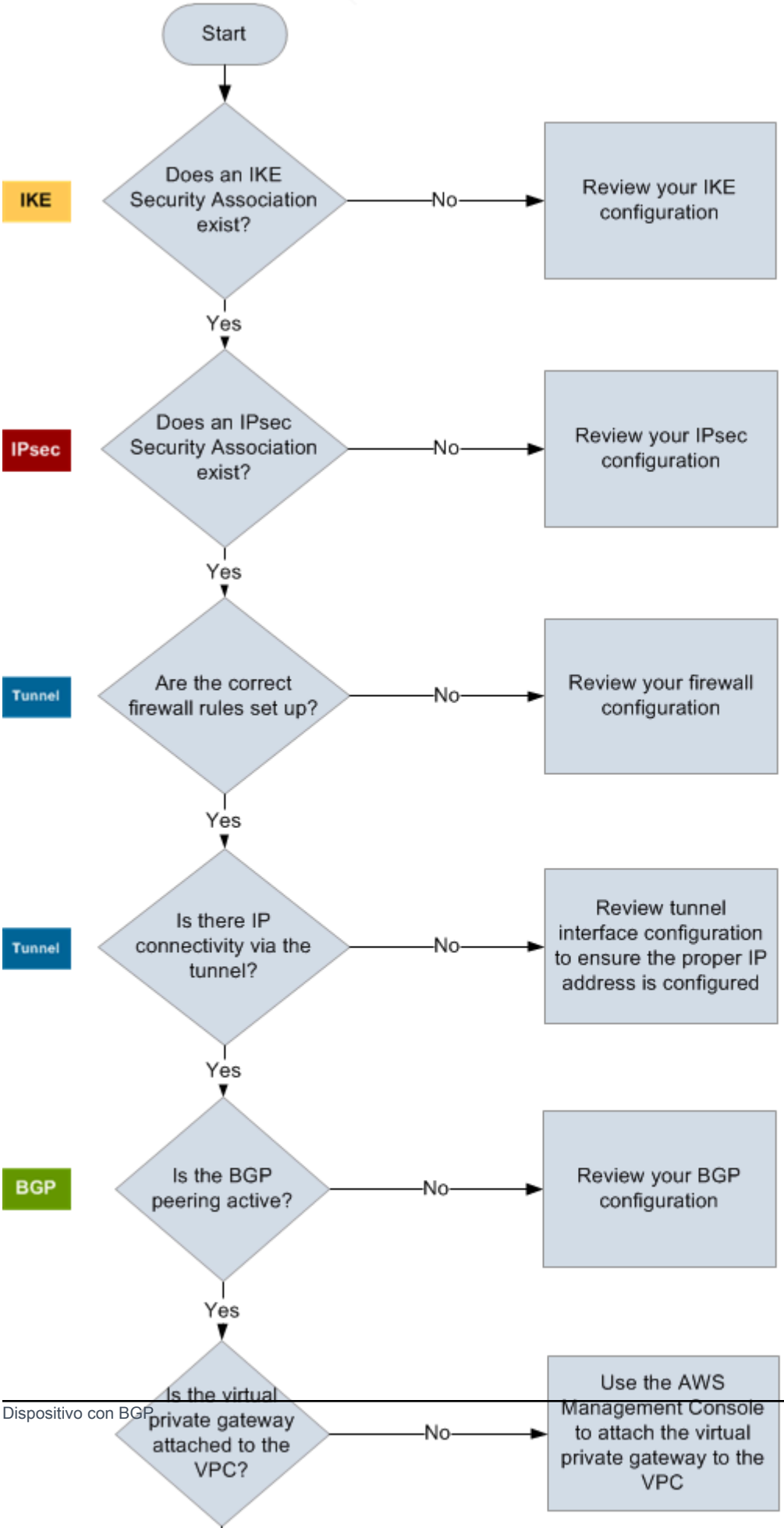
- Solucione los problemas de AWS Site-to-Site VPN conectividad al utilizar el protocolo Border Gateway
- Solucione los problemas de AWS Site-to-Site VPN conectividad sin el protocolo Border Gateway
- Solucione los problemas de AWS Site-to-Site VPN conectividad con un dispositivo de puerta de enlace para clientes Cisco ASA
- Solucione los problemas de AWS Site-to-Site VPN conectividad con un dispositivo de puerta de enlace para clientes Cisco IOS
- Solucione los problemas de AWS Site-to-Site VPN conectividad con un dispositivo de puerta de enlace para clientes Cisco IOS sin el protocolo Border Gateway
- Solucione problemas de AWS Site-to-Site VPN conectividad con un dispositivo de puerta de enlace para clientes JunOS de Juniper
- Solucione problemas de AWS Site-to-Site VPN conectividad con un dispositivo de puerta de enlace para clientes Juniper ScreenOS
- Solucione los problemas de AWS Site-to-Site VPN conectividad con un dispositivo de pasarela de clientes de Yamaha

Recursos adicionales

- Foro de Amazon VPC

Solucione los problemas de AWS Site-to-Site VPN conectividad al utilizar el protocolo Border Gateway

El siguiente diagrama y la siguiente tabla proporcionan instrucciones generales para solucionar problemas de un dispositivo de gateway de cliente que utiliza el protocolo de gateway fronteriza (BGP). También recomendamos que habilite las características de depuración de su dispositivo. Consulte al proveedor de su dispositivo de gateway para obtener detalles.

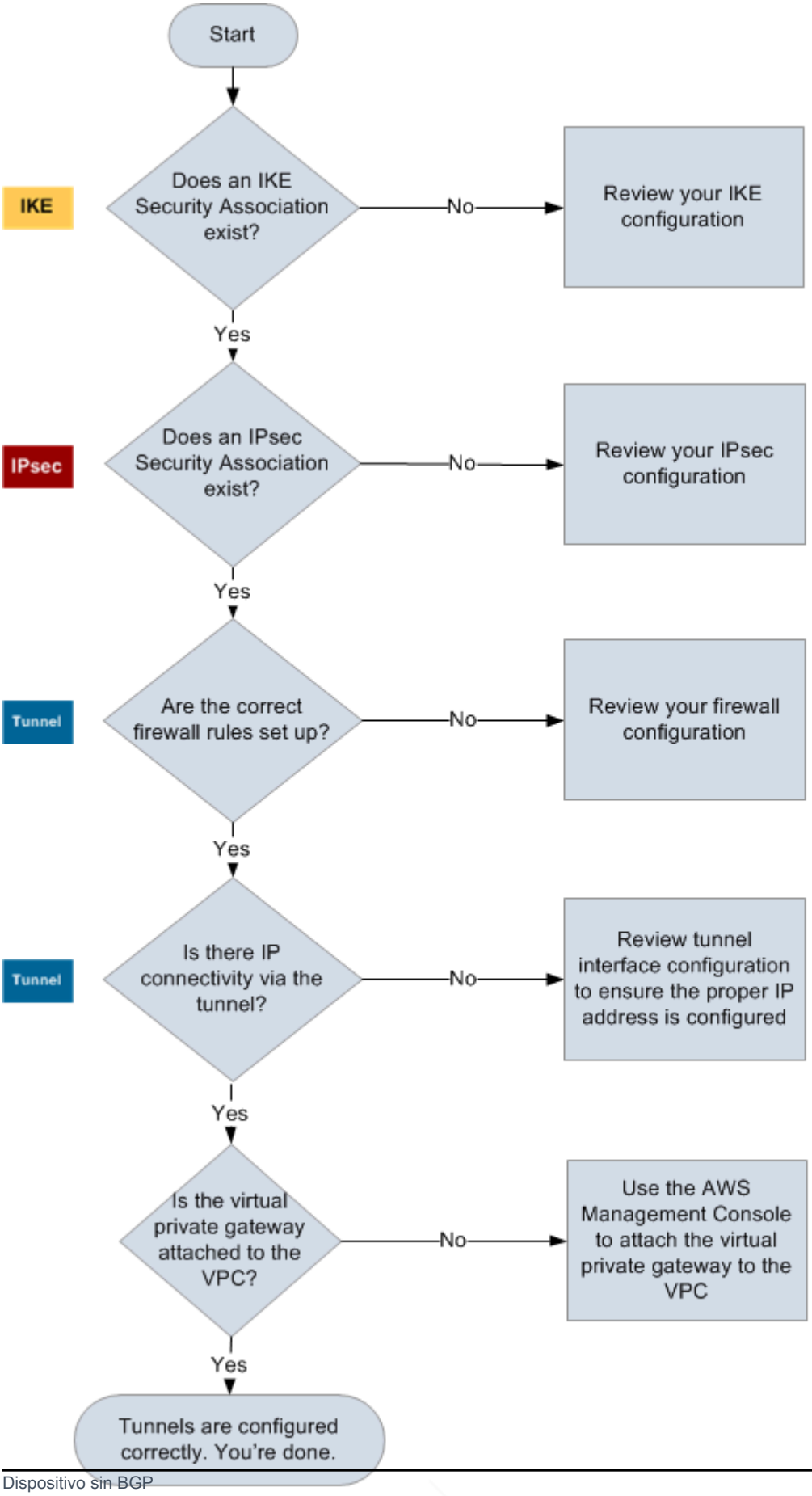

Start
IKE
Does an IKE Security Association exist?
No
Review your IKE configuration
Yes
IPsec
Does an IPsec Security Association exist?
No
Review your IPsec configuration
Yes
Tunnel
Are the correct firewall rules set up?
No
Review your firewall configuration
Yes
Tunnel
Is there IP connectivity via the 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	Determine si existe una asociación de seguridad de IKE. Se necesita una asociación de seguridad IKE para intercambiar las claves que se utilizan para establecer la asociación de IPsec seguridad. Si no existe ninguna asociación de seguridad de IKE, revise sus opciones de configuración de IKE. Debe configurar los parámetros de cifrado, autenticación, confidencialidad directa total y modo según lo que se indica en el archivo de configuración. Si existe una asociación de seguridad IKE, pase a 'IPsec'.
IPsec	Determine si existe una asociación de IPsec seguridad (SA). Una IPsec SA es el túnel en sí mismo. Consulte el dispositivo de puerta de enlace del cliente para determinar si una IPsec SA está activa. Asegúrese de configurar los parámetros de cifrado, autenticación, confidencialidad directa total y modo según lo mostrado en el archivo de configuración. Si no existe ninguna IPsec SA, revise su IPsec configuración. Si existe una IPsec SA, pase a «Túnel».
Túnel	Asegúrese de que se han configurado las reglas de firewall necesarias (para ver una lista de las reglas, consulte Reglas de firewall para un dispositivo de puerta de enlace del AWS Site-to-Site VPN cliente). Si están correctamente configuradas, continúe. Determine si hay conectividad IP a través del túnel. Cada lado del túnel tiene una dirección IP según lo especificado en el archivo de configuración. La dirección de gateway privada virtual es la dirección utilizada como la dirección vecina de BGP. Desde su dispositivo de gateway de cliente, haga ping a esta dirección para determinar si el tráfico IP se está cifrando y descifrando correctamente. Si el ping no se realiza correctamente, revise la configuración de la interfaz del túnel para asegurarse de que se ha configurado la dirección IP adecuada.

	Si el ping es correcto, vaya a “BGP”.
BGP	Determine si la sesión de intercambio de tráfico BGP está activa. Para cada túnel, haga lo siguiente: • En su dispositivo de gateway de cliente, determine si el estado de BGP es `Active` o `Established` . El intercambio de tráfico BGP puede tardar aproximadamente 30 segundos en activarse. • Asegúrese de que el dispositivo de gateway de cliente indica la ruta predeterm inada (0.0.0.0/0) hacia la gateway privada virtual. Si los túneles no se encuentran en este estado, revise su configuración de BGP. Si se establece el intercambio de tráfico BGP, recibe un prefijo y se indica un prefijo, el túnel estará configurado correctamente. Asegúrese de que los dos túneles tienen este estado.

Solucione los problemas de AWS Site-to-Site VPN conectividad sin el protocolo Border Gateway

El siguiente diagrama y la siguiente tabla proporcionan instrucciones generales para solucionar problemas en un dispositivo de gateway de cliente que no utiliza el protocolo de gateway fronteriza (BGP). También recomendamos que habilite las características de depuración de su dispositivo. Consulte al proveedor de su dispositivo de gateway para obtener detalles.


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	Determine si existe una asociación de seguridad de IKE. Se necesita una asociación de seguridad IKE para intercambiar las claves que se utilizan para establecer la asociación IPsec de seguridad. Si no existe ninguna asociación de seguridad de IKE, revise sus opciones de configuración de IKE. Debe configurar los parámetros de cifrado, autenticación, confidencialidad directa total y modo según lo que se indica en el archivo de configuración. Si existe una asociación de seguridad IKE, pase a 'IPsec'.
IPsec	Determine si existe una asociación de IPsec seguridad (SA). Una IPsec SA es el túnel en sí mismo. Consulte el dispositivo de puerta de enlace del cliente para determinar si una IPsec SA está activa. Asegúrese de configurar los parámetros de cifrado, autenticación, confidencialidad directa total y modo según lo mostrado en el archivo de configuración. Si no existe ninguna IPsec SA, revise su IPsec configuración. Si existe una IPsec SA, pase a «Túnel».
Túnel	Asegúrese de que se han configurado las reglas de firewall necesarias (para ver una lista de las reglas, consulte Reglas de firewall para un dispositivo de puerta de enlace del AWS Site-to-Site VPN cliente). Si están correctamente configuradas, continúe. Determine si hay conectividad IP a través del túnel. Cada lado del túnel tiene una dirección IP según lo especificado en el archivo de configuración. La dirección de gateway privada virtual es la dirección utilizada como la dirección vecina de BGP. Desde su dispositivo de gateway de cliente, haga ping a esta dirección para determinar si el tráfico IP se está cifrando y descifrando correctamente. Si el ping no se realiza correctamente, revise la configuración de la interfaz del túnel para asegurarse de que se ha configurado la dirección IP adecuada.

	Si el ping se realiza correctamente, vaya a “Rutas estáticas”.
Rutas estáticas	Para cada túnel, haga lo siguiente: • Compruebe que ha añadido una ruta estática a su CIDR de VPC con los túneles como el siguiente salto. • Asegúrese de que ha agregado una ruta estática en la consola de Amazon VPC para indicar a la gateway privada virtual que direccione el tráfico de vuelta a sus redes internas. Si los túneles no se encuentran en este estado, revise la configuración de su dispositivo. Asegúrese de que los dos túneles tienen este estado, y ya habrá terminado.

Solucione los problemas de AWS Site-to-Site VPN conectividad con un dispositivo de puerta de enlace para clientes Cisco ASA

Cuando solucione los problemas de conectividad de un dispositivo de puerta de enlace para clientes de Cisco, considere el IKE y el enrutamiento. IPsec Puede solucionar problemas en estas áreas en cualquier orden, pero recomendamos empezar por IKE (en la parte inferior de stack de red) y continuar de forma ascendente.

> **Important**
>
> Algunos ASAs solo son compatibles con Cisco Active/Standby . Cuando utiliza estos Cisco ASAs, solo puede tener un túnel activo a la vez. El otro túnel en espera se activará solo si el primer túnel se vuelve no disponible. El túnel en espera puede producir el siguiente error en sus archivos de registro, que puede ignorarse: `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

Use el siguiente comando. La respuesta mostrará un dispositivo de gateway de cliente con el IKE configurado correctamente.

```
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
```

Debería ver una o varias líneas con el valor de `src` para la gateway remota que se especifica en los túneles. El valor `state` debería ser `MM_ACTIVE` y el `status` debería ser `ACTIVE`. La ausencia de entradas o la aparición de una entrada con otro estado indican que IKE no se ha configurado correctamente.

Para realizar una solución de problemas más profunda, ejecute los siguientes comandos para permitir que los mensajes de log proporcionen información de diagnóstico.

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

Para deshabilitar la depuración, utilice el siguiente comando.

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

IPsec

Use el siguiente comando. La respuesta muestra un dispositivo de puerta de enlace del cliente IPsec configurado correctamente.

```
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 integeg-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
```

Por cada interfaz del túnel, debería ver tanto `inbound esp sas` como `outbound esp sas`. Esto supone que aparece una SA (por ejemplo,`spi: 0x48B456A6`) y que IPsec está configurada correctamente.

En Cisco ASA, IPsec solo aparece después de enviar tráfico interesante (tráfico que debe estar cifrado). Para mantener siempre el SLA IPsec activo, recomendamos configurar un monitor de SLA. El monitor de SLA sigue enviando tráfico interesante y lo mantiene activo. IPsec

También puede usar el siguiente comando ping para forzar el inicio IPsec de la negociación y avanzar.

```
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
```

Para una solución de problemas más profunda, utilice el siguiente comando para permitir la depuración.

```
router# debug crypto ipsec
```

Para deshabilitar la depuración, utilice el siguiente comando.

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

Enrutamiento

Haga ping al otro extremo del túnel. Si esto funciona, entonces IPsec deberías estar establecido. Si esto no funciona, compruebe sus listas de acceso y consulte la IPsec sección anterior.

Si no puede obtener acceso a sus instancias, compruebe la siguiente información:

1. Verifique que la lista de acceso esté configurada para permitir el tráfico asociado al mapa criptográfico.

   Puede hacerlo con el siguiente comando.

   ```
   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. Compruebe la lista de acceso mediante el siguiente comando.

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

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

3. Verifique si la lista de acceso es correcta. La siguiente lista de acceso de ejemplo permite todo el tráfico interno a la subred de VPC 10.0.0.0/16.

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

4. Ejecute un traceroute desde el dispositivo Cisco ASA para ver si llega a los routers Amazon (por ejemplo,*AWS_ENDPOINT_1*/). *AWS_ENDPOINT_2*

   Si llega al enrutador de Amazon, compruebe las rutas estáticas que agregó en la consola de Amazon VPC, así como los grupos de seguridad de las instancias particulares.

5. Para una solución de problemas más profunda, revise la configuración.

Haga rebotar la interfaz del túnel

Si el túnel parece estar activo pero el tráfico no fluye correctamente, rebotar (deshabilitar y volver a activar) la interfaz del túnel suele resolver los problemas de conectividad. Para hacer rebotar la interfaz del túnel en un Cisco ASA:

1. Ejecuta lo siguiente:

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

Como alternativa, puede utilizar un comando de una sola línea:

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

2. Después de hacer rebotar la interfaz, compruebe si la conexión VPN se ha restablecido y si el tráfico fluye ahora correctamente.

Solucione los problemas de AWS Site-to-Site VPN conectividad con un dispositivo de puerta de enlace para clientes Cisco IOS

Al solucionar los problemas de conectividad de un dispositivo de puerta de enlace para clientes de Cisco, tenga en cuenta cuatro aspectos: el IKE IPsec, el túnel y el BGP. Puede solucionar problemas en estas áreas en cualquier orden, pero recomendamos empezar por IKE (en la parte inferior de stack de red) y continuar de forma ascendente.

IKE

Use el siguiente comando. La respuesta mostrará un dispositivo de gateway de cliente con el IKE configurado correctamente.

```
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
```

Debería ver una o varias líneas con el valor de `src` para la gateway remota que se especifica en los túneles. El `state` debería ser `QM_IDLE` y el `status` debería ser `ACTIVE`. La ausencia de entradas o la aparición de una entrada con otro estado indican que IKE no se ha configurado correctamente.

Para realizar una solución de problemas más profunda, ejecute los siguientes comandos para permitir que los mensajes de log proporcionen información de diagnóstico.

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

Para deshabilitar la depuración, utilice el siguiente comando.

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

IPsec

Use el siguiente comando. La respuesta muestra un dispositivo de puerta de enlace del cliente IPsec configurado correctamente.

```
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:
```

Por cada interfaz del túnel, debería ver tanto `inbound esp sas` como `outbound esp sas`. Suponiendo que una SA aparezca en la lista (`spi: 0xF95D2F3C`por ejemplo) y que IPsec esté configurada correctamente. `Status ACTIVE`

Para una solución de problemas más profunda, utilice el siguiente comando para permitir la depuración.

```
router# debug crypto ipsec
```

Utilice el siguiente comando para deshabilitar la depuración.

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

Túnel

En primer lugar, compruebe si tiene las reglas de firewall necesarias aplicadas. Para obtener más información, consulte Reglas de firewall para un dispositivo de puerta de enlace del AWS Site-to-Site VPN cliente.

Si sus reglas de firewall están configuradas correctamente, continúe realizando la solución de problemas con el siguiente comando.

```
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
```

Asegúrese de que el `line protocol` está activo. Compruebe que la dirección IP de origen del túnel, la interfaz de origen y el destino coinciden respectivamente con la configuración del túnel de la dirección IP externa del dispositivo de gateway de cliente, la interfaz y la dirección IP externa de la gateway privada virtual. Asegúrese de que `Tunnel protection via IPSec` está presente. Ejecute el comando en ambas interfaces del túnel. Para resolver cualquier problema, revise la configuración y compruebe las conexiones físicas de su dispositivo de gateway de cliente.

Asimismo, utilice el siguiente comando, reemplazando `169.254.255.1` por la dirección IP interna de su gateway privada virtual.

```
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
!!!!!
```

Debería ver cinco signos de exclamación.

Para una solución de problemas más profunda, revise la configuración.

BGP

Use el siguiente comando.

```
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
```

Deberían aparecer los dos vecinos. Para cada uno, debería ver un valor de `State/PfxRcd` de 1.

Si el intercambio de tráfico BGP está activado, compruebe si el dispositivo de gateway de cliente indica la ruta predeterminada (0.0.0.0/0) a la 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
```

Asimismo, asegúrese de estar recibiendo el prefijo correspondiente a su VPC desde la gateway privada virtual.

```
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
```

Para una solución de problemas más profunda, revise la configuración.

Solucione los problemas de AWS Site-to-Site VPN conectividad con un dispositivo de puerta de enlace para clientes Cisco IOS sin el protocolo Border Gateway

Al solucionar los problemas de conectividad de un dispositivo de puerta de enlace para clientes de Cisco, tenga en cuenta tres aspectos: el IKE y el IPsec túnel. Puede solucionar problemas en estas áreas en cualquier orden, pero recomendamos empezar por IKE (en la parte inferior de stack de red) y continuar de forma ascendente.

IKE

Use el siguiente comando. La respuesta mostrará un dispositivo de gateway de cliente con el IKE configurado correctamente.

```
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
```

Debería ver una o varias líneas con el valor de `src` para la gateway remota que se especifica en los túneles. El `state` debería ser `QM_IDLE` y el `status` debería ser `ACTIVE`. La ausencia de entradas o la aparición de una entrada con otro estado indican que IKE no se ha configurado correctamente.

Para realizar una solución de problemas más profunda, ejecute los siguientes comandos para permitir que los mensajes de log proporcionen información de diagnóstico.

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

Para deshabilitar la depuración, utilice el siguiente comando.

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

IPsec

Use el siguiente comando. La respuesta muestra un dispositivo de puerta de enlace del cliente IPsec configurado correctamente.

```
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:
```

Por cada interfaz del túnel, debería ver tanto inbound `esp sas` como outbound `esp sas`. Esto supone que aparece una SA (por ejemplo,`spi: 0x48B456A6`), que el estado es `ACTIVE` y que IPsec está configurada correctamente.

Para una solución de problemas más profunda, utilice el siguiente comando para permitir la depuración.

```
router# debug crypto ipsec
```

Para deshabilitar la depuración, utilice el siguiente comando.

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

Túnel

En primer lugar, compruebe si tiene las reglas de firewall necesarias aplicadas. Para obtener más información, consulte Reglas de firewall para un dispositivo de puerta de enlace del AWS Site-to-Site VPN cliente.

Si sus reglas de firewall están configuradas correctamente, continúe realizando la solución de problemas con el siguiente comando.

```
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
```

Asegúrese de que el line protocol está activo. Compruebe que la dirección IP de origen del túnel, la interfaz de origen y el destino coinciden respectivamente con la configuración del túnel de la dirección IP externa del dispositivo de gateway de cliente, la interfaz y la dirección IP externa de la gateway privada virtual. Asegúrese de que `Tunnel protection through IPSec` está presente. Ejecute el comando en ambas interfaces del túnel. Para resolver cualquier problema, revise la configuración y compruebe las conexiones físicas de su dispositivo de gateway de cliente.

También puede utilizar el siguiente comando, reemplazando `169.254.249.18` por la dirección IP interna de su gateway privada virtual.

```
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
!!!!!
```

Debería ver cinco signos de exclamación.

Enrutamiento

Para ver su tabla de ruteo estática, utilice el siguiente comando.

```
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
```

Debería ver que la ruta estática de CIDR de VPC a través de ambos túneles existe. Si no existe, añada las rutas estáticas tal y como se indica a continuación.

```
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
```

Comprobación de la monitorización de 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
```

El valor de `Number of successes` indica si la monitorización de SLA se ha configurado correctamente.

Para una solución de problemas más profunda, revise la configuración.

Solucione problemas de AWS Site-to-Site VPN conectividad con un dispositivo de puerta de enlace para clientes JunOS de Juniper

Al solucionar los problemas de conectividad de un dispositivo de pasarela de cliente de Juniper, tenga en cuenta cuatro aspectos: IKE IPsec, túnel y BGP. Puede solucionar problemas en estas áreas en cualquier orden, pero recomendamos empezar por IKE (en la parte inferior de stack de red) y continuar de forma ascendente.

IKE

Use el siguiente comando. La respuesta mostrará un dispositivo de gateway de cliente con el IKE configurado correctamente.

```
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
```

Debería ver una o varias líneas que contienen una dirección remota de la gateway remota especificada en los túneles. El valor de `State` debería ser `UP`. La ausencia de entradas o la aparición de una entrada con otro estado (como `DOWN`) indican que IKE no se ha configurado correctamente.

Para realizar una solución de problemas más profunda, habilite las opciones de seguimiento de IKE, según lo recomendado en el archivo de configuración de ejemplo. A continuación, ejecute el siguiente comando para imprimir diversos mensajes de depuración en la pantalla.

```
user@router> monitor start kmd
```

Desde un host externo, puede recuperar el archivo completo de log con el siguiente comando.

```
scp username@router.hostname:/var/log/kmd
```

IPsec

Use el siguiente comando. La respuesta muestra un dispositivo de pasarela de cliente configurado correctamente. IPsec

```
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
```

En concreto, debería ver al menos dos líneas por dirección de gateway (correspondientes a la gateway remota). Los signos de intercalación al principio de cada línea (**< >**) indican la dirección del tráfico de la entrada en particular. El resultado son líneas separadas para el tráfico entrante ("**<**", tráfico de la gateway privada virtual a ese dispositivo de gateway de cliente) y el tráfico saliente ("**>**").

Para realizar una solución de problemas más profunda, habilite las opciones de seguimiento de IKE (para obtener más información, consulte la sección anterior acerca de IKE).

Túnel

En primer lugar, vuelva a comprobar si tiene las reglas de firewall necesarias aplicadas. Para obtener una lista de reglas, consulte Reglas de firewall para un dispositivo de puerta de enlace del AWS Site-to-Site VPN cliente.

Si sus reglas de firewall están configuradas correctamente, continúe realizando la solución de problemas con el siguiente comando.

```
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
```

Asegúrese de que el valor de `Security: Zone` es correcto y de que la dirección de `Local` coincide con el túnel del dispositivo de gateway de cliente dentro de la dirección.

A continuación, utilice el siguiente comando, reemplazando `169.254.255.1` por la dirección IP interna de su gateway privada virtual. Sus resultados deberían ser parecidos a la respuesta que se muestra aquí.

```
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
```

Para una solución de problemas más profunda, revise la configuración.

BGP

Ejecute el siguiente comando.

```
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
```

Para una solución de problemas más profunda, utilice el siguiente comando, reemplazando `169.254.255.1` por la dirección IP interna de su gateway privada virtual.

```
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
```

Aquí debería ver `Received prefixes` y `Advertised prefixes` enumerados en 1 cada uno. Esto debería encontrarse en la sección `Table inet.0`.

Si el valor de `State` no es `Established`, compruebe `Last State` y `Last Error` para ver los detalles de lo que se necesita para corregir el problema.

Si el intercambio de tráfico BGP está activado, compruebe si el dispositivo de gateway de cliente indica la ruta predeterminada (0.0.0.0/0) a la 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
```

Asimismo, asegúrese de estar recibiendo el prefijo correspondiente a su VPC desde la gateway privada virtual.

```
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
```

Solucione problemas de AWS Site-to-Site VPN conectividad con un dispositivo de puerta de enlace para clientes Juniper ScreenOS

Cuando solucione los problemas de conectividad de un dispositivo de pasarela de cliente basado en Juniper ScreenOS, tenga en cuenta cuatro aspectos: IKE IPsec, túnel y BGP. Puede solucionar problemas en estas áreas en cualquier orden, pero recomendamos empezar por IKE (en la parte inferior de stack de red) y continuar de forma ascendente.

IKE y IPsec

Use el siguiente comando. La respuesta mostrará un dispositivo de gateway de cliente con el IKE configurado correctamente.

```
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
```

Debería ver una o varias líneas con una dirección remota de la gateway remota que se especifica en los túneles. El valor de `Sta` debería ser `A/-`, y el valor de `SPI` debería ser un número hexadecimal distinto de `00000000`. Unas entradas con unos estados diferentes indican que IKE no se ha configurado correctamente.

Para realizar una resolución de problemas más profunda, habilite las opciones de seguimiento de IKE (según lo recomendado en la información de configuración de ejemplo).

Túnel

En primer lugar, vuelva a comprobar si tiene las reglas de firewall necesarias aplicadas. Para obtener una lista de reglas, consulte Reglas de firewall para un dispositivo de puerta de enlace del AWS Site-to-Site VPN cliente.

Si sus reglas de firewall están configuradas correctamente, continúe realizando la solución de problemas con el siguiente comando.

```
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
```

Asegúrese de que puede ver `link:ready` y de que la dirección de `IP` coincide con el túnel del dispositivo de gateway de cliente dentro de la dirección.

A continuación, utilice el siguiente comando, reemplazando `169.254.255.1` por la dirección IP interna de su gateway privada virtual. Sus resultados deberían ser parecidos a la respuesta que se muestra aquí.

```
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
```

Para una solución de problemas más profunda, revise la configuración.

BGP

Ejecute el siguiente comando.

```
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
```

El estado de los dos BGP del mismo nivel debería ser `ESTABLISH`, lo que significa que la conexión de BGP con la gateway privada virtual está activa.

Para una solución de problemas más profunda, utilice el siguiente comando, reemplazando `169.254.255.1` por la dirección IP interna de su gateway privada virtual.

```
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 el intercambio de tráfico BGP está activado, compruebe si el dispositivo de gateway de cliente indica la ruta predeterminada (0.0.0.0/0) a la VPC. Este comando se aplica a ScreenOS 6.2.0 y versiones superiores.

```
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
```

Asimismo, asegúrese de estar recibiendo el prefijo correspondiente a su VPC desde la gateway privada virtual. Este comando se aplica a ScreenOS 6.2.0 y versiones superiores.

```
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
```

Solucione los problemas de AWS Site-to-Site VPN conectividad con un dispositivo de pasarela de clientes de Yamaha

Al solucionar los problemas de conectividad de un dispositivo de pasarela de clientes de Yamaha, tenga en cuenta cuatro aspectos: IKE IPsec, túnel y BGP. Puede solucionar problemas en estas

áreas en cualquier orden, pero recomendamos empezar por IKE (en la parte inferior de stack de red) y continuar de forma ascendente.

> **Note**
>
> La configuración del `proxy ID` utilizada en la fase 2 de IKE está desactivada de forma predeterminada en el enrutador Yamaha. Esto puede provocar problemas al conectarse a Site-to-Site la VPN. Si no `proxy ID` está configurado en su router, consulte el ejemplo de archivo AWS de configuración proporcionado para que Yamaha lo configure correctamente.

IKE

Ejecute el siguiente comando. La respuesta mostrará un dispositivo de gateway de cliente con el IKE configurado correctamente.

```
# 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
```

Debería ver una línea con el valor de `remote-id` de la gateway remota que se especifica en los túneles. Puede enumerar todas las asociaciones de seguridad (SAs) omitiendo el número de túnel.

Para realizar una solución de problemas más profunda, ejecute los siguientes comandos para permitir que los mensajes de log de nivel DEBUG proporcionen información de diagnóstico.

```
# syslog debug on
# ipsec ike log message-info payload-info key-info
```

Para cancelar los elementos registrados, ejecute el siguiente comando.

```
# no ipsec ike log
# no syslog debug on
```

IPsec

Ejecute el siguiente comando. La respuesta muestra un dispositivo de pasarela del cliente IPsec configurado correctamente.

```
# 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)   ** ** ** ** **
-------------------------------------------------
```

Por cada interfaz del túnel, debería ver tanto `receive sas` como `send sas`.

Para una solución de problemas más profunda, utilice el siguiente comando para permitir la depuración.

```
# syslog debug on
# ipsec ike log message-info payload-info key-info
```

Ejecute el siguiente comando para deshabilitar la depuración.

```
# no ipsec ike log
# no syslog debug on
```

Túnel

En primer lugar, compruebe si tiene las reglas de firewall necesarias aplicadas. Para obtener una lista de reglas, consulte Reglas de firewall para un dispositivo de puerta de enlace del AWS Site-to-Site VPN cliente.

Si sus reglas de firewall están configuradas correctamente, continúe realizando la solución de problemas con el siguiente comando.

```
# 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]
```

Asegúrese de que el `current status` valor esté en línea y así `Interface type` es IPsec. Asegúrese de ejecutar el comando en ambas interfaces del túnel. Para resolver cualquier problema aquí, revise la configuración.

BGP

Ejecute el siguiente comando.

```
# 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:
```

Deberían aparecer los dos vecinos. Para cada uno, debería ver un valor de BGP `state` de `Active`.

Si el intercambio de tráfico BGP está activado, compruebe si el dispositivo de gateway de cliente indica la ruta predeterminada (0.0.0.0/0) a la 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
```

Asimismo, asegúrese de estar recibiendo el prefijo correspondiente a su VPC desde la gateway privada virtual.

```
# 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
```

Trabaja con AWS Site-to-Site VPN

Puede trabajar con recursos de Site-to-Site VPN mediante la consola de Amazon VPC o la. AWS CLI

Temas

Crear un AWS Site-to-Site VPN archivo adjunto para AWS Cloud WAN

Puedes crear un adjunto de Site-to-Site VPN para AWS Cloud WAN siguiendo el procedimiento que se indica a continuación. Para obtener más información sobre los adjuntos de VPN y Cloud WAN, consulta los adjuntos de Site-to-site VPN en AWS Cloud WAN en la Guía del usuario de AWS Cloud WAN.

Los adjuntos de VPN de Cloud WAN son compatibles con ambos IPv4 IPv6 protocolos. Para obtener más información sobre el uso de cualquiera de estos protocolos para un adjunto de VPN de WAN en la nube, consulte IPv4 IPv6 Tráfico en AWS Site-to-Site VPN.

Para crear un adjunto de VPN para AWS Cloud WAN mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.

2. En el panel de navegación, selecciona Conexiones Site-to-Site VPN.
3. Elija Create VPN Connection (Crear conexión VPN).
4. (Opcional) En Etiqueta de nombre, escriba el nombre de la conexión. Esta acción creará una etiqueta con una clave de `Name` y el valor que especifique.
5. En Target gateway type (Tipo de puerta de enlace de destino), elija Not associated (No asociada).
6. En Customer gateway (Puerta de enlace de cliente), realice alguna de las siguientes operaciones:
   - Para usar una pasarela de clientes existente, seleccione Existente y, a continuación, elija el ID de la pasarela de clientes.
   - Para crear una nueva pasarela de clientes, elija Nueva.
     1. Para la dirección IP, introduzca una IPv6dirección estática IPv4o.
     2. (Opcional) Para el ARN del certificado, elija el ARN de su certificado privado (si utiliza la autenticación basada en certificados).
     3. En BGP ASN, escriba el número de sistema autónomo (ASN) para protocolo de gateway fronteriza (BGP) de la gateway de cliente. Para obtener más información, consulte Opciones de gateway de cliente.
7. Para las opciones de enrutamiento, elija Dinámico (requiere BGP) o Estático.
8. Para el almacenamiento de claves previamente compartidas, elija Standard o Secrets Manager. La selección predeterminada es Estándar. Para obtener más información acerca del uso de AWS Secrets Manager, consulte Seguridad.
9. Para la versión Tunnel inside IP, seleccione IPv4o IPv6.
10. (Opcional) En Habilitar la aceleración, seleccione la casilla de verificación para habilitar la aceleración. Para obtener más información, consulte Conexiones de VPN aceleradas.

    Si habilita la aceleración, creamos dos aceleradores que utilizan su conexión de VPN. Se aplican cargos adicionales de .
11. (Opcional) Según la versión de túnel dentro de IP que haya elegido, realice una de las siguientes acciones:
    - IPv4 — Para el CIDR de IPv4 red local, especifique el rango de IPv4 CIDR en la puerta de enlace del cliente (local) que puede comunicarse a través de los túneles de la VPN. Para el CIDR IPv4 de red remota, elija el rango de CIDR en el AWS lado que puede comunicarse a través de los túneles de la VPN. El valor predeterminado para ambos campos es. `0.0.0.0/0`

- IPv6 — Para el CIDR de IPv6 red local, especifique el rango de IPv6 CIDR en la puerta de enlace del cliente (local) que puede comunicarse a través de los túneles de la VPN. Para el CIDR IPv6 de red remota, elija el rango de CIDR en el AWS lado que puede comunicarse a través de los túneles de la VPN. El valor predeterminado para ambos campos es `::/0`

12. Para el tipo de dirección IP externa, elija una de las siguientes opciones:

    - Público IPv4: (predeterminado) Usa IPv4 direcciones para el túnel exterior IPs.
    - Privado IPv4: utilice una IPv4 dirección privada para utilizarla en redes privadas.
    - IPv6- Usa IPv6 las direcciones del túnel exterior IPs. Esta opción requiere que el dispositivo de pasarela de clientes sea compatible con el IPv6 direccionamiento.

    > **Note**
    >
    > Si selecciona el tipo IPv6de dirección IP externa, debe crear una pasarela de clientes con una IPv6 dirección

13. (Opcional) Para las opciones del túnel 1, puede especificar la siguiente información para cada túnel:

    - Un bloque IPv4 CIDR de tamaño /30 del `169.254.0.0/16` rango de las direcciones del túnel IPv4 interior.
    - Si especificó IPv6para la versión Tunnel inside IP, un bloque IPv6 CIDR /126 del `fd00::/8` rango para las direcciones del túnel interno. IPv6
    - La clave previamente compartida de IKE (PSK). Se admiten las siguientes versiones: IKEv1 o. IKEv2
    - Para editar las opciones avanzadas del túnel, seleccione Editar opciones de túnel. Para obtener más información, consulte Opciones de túnel de VPN.
    - (Opcional) Seleccione Activar en el registro de actividad del túnel para capturar los mensajes de registro de IPsec la actividad y los mensajes del protocolo DPD.
    - (Opcional) Seleccione Activar para el ciclo de vida de los puntos finales del túnel para controlar la programación de las sustituciones de los puntos finales. Para obtener más información sobre el ciclo de vida de los puntos finales del túnel, consulteCiclo de vida del punto de conexión del túnel.

14. (Opcional) Elija las opciones del túnel 2 y siga los pasos anteriores para configurar un segundo túnel.

15. Elija Create VPN Connection (Crear conexión VPN).

Para crear una conexión Site-to-Site VPN mediante la línea de comandos o la API

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

  Ejemplo de creación de una conexión VPN con un túnel IPv6 exterior IPs y un túnel IPv6 interior IPs:

```
aws ec2 create-vpn-connection --type ipsec.1 --customer-gateway-id
 cgw-001122334455aabbc --options
 OutsideIPAddressType=Ipv6,TunnelInsideIpVersion=pv6,TunnelOptions=[{StartupAction=start},
{StartupAction=start}]
```

Crear un AWS Site-to-Site VPN adjunto a una pasarela de transporte

Para crear una conexión de VPN en una puerta de enlace de tránsito, debe especificar la puerta de enlace de tránsito y la puerta de enlace de cliente. Será necesario crear la puerta de enlace de tránsito antes de seguir este procedimiento. Para obtener más información acerca de cómo crear una gateway de tránsito, consulte Gateways de tránsito en Gateways de tránsito de Amazon VPC.

Los archivos adjuntos de la VPN de Transit Gateway admiten ambas IPv4 opciones IPv6. Para obtener más información sobre el uso de cualquiera de estos protocolos para un adjunto de VPN de pasarela de tránsito, consulte IPv4 IPv6 Tráfico en AWS Site-to-Site VPN.

Para crear una conexión de VPN en una puerta de enlace de tránsito con la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija conexiones Site-to-Site VPN.
3. Elija Create VPN Connection (Crear conexión VPN).
4. (Opcional) En Etiqueta de nombre, escriba el nombre de la conexión. Esta acción creará una etiqueta con una clave de `Name` y el valor que especifique.
5. En Tipo de puerta de enlace de destino, elija Puerta de enlace de tránsito y, a continuación, elija la puerta de enlace de tránsito.

6. En Customer gateway (Puerta de enlace de cliente), realice alguna de las siguientes operaciones:
   - Para usar una pasarela de clientes existente, seleccione Existente y, a continuación, elija el ID de la pasarela de clientes.
   - Para crear una nueva pasarela de clientes, elija Nueva.

     1. Para la dirección IP, introduzca una IPv6dirección estática IPv4o.
     2. (Opcional) Para el ARN del certificado, elija el ARN de su certificado privado (si utiliza la autenticación basada en certificados).
     3. En BGP ASN, escriba el número de sistema autónomo (ASN) para protocolo de gateway fronteriza (BGP) de la gateway de cliente. Para obtener más información, consulte Opciones de gateway de cliente.
7. Para las opciones de enrutamiento, elija Dinámico (requiere BGP) o Estático.
8. Para el almacenamiento de claves previamente compartidas, elija Standard o Secrets Manager. La selección predeterminada es Estándar. Para obtener más información acerca del uso de AWS Secrets Manager, consulte Seguridad.
9. Para la versión Tunnel inside IP, seleccione IPv4o IPv6.
10. (Opcional) En Habilitar la aceleración, seleccione la casilla de verificación para habilitar la aceleración. Para obtener más información, consulte Conexiones de VPN aceleradas.

    Si habilita la aceleración, creamos dos aceleradores que utilizan su conexión de VPN. Se aplican cargos adicionales de .
11. (Opcional) Según la versión de túnel dentro de IP que haya elegido, realice una de las siguientes acciones:

    - IPv4 — Para el CIDR de IPv4 red local, especifique el rango de IPv4 CIDR en la puerta de enlace del cliente (local) que puede comunicarse a través de los túneles de la VPN. Para el CIDR IPv4 de red remota, elija el rango de CIDR en el AWS lado que puede comunicarse a través de los túneles de la VPN. El valor predeterminado para ambos campos es. `0.0.0.0/0`
    - IPv6 — Para el CIDR de IPv6 red local, especifique el rango de IPv6 CIDR en la puerta de enlace del cliente (local) que puede comunicarse a través de los túneles de la VPN. Para el CIDR IPv6 de red remota, elija el rango de CIDR en el AWS lado que puede comunicarse a través de los túneles de la VPN. El valor predeterminado para ambos campos es `::/0`
12. Para el tipo de dirección IP externa, elija una de las siguientes opciones:

    - Público IPv4: (predeterminado) Usa IPv4 direcciones para el túnel exterior IPs.

- Privado IPv4: utilice una IPv4 dirección privada para utilizarla en redes privadas.
- IPv6- Usa IPv6 las direcciones del túnel exterior IPs. Esta opción requiere que el dispositivo de pasarela de clientes sea compatible con el IPv6 direccionamiento.

> **Note**
>
> Si selecciona el tipo IPv6de dirección IP externa, debe crear una pasarela de clientes con una IPv6 dirección

13. (Opcional) Para las opciones del túnel 1, puede especificar la siguiente información para cada túnel:

    - Un bloque IPv4 CIDR de tamaño /30 del `169.254.0.0/16` rango de las direcciones del túnel IPv4 interior.
    - Si especificó IPv6para la versión Tunnel inside IP, un bloque IPv6 CIDR /126 del `fd00::/8` rango para las direcciones del túnel interno. IPv6
    - La clave previamente compartida de IKE (PSK). Se admiten las siguientes versiones: IKEv1 o. IKEv2
    - Para editar las opciones avanzadas del túnel, seleccione Editar opciones de túnel. Para obtener más información, consulte Opciones de túnel de VPN.
    - (Opcional) Seleccione Activar en el registro de actividad del túnel para capturar los mensajes de registro de IPsec la actividad y los mensajes del protocolo DPD.
    - (Opcional) Seleccione Activar para el ciclo de vida de los puntos finales del túnel para controlar la programación de las sustituciones de los puntos finales. Para obtener más información sobre el ciclo de vida de los puntos finales del túnel, consulteCiclo de vida del punto de conexión del túnel.
14. (Opcional) Elija las opciones del túnel 2 y siga los pasos anteriores para configurar un segundo túnel.
15. Elija Create VPN Connection (Crear conexión VPN).

Creación de un adjunto de VPN mediante la CLI

Use el create-vpn-connectioncomando y especifique el ID de la puerta de enlace de tránsito para la `--transit-gateway-id` opción.

Ejemplo de creación de una conexión VPN con un túnel IPv6 exterior IPs y un túnel IPv6 interior IPs:

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

Ejemplo de creación de una conexión VPN con un túnel IPv6 exterior IPs y un túnel IPv4 interior IPs:

```
aws ec2 create-vpn-connection --type ipsec.1 --transit-gateway-id
 tgw-12312312312312312 --customer-gateway-id cgw-001122334455aabbc --options
 OutsideIPAddressType=Ipv6,TunnelInsideIpVersion=ipv4,TunnelOptions=[{StartupAction=start},
{StartupAction=start}]
```

Visualización IPv6 de las direcciones de su conexión VPN

Después de crear una conexión VPN con el túnel IPv6 exterior IPs, puede ver las IPv6 direcciones asignadas mediante el comando `describe-vpn-connections` CLI:

```
aws ec2 describe-vpn-connections --vpn-connection-ids vpn-12345678901234567
```

En la respuesta, busque el `OutsideIpAddress` campo en la `TunnelOptions` sección. En el IPv6 caso de las conexiones VPN, este campo contendrá las IPv6 direcciones asignadas a los AWS lados de los túneles VPN.

Ejemplo de extracto de respuesta:

```
"Options": {
    "OutsideIPAddressType": "Ipv6",
    "TunnelInsideIpVersion": "ipv6",
    "TunnelOptions": [
        {
            "OutsideIpAddress": "2600:1f14:2dcf:d556:c3db:e57f:2414:2d9a",
            "TunnelInsideCidr": "2001:db8:1001:b110::/64",
            ...
        },
        {
            "OutsideIpAddress": "2600:1f14:2dcf:d57d:6318:60af:37c5:7ce1",
            "TunnelInsideCidr": "2001:db8:1001:b111::/64",
```

```
            ...
        }
    ]
}
```

Probar una AWS Site-to-Site VPN conexión

Tras crear la AWS Site-to-Site VPN conexión y configurar la puerta de enlace del cliente, puede lanzar una instancia y probar la conexión haciendo ping a la instancia.

Antes de comenzar, asegúrese de lo siguiente:

- Utilizar una AMI que responda a las solicitudes de ping. Le recomendamos que utilice uno de los sistemas Amazon Linux AMIs.
- Configure el grupo de seguridad o la ACL de red en su VPC para filtrar el tráfico entrante de la instancia para permitir el tráfico ICMP entrante y saliente. Esto permite que la instancia reciba solicitudes `ping`.
- Si utiliza instancias que ejecutan Windows Server, conéctese a la instancia y habilite la entrada ICMPv4 en el firewall de Windows para hacer ping a la instancia.
- (Enrutamiento estático) Asegúrese de que el dispositivo de gateway de cliente tenga una ruta estática a la VPC, y de que su conexión VPN tenga una ruta estática, para poder redirigir el tráfico a su dispositivo de gateway de cliente.
- (Enrutamiento dinámico) Asegúrese de que el estado de BGP en su dispositivo de gateway de cliente esté establecido. Una sesión de intercambio de tráfico BGP tarda aproximadamente 30 segundos en activarse. Compruebe que las rutas se anuncien con BGP correctamente y muestren una tabla de enrutamiento de subred para que el tráfico pueda regresar al gateway de cliente. Asegúrese de que los dos túneles estén configurados con la política de direccionamiento de BGP.
- Compruebe que haya configurado el enrutamiento de las tablas de enrutamiento de subred para la conexión de VPN.

Para probar la conectividad

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel, elija Iniciar instancia.
3. (Opcional) En Nombre, introduzca un nombre descriptivo para su instancia.

4. En Imágenes de aplicación y sistema operativo (Imagen de máquina de Amazon), elija Inicio rápido y, a continuación, elija el sistema operativo correspondiente a su instancia.
5. En Nombre del par de claves, seleccione un par de claves existente o cree uno nuevo.
6. En Configuración de red, elija Seleccionar un grupo de seguridad existente y, a continuación, elija el grupo de seguridad que configuró.
7. En el panel Resumen, elija Iniciar instancia.
8. Cuando la instancia esté en ejecución, obtenga su dirección IP privada (por ejemplo, 10.0.0.4). La EC2 consola de Amazon muestra la dirección como parte de los detalles de la instancia.
9. Desde un equipo de su red que se encuentre detrás del dispositivo de gateway de cliente, utilice el comando ping con la dirección IP privada de la instancia.

   ```
   ping 10.0.0.4
   ```

   La respuesta correcta será similar a la que se muestra a continuación.

   ```
   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
   ```

   Para probar la conmutación por error de los túneles, puede desactivar temporalmente uno de los túneles de su dispositivo de puerta de enlace de cliente y, a continuación, repetir este paso. No se pueden deshabilitar los túneles en el lado de AWS de la conexión de VPN.
10. Para probar la conexión desde AWS la red local, puedes usar SSH o RDP para conectarte a la instancia desde la red. A continuación, puede ejecutar el comando `ping` con la dirección IP privada de otro equipo de la red para comprobar que ambos lados de la conexión pueden iniciar y recibir solicitudes.

    Para obtener más información sobre cómo conectarse a una instancia de Linux, consulta Conéctate a tu instancia de Linux en la Guía del EC2 usuario de Amazon. Para obtener más

información sobre cómo conectarse a una instancia de Windows, consulte Conectarse a una instancia de Windows en la Guía del EC2 usuario de Amazon.

Eliminar una AWS Site-to-Site VPN conexión y una puerta de enlace

Si ya no necesitas una AWS Site-to-Site VPN conexión, puedes eliminarla. Cuando eliminas una conexión Site-to-Site VPN, no eliminamos la puerta de enlace del cliente ni la puerta de enlace privada virtual que estaba asociada a la conexión Site-to-Site VPN. Si ya no necesita la gateway de cliente ni la gateway privada virtual, puede eliminarlas.

> **Warning**
>
> Si elimina su conexión Site-to-Site VPN y, a continuación, crea una nueva, debe descargar un nuevo archivo de configuración y volver a configurar el dispositivo de puerta de enlace del cliente.

Tareas

- Eliminar una conexión AWS Site-to-Site VPN
- Eliminar una pasarela AWS Site-to-Site VPN de clientes
- Separe y elimine una puerta de enlace privada virtual en AWS Site-to-Site VPN

Eliminar una conexión AWS Site-to-Site VPN

Tras eliminar la conexión Site-to-Site VPN, permanece visible durante un breve periodo de tiempo con un estado de `ydeleted`, a continuación, la entrada se elimina automáticamente.

Para eliminar una conexión de VPN con la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, selecciona Conexiones Site-to-Site VPN.
3. Seleccione la conexión de VPN y elija Acciones, Eliminar conexión de VPN.
4. Cuando le pidan confirmación, escriba **`delete`** y elija Eliminar.

Para eliminar una conexión de VPN mediante la línea de comandos o la API

- DeleteVpnConnection(API de Amazon EC2 Query)
- delete-vpn-connection (AWS CLI)
- Remove-EC2VpnConnection (AWS Tools for Windows PowerShell)

Eliminar una pasarela AWS Site-to-Site VPN de clientes

Si ya no necesita una gateway de cliente, puede eliminarla. No puedes eliminar una pasarela de clientes que se esté utilizando en una conexión Site-to-Site VPN.

Para eliminar una gateway de cliente con la consola

1. En el panel de navegación, elija Puertas de enlace de cliente.
2. Elija la puerta de enlace de cliente y elija Acciones, Eliminar puerta de enlace de cliente.
3. Cuando le pidan confirmación, escriba **`delete`** y elija Eliminar.

Para eliminar una gateway de cliente mediante la línea de comando o API

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

Separe y elimine una puerta de enlace privada virtual en AWS Site-to-Site VPN

Si ya no necesita una gateway privada virtual para su VPC, puede de cliente, puede separarla del VPC.

Para desasociar una gateway privada virtual con la consola

1. En el panel de navegación, elija Puertas de enlace privadas virtuales.
2. Seleccione la gateway privada virtual y elija Actions, Detach from VPC.
3. Elija Desasociar puerta de enlace privada virtual.

Si ya no necesita la gateway privada virtual separada, puede eliminarla. Tenga en cuenta que no podrá eliminar la gateway privada virtual si sigue adjunta a la VPC. Después de que borre una puerta de enlace privada virtual, esta permanece visible durante un breve periodo de tiempo con un estado de `deleted` y, a continuación, la entrada se elimina automáticamente.

Para eliminar una gateway privada virtual con la consola

1. En el panel de navegación, elija Puertas de enlace privadas virtuales.
2. Seleccione la puerta de enlace privada virtual y elija Acciones, Eliminar puerta de enlace privada virtual.
3. Cuando le pidan confirmación, escriba **`delete`** y elija Eliminar.

Para desasociar una gateway privada virtual mediante la línea de comando o API

- DetachVpnGateway(API de Amazon EC2 Query)
- detach-vpn-gateway (AWS CLI)
- Dismount-EC2VpnGateway (AWS Tools for Windows PowerShell)

Para eliminar una gateway privada virtual mediante la línea de comando o API

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

Modificar la puerta de enlace de destino de una AWS Site-to-Site VPN conexión

Puede modificar la puerta de enlace de destino de una AWS Site-to-Site VPN conexión. Hay disponibles las siguientes opciones de migración:

- De una gateway privada virtual existente a una gateway de tránsito
- Una gateway privada virtual existente a otra gateway privada virtual
- De una gateway de tránsito existente a otra gateway de tránsito
- De una gateway de tránsito existente a una gateway privada virtual

Después de modificar la puerta de enlace de destino, su conexión Site-to-Site VPN no estará disponible temporalmente durante un breve período mientras aprovisionamos los nuevos puntos de conexión.

Las siguientes tareas le ayudan a realizar la migración a una nueva gateway.

Tareas

- Paso 1: Crear la puerta de enlace de destino nueva
- Paso 2: Actualizar las rutas estáticas (condicional)
- Paso 3: Migrar a una nueva gateway
- Paso 4: Actualizar tablas de enrutamiento de VPC
- Paso 5: Actualizar el enrutamiento de la puerta de enlace de destino (condicional)
- Paso 6: Actualizar el ASN de la puerta de enlace de cliente (condicional)

Paso 1: Crear la puerta de enlace de destino nueva

Antes de realizar la migración a la nueva puerta de enlace de destino, debe configurarla. Para obtener más información acerca de cómo añadir una gateway privada virtual, consulte the section called “Creación de una gateway privada virtual”. Para obtener más información acerca de cómo agregar una gateway de tránsito, consulte Crear una gateway de tránsito en Gateways de tránsito de Amazon VPC.

Si la nueva puerta de enlace de destino es una puerta de enlace de tránsito, conéctela VPCs a la puerta de enlace de tránsito. Para obtener más información sobre las conexiones de la VPC, consulte Vinculaciones de una gateway de tránsito a una VPC en Gateways de tránsito de Amazon VPC .

Cuando el destino cambia de una gateway privada virtual a una gateway de tránsito, se puede configurar el ASN de la gateway de tránsito para que tenga el mismo valor que el ASN de la gateway privada virtual. Si prefiere tener un ASN diferente, debe establecer el ASN del dispositivo de gateway de cliente en el ASN de la gateway de tránsito. Para obtener más información, consulte the section called “Paso 6: Actualizar el ASN de la puerta de enlace de cliente (condicional)”.

Paso 2: Actualizar las rutas estáticas (condicional)

Este paso es necesario cuando se pasa de una gateway privada virtual con rutas estáticas a una gateway de destino.

Debe eliminar las rutas estáticas antes de migrar a la nueva gateway.

> **Tip**
>
> Mantenga una copia de la ruta estática antes de eliminarla. Tendrá que volver a agregar estas rutas a la gateway de tránsito cuando haya terminado de migrar la conexión de VPN.

Para eliminar una ruta de una tabla de ruteo

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Route tables y, a continuación, seleccione la tabla de enrutamiento.
3. En la pestaña Rutas, elija Editar rutas.
4. Elija Eliminar para la ruta estática hacia la puerta de enlace privada virtual.
5. Elija Guardar cambios.

Paso 3: Migrar a una nueva gateway

Para cambiar la puerta de enlace de destino

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, selecciona Conexiones Site-to-Site VPN.
3. Elija la conexión de VPN y elija Acciones, Modificar conexión de VPN.
4. En Tipo de destino, elija el tipo de puerta de enlace.
   a. Si la puerta de enlace de destino nueva es una puerta de enlace privada virtual, elija la puerta de enlace de VPN.
   b. Si la puerta de enlace de destino nueva es una puerta de enlace de tránsito, elija la puerta de enlace de tránsito.
5. Elija Guardar cambios.

Para modificar una conexión Site-to-Site VPN mediante la línea de comandos o la API

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

Paso 4: Actualizar tablas de enrutamiento de VPC

Después de migrar a la nueva gateway, es posible que tenga que modificar la tabla de ruteo de VPC. Para obtener más información, consulte Tablas de ruteo en la Guía del usuario de Amazon VPC.

En la siguiente tabla se proporciona información sobre las actualizaciones de la tabla de enrutamiento de VPC que se deben llevar a cabo después de modificar el destino de la puerta de enlace VPN.

Gateway existente	Nueva gateway	Cambio en la tabla de ruteo de VPC
Gateway privada virtual con rutas propagadas	Puerta de enlace de tránsito	Agregue una ruta que contenga el ID de la puerta de enlace de tránsito.
Gateway privada virtual con rutas propagadas	Gateway privada virtual con rutas propagadas	No se requiere ninguna acción.
Gateway privada virtual con rutas propagadas	Gateway privada virtual con ruta estática	Agregue una ruta que contenga el ID de la nueva puerta de enlace privada virtual.
Gateway privada virtual con rutas estáticas	Puerta de enlace de tránsito	Actualice la ruta que contiene el ID de la puerta de enlace privada virtual al ID de la puerta de enlace de tránsito.
Gateway privada virtual con rutas estáticas	Gateway privada virtual con rutas estáticas	Actualice la ruta que contiene el ID de la puerta de enlace virtual privada al ID de la nueva puerta de enlace virtual privada.
Gateway privada virtual con rutas estáticas	Gateway privada virtual con rutas propagadas	Elimine la ruta que contiene el ID de la puerta de enlace privada virtual.

Gateway existente	Nueva gateway	Cambio en la tabla de ruteo de VPC
Puerta de enlace de tránsito	Gateway privada virtual con rutas estáticas	Actualice la ruta que contiene el ID de la puerta de enlace de tránsito al ID de la puerta de enlace privada virtual.
Puerta de enlace de tránsito	Gateway privada virtual con rutas propagadas	Elimine la ruta que contiene el ID de la puerta de enlace de tránsito.
Puerta de enlace de tránsito	Puerta de enlace de tránsito	Actualice la ruta que contiene el ID de la puerta de enlace de tránsito por el ID de la nueva puerta de enlace de tránsito.

Paso 5: Actualizar el enrutamiento de la puerta de enlace de destino (condicional)

Cuando la nueva puerta de enlace sea una puerta de enlace de tránsito, modifique la tabla de rutas de la puerta de enlace de tránsito para permitir el tráfico entre la VPC y la Site-to-Site VPN. Para obtener más información, consulte Tablas de enrutamiento de Transit Gateway en Transit Gateways de Amazon VPC.

Si eliminó las rutas estáticas de VPN, debe agregarlas en la tabla de enrutamiento de la gateway de tránsito.

A diferencia de una puerta de enlace privada virtual, una puerta de enlace de tránsito establece el mismo valor para el discriminador de salida múltiple (MED) en todos los túneles de una conexión de VPN. Si está migrando de una puerta de enlace privada virtual a una puerta de enlace de tránsito y ha confiado en el valor del MED para la selección de túnel, le recomendamos que implemente cambios de enrutamiento para evitar problemas de conexión. Por ejemplo, puede anunciar rutas más específicas en su puerta de enlace de tránsito. Para obtener más información, consulte Tablas de enrutamiento y prioridad de rutas de AWS Site-to-Site VPN.

Paso 6: Actualizar el ASN de la puerta de enlace de cliente (condicional)

Cuando la nueva gateway tenga un ASN diferente que la gateway antigua, debe actualizar el ASN en su dispositivo de gateway de cliente para que apunte al nuevo ASN. Para obtener más información, consulte Opciones de pasarela de clientes para su AWS Site-to-Site VPN conexión.

Modificar las opciones de AWS Site-to-Site VPN conexión

Puede modificar las opciones de conexión de su conexión Site-to-Site VPN. Puede modificar las siguientes opciones:

- El IPv4 CIDR se encuentra en el lado local (puerta de enlace del cliente) y en el lado remoto (AWS) de la conexión VPN, que pueden comunicarse a través de los túneles VPN. El valor predeterminado es `0.0.0.0/0` para ambos rangos.
- El IPv6 CIDR se encuentra en el lado local (puerta de enlace del cliente) y en el remoto (AWS) de la conexión VPN, que puede comunicarse a través de los túneles de la VPN. El valor predeterminado es `::/0` para ambos rangos.

Al modificar las opciones de conexión de la VPN, las direcciones IP de los puntos de conexión de la VPN AWS laterales no cambian y las opciones del túnel no cambian. Su conexión de VPN no estará disponible temporalmente durante un breve período mientras se actualiza la conexión de VPN.

Para modificar las opciones de conexión de VPN mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, selecciona las conexiones Site-to-Site VPN.
3. Seleccione su conexión de VPN y elija Acciones, Modificar las opciones de conexión de VPN.
4. Introduzca nuevos intervalos de CIDR según sea necesario.
5. Elija Guardar cambios.

Para modificar las opciones de conexión de VPN utilizando la línea de comandos o la API

- modify-vpn-connection-options (AWS CLI)
- ModifyVpnConnectionOptions(API de Amazon EC2 Query)

Modificar las opciones AWS Site-to-Site VPN del túnel

Puede modificar las opciones de túnel para los túneles VPN de su conexión Site-to-Site VPN. Puede modificar un túnel de VPN al mismo tiempo.

> **Important**
>
> Al modificar un túnel de VPN, la conectividad a través del túnel se interrumpe durante varios minutos. Asegúrese de tener previsto el tiempo de inactividad esperado.

Para modificar las opciones del túnel de VPN utilizando la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, selecciona Conexiones Site-to-Site VPN.
3. Seleccione la conexión Site-to-Site VPN y elija Acciones, Modificar las opciones del túnel VPN.
4. En Dirección IP externa del túnel de VPN, elija la IP del punto de conexión del túnel de VPN.
5. Elija o introduzca nuevos valores para las opciones de túnel según sea necesario. Para obtener más información sobre las opciones de túnel, consulte Opciones de túnel de VPN.

   > **Note**
   >
   > Algunas opciones de túnel tienen varios valores predeterminados. Haga clic para eliminar cualquier valor predeterminado. A continuación, ese valor predeterminado se elimina de la opción de túnel.

6. Elija Guardar cambios.

Para modificar las opciones del túnel de VPN utilizando la línea de comandos o la API

- (AWS CLI) Se utiliza describe-vpn-connectionspara ver las opciones de túnel actuales y modify-vpn-tunnel-optionspara modificarlas.
- (Amazon EC2 Query API) DescribeVpnConnectionsSe utiliza para ver las opciones de túnel actuales y ModifyVpnTunnelOptionspara modificarlas.

Edición de rutas estáticas para una AWS Site-to-Site VPN conexión

En el caso de una conexión Site-to-Site VPN en una puerta de enlace privada virtual configurada para el enrutamiento estático, puede añadir o eliminar rutas estáticas de la configuración de la VPN.

Para agregar o eliminar una ruta estática mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, selecciona conexiones Site-to-Site VPN.
3. Seleccione la conexión de VPN.
4. Elija Editar rutas estáticas.
5. Agregue o elimine rutas según sea necesario.
6. Elija Guardar cambios.
7. Si no ha habilitado la propagación de rutas en la tabla de ruteo, deberá actualizar manualmente las rutas de su tabla de ruteo para que reflejen los prefijos IP estáticos actualizados en su conexión de VPN. Para obtener más información, consulte (Gateway privada virtual) Habilitar la propagación de rutas en la tabla de enrutamiento.
8. Para una conexión de VPN en una puerta de enlace de tránsito, agregue, modifique o elimine las rutas estáticas de la tabla de enrutamiento de la puerta de enlace de tránsito. Para obtener más información, consulte Tablas de enrutamiento de Transit Gateway en Transit Gateways de Amazon VPC.

Para añadir una ruta estática mediante la línea de comando o un API

- CreateVpnConnectionRoute(API de Amazon EC2 Query)
- create-vpn-connection-route (AWS CLI)
- New-EC2VpnConnectionRoute (AWS Tools for Windows PowerShell)

Para eliminar una ruta estática mediante la línea de comando o un API

- DeleteVpnConnectionRoute(API de Amazon EC2 Query)
- delete-vpn-connection-route (AWS CLI)
- Remove-EC2VpnConnectionRoute (AWS Tools for Windows PowerShell)

Cambiar la pasarela del cliente por una AWS Site-to-Site VPN conexión

Puede cambiar la pasarela de cliente de su conexión Site-to-Site VPN mediante la consola de Amazon VPC o una herramienta de línea de comandos.

Después de cambiar la puerta de enlace de cliente, su conexión de VPN no estará disponible temporalmente durante un breve periodo mientras aprovisionamos los nuevos puntos de conexión.

Para cambiar la gateway de cliente mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, selecciona conexiones Site-to-Site VPN.
3. Seleccione la conexión de VPN.
4. Elija Acciones, Modificar la conexión de VPN.
5. En Tipo de destino, elija Puerta de enlace de cliente.
6. En Puerta de enlace de cliente de destino, elija la nueva puerta de enlace de cliente.
7. Elija Guardar cambios.

Para modificar la gateway de cliente mediante la línea de comando o API

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

Sustituir las credenciales comprometidas por una AWS Site-to-Site VPN conexión

Si cree que las credenciales del túnel de su conexión Site-to-Site VPN se han visto comprometidas, puede cambiar la clave previamente compartida de IKE o cambiar el certificado ACM. El método que utilice depende de la opción de autenticación que haya utilizado para los túneles de la VPN. Para obtener más información, consulte AWS Site-to-Site VPN opciones de autenticación de túnel.

Para cambiar la clave de IKE previamente compartida

Puede modificar las opciones de los túneles de la conexión de VPN y especificar una nueva clave de IKE previamente compartida para cada túnel. Para obtener más información, consulte Modificar las opciones AWS Site-to-Site VPN del túnel.

Si lo desea, también puede eliminar la conexión de VPN. Para obtener más información, consulte Eliminación de una conexión de VPN y una puerta de enlace. No es necesario eliminar la VPC ni la gateway privada virtual. A continuación, cree una nueva conexión de VPN mediante la misma puerta de enlace privada virtual y configure las nuevas claves en su dispositivo de puerta de enlace de cliente. Puedes especificar tus propias claves previamente compartidas para los túneles o dejar que se AWS generen nuevas claves previamente compartidas por ti. Para obtener más información, consulte Creación de una conexión de VPN. Las direcciones internas y externas del túnel podrían cambiar al crear de nuevo la conexión de VPN.

Para cambiar el certificado del extremo AWS lateral del túnel

Gire el certificado. Para obtener más información, consulte Rotación de certificados de punto de conexión de túnel de VPN.

Para cambiar el certificado en el dispositivo de gateway de cliente

1. Cree un nuevo certificado. Para obtener información, consulte Emisión y administración de certificados en la Guía del usuario de AWS Certificate Manager .
2. Agregue el certificado al dispositivo de gateway de cliente.

Certificados de punto final de AWS Site-to-Site VPN túnel rotativo

Puede rotar los certificados de los extremos AWS laterales del túnel mediante la consola de Amazon VPC. Cuando el certificado de un punto final de túnel está a punto de caducar, lo rota AWS automáticamente utilizando la función vinculada al servicio. Para obtener más información, consulte the section called “Roles vinculados a servicios”.

Para rotar el certificado del punto final del túnel Site-to-Site VPN mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija conexiones Site-to-Site VPN.
3. Seleccione la conexión Site-to-Site VPN y, a continuación, elija Acciones, Modificar el certificado del túnel VPN.
4. Seleccione el punto de conexión del túnel.

5. Seleccione Guardar.

Para rotar el certificado de punto final del túnel Site-to-Site VPN mediante el AWS CLI

Utilice el comando modify-vpn-tunnel-certificate.

IP privada AWS Site-to-Site VPN con AWS Direct Connect

Con una VPN con IP privada, puede implementar IPsec una VPN a través de ella AWS Direct Connect, cifrando el tráfico entre su red local y AWS sin el uso de direcciones IP públicas ni equipos VPN adicionales de terceros.

Uno de los principales usos de la VPN con IP privada AWS Direct Connect es ayudar a los clientes de los sectores financiero, sanitario y federal a cumplir sus objetivos normativos y de cumplimiento. La conexión VPN con IP privada AWS Direct Connect garantiza que el tráfico entre las redes locales AWS y entre ellas sea seguro y privado, lo que permite a los clientes cumplir con sus requisitos normativos y de seguridad.

Beneficios de la VPN de IP privada

- Administración y operaciones de red simplificadas: sin una VPN IP privada, los clientes tienen que implementar VPN y enrutadores de terceros para implementar redes privadas a VPNs través de AWS Direct Connect redes. Con la capacidad de VPN de IP privada, los clientes no tienen que implementar ni administrar su propia infraestructura de VPN. De este modo, se simplifican las operaciones de la red y se reducen los costos.
- Mejora de la seguridad: anteriormente, los clientes tenían que utilizar una interfaz AWS Direct Connect virtual pública (VIF) para cifrar el tráfico AWS Direct Connect, lo que requería direcciones IP públicas para los puntos finales de la VPN. El uso del IPs sistema público aumenta la probabilidad de sufrir ataques externos (DOS), lo que a su vez obliga a los clientes a implementar equipos de seguridad adicionales para proteger la red. Además, un VIF público abre el acceso entre todos los servicios AWS públicos y las redes locales de los clientes, lo que aumenta la gravedad del riesgo. La función de VPN con IP privada permite el cifrado en AWS Direct Connect tránsito VIFs (en lugar de hacerlo público VIFs), además de la posibilidad de configurarlo de forma privada. IPs Esto proporciona conectividad end-to-end privada además del cifrado, lo que mejora la seguridad general.

- Mayor escala de rutas: las conexiones VPN IP privadas ofrecen límites de ruta más altos (5000 rutas de salida y 1000 rutas de entrada) en comparación con las conexiones individuales AWS Direct Connect , que actualmente tienen un límite de 200 rutas de salida y 100 de entrada.

Cómo funciona la VPN de IP privada

La Site-to-Site VPN IP privada funciona a través de una interfaz virtual de AWS Direct Connect tránsito (VIF). Utiliza una AWS Direct Connect puerta de enlace y una puerta de enlace de tránsito para interconectar sus redes locales. AWS VPCs Una conexión VPN IP privada tiene puntos de terminación en la pasarela de tránsito, por un AWS lado, y en el dispositivo de puerta de enlace del cliente, en el lado local. Debe asignar direcciones IP privadas a los extremos de los IPsec túneles de la pasarela de tránsito y del dispositivo de puerta de enlace del cliente. Puede usar direcciones IP privadas de uno RFC1918 o varios rangos de IPv4 direcciones RFC6598 privadas.

Adjunta una conexión de VPN de IP privada a una puerta de enlace de tránsito. A continuación, enruta el tráfico entre el adjunto de la VPN y cualquier otra red VPCs (o cualquier otra red) que también esté conectada a la puerta de enlace de tránsito. Esto se hace asociando una tabla de enrutamiento con la conexión de VPN. En la dirección contraria, puede enrutar el tráfico desde su adjunto VPCs a la VPN con IP privada mediante tablas de enrutamiento asociadas a VPCs.

La tabla de rutas asociada al adjunto de la VPN puede ser la misma o diferente de la asociada al AWS Direct Connect adjunto subyacente. Esto le permite enrutar el tráfico cifrado y no cifrado simultáneamente entre su red VPCs y la local.

Para obtener más información sobre la ruta de tráfico que sale de la VPN, consulte las políticas de enrutamiento de la interfaz virtual privada y de la interfaz virtual de tránsito en la Guía del usuario de AWS Direct Connect .

Tareas

- Crear una IP privada a AWS Site-to-Site VPN través de AWS Direct Connect

Crear una IP privada a AWS Site-to-Site VPN través de AWS Direct Connect

Para crear una VPN con IP privada, AWS Direct Connect sigue estos pasos. Antes de crear la VPN de IP privada a través de Direct Connect, debe asegurarse de crear primero una puerta de enlace de tránsito y una puerta de enlace de Direct Connect. Después de crear las dos puertas de enlace,

debe crear una asociación entre las dos. Estos requisitos previos se describen en la tabla siguiente. Una vez que haya creado y asociado las dos puertas de enlace, creará una puerta de enlace para clientes de VPN y una conexión mediante esa asociación.

Requisitos previos

En la siguiente tabla se describen los requisitos previos a la creación de una VPN de IP privada a través de Direct Connect.

Elemento	Pasos	Información
Prepare la puerta de enlace de tránsito para la Site-to-Site VPN.	Cree la puerta de enlace de tránsito mediante la consola Amazon Virtual Private Cloud (VPC) o mediante la línea de comandos o la API. Consulte Puertas de enlace de tránsito en la Guía de puertas de enlace de tránsito de Amazon VPC.	Una puerta de enlace de tránsito es un centro de tránsito de red que puede usar para interconectar sus VPCs redes con las locales. Puede crear una nueva puerta de enlace de tránsito o utilizar una ya existente para la conexión de VPN de IP privada. Al crear la puerta de enlace de tránsito, o al modificar una ya existente, se especifica un bloque de CIDR de IP privada para la conexión. **Note** Al especificar el bloque de CIDR de la puerta de enlace de tránsito que se va a asociar a su VPN de IP privada, asegúrese de que el bloque de CIDR no se solapa con ninguna dirección

Elemento	Pasos	Información
		IP de ninguna otra conexión de red en la puerta de enlace de tránsito. Si algún bloque de CIDR de IP se solapa, puede provocar problemas de configuración con su dispositivo de puerta de enlace de cliente.
Cree la AWS Direct Connect puerta de enlace para Site-to-Site la VPN.	Cree la puerta de enlace de Direct Connect mediante la consola de Direct Connect o mediante la línea de comandos o la API. Consulte Crear una puerta de enlace AWS Direct Connect en la Guía AWS Direct Connect del usuario.	Una puerta de enlace Direct Connect le permite conectar interfaces virtuales (VIFs) en varias AWS regiones. Esta puerta de enlace se utiliza para conectarse a VIF.

Elemento	Pasos	Información
Cree la asociación de pasarelas de tránsito para la Site-to-Site VPN.	Cree la asociación entre la puerta de enlace de Direct Connect y la puerta de enlace de tránsito mediante la consola de Direct Connect o mediante la línea de comandos o la API. Consulte Asociar o AWS Direct Connect desasociar una pasarela de tránsito en la Guía del AWS Direct Connect usuario.	Después de crear la AWS Direct Connect puerta de enlace, cree una asociación de puerta de enlace de tránsito para la AWS Direct Connect puerta de enlace. Especifique el CIDR de IP privada para la puerta de enlace de tránsito que se identificó anteriormente en la lista de prefijos permitidos.

Cree la puerta de enlace del cliente y la conexión para la Site-to-Site VPN

Una pasarela de clientes es un recurso que se crea en él AWS. Representa el dispositivo de puerta de enlace de cliente en las instalaciones. Cuando crea una pasarela de clientes, proporciona información sobre su dispositivo a AWS. Para obtener más información, consulta Puerta de enlace de cliente.

Para crear una gateway de cliente con la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Puertas de enlace de cliente.
3. Elija Crear puerta de enlace de cliente.
4. (Opcional) En Name tag (Etiqueta de nombre), ingrese un nombre para la puerta de enlace de cliente. Esta acción creará una etiqueta con una clave de `Name` y el valor que especifique.
5. En BGP ASN, ingrese un número de sistema autónomo (ASN) para protocolo de puerta de enlace fronteriza (BGP) de la puerta de enlace de cliente.
6. En IP address (Dirección IP), ingrese la dirección IP privada de su dispositivo de puerta de enlace de cliente.

> **Important**
>
> Al configurar la IP AWS privada AWS Site-to-Site VPN, debe especificar sus propias direcciones IP de punto final del túnel mediante las direcciones RFC 1918. No utilice las direcciones point-to-point IP para la interconexión eBGP entre el router de puerta de enlace del cliente y el punto final. AWS Direct Connect AWS recomienda utilizar una interfaz LAN o de bucle invertido en el router de puerta de enlace del cliente como dirección de origen o destino en lugar de conexiones. point-to-point
> Para obtener más información sobre la RFC 1918, consulte Address Allocation for Private Internets.

7. (Opcional) En Device (Dispositivo), ingrese un nombre para el dispositivo que aloja esta puerta de enlace de cliente.
8. Elija Crear puerta de enlace de cliente.
9. En el panel de navegación, seleccione las conexiones Site-to-Site VPN.
10. Elija Create VPN Connection (Crear conexión VPN).
11. (Opcional) En la etiqueta de nombre, introduzca un nombre para la conexión Site-to-Site VPN. Esta acción creará una etiqueta con una clave de `Name` y el valor que especifique.
12. En Target gateway type (Tipo de puerta de enlace de destino), elija Transit gateway (Puerta de enlace de tránsito). A continuación, elija la puerta de enlace de tránsito que identificó anteriormente.
13. En Customer gateway (Puerta de enlace de cliente), seleccione Existing (Existente). A continuación, elija la puerta de enlace de cliente que creó anteriormente.
14. Seleccione una de las opciones de direccionamiento en función de si el dispositivo de gateway de cliente da soporte al protocolo de gateway fronteriza (BGP):
    - Si el dispositivo de gateway de cliente da soporte a BGP, elija Dynamic (requires BGP) (Dinámico [requiere BGP]).
    - Si el dispositivo de gateway de cliente no da soporte a BGP, elija Static (Estático).
15. En la versión Túnel dentro de IP, especifique si los túneles VPN admiten IPv4 IPv6 tráfico.
16. (Opcional) Si especificó IPv4la versión Túnel dentro de IP, también puede especificar los rangos de IPv4 CIDR para la puerta de enlace del cliente y AWS los lados que pueden comunicarse a través de los túneles VPN. El valor predeterminado es `0.0.0.0/0`.

Si especificó IPv6la versión Tunnel inside IP, si lo desea, puede especificar los rangos de IPv6 CIDR para la puerta de enlace del cliente y AWS los lados que pueden comunicarse a través de los túneles VPN. El valor predeterminado para ambos rangos es `::/0`.

17. Para el tipo de dirección IP externa, elija PrivateIpv4.
18. En el campo ID del adjunto de transporte, elija el adjunto de la pasarela de tránsito correspondiente a la AWS Direct Connect pasarela correspondiente.
19. Elija Create VPN Connection (Crear conexión VPN).

> **Note**
>
> La opción Enable acceleration (Habilitar aceleración) no es aplicable a las conexiones de VPN sobre AWS Direct Connect.

Para crear una gateway de cliente mediante la línea de comando o API

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

Seguridad en AWS Site-to-Site una VPN

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de los centros de datos y las arquitecturas de red diseñados para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre AWS usted y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la Nube de AWS. AWS también le proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los AWS programas de de . Para obtener más información sobre los programas de cumplimiento que se aplican a las AWS Site-to-Site VPN, consulte AWS Servicios incluidos .AWS
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. También eres responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y la normativa aplicables.

Esta documentación le ayuda a entender cómo aplicar el modelo de responsabilidad compartida al utilizar Site-to-Site una VPN. Los siguientes temas le muestran cómo configurar la Site-to-Site VPN para cumplir sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger sus recursos de Site-to-Site VPN.

Contenido

Funciones AWS Site-to-Site VPN de seguridad mejoradas con Secrets Manager

La función Security Rebase de AWS Site-to-Site VPN proporciona capacidades de seguridad mejoradas que le proporcionan un mayor control y visibilidad de sus conexiones de VPN. Una mejora

clave es la capacidad de almacenar las claves previamente compartidas (PSKs) en el servicio de Site-to-Site VPN, en AWS Secrets Manager lugar de directamente, lo que permite una mejor gestión de los secretos y el cumplimiento de las mejores prácticas de seguridad. La función también incluye una `GetActiveVpnTunnelStatus` API que proporciona visibilidad en tiempo real de los parámetros de seguridad que se utilizan en los túneles VPN activos, incluidos los algoritmos de cifrado, los algoritmos de integridad y los grupos Diffie-Hellman para ambas fases del IKE. Además, ahora puede generar las configuraciones de seguridad recomendadas que imponen el uso de protocolos modernos, excluyendo opciones heredadas, como: IKEv1 Estas mejoras son especialmente valiosas si su organización necesita mantener estándares de seguridad estrictos, requiere registros de auditoría detallados de sus configuraciones de VPN o quiere asegurarse de que sus conexiones VPN utilizan los protocolos más seguros disponibles.

Contenido

Cambie la clave previamente compartida de Secrets Manager en AWS Site-to-Site VPN

Si no se puede acceder a tu túnel en Secrets Manager, puedes cambiar la clave previamente compartida de ese túnel.

> **Note**
>
> - Al cambiar la clave previamente compartida, asegúrese de tener los permisos de IAM necesarios para ambos servicios Secrets Manager.
> - Tras cambiar la clave previamente compartida de un túnel VPN, la conectividad se interrumpe durante varios minutos. Asegúrese de planificar el tiempo de inactividad previsto.

Para cambiar la clave previamente compartida de Secrets Manager para un túnel VPN

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, selecciona Conexiones Site-to-Site VPN.
3. Seleccione la conexión Site-to-Site VPN y elija Acciones, Modificar las opciones del túnel VPN.

4. En Dirección IP externa del túnel de VPN, elija la IP del punto de conexión del túnel de VPN.
5. En la Nueva clave previamente compartida, elige una nueva clave previamente compartida.

> **Note**
>
> Esta opción solo está disponible para las claves almacenadas en Secrets Manager.

6. Seleccione Save changes (Guardar cambios).
7. Repita estos pasos para cualquier otro túnel.

Cambie el modo de almacenamiento de claves previamente compartidas en AWS Site-to-Site VPN

Cambie el modo de almacenamiento de claves previamente compartidas para un túnel VPN existente.

> **Note**
>
> - Al cambiar los modos de almacenamiento, asegúrese de tener los permisos de IAM necesarios para los servicios Site-to-Site VPN y Secrets Manager.
> - Tras cambiar el modo de almacenamiento de un túnel VPN, la conectividad se interrumpe durante varios minutos. Asegúrese de planificar el tiempo de inactividad previsto.

Para cambiar el modo de almacenamiento de claves previamente compartidas

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, selecciona las conexiones Site-to-Site VPN.
3. Seleccione la conexión Site-to-Site VPN y elija Acciones, Modificar las opciones del túnel VPN.
4. En Dirección IP externa del túnel de VPN, elija la IP del punto de conexión del túnel de VPN.
5. En Almacenamiento de claves previamente compartidas, elige uno de los siguientes tipos de almacenamiento de claves previamente compartidas.

   - Estándar: la clave previamente compartida se almacena directamente en el Site-to-Site servicio de VPN.

- Secrets Manager: la clave previamente compartida se almacena mediante AWS Secrets Manager. Para obtener más información sobre Secrets Manager, consulteFunciones de seguridad mejoradas con Secrets Manager.

6. Seleccione Save changes (Guardar cambios).

Al cambiar el modo de almacenamiento de Secrets Manager a Standard:

- La clave previamente compartida se elimina de Secrets Manager y se traslada al servicio Site-to-Site VPN.
- La entrada al túnel se elimina del secreto de Secrets Manager.

Al cambiar el modo de almacenamiento de Standard a Secrets Manager:

- La clave previamente compartida se elimina del Site-to-Site servicio VPN
- Se crea un nuevo secreto de Secrets Manager, si aún no existe uno.
- La nueva clave previamente compartida se guarda en Secrets Manager.

Protección de datos en VPN AWS Site-to-Site

El modelo de se aplica a protección de datos en las AWS Site-to-Site VPN. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global en la que se ejecutan todos los Nube de AWS. Eres responsable de mantener el control sobre el contenido alojado en esta infraestructura. También eres responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulta las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulta la publicación de blog sobre el Modelo de responsabilidad compartida de AWS y GDPR en el Blog de seguridad de AWS .

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utiliza la autenticación multifactor (MFA) en cada cuenta.

- Se utiliza SSL/TLS para comunicarse con AWS los recursos. Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con AWS CloudTrail. Para obtener información sobre el uso de CloudTrail senderos para capturar AWS actividades, consulte Cómo trabajar con CloudTrail senderos en la Guía del AWS CloudTrail usuario.
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utiliza servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-3 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulta Estándar de procesamiento de la información federal (FIPS) 140-3.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabaja con Site-to-Site una VPN u otra Servicios de AWS mediante la consola, la API o. AWS CLI AWS SDKs Cualquier dato que ingrese en etiquetas o campos de texto de formato libre utilizados para nombres se puede emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

Privacidad del tráfico entre redes

Una conexión Site-to-Site VPN conecta de forma privada la VPC a la red local. Los datos que se transfieren entre su VPC y su red se direccionan a través de una conexión de VPN cifrada para ayudarlo a mantener la confidencialidad y la integridad de los datos en tránsito. Amazon admite conexiones VPN de seguridad mediante el Protocolo de Internet (IPsec). IPsec es un conjunto de protocolos para proteger las comunicaciones IP mediante la autenticación y el cifrado de cada paquete IP de un flujo de datos.

Cada conexión Site-to-Site VPN consta de dos túneles IPsec VPN cifrados que enlazan con AWS su red. El tráfico de cada túnel se puede cifrar con AES128 o AES256 utilizar grupos Diffie-Hellman para el intercambio de claves, lo que proporciona un secreto directo perfecto. AWS se autentica con nuestras funciones de hash. SHA1 SHA2

Las instancias de la VPC no requieren una dirección IP pública para conectarse a los recursos del otro lado de la conexión de la Site-to-Site VPN. Las instancias pueden enrutar su tráfico de Internet a través de la conexión Site-to-Site VPN a la red local. A continuación, pueden obtener acceso a Internet a través de los puntos de tráfico salientes y de sus dispositivos de monitoreo y seguridad de la red.

Consulte los siguientes temas para obtener más información:

- Opciones de túnel para su AWS Site-to-Site VPN conexión: Proporciona información sobre IPsec las opciones de intercambio de claves de Internet (IKE) disponibles para cada túnel.
- AWS Site-to-Site VPN opciones de autenticación de túnel: proporciona información sobre las opciones de autenticación de los puntos de enlace del túnel de VPN.
- Requisitos para un dispositivo de pasarela de AWS Site-to-Site VPN clientes: proporciona información sobre los requisitos del dispositivo de gateway de cliente en su extremo de la conexión de VPN.
- Comunicación segura entre AWS Site-to-Site VPN conexiones mediante VPN CloudHub: Si tiene varias conexiones de Site-to-Site VPN, puede proporcionar una comunicación segura entre sus sitios locales mediante la AWS VPN CloudHub.

Administración de identidad y acceso para VPN AWS Site-to-Site

AWS Identity and Access Management (IAM) es un sistema Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a AWS los recursos. Los administradores de IAM controlan quién puede autenticarse (iniciar sesión) y quién puede autorizarse (tener permisos) para usar Site-to-Site los recursos de la VPN. El IAM es un Servicio de AWS servicio que puede utilizar sin coste adicional.

Temas

- Público
- Autenticación con identidades
- Administración de acceso mediante políticas
- Cómo funciona la AWS Site-to-Site VPN con IAM
- Ejemplos de políticas de VPN basadas en la identidad AWS Site-to-Site
- Solución de problemas de identidad y acceso a la AWS Site-to-Site VPN

- AWS políticas gestionadas para VPN Site-to-Site
- Uso de funciones vinculadas a servicios para la VPN Site-to-Site

Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo que realices en Site-to-Site la VPN.

Usuario del servicio: si utiliza el servicio de Site-to-Site VPN para realizar su trabajo, el administrador le proporcionará las credenciales y los permisos que necesita. A medida que vaya utilizando más funciones de la Site-to-Site VPN para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarle a solicitar los permisos correctos al administrador. Si no puede acceder a una función de la Site-to-Site VPN, consulteSolución de problemas de identidad y acceso a la AWS Site-to-Site VPN.

Administrador de servicios: si estás a cargo de los recursos de Site-to-Site VPN de tu empresa, probablemente tengas acceso total a la Site-to-Site VPN. Tu trabajo consiste en determinar a qué funciones y recursos de la Site-to-Site VPN deben acceder los usuarios del servicio. Luego, debe enviar solicitudes a su gestionador de IAM para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información sobre cómo su empresa puede utilizar la IAM con Site-to-Site una VPN, consulteCómo funciona la AWS Site-to-Site VPN con IAM.

Administrador de IAM: si es administrador de IAM, puede que le interese obtener más información sobre cómo redactar políticas para administrar el acceso a la VPN. Site-to-Site Para ver ejemplos de políticas de Site-to-Site VPN basadas en la identidad que puede usar en IAM, consulte. Ejemplos de políticas de VPN basadas en la identidad AWS Site-to-Site

Autenticación con identidades

La autenticación es la forma en que inicias sesión para AWS usar tus credenciales de identidad. Debe estar autenticado (con quien haya iniciado sesión AWS) como usuario de IAM o asumiendo una función de IAM. Usuario raíz de la cuenta de AWS

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (Centro de identidades de IAM), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada,

su gestionador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accedes AWS mediante la federación, estás asumiendo un rol de forma indirecta.

Según el tipo de usuario que sea, puede iniciar sesión en el portal AWS Management Console o en el de AWS acceso. Para obtener más información sobre cómo iniciar sesión AWS, consulte Cómo iniciar sesión Cuenta de AWS en su Guía del AWS Sign-In usuario.

Si accede AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente sus solicitudes con sus credenciales. Si no utilizas AWS herramientas, debes firmar las solicitudes tú mismo. Para obtener más información sobre la firma de solicitudes, consulte AWS Signature Versión 4 para solicitudes API en la Guía del usuario de IAM.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, le AWS recomienda que utilice la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte Autenticación multifactor en la Guía del usuario de AWS IAM Identity Center y Autenticación multifactor AWS en IAM en la Guía del usuario de IAM.

Cuenta de AWS usuario root

Al crear una Cuenta de AWS, comienza con una identidad de inicio de sesión que tiene acceso completo a todos Servicios de AWS los recursos de la cuenta. Esta identidad se denomina usuario Cuenta de AWS raíz y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizaste para crear la cuenta. Recomendamos encarecidamente que no utiliza el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulta Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos, incluidos los que requieren acceso de administrador, que utilicen la federación con un proveedor de identidades para acceder Servicios de AWS mediante credenciales temporales.

Una identidad federada es un usuario del directorio de usuarios de su empresa, un proveedor de identidades web AWS Directory Service, el directorio del Centro de Identidad o cualquier usuario al que acceda Servicios de AWS mediante las credenciales proporcionadas a través de una fuente de

identidad. Cuando las identidades federadas acceden Cuentas de AWS, asumen funciones y las funciones proporcionan credenciales temporales.

Para una administración de acceso centralizada, le recomendamos que utiliza AWS IAM Identity Center. Puede crear usuarios y grupos en el Centro de identidades de IAM, o puede conectarse y sincronizarse con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todas sus Cuentas de AWS aplicaciones. Para obtener más información, consulta ¿Qué es el Centro de identidades de IAM? en la Guía del usuario de AWS IAM Identity Center .

Usuarios y grupos de IAM

Un usuario de IAM es una identidad propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos emplear credenciales temporales, en lugar de crear usuarios de IAM que tengan credenciales de larga duración como contraseñas y claves de acceso. No obstante, si tiene casos de uso específicos que requieran credenciales de larga duración con usuarios de IAM, recomendamos rotar las claves de acceso. Para más información, consulte Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración en la Guía del usuario de IAM.

Un grupo de IAM es una identidad que especifica un conjunto de usuarios de IAM. No puedes iniciar sesión como grupo. Puedes usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos para grandes conjuntos de usuarios. Por ejemplo, puede asignar un nombre a un grupo IAMAdminsy concederle permisos para administrar los recursos de IAM.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales de larga duración permanentes; no obstante, los roles proporcionan credenciales temporales. Para obtener más información, consulte Casos de uso para usuarios de IAM en la Guía del usuario de IAM.

Roles de IAM

Un rol de IAM es una identidad dentro de usted Cuenta de AWS que tiene permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una persona determinada. Para asumir temporalmente un rol de IAM en el AWS Management Console, puede cambiar de un rol de usuario a uno de IAM (consola). Puedes asumir un rol llamando a una operación de AWS API AWS CLI o usando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulta Métodos para asumir un rol en la Guía del usuario de IAM.

Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

- Acceso de usuario federado: para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información acerca de roles de federación, consulte Crear un rol para un proveedor de identidad de terceros (federación) en la Guía de usuario de IAM. Si utiliza el IAM Identity Center, debe configurar un conjunto de permisos. IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué pueden acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulta Conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center .
- Permisos de usuario de IAM temporales: un usuario de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- Acceso entre cuentas: puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunas Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para obtener información acerca de la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulta Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.
- Acceso entre servicios: algunos Servicios de AWS utilizan funciones en otros Servicios de AWS. Por ejemplo, cuando realizas una llamada en un servicio, es habitual que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado al servicio.
  - Sesiones de acceso directo (FAS): cuando utilizas un usuario o un rol de IAM para realizar acciones en AWS ellas, se te considera principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. El FAS utiliza los permisos del principal que llama Servicio de AWS y los solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.
  - Rol de servicio: un rol de servicio es un rol de IAM que adopta un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio

desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

- Función vinculada al servicio: una función vinculada a un servicio es un tipo de función de servicio que está vinculada a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

- Aplicaciones que se ejecutan en Amazon EC2: puedes usar un rol de IAM para administrar las credenciales temporales de las aplicaciones que se ejecutan en una EC2 instancia y realizan AWS CLI solicitudes a la AWS API. Esto es preferible a almacenar las claves de acceso en la EC2 instancia. Para asignar un AWS rol a una EC2 instancia y ponerlo a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene el rol y permite que los programas que se ejecutan en la EC2 instancia obtengan credenciales temporales. Para obtener más información, consulte Usar un rol de IAM para conceder permisos a las aplicaciones que se ejecutan en EC2 instancias de Amazon en la Guía del usuario de IAM.

Administración de acceso mediante políticas

El acceso se controla AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política es un objeto AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando un director (usuario, usuario raíz o sesión de rol) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulte Información general de políticas JSON en la Guía del usuario de IAM.

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Las políticas de IAM definen permisos para una acción independientemente del método que se utiliza para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción

`iam:GetRole`. Un usuario con esa política puede obtener información sobre el rol de la API AWS Management Console AWS CLI, la o la AWS API.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Las políticas basadas en identidades pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede adjuntar a varios usuarios, grupos y roles de su Cuenta de AWS empresa. Las políticas administradas incluyen políticas AWS administradas y políticas administradas por el cliente. Para obtener más información sobre cómo elegir una política administrada o una política insertada, consulte Elegir entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

Listas de control de acceso () ACLs

Las listas de control de acceso (ACLs) controlan qué responsables (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLs son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Amazon S3 y Amazon VPC son ejemplos de servicios compatibles. AWS WAF ACLs Para obtener más información ACLs, consulte la descripción general de la lista de control de acceso (ACL) en la Guía para desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

AWS admite tipos de políticas adicionales y menos comunes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- Límites de permisos: un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM (usuario o rol de IAM). Puedes establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicios (SCPs): SCPs son políticas de JSON que especifican los permisos máximos para una organización o unidad organizativa (OU). AWS Organizations AWS Organizations es un servicio para agrupar y administrar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilitas todas las funciones de una organización, puedes aplicar políticas de control de servicios (SCPs) a una o a todas tus cuentas. El SCP limita los permisos de las entidades en las cuentas de los miembros, incluidas las de cada una Usuario raíz de la cuenta de AWS. Para obtener más información sobre Organizations SCPs, consulte las políticas de control de servicios en la Guía del AWS Organizations usuario.
- Políticas de control de recursos (RCPs): RCPs son políticas de JSON que puedes usar para establecer los permisos máximos disponibles para los recursos de tus cuentas sin actualizar las políticas de IAM asociadas a cada recurso que poseas. El RCP limita los permisos de los recursos en las cuentas de los miembros y puede afectar a los permisos efectivos de las identidades, incluidos los permisos Usuario raíz de la cuenta de AWS, independientemente de si pertenecen a su organización. Para obtener más información sobre Organizations e RCPs incluir una lista de Servicios de AWS ese apoyo RCPs, consulte Políticas de control de recursos (RCPs) en la Guía del AWS Organizations usuario.
- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades

del rol y las políticas de la sesión. Los permisos también pueden proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para más información, consulte Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo se AWS determina si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la Guía del usuario de IAM.

Cómo funciona la AWS Site-to-Site VPN con IAM

Antes de utilizar IAM para gestionar el acceso a la Site-to-Site VPN, infórmese sobre las funciones de IAM disponibles para su uso con la VPN. Site-to-Site

Funciones de IAM que puede utilizar con una VPN AWS Site-to-Site

Característica de IAM	Site-to-Site Soporte de VPN
Políticas basadas en identidades	Sí
Políticas basadas en recursos	No
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política (específicas del servicio)	Sí
ACLs	No
ABAC (etiquetas en políticas)	No
Credenciales temporales	Sí
Permisos de entidades principales	Sí

Característica de IAM	Site-to-Site Soporte de VPN
Roles de servicio	Sí
Roles vinculados al servicio	Sí

Para obtener una visión general de cómo funcionan la Site-to-Site VPN y otros AWS servicios con la mayoría de las funciones de IAM, consulte AWS los servicios que funcionan con IAM en la Guía del usuario de IAM.

Políticas de VPN basadas en la identidad Site-to-Site

Compatibilidad con las políticas basadas en identidad: sí

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está asociada. Para obtener más información sobre los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de las políticas de JSON de IAM en la Guía del usuario de IAM.

Ejemplos de políticas de VPN basadas en la identidad Site-to-Site

Para ver ejemplos de políticas de Site-to-Site VPN basadas en la identidad, consulte. Ejemplos de políticas de VPN basadas en la identidad AWS Site-to-Site

Políticas basadas en recursos dentro de la VPN Site-to-Site

Admite políticas basadas en recursos: no

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los

administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Añadir a una política en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando el principal y el recurso son diferentes Cuentas de AWS, el administrador de IAM de la cuenta de confianza también debe conceder a la entidad principal (usuario o rol) permiso para acceder al recurso. Para conceder el permiso, adjunte la entidad a una política basada en identidad. Sin embargo, si la política basada en recursos concede acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para obtener más información, consulte Cross account resource access in IAM en la Guía del usuario de IAM.

Acciones políticas para la VPN Site-to-Site

Compatibilidad con las acciones de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Las acciones políticas suelen tener el mismo nombre que la operación de AWS API asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de las acciones de la Site-to-Site VPN, consulte las acciones definidas por la AWS Site-to-Site VPN en la Referencia de autorización del servicio.

Las acciones políticas de la Site-to-Site VPN utilizan el siguiente prefijo antes de la acción:

```
ec2
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

```
"Action": [
      "ec2:action1",
      "ec2:action2"
         ]
```

Para ver ejemplos de políticas de Site-to-Site VPN basadas en la identidad, consulte. Ejemplos de políticas de VPN basadas en la identidad AWS Site-to-Site

Recursos de políticas para VPN Site-to-Site

Compatibilidad con los recursos de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puedes realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Puedes hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utiliza un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

```
"Resource": "*"
```

Para ver una lista de los tipos de recursos de Site-to-Site VPN y sus tipos ARNs, consulte los recursos definidos por la AWS Site-to-Site VPN en la Referencia de autorización de servicios. Para saber con qué acciones puede especificar el ARN de cada recurso, consulte Acciones definidas por AWS Site-to-Site la VPN.

Para ver ejemplos de políticas de Site-to-Site VPN basadas en la identidad, consulte. Ejemplos de políticas de VPN basadas en la identidad AWS Site-to-Site

Claves de condición de política para la VPN Site-to-Site

Compatibilidad con claves de condición de políticas específicas del servicio: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puedes realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puedes crear expresiones condicionales que utilizan operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación `AND` lógica. Si especifica varios valores para una única clave de condición, AWS evalúa la condición mediante una `OR` operación lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puedes utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puedes conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para más información, consulta Elementos de la política de IAM: variables y etiquetas en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

Para ver una lista de las claves de condición de la Site-to-Site VPN, consulte las claves de condición de la AWS Site-to-Site VPN en la Referencia de autorización de servicios. Para saber con qué acciones y recursos puede utilizar una clave condicionada, consulte Acciones definidas por la AWS Site-to-Site VPN.

Para ver ejemplos de políticas de Site-to-Site VPN basadas en la identidad, consulte. Ejemplos de políticas de VPN basadas en la identidad AWS Site-to-Site

ACLs en una VPN Site-to-Site

Soporta ACLs: No

Las listas de control de acceso (ACLs) controlan qué directores (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLs son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

ABAC con VPN Site-to-Site

Compatibilidad con ABAC (etiquetas en las políticas): no

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos. En AWS, estos atributos se denominan etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a muchos AWS recursos. El etiquetado de entidades y recursos es el primer paso de ABAC. A continuación, designa las políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso al que se intenta acceder.

ABAC es útil en entornos que crecen con rapidez y ayuda en situaciones en las que la administración de las políticas resulta engorrosa.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte Definición de permisos con la autorización de ABAC en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

Uso de credenciales temporales con una VPN Site-to-Site

Compatibilidad con credenciales temporales: sí

Algunas Servicios de AWS no funcionan cuando inicias sesión con credenciales temporales. Para obtener información adicional, incluidas las que Servicios de AWS funcionan con credenciales temporales, consulta Cómo Servicios de AWS funcionan con IAM en la Guía del usuario de IAM.

Utiliza credenciales temporales si inicia sesión en ellas AWS Management Console mediante cualquier método excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accedes

AWS mediante el enlace de inicio de sesión único (SSO) de tu empresa, ese proceso crea automáticamente credenciales temporales. También crea credenciales temporales de forma automática cuando inicia sesión en la consola como usuario y luego cambia de rol. Para obtener más información sobre el cambio de roles, consulte Cambio de un usuario a un rol de IAM (consola) en la Guía del usuario de IAM.

Puedes crear credenciales temporales manualmente mediante la AWS CLI API o. AWS A continuación, puede utilizar esas credenciales temporales para acceder AWS. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para obtener más información, consulte Credenciales de seguridad temporales en IAM.

Permisos principales entre servicios para VPN Site-to-Site

Admite sesiones de acceso directo (FAS): sí

Cuando utilizas un usuario o un rol de IAM para realizar acciones en él AWS, se te considera principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos del principal que llama y los que solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Servicio de AWS Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.

Funciones de servicio para la Site-to-Site VPN

Compatibilidad con roles de servicio: sí

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

> **Warning**
>
> Cambiar los permisos de un rol de servicio podría interrumpir la funcionalidad de la Site-to-Site VPN. Edite las funciones de servicio solo cuando la Site-to-Site VPN proporcione instrucciones para hacerlo.

Funciones vinculadas al servicio para la VPN Site-to-Site

Admite roles vinculados a servicios: sí

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puedes ver, pero no editar, los permisos de los roles vinculados a servicios.

Para más información sobre cómo crear o administrar roles vinculados a servicios, consulta Servicios de AWS que funcionan con IAM. Busque un servicio en la tabla que incluya `Yes` en la columna Rol vinculado a un servicio. Seleccione el vínculo Sí para ver la documentación acerca del rol vinculado a servicios para ese servicio.

Ejemplos de políticas de VPN basadas en la identidad AWS Site-to-Site

De forma predeterminada, los usuarios y los roles no tienen permiso para crear o modificar los recursos de la Site-to-Site VPN. Tampoco pueden realizar tareas mediante la AWS Management Console, AWS Command Line Interface (AWS CLI) o la AWS API. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puedes añadir las políticas de IAM a roles y los usuarios puedes asumirlos.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte Creación de políticas de IAM (consola) en la Guía del usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos por la Site-to-Site VPN, incluido el ARNs formato de cada uno de los tipos de recursos, consulte Acciones, recursos y claves de condición de la AWS Site-to-Site VPN en la Referencia de autorización de servicios.

Temas

- Prácticas recomendadas sobre las políticas
- Uso de la consola VPN Site-to-Site
- Describa las conexiones Site-to-Site VPN específicas
- Cree y describa los recursos necesarios para una AWS Site-to-Site VPN conexión

Prácticas recomendadas sobre las políticas

Las políticas basadas en la identidad determinan si alguien puede crear recursos de Site-to-Site VPN de su cuenta, acceder a ellos o eliminarlos. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulta las políticas administradas por AWS o las políticas administradas por AWS para funciones de tarea en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulta Políticas y permisos en IAM en la Guía del usuario de IAM.
- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo AWS CloudFormation. Para obtener más información, consulta Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utiliza el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte Validación de políticas con el Analizador de acceso de IAM en la Guía del usuario de IAM.
- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para exigir la

MFA cuando se invoquen las operaciones de la API, añada condiciones de MFA a sus políticas. Para más información, consulte Acceso seguro a la API con MFA en la Guía del usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Uso de la consola VPN Site-to-Site

Para acceder a la consola AWS Site-to-Site VPN, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver detalles sobre los recursos de Site-to-Site VPN de su propiedad Cuenta de AWS. Si crea una política basada en identidades que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

No es necesario que concedas permisos mínimos de consola a los usuarios que solo realicen llamadas a la API AWS CLI o a la AWS API. En su lugar, permite el acceso únicamente a las acciones que coincidan con la operación de API que intentan realizar.

Para garantizar que los usuarios y los roles puedan seguir utilizando la consola Site-to-Site VPN, asocie también la Site-to-Site VPN `AmazonVPCFullAccess` o la política `AmazonVPCReadOnlyAccess` AWS gestionada a las entidades. Para obtener más información, consulte Adición de permisos a un usuario en la Guía del usuario de IAM:

Describa las conexiones Site-to-Site VPN específicas

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "ec2:DescribeVpnConnections"
         ],
         "Resource": ["*"]
      }
   ]
}
```

Cree y describa los recursos necesarios para una AWS Site-to-Site VPN conexión

```
{
   "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"
            }
         }
      }
   ]
}
```

Solución de problemas de identidad y acceso a la AWS Site-to-Site VPN

Utilice la siguiente información como ayuda para diagnosticar y solucionar los problemas más comunes que pueden surgir al trabajar con Site-to-Site VPN e IAM.

Temas

- No estoy autorizado a realizar ninguna acción en la VPN Site-to-Site

- No estoy autorizado a realizar tareas como: PassRole
- Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos de Site-to-Site VPN

No estoy autorizado a realizar ninguna acción en la VPN Site-to-Site

Si recibe un error que indica que no tiene autorización para realizar una acción, las políticas se deben actualizar para permitirle realizar la acción.

En el siguiente ejemplo, el error se produce cuando el usuario de IAM `mateojackson` intenta utilizar la consola para consultar los detalles acerca de un recurso ficticio *`my-example-widget`*, pero no tiene los permisos ficticios `ec2:`*`GetWidget`*.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 ec2:GetWidget on resource: my-example-widget
```

En este caso, la política del usuario `mateojackson` debe actualizarse para permitir el acceso al recurso *`my-example-widget`* mediante la acción `ec2:`*`GetWidget`*.

Si necesita ayuda, póngase en contacto con su AWS administrador. El gestionador es la persona que le proporcionó las credenciales de inicio de sesión.

No estoy autorizado a realizar tareas como: PassRole

Si recibes un mensaje de error que indica que no estás autorizado a realizar la `iam:PassRole` acción, debes actualizar tus políticas para que puedas transferir una función a la Site-to-Site VPN.

Algunas Servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada al servicio. Para ello, debe tener permisos para transferir el rol al servicio.

El siguiente ejemplo de error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en la VPN. Site-to-Site Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su AWS administrador. El gestionador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos de Site-to-Site VPN

Puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admiten políticas basadas en recursos o listas de control de acceso (ACLs), puedes usar esas políticas para permitir que las personas accedan a tus recursos.

Para obtener más información, consulte lo siguiente:

- Para saber si la Site-to-Site VPN admite estas funciones, consulte. Cómo funciona la AWS Site-to-Site VPN con IAM
- Para obtener información sobre cómo proporcionar acceso a los recursos de su Cuentas de AWS propiedad, consulte Proporcionar acceso a un usuario de IAM en otro usuario de su propiedad Cuenta de AWS en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo proporcionar acceso a recursos que Cuentas de AWS son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulta Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.
- Para conocer sobre la diferencia entre las políticas basadas en roles y en recursos para el acceso entre cuentas, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

AWS políticas gestionadas para VPN Site-to-Site

Para añadir permisos a usuarios, grupos y roles, es más fácil usar políticas AWS administradas que escribirlas usted mismo. Se necesita tiempo y experiencia para crear políticas administradas por el cliente de IAM que proporcionen a su equipo solo los permisos necesarios. Para empezar rápidamente, puedes usar nuestras políticas AWS gestionadas. Estas políticas cubren casos de uso

comunes y están disponibles en tu AWS cuenta. Para obtener más información sobre las políticas AWS administradas, consulte las políticas AWS administradas en la Guía del usuario de IAM.

AWS los servicios mantienen y AWS actualizan las políticas gestionadas. No puede cambiar los permisos en las políticas AWS gestionadas. En ocasiones, los servicios agregan permisos adicionales a una política administrada de AWS para admitir características nuevas. Este tipo de actualización afecta a todas las identidades (usuarios, grupos y roles) donde se asocia la política. Es más probable que los servicios actualicen una política gestionada por AWS cuando se lanza una nueva característica o cuando se ponen a disposición nuevas operaciones. Los servicios no eliminan los permisos de una política AWS administrada, por lo que las actualizaciones de la política no afectarán a los permisos existentes.

Además, AWS admite políticas administradas para funciones laborales que abarcan varios servicios. Por ejemplo, la política `ReadOnlyAccess` AWS gestionada proporciona acceso de solo lectura a todos los AWS servicios y recursos. Cuando un servicio lanza una nueva función, AWS agrega permisos de solo lectura para nuevas operaciones y recursos. Para obtener una lista y descripciones de las políticas de funciones de trabajo, consulte Políticas administradas de AWS para funciones de trabajo en la Guía del usuario de IAM.

AWS política gestionada: AWSVPCS2 SVpn ServiceRolePolicy

Puede adjuntar la política `AWSVPCS2SVpnServiceRolePolicy` a las identidades de IAM. Esta política permite a la Site-to-Site VPN administrar un AWS Secrets Manager secreto dentro de la Site-to-Site VPN. Para obtener más información, consulte the section called “Cómo utilizar roles vinculados a servicios”.

Para ver los permisos de esta política, consulte AWSVPCS2SVpnServiceRolePolicy en la Referencia de la política administrada de AWS .

Site-to-Site La VPN actualiza las políticas AWS gestionadas

Consulta los detalles sobre las actualizaciones de las políticas AWS administradas de Site-to-Site VPN desde que este servicio comenzó a rastrear estos cambios en mayo de 2025.

Cambio	Descripción	Fecha
AWSVPCS2SVpnServiceRolePolicy- Política actualizada.	Se han añadido nuevos permisos a la política que permiten a la Site-to-Site VPN	14 de mayo de 2025

Cambio	Descripción	Fecha
	gestionar el secreto AWS Secrets Manager `s2svpn` gestionado de la conexión VPN.	

Uso de funciones vinculadas a servicios para la VPN Site-to-Site

AWS Site-to-Site La VPN usa roles AWS Identity and Access Management vinculados al servicio (IAM). Un rol vinculado a un servicio es un tipo único de rol de IAM que está vinculado directamente a la VPN. Site-to-Site La Site-to-Site VPN predefine las funciones vinculadas al servicio e incluyen todos los permisos que el servicio requiere para llamar a otros AWS servicios en su nombre.

Un rol vinculado a un servicio facilita la configuración de la Site-to-Site VPN, ya que no es necesario añadir manualmente los permisos necesarios. Site-to-Site La VPN define los permisos de sus funciones vinculadas al servicio y, a menos que se defina lo contrario, solo la Site-to-Site VPN puede asumir sus funciones. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se pueda adjuntar a ninguna otra entidad de IAM.

Solo es posible eliminar un rol vinculado a un servicio después de eliminar sus recursos relacionados. Esto protege sus recursos de Site-to-Site VPN porque no puede eliminar inadvertidamente el permiso de acceso a los recursos.

Permisos de rol vinculados al servicio para la VPN Site-to-Site

Site-to-Site La VPN usa la función vinculada al servicio denominada AWSServiceRoleForVPCS2SVPN: permite que la Site-to-Site VPN cree y administre los recursos relacionados con sus conexiones de VPN.

El rol vinculado al servicio de AWSService RoleFor VPCS2 SVPN confía en que el siguiente servicio asuma el rol:

- `s2svpn.amazonaws.com`

Este rol vinculado al servicio usa la política administrada AWSVPCS2 SVpn ServiceRolePolicy para completar las siguientes acciones en los recursos especificados:

- Al utilizar la autenticación mediante certificados para su conexión VPN, AWS Site-to-Site VPN exporta los AWS Certificate Manager certificados del túnel VPN para usarlos en los puntos finales del túnel VPN.
- Al utilizar la autenticación mediante certificados para su conexión VPN, AWS Site-to-Site VPN gestiona la renovación de los AWS Certificate Manager certificados del túnel VPN.
- Al utilizar el almacenamiento de claves SecretsManager previamente compartidas para su conexión VPN, AWS Site-to-Site VPN administra el secreto gestionado AWS Secrets Manager s2svpn de la conexión VPN.

Para ver los permisos de esta política, consulte AWSVPCS2SVpnServiceRolePolicy en la Referencia de la política administrada de AWS .

Cree un rol vinculado a un servicio para la VPN Site-to-Site

No necesita crear manualmente un rol vinculado a servicios. Al crear una pasarela de cliente con un certificado privado de ACM asociado en la AWS Management Console, la o la AWS API AWS CLI, la Site-to-Site VPN crea automáticamente la función vinculada al servicio.

Si elimina este rol vinculado a servicios y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Al crear una pasarela de clientes con un certificado privado de ACM asociado, la Site-to-Site VPN vuelve a crear la función vinculada al servicio para usted.

Edita un rol vinculado a un servicio para la VPN Site-to-Site

Site-to-Site La VPN no le permite editar el rol vinculado al servicio de AWSService RoleFor VPCS2 SVPN. Después de crear un rol vinculado al servicio, no podrá cambiar el nombre del rol, ya que varias entidades podrían hacer referencia al rol. Sin embargo, sí puede editar la descripción del rol con IAM. Para obtener más información, consulte la Descripción sobre cómo editar un rol vinculado al servicio en la Guía del usuario de IAM.

Elimine un rol vinculado a un servicio para la VPN Site-to-Site

Si ya no necesita usar una característica o servicio que requieran un rol vinculado a un servicio, le recomendamos que elimine dicho rol. Así no tendrá una entidad no utilizada que no se supervise ni mantenga de forma activa. Sin embargo, debe limpiar los recursos de su rol vinculado al servicio antes de eliminarlo manualmente.

> **Note**
>
> Si el servicio de Site-to-Site VPN utiliza el rol al intentar eliminar los recursos, es posible que la eliminación no se realice correctamente. En tal caso, espere unos minutos e intente de nuevo la operación.

Para eliminar los recursos de Site-to-Site VPN utilizados por la AWSService RoleFor VPCS2 SVPN

Este rol vinculado a servicios solo se puede eliminar después de suprimir todas las gateways de cliente que tienen un certificado privado de ACM asociado. Esto garantiza que no pueda eliminar inadvertidamente el permiso de acceso a los certificados ACM que utilizan las conexiones VPN. Site-to-Site

Para eliminar manualmente el rol vinculado a servicios mediante IAM

Utilice la consola de IAM AWS CLI, la o la AWS API para eliminar la función vinculada al servicio de SVPN. AWSService RoleFor VPCS2 Para obtener más información, consulte Eliminación de un rol vinculado a servicios en la Guía del usuario de IAM.

Resiliencia en AWS Site-to-Site VPN

La infraestructura AWS global se basa en AWS regiones y zonas de disponibilidad. AWS Las regiones proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que están conectadas mediante redes de baja latencia, alto rendimiento y alta redundancia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre las zonas sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de uno o varios centros de datos.

Para obtener más información sobre AWS las regiones y las zonas de disponibilidad, consulte Infraestructura global.AWS

Además de la infraestructura AWS global, la Site-to-Site VPN ofrece funciones que ayudan a satisfacer sus necesidades de respaldo y resiliencia de datos.

Dos túneles por conexión de VPN

Una conexión Site-to-Site VPN consta de dos túneles, cada uno de los cuales termina en una zona de disponibilidad diferente, para proporcionar una mayor disponibilidad a la VPC. Si se produce un

fallo en un dispositivo interno AWS, la conexión VPN pasa automáticamente al segundo túnel para que el acceso no se interrumpa. De vez en cuando, AWS también realiza un mantenimiento rutinario de la conexión VPN, lo que puede desactivar brevemente uno de los dos túneles de la conexión VPN. Para obtener más información, consulte AWS Site-to-Site VPN reemplazos de puntos finales de túneles. Al configurar su gateway de cliente, por tanto es importante que configure ambos túneles.

Redundancia

Para protegerte de una pérdida de conectividad en caso de que tu pasarela de cliente deje de estar disponible, puedes configurar una segunda conexión Site-to-Site VPN. Para obtener más información, consulte la siguiente documentación sobre :

- AWS Site-to-Site VPN Conexiones redundantes para conmutación por error
- Opciones de conectividad de Amazon Virtual Private Cloud
- Creación de una infraestructura de red multiVPC AWS escalable y segura

Seguridad de infraestructura en VPN AWS Site-to-Site

Como servicio gestionado, la AWS Site-to-Site VPN está protegida por la seguridad de la red AWS global. Para obtener información sobre los servicios AWS de seguridad y cómo se AWS protege la infraestructura, consulte Seguridad AWS en la nube. Para diseñar su AWS entorno utilizando las mejores prácticas de seguridad de la infraestructura, consulte Protección de infraestructuras en un marco de buena AWS arquitectura basado en el pilar de la seguridad.

Utiliza las llamadas a la API AWS publicadas para acceder a la Site-to-Site VPN a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con confidencialidad directa total (PFS) como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad principal de IAM. También puedes utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Supervisar una AWS Site-to-Site VPN conexión

La supervisión es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de la AWS Site-to-Site VPN conexión. Debe recopilar datos de monitorización de todas las partes de su solución para que le resulte más sencillo depurar un error que se produce en distintas partes del código, en caso de que ocurra. Sin embargo, antes de comenzar a monitorear su conexión Site-to-Site VPN, debe crear un plan de monitoreo que incluya respuestas a las siguientes preguntas:

- ¿Cuáles son los objetivos de la supervisión?
- ¿Qué recursos va a supervisar?
- ¿Con qué frecuencia va a supervisar estos recursos?
- ¿Qué herramientas de supervisión va a utilizar?
- ¿Quién se encargará de realizar las tareas de supervisión?
- ¿Quién debería recibir una notificación cuando surjan problemas?

El siguiente paso consiste en establecer un punto de referencia del desempeño de VPN normal en su entorno. Para ello se mide el desempeño en distintos momentos y bajo distintas condiciones de carga. A medida que monitorice su VPN, almacene los datos de monitorización históricos para que pueda compararlos con los datos de desempeño actual, identificar los patrones de desempeño normal y las anomalías en el desempeño, así como desarrollar métodos para la resolución de problemas.

Para establecer un punto de referencia, debe monitorizar los elementos siguientes:

- El estado de sus túneles de VPN
- Los datos que entran en el túnel
- Los datos que salen del túnel

Temas

Herramientas de supervisión

AWS proporciona varias herramientas que puede utilizar para supervisar una conexión Site-to-Site VPN. Puede configurar algunas de estas herramientas para que monitoricen por usted, pero otras herramientas requieren intervención manual. Le recomendamos que automatice las tareas de monitorización en la medida de lo posible.

Herramientas de supervisión automatizadas

Puede utilizar las siguientes herramientas de supervisión automática para vigilar una conexión Site-to-Site VPN e informar cuando algo vaya mal:

- Amazon CloudWatch Alarms: observe una sola métrica durante un período de tiempo que especifique y realice una o más acciones en función del valor de la métrica en relación con un umbral determinado durante varios períodos de tiempo. La acción es una notificación que se envía a un tema de Amazon SNS. CloudWatch las alarmas no invocan acciones simplemente porque se encuentran en un estado determinado; el estado debe haber cambiado y se ha mantenido durante un número específico de períodos. Para obtener más información, consulte Supervisa AWS Site-to-Site VPN los túneles con Amazon CloudWatch.
- AWS CloudTrail Supervisión de registros: comparta archivos de registro entre cuentas, supervise los archivos de CloudTrail registro en tiempo real enviándolos a CloudWatch Logs, cree aplicaciones de procesamiento de registros en Java y valide que los archivos de registro no hayan cambiado después de la entrega. CloudTrail Para obtener más información, consulta Cómo registrar llamadas a la API AWS CloudTrail en la referencia de la EC2 API de Amazon y Cómo trabajar con archivos de CloudTrail registro en la Guía del AWS CloudTrail usuario.
- AWS Health eventos: reciba alertas y notificaciones relacionadas con los cambios en el estado de sus túneles de Site-to-Site VPN, las recomendaciones de configuración recomendadas o cuando se acerque a los límites de escalado. Utilice los eventos de Personal Health Dashboard para activar conmutaciones por error automatizadas, reducir el tiempo de resolución de problemas y optimizar las conexiones para disfrutar de una alta disponibilidad. Para obtener más información, consulte AWS Health y AWS Site-to-Site VPN eventos.

Herramientas de supervisión manuales

Otra parte importante de la supervisión de una conexión Site-to-Site VPN consiste en supervisar manualmente los elementos que no cubren CloudWatch las alarmas. Los paneles de Amazon VPC y de CloudWatch consola ofrecen una at-a-glance visión del estado de su entorno. AWS

> **Note**
>
> En la consola de Amazon VPC, es posible que los parámetros de estado del túnel Site-to-Site VPN, como «Estado» y «Último cambio de estado», no reflejen los cambios de estado transitorios ni los cambios momentáneos del túnel. Se recomienda utilizar CloudWatch métricas y registros para actualizar de forma pormenorizada los cambios en el estado del túnel.

- En el panel de control de Amazon VPC se indica:
  - El estado de los servicios en cada región
  - Site-to-Site Conexiones VPN
  - Estado del túnel VPN (en el panel de navegación, elija Conexiones Site-to-Site VPN, seleccione una conexión Site-to-Site VPN y, a continuación, seleccione Detalles del túnel)
- La página de CloudWatch inicio muestra:
  - Alarmas y estado actual
  - Gráficos de alarmas y recursos
  - Estado de los servicios

  Además, puede CloudWatch hacer lo siguiente:
  - Crear paneles personalizados para monitorizar los servicios que le interesan
  - Realizar un gráfico con los datos de las métricas para resolver problemas y descubrir tendencias
  - Busque y explore todas sus métricas AWS de recursos
  - Crear y editar las alarmas de notificación de problemas

AWS Site-to-Site VPN registros

AWS Site-to-Site VPN los registros le proporcionan una mayor visibilidad de sus despliegues de Site-to-Site VPN. Con esta función, tiene acceso a los registros de conexión Site-to-Site VPN que proporcionan detalles sobre el establecimiento del túnel de seguridad IP (IPsec), las negociaciones sobre el intercambio de claves de Internet (IKE) y los mensajes del protocolo de detección de pares muertos (DPD).

Site-to-Site Los registros de VPN se pueden publicar en Amazon CloudWatch Logs. Esta función proporciona a los clientes una forma única y coherente de acceder a los registros detallados de todas sus conexiones Site-to-Site VPN y analizarlos.

Temas

Ventajas de los registros de Site-to-Site VPN

- Solución de problemas simplificada con la Site-to-Site VPN: los registros de la VPN le ayudan a detectar las discrepancias de configuración entre AWS el dispositivo de puerta de enlace del cliente y a solucionar los problemas iniciales de conectividad de la VPN. Las conexiones de VPN pueden cambiar de forma intermitente con el tiempo debido a ajustes mal configurados (como tiempos de espera mal ajustados), puede haber problemas en las redes de transporte subyacentes (como el tiempo de Internet) o los cambios de enrutamiento o los errores de ruta pueden provocar la interrupción de la conectividad a través de VPN. Esta característica le permite diagnosticar con precisión la causa de los errores de conexión intermitentes y ajustar la configuración del túnel de bajo nivel para lograr un funcionamiento fiable.
- AWS Site-to-Site VPN Visibilidad centralizada: los registros de Site-to-Site VPN pueden proporcionar registros de actividad de túneles para todas las diferentes formas en que se conecta la Site-to-Site VPN: Virtual Gateway, Transit Gateway y CloudHub, tanto a través de Internet AWS Direct Connect como de transporte. Esta función proporciona a los clientes una forma única y coherente de acceder a los registros detallados de todas sus conexiones Site-to-Site VPN y analizarlos.
- Seguridad y conformidad: los registros de Site-to-Site VPN se pueden enviar a Amazon CloudWatch Logs para un análisis retrospectivo del estado y la actividad de la conexión VPN a lo largo del tiempo. Esto puede ayudarle a cumplir con los requisitos reglamentarios y de conformidad.

Restricciones de tamaño de la política de recursos de Amazon CloudWatch Logs

CloudWatch Las políticas de recursos de Logs están limitadas a 5120 caracteres. Cuando CloudWatch Logs detecta que una política se acerca a este límite de tamaño, habilita automáticamente los grupos de registros que comiencen por. `/aws/vendedlogs/` Cuando habilita el registro, la Site-to-Site VPN debe actualizar su política de recursos de CloudWatch registros con el grupo de registros que especifique. Para evitar alcanzar el límite de tamaño de la política de recursos de CloudWatch registros, añada el prefijo a los nombres de los grupos de registros. `/aws/vendedlogs/`

Site-to-Site Contenido del registro de la VPN

La siguiente información se incluye en el registro de actividad del túnel Site-to-Site VPN. El nombre del archivo de flujo de registro utiliza VpnConnection ID y TunnelOutsideIPAddress.

Campo	Descripción
VpnLogCreationTimestamp (`event_timestamp`)	Marca temporal de creación de registros en formato legible por humanos.
Túnel DPDEnabled (`dpd_enabled`)	Estado habilitado del protocolo de detección de pares muertos (verdadero/falso).
CGWNATTDetectionEstado del túnel (`nat_t_detected`)	NAT-T detectado en el dispositivo de puerta de enlace de cliente (verdadero/falso).
IKEPhase1Estado del túnel (`ike_phase1_state`)	Estado del protocolo de fase 1 de IKE (Establecido | Cambio de clave | Negociación | Inactivo).
IKEPhase2Estado del túnel (`ike_phase2_state`)	Estado del protocolo de fase 2 de IKE (Establecido | Cambio de clave | Negociación | Inactivo).
VpnLogDetail (`details`)	Mensajes detallados para IPsec los protocolos IKE y DPD.

Contenido

IKEv1 Mensajes de error

Mensaje	Explicación
El par no responde: declarar muerto al par	El par no ha respondido a los mensajes de DPD, por lo que se ha impuesto la acción de tiempo de espera del DPD.
AWS El descifrado de la carga útil del túnel no se pudo realizar debido a que la clave previamente compartida no era válida	Se debe configurar la misma clave previamente compartida en ambos pares de IKE.
No se encontró ninguna propuesta que coincidiera AWS	El punto de conexión de AWS VPN no admite los atributos propuestos para la fase 1 (cifrado, hash y grupo DH), por ejemplo, `3DES`.
No se encontró ninguna coincidencia de propuesta. Notificación con la opción «No se ha elegido ninguna propuesta»	Los pares no intercambian ningún mensaje de error de propuesta elegida para informar de que se deben configurar las propuestas/políticas correctas para la fase 2 en pares de IKE.
AWS tunnel recibió DELETE para la SA de fase 2 con el SPI: xxxx	CGW ha enviado el mensaje Delete_SA para la fase 2.
AWS tunnel recibió el comando DELETE para IKE_SA de CGW	CGW ha enviado el mensaje Delete_SA para la fase 1.

IKEv2 Mensajes de error

Mensaje	Explicación
AWS Se agotó el tiempo de espera del DPD del túnel después de la retransmisión de {retry_count}	El par no ha respondido a los mensajes de DPD, por lo que se ha impuesto la acción de tiempo de espera del DPD.
AWS El túnel recibió el comando DELETE para IKE_SA de CGW	Peer ha enviado el mensaje Delete_SA para Parent/IKE_SA.
AWS tunnel recibió el comando DELETE para la SA de fase 2 con el SPI: xxxx	Peer envió el mensaje Delete_SA para CHILD_SA.
AWS El túnel detectó una colisión (CHILD_RE KEY) como CHILD_DELETE	CGW ha enviado el mensaje Delete_SA para la SA activa, a la que se le está cambiando la clave.
AWS La SA redundante del túnel (CHILD_SA) se está eliminando debido a una colisión detectada	Debido a una colisión, si SAs se generan redundantes, Peers cerrará la SA redundant e después de hacer coincidir los valores de nonce según la RFC.
AWS No se pudo establecer la fase 2 del túnel mientras se mantenía la fase 1	El par no pudo establecer CHILD_SA debido a un error de negociación, por ejemplo, a una propuesta incorrecta.
AWS: Selector de tráfico: TS_UNACCE PTABLE: recibido del agente de respuesta	El par ha propuesto selectores de tráfico o dominio de cifrado incorrectos. Los pares deben configurarse de forma idéntica y correcta CIDRs.
AWS el túnel envía AUTHENTICATION_FAI LED como respuesta	El par no puede autenticar al par al verificar el contenido del mensaje IKE_AUTH
AWS tunnel detectó una falta de coincidencia de claves previamente compartidas con cgw: xxxx	Se debe configurar la misma clave previamente compartida en ambos pares de IKE.

Mensaje	Explicación
AWS Tiempo de espera del túnel: eliminar el IKE_SA de fase 1 no establecido con cgw: xxxx	La eliminación de IKE_SA semiabierto como par no ha continuado con las negociaciones
No se encontró ninguna coincidencia de propuesta. Notificación con la opción «No se ha elegido ninguna propuesta»	Los pares no intercambian ningún mensaje de error de propuesta elegida para informar que las propuestas correctas se deben configurar en pares de IKE.
No se encontró ninguna propuesta que coincidiera AWS	AWS VPN Endpoint no admite los atributos propuestos para la fase 1 o la fase 2 (cifrado, hash y grupo DH), 3DES por ejemplo.

IKEv2 Mensajes de negociación

Mensaje	Explicación
AWS solicitud procesada por túnel (id=xxx) para CREATE_CHILD_SA	AWS ha recibido la solicitud CREATE_CHILD_SA de CGW.
AWS tunnel está enviando una respuesta (id=xxx) para CREATE_CHILD_SA	AWS está enviando la respuesta CREATE_CHILD_SA a CGW.
AWS tunnel está enviando una solicitud (id=xxx) para CREATE_CHILD_SA	AWS está enviando la solicitud CREATE_CHILD_SA a CGW.
AWS respuesta procesada por túnel (id=xxx) para CREATE_CHILD_SA	AWS ha recibido la respuesta CREATE_CHILD_SA de CGW.

Requisitos de IAM para publicar en Logs CloudWatch

Para que la característica de registro funcione correctamente, la política de IAM asociada a la entidad principal de IAM que se está utilizando para configurar la característica debe incluir los siguientes permisos como mínimo. También puedes encontrar más información en la sección Habilitar el registro desde determinados AWS servicios de la Guía del usuario de 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"
    }
  ]
}
```

Vea la configuración AWS Site-to-Site VPN de los registros

Vea el registro de actividad de una conexión Site-to-Site VPN. Aquí puede ver los detalles sobre la configuración, como los algoritmos de cifrado o si los registros de VPN de túnel están habilitados. También puede ver el estado del túnel. Esto le ayuda a realizar un mejor seguimiento de cualquier problema o conflicto que pueda tener con una conexión de VPN.

Para consultar la configuración actual de registro de túnel

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.

2. En el panel de navegación, selecciona Conexiones Site-to-Site VPN.
3. Seleccione la conexión de VPN que desea ver en la lista VPN connections (Conexiones de VPN).
4. Elija la pestaña Tunnel details (Detalles de túnel).
5. Amplíe las secciones Tunnel 1 options (Opciones de túnel 1) y Tunnel 2 options (Opciones de túnel 2) para ver todos los detalles de configuración de los túneles.
6. Puede ver el estado actual de la función de registro en el registro de Tunnel VPN y el grupo de CloudWatch registros actualmente configurado (si lo hay) en el grupo de CloudWatch registros.

Para ver la configuración actual del registro de túneles en una conexión Site-to-Site VPN mediante la línea de AWS comandos o la API

- DescribeVpnConnections(API de Amazon EC2 Query)
- describe-vpn-connections (AWS CLI)

Habilitar AWS Site-to-Site VPN los registros

Habilite Site-to-Site los registros de VPN para registrar la actividad de la VPN, como el estado del túnel y otros detalles. Puede habilitar el registro en una conexión nueva o modificar una conexión existente para iniciar el registro de la actividad. Si desea desactivar el registro de una conexión, consulte Deshabilite los registros de Site-to-Site VPN.

> **Note**
>
> Al habilitar los registros de Site-to-Site VPN para un túnel de conexión VPN existente, la conectividad a través de ese túnel puede interrumpirse durante varios minutos. Sin embargo, cada conexión de VPN ofrece dos túneles para una alta disponibilidad, por lo que puede habilitar el registro en un túnel a la vez mientras mantiene la conectividad a través del túnel que no se modifica. Para obtener más información, consulte AWS Site-to-Site VPN reemplazos de puntos finales de túneles.

Para habilitar el registro de VPN durante la creación de una nueva conexión Site-to-Site VPN

Siga el procedimiento indicado en Paso 5: Crear una conexión de VPN. En las Tunnel Options (Opciones de túnel) del Paso 9, puede especificar todas las opciones que desea usar para ambos

túneles, como las opciones de VPN logging (Registro de VPN). Para obtener más información sobre estas opciones, consulte Opciones de túnel para su AWS Site-to-Site VPN conexión.

Para habilitar el registro por túnel en una nueva conexión Site-to-Site VPN mediante la línea de AWS comandos o la API

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

Para habilitar el registro de túneles en una conexión Site-to-Site VPN existente

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, selecciona conexiones Site-to-Site VPN.
3. Seleccione la conexión de VPN que desea modificar de la lista VPN connections (Conexiones de VPN).
4. Seleccione Actions (Acciones), Modify VPN tunnel options (Modificar opciones de túnel de VPN).
5. Seleccione el túnel que desea modificar; para ello, elija la dirección IP adecuada en la lista VPN tunnel outside IP address (Túnel de VPN fuera de la dirección IP).
6. En Tunnel activity log (Registro de actividad de túnel), seleccione Enable (Habilitar).
7. En Grupo de CloudWatch registros de Amazon, selecciona el grupo de CloudWatch registros de Amazon al que quieres que se envíen los registros.
8. (Opcional) En Output format (Formato de salida), elija el formato deseado para la salida del registro, ya sea json o text (texto).
9. Seleccione Save changes (Guardar cambios).
10. (Opcional) Repita los pasos 4 a 9 para el otro túnel si lo desea.

Para habilitar el registro de túneles en una conexión Site-to-Site VPN existente mediante la línea de AWS comandos o la API

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

Inhabilitar AWS Site-to-Site VPN los registros

Desactive el registro de VPN en una conexión si ya no quiere seguir rastreando ninguna actividad en esa conexión. Esta acción solo desactiva el registro y no afecta a ninguna otra cosa de esa conexión. Para habilitar o volver a habilitar el registro en una conexión, consulte Habilite los registros de Site-to-Site VPN.

Para deshabilitar el registro de túneles en una conexión Site-to-Site VPN

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Site-to-Site VPN Connections.
3. Seleccione la conexión de VPN que desea modificar de la lista VPN connections (Conexiones de VPN).
4. Seleccione Actions (Acciones), Modify VPN tunnel options (Modificar opciones de túnel de VPN).
5. Seleccione el túnel que desea modificar; para ello, elija la dirección IP adecuada en la lista VPN tunnel outside IP address (Túnel de VPN fuera de la dirección IP).
6. En Tunnel activity log (Registro de actividad de túnel), desactive Enable (Habilitar).
7. Seleccione Save changes (Guardar cambios).
8. (Opcional) Repita los pasos 4 a 7 para el otro túnel si lo desea.

Para deshabilitar el registro de túneles en una conexión Site-to-Site VPN mediante la línea de AWS comandos o la API

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

Supervisa AWS Site-to-Site VPN los túneles con Amazon CloudWatch

Puede monitorizar los túneles de la VPN mediante CloudWatch el cual se recopilan y procesan los datos sin procesar del servicio VPN para convertirlos en métricas legibles y prácticamente en tiempo real. Estas estadísticas se registran durante un periodo de 15 meses, de forma que pueda obtener acceso a información de historial y obtener una mejor perspectiva acerca del desempeño de su aplicación web o servicio. Los datos de las métricas de la VPN se envían automáticamente a CloudWatch medida que están disponibles.

Para obtener más información, consulta la Guía del CloudWatch usuario de Amazon.

Contenido

Dimensiones y métricas de VPN

Las siguientes CloudWatch métricas están disponibles para sus conexiones Site-to-Site VPN.

Métrica	Descripción
`TunnelState`	El estado de los túneles. En el caso de la estática VPNs, 0 indica ABAJO y 1 indica ARRIBA. Para BGP VPNs, 1 indica ESTABLECIDO y 0 se usa para todos los demás estados. Para ambos tipos de VPNs, los valores entre 0 y 1 indican que al menos un túnel no está ACTIVO. Unidades: valor fraccional entre 0 y 1
`TunnelDataIn` †	Los bytes recibidos en el AWS lateral de la conexión a través del túnel VPN desde una pasarela de cliente. Cada punto de datos de la métrica representa el número de bytes recibidos después del punto de datos anterior. Use la estadística Sum para mostrar el número total de bytes recibidos durante el periodo. Esta métrica cuenta los datos después del descifrado. Unidades: bytes
`TunnelDataOut` †	Los bytes enviados desde el AWS lado de la conexión a través del túnel VPN hasta la

Métrica	Descripción
	pasarela del cliente. Cada punto de datos de la métrica representa el número de bytes enviados después del punto de datos anterior. Use la estadística Sum para mostrar el número total de bytes enviados durante el periodo. Esta métrica cuenta los datos antes del cifrado. Unidades: bytes

† Estas métricas pueden dar información sobre el uso de la red incluso cuando el túnel no está operativo. Esto se debe a las comprobaciones periódicas de estado realizadas en el túnel y a las solicitudes de ARP y BGP en segundo plano.

Para filtrar los datos de las métricas, use las siguientes dimensiones.

Dimensión	Descripción
`VpnId`	Filtra los datos métricos por el ID de conexión de la Site-to-Site VPN.
`TunnelIpAddress`	Filtra los datos de las métricas en función de la dirección IP del túnel de la gateway privada virtual.

Ver las métricas CloudWatch de Amazon Logs para AWS Site-to-Site VPN

Cuando creas una conexión Site-to-Site VPN, el servicio VPN envía métricas sobre tu conexión VPN a CloudWatch medida que están disponibles. Puede ver las métricas de la conexión de VPN de la siguiente manera.

Para ver las métricas mediante la CloudWatch consola

Las métricas se agrupan en primer lugar por el espacio de nombres de servicio y, a continuación, por las diversas combinaciones de dimensiones dentro de cada espacio de nombres.

1. Abra la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/.

2. En el panel de navegación, seleccione Métricas.
3. En All metrics elija el espacio de nombres de métricas VPN.
4. Seleccione la dimensión de métrica para ver las métricas, por ejemplo, Métricas de túneles de VPN.

> **Note**
>
> El espacio de nombres de la VPN no aparecerá en la CloudWatch consola hasta que se haya creado una conexión Site-to-Site VPN en la AWS región que está viendo.

Para ver las métricas mediante el AWS CLI

En el símbolo del sistema, ejecute el siguiente comando:

```
aws cloudwatch list-metrics --namespace "AWS/VPN"
```

Crea CloudWatch alarmas de Amazon para monitorear AWS Site-to-Site VPN los túneles

Puede crear una CloudWatch alarma que envíe un mensaje de Amazon SNS cuando la alarma cambie de estado. Una alarma vigila una única métrica durante el período especificado y envía una notificación a un tema de Amazon SNS según el valor de la métrica relativo a un determinado umbral durante varios períodos de tiempo.

Por ejemplo, puede crear una alarma que monitoree el estado de un único túnel de VPN y envíe una notificación cuando el estado del túnel sea INACTIVO durante 3 puntos de datos en 15 minutos.

Para crear una alarma para el estado de un único túnel

1. Abra la CloudWatch consola en. https://console.aws.amazon.com/cloudwatch/
2. En el panel de navegación, amplíe Alarmas y, a continuación, elija Todas las alarmas.
3. Elija Crear alarma y, a continuación, elija Seleccionar métrica.
4. Elija VPN y, a continuación, elija Métricas de túnel de VPN.
5. Seleccione la dirección IP del túnel deseado, en la misma línea que la TunnelStatemétrica. Elija Seleccionar métrica.

6. Para siempre que TunnelState sea... , seleccione Inferior y, a continuación, introduzca «1" en el campo de entrada situado debajo de... .
7. En Configuración adicional, establezca las entradas en “3 de 3” para los Puntos de datos para la alarma.
8. Elija Next (Siguiente).
9. En Enviar una notificación al siguiente tema de SNS, seleccione una lista de notificación existente o cree una nueva.
10. Elija Next (Siguiente).
11. Escriba un nombre para la alarma. Elija Next (Siguiente).
12. Compruebe la configuración de la alarma y, a continuación, elija Create alarm (Crear alarma).

Puede crear una alarma que supervise el estado de la conexión Site-to-Site VPN. Por ejemplo, puede crear una alarma que envíe una notificación cuando el estado de uno o ambos túneles esté INACTIVO durante un período de 5 minutos.

Para crear una alarma para el estado de la conexión Site-to-Site VPN

1. Abra la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, amplíe Alarmas y, a continuación, elija Todas las alarmas.
3. Elija Crear alarma y, a continuación, elija Seleccionar métrica.
4. Elija VPN y, a continuación, elija VPN Connection Metrics (Métricas de conexión VPN).
5. Seleccione su conexión Site-to-Site VPN y la TunnelStatemétrica. Elija Select metric (Seleccionar métrica).
6. En Statistic (Estadística), especifique Maximum (Máximo).

   Como alternativa, si has configurado tu conexión Site-to-Site VPN para que ambos túneles estén activos, puedes especificar una estadística de Mínimo para enviar una notificación cuando al menos un túnel esté inactivo.
7. En Whenever (Siempre), elija Lower/Equal (Menor o igual) (<=) e ingrese 0 (o 0,5 para cuando hay al menos un túnel desactivado). Elija Next (Siguiente).
8. En Select an SNS topic (Seleccionar un tema de SNS), seleccione una notificación existente o elija New list (Nueva lista) para crear una. Elija Next (Siguiente).
9. Escriba un nombre y la descripción de su alarma. Elija Next (Siguiente).
10. Compruebe la configuración de la alarma y, a continuación, elija Create alarm (Crear alarma).

También puede crear alarmas que monitoricen la cantidad de tráfico que entra o sale del túnel de VPN. Por ejemplo, la siguiente alarma monitoriza la cantidad de tráfico que entra en el túnel de VPN desde su red, y envía una notificación cuando el número de bytes alcanza un umbral de 5 000 000 durante un periodo de 15 minutos.

Para crear una alarma para el tráfico de red entrante

1. Abre la CloudWatch consola en. https://console.aws.amazon.com/cloudwatch/
2. En el panel de navegación, amplíe Alarmas y, a continuación, elija Todas las alarmas.
3. Elija Crear alarma y, a continuación, elija Seleccionar métrica.
4. Seleccione VPN y, a continuación, elija VPN Tunnel Metrics (Métricas de túnel de VPN).
5. Seleccione la dirección IP del túnel VPN y la TunnelDataInmétrica. Elija Select metric (Seleccionar métrica).
6. En Statistic (Estadística), especifique Sum (Suma).
7. En Period (Periodo), seleccione 15 minutes (15 minutos).
8. En Whenever (Siempre), elija Greater/Equal (Mayor o igual)(**>=**) y escriba 5000000. Elija Next (Siguiente).
9. En Select an SNS topic (Seleccionar un tema de SNS), seleccione una notificación existente o elija New list (Nueva lista) para crear una. Elija Next (Siguiente).
10. Escriba un nombre y la descripción de su alarma. Elija Next (Siguiente).
11. Compruebe la configuración de la alarma y, a continuación, elija Create alarm (Crear alarma).

La siguiente alarma monitoriza la cantidad de tráfico que sale del túnel de VPN a su red, y envía una notificación cuando el número de bytes sea inferior a 1 000 000 durante un periodo de 15 minutos.

Para crear una alarma para el tráfico de red saliente

1. Abra la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, amplíe Alarmas y, a continuación, elija Todas las alarmas.
3. Elija Crear alarma y, a continuación, elija Seleccionar métrica.
4. Seleccione VPN y, a continuación, elija VPN Tunnel Metrics (Métricas de túnel de VPN).
5. Seleccione la dirección IP del túnel VPN y la TunnelDataOutmétrica. Elija Select metric (Seleccionar métrica).
6. En Statistic (Estadística), especifique Sum (Suma).

7. En Period (Periodo), seleccione 15 minutes (15 minutos).
8. En Whenever (Siempre que sea), elija Lower/Equal (Menor o igual)(<=) y escriba `1000000`. Elija Next (Siguiente).
9. En Select an SNS topic (Seleccionar un tema de SNS), seleccione una notificación existente o elija New list (Nueva lista) para crear una. Elija Next (Siguiente).
10. Escriba un nombre y la descripción de su alarma. Elija Next (Siguiente).
11. Compruebe la configuración de la alarma y, a continuación, elija Create alarm (Crear alarma).

Para ver más ejemplos de creación de alarmas, consulta Cómo crear CloudWatch alarmas de Amazon en la Guía del CloudWatch usuario de Amazon.

AWS Health y AWS Site-to-Site VPN eventos

AWS Site-to-Site VPN envía automáticamente notificaciones a AWS Health Dashboard. Este panel no requiere configuración y está listo para ser utilizado por AWS los usuarios autenticados. Puede configurar varias acciones en respuesta a las notificaciones de eventos a través de AWS Health Dashboard.

AWS Health Dashboard Proporciona los siguientes tipos de notificaciones para sus conexiones VPN:

- Notificaciones de sustitución de puntos de enlace de un túnel
- Notificaciones de VPN con un solo túnel

Notificaciones de sustitución de puntos de enlace de un túnel

Recibirá una notificación de sustitución del punto final del túnel AWS Health Dashboard cuando se sustituya uno o ambos puntos finales del túnel VPN de su conexión VPN. El punto de enlace de un túnel se reemplaza cuando AWS realiza actualizaciones en el túnel o cuando se modifica su conexión de VPN. Para obtener más información, consulte AWS Site-to-Site VPN reemplazos de puntos finales de túneles.

Cuando se completa el reemplazo del punto final del túnel, AWS envía la notificación de reemplazo del punto final del túnel a través de un AWS Health Dashboard evento.

Notificaciones de VPN con un solo túnel

Una conexión Site-to-Site VPN consta de dos túneles para garantizar la redundancia. Se recomienda encarecidamente que configure ambos túneles para disfrutar de una alta disponibilidad. Si la conexión VPN tiene un único túnel activo y el otro se mantiene inactivo durante más de una hora al día, recibirá una notificación de túnel de VPN único mensual a través de un evento de AWS Health Dashboard . Este evento se actualizará diariamente con cualquier conexión VPN nueva detectada como túnel único, y las notificaciones se enviarán semanalmente. Cada mes se creará un nuevo evento que borrará todas las conexiones de VPN que ya no se detecten como túnel único.

AWS Site-to-Site VPN cuotas

Su AWS cuenta tiene las siguientes cuotas, anteriormente denominadas límites, relacionadas con la Site-to-Site VPN. A menos que se indique lo contrario, cada cuota es específica de la región de . Puede solicitar el aumento de algunas cuotas, pero otras no se pueden aumentar.

Para solicitar un aumento de una cuota ajustable, elija Yes (Sí) en la columna Adjustable (Ajustable). Para obtener más información, consulte Solicitud de aumento de cuota en la Guía del usuario de Service Quotas.

Site-to-Site Recursos de VPN

Nombre	Valor predeterminado	Ajustable
Gateways de cliente por región	50	Sí
Gateways privadas virtuales por región	5	Sí
Site-to-Site Conexiones VPN por región	50	Sí
Site-to-Site Conexiones VPN por puerta de enlace privada virtual	10	Sí
Conexiones Site-to-Site VPN aceleradas por región	10	Sí
Conexiones Site-to-Site VPN no asociadas por región	10	Sí

> **Note**
>
> Tanto las conexiones aceleradas como las no asociadas se incluyen en la cuota total de conexiones Site-to-Site VPN por región.

Puede asociar una gateway privada virtual a una VPC a la vez. Para conectar la misma conexión Site-to-Site VPN a varias VPCs, te recomendamos que consideres la posibilidad de utilizar una

pasarela de tránsito en su lugar. Para obtener más información, consulte Gateways de tránsito en Gateways de tránsito de Amazon VPC.

Site-to-Site Las conexiones VPN en una pasarela de tránsito están sujetas al límite total de adjuntos de la pasarela de tránsito. Para obtener más información, consulte Cuotas de gateway de tránsito.

Rutas

Las fuentes de rutas anunciadas son las rutas de VPC, otras rutas de VPN y las rutas de las interfaces virtuales de AWS Direct Connect . Las rutas anunciadas proceden de la tabla de enrutamiento vinculada a la conexión de VPN.

> **Note**
>
> Si utiliza una puerta de enlace privada virtual y la propagación de rutas está habilitada en la tabla de enrutamiento de la VPC, se agregarán automáticamente rutas dinámicas y estáticas a la conexión de VPN, hasta el límite de la tabla de enrutamiento de la VPC. Consulte las cuotas de Amazon VPC en la Guía del usuario de Amazon VPC para obtener más información.

Nombre	Valor predeterminado	Ajustable
Rutas dinámicas anunciadas desde un dispositivo de puerta de enlace del cliente a una conexión Site-to-Site VPN en una puerta de enlace privada virtual	100	No
Rutas anunciadas desde una conexión Site-to-Site VPN en una puerta de enlace privada virtual a un dispositivo de puerta de enlace de un cliente	1 000	No
Rutas dinámicas anunciadas desde un dispositivo de puerta de enlace del cliente a una conexión Site-to-Site VPN en una puerta de enlace de tránsito	1 000	No

Nombre	Valor predeterminado	Ajustable
Rutas anunciadas desde una conexión Site-to-Site VPN en una pasarela de tránsito a un dispositivo de pasarela del cliente	5 000	No
Rutas estáticas desde un dispositivo de puerta de enlace del cliente a una conexión Site-to-Site VPN en una puerta de enlace privada virtual	100	No

Ancho de banda y rendimiento

Hay muchos factores que pueden afectar al ancho de banda obtenido a través de una conexión Site-to-Site VPN, entre los que se incluyen, entre otros, el tamaño del paquete, la combinación de tráfico (TCP/UDP), las políticas de configuración o limitación en las redes intermedias, el clima de Internet y los requisitos específicos de las aplicaciones.

Nombre	Valor predeterminado	Ajustable
Ancho de banda máximo por túnel de VPN	Hasta 1,25 Gbps	No
Paquetes máximos por segundo (PPS) por túnel de VPN	Hasta 140 000	No

En el caso de las conexiones Site-to-Site VPN en una pasarela de tránsito, puede utilizar el ECMP para obtener un mayor ancho de banda de la VPN mediante la agregación de varios túneles de VPN. Para utilizar ECMP, la conexión de VPN debe estar configurada para el enrutamiento dinámico. ECMP no es compatible con conexiones de VPN que utilizan enrutamiento estático. Para obtener más información, consulte Gateway de tránsito.

> **Note**
>
> IPv6 VPNs admiten los mismos límites de rendimiento (Gbps y PPS), MTU y ruta que. IPv4 VPNs No hay diferencias de rendimiento entre IPv4 las conexiones VPN. IPv6

Unidad de transmisión máxima (MTU).

Site-to-Site La VPN admite una unidad de transmisión máxima (MTU) de 1446 bytes y un tamaño de segmento máximo (MSS) correspondiente de 1406 bytes. Sin embargo, ciertos algoritmos que utilizan encabezados TCP más grandes pueden reducir eficazmente ese valor máximo. Para evitar la fragmentación, le recomendamos que configure la MTU y el MSS en función de los algoritmos seleccionados. Para obtener más información sobre MTU, MSS y los valores óptimos, consulte Prácticas recomendadas para un dispositivo de puerta de enlace para clientes AWS Site-to-Site VPN.

No se admiten tramas gigantes. Para obtener más información, consulta los marcos Jumbo en la Guía del EC2 usuario de Amazon.

Una conexión Site-to-Site VPN no admite Path MTU Discovery.

Las limitaciones de la MTU se aplican tanto a las conexiones IPv6 VPN como a IPv4 las conexiones.

Recursos de cuotas adicionales

Para obtener información sobre las cuotas relacionadas con las gateways de tránsito, como el número de conexiones de una gateway de tránsito, consulte Cuotas de las gateways de tránsito en la Guía de gateways de tránsito de Amazon VPC.

Para ampliar las cuotas de VPC, consulte Cuotas de Amazon VPC en la Guía del usuario de Amazon VPC.

Historial de documentos de la Guía del usuario de Site-to-Site VPN

En la siguiente tabla se describen las actualizaciones de la Guía AWS Site-to-Site VPN del usuario.

Cambio	Descripción	Fecha
IPv6 soporte para AWS Site-to-Site VPN para el túnel exterior IPs	Site-to-Site La VPN ahora admite IPv6 direcciones para el túnel exterior IPs en las conexiones VPN Transit Gateway y Cloud WAN. Esto permite una IPv6 migración completa con IPv6 direcciones tanto para el túnel IPs exterior como para el paquete interno IPs (IPv6-in-IPv6), así como para el túnel IPv6 exterior IPs con el paquete IPv4 interno IPs (IPv4-in-IPv6).	1 de julio de 2025
Se actualizó la política AWSVPCS2 SVpn ServiceRolePolicy AWS gestionada	Se agregaron nuevos permisos a la política AWS administrada que permiten a la Site-to-Site VPN administrar el secreto AWS Secrets Manager administrado de la conexión VPN.	27 de mayo de 2025
Se actualizaron las opciones de almacenamiento de claves previamente compartidas	Site-to-Site La VPN ahora permite AWS Secrets Manager almacenar una clave previamente compartida.	27 de mayo de 2025

Información de VPN clásica eliminada	Se ha eliminado la información sobre la VPN clásica de la guía.	19 de enero de 2023
Mensajes de ejemplo de registro de VPN	Se han añadido registros de muestra para las conexiones Site-to-Site VPN.	9 de diciembre de 2022
Utilidad de la configuración de descarga actualizada	Site-to-Site Los clientes de VPN pueden generar plantillas de configuración para dispositivos Customer Gateway (CGW) compatibles, lo que facilita la creación de conexiones VPN a AWS ellos. Esta actualización añade compatibilidad con los parámetros de la versión 2 (IKEv2) de Internet Key Exchange para muchos de los dispositivos CGW más populares e incluye dos nuevos APIs : GetVpnConnectionDeviceTypes y. GetVpnConnectionDeviceSampleConfiguration	21 de septiembre de 2021
Notificaciones de la conexión de VPN	Site-to-Site La VPN envía automáticamente notificaciones sobre su conexión VPN al AWS Health Dashboard.	29 de octubre de 2020
Iniciación de túnel de VPN	Puede configurar sus túneles de VPN para AWS que aparezcan los túneles.	27 de agosto de 2020

Modificar las opciones de conexión de VPN	Puede modificar las opciones de conexión de su conexión Site-to-Site VPN.	27 de agosto de 2020
Algoritmos de seguridad adicionales	Puede aplicar algoritmos de seguridad adicionales a sus túneles VPN.	14 de agosto de 2020
IPv6 soporte	Sus túneles VPN pueden soportar IPv6 el tráfico dentro de los túneles.	12 de agosto de 2020
AWS Site-to-Site VPN Guías de fusión	Esta versión combina el contenido de la Guía del administrador de AWS Site-to-Site VPN red en esta guía.	31 de marzo de 2020
Conexiones aceleradas AWS Site-to-Site VPN	Puede activar la aceleración de la AWS Site-to-Site VPN conexión.	3 de diciembre de 2019
Modifique las opciones AWS Site-to-Site VPN del túnel	Puede modificar las opciones de un túnel VPN en una AWS Site-to-Site VPN conexión. También puede configurar opciones de túnel adicionales.	29 de agosto de 2019
AWS Private Certificate Authority soporte para certificados privados	Puede utilizar un certificado privado de AWS Private Certificate Authority para autenticar su VPN.	15 de agosto de 2019
Guía del usuario de la nueva Site-to-Site VPN	Esta versión separa el contenido AWS Site-to-Site VPN (anteriormente denominado VPN AWS gestionada) de la Guía del usuario de Amazon VPC.	18 de diciembre de 2018

Modificar la gateway de destino	Puede modificar la puerta de enlace de destino de la AWS Site-to-Site VPN conexión.	18 de diciembre de 2018
ASN personalizado	Al crear una gateway privada virtual, puede especificar el número de sistema autónomo (ASN) privado en el lado de Amazon de la gateway.	10 de octubre de 2017
Opciones de túnel de VPN	Puede especificar bloques de CIDR de túnel interior y claves compartidas previamente personalizadas para sus túneles de VPN.	3 de octubre de 2017
Métricas de VPN	Puede ver CloudWatch las métricas de sus conexiones VPN.	15 de mayo de 2017
Mejoras de VPN	La conexión de VPN ahora admite la función de cifrado AES de 256 bits, la función de hash SHA-256, NAT traversal y los grupos Diffie-Hellman adicionales durante las fases 1 y 2 de la conexión. Además, podrá utilizar la misma dirección IP de gateway de cliente para cada conexión de VPN que utilice el mismo dispositivo de gateway de cliente.	28 de octubre de 2015

Conexiones de VPN mediante configuración de direccionamiento estático	Puede crear conexiones IPsec VPN a Amazon VPC mediante configuraciones de enrutamiento estático. Anteriormente, las conexiones de VPN requerían el uso del protocolo de gateway fronteriza (BGP). Ahora admitimos ambos tipos de conexiones y podrá establecer conectividad desde dispositivos que no son compatibles con BGP, incluidos Cisco ASA y Microsoft Windows Server 2008 R2.	13 de septiembre de 2012
Propagación de ruta automática	Ahora puede configurar la propagación automática de las rutas desde la VPN y AWS Direct Connect los enlaces a las tablas de enrutamiento de la VPC.	13 de septiembre de 2012
AWS VPN CloudHub y conexiones VPN redundantes	Puede comunicarse de forma segura de un sitio a otro con y sin VPC. Puede utilizar conexiones de VPN redundantes para proporcionar una conexión tolerante a errores a su VPC.	29 de septiembre de 2011

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.